KLAS RESEARCH | Healthcare IT Insights

Segment Insights

Cybersecurity Solutions for Healthcare 2025

A Look at Vendor- & Firm-Reported Capabilities

June 2025

Table of Contents

2 Executive Insights

14 Vendor & Firm Insights

15 Armis
16 Asimily
17 AuthX
18 AvePoint
19 Censinet
20 Cisco
21 Claroty
22 Clearwater
23 CloudWave
24 ColorTokens
25 Commvault
26 CyberProof
27 Cyber Salus
28 Cyderes
29 Cynerio
30 Darktrace
31 DigiCert
32 EY
33 Forescout
34 Fortified Health Security
35 GYTPOL
36 ID.me
37 Illumio
38 Imprivata
39 Intraprise Health
40 Intruno
41 LevelBlue
42 ManageEngine
43 Meditology Services
44 MorganFranklin Consulting
45 NCC Group
46 Netwrix
47 Okta
48 OnDefend
49 Optiv
50 Palo Alto Networks
51 Ping Identity
52 Proofpoint
53 PwC
54 Radware
55 Rubrik
56 SailPoint
57 SANS Institute
58 SecureAuth
59 Security Compliance Associates
60 Splunk
61 ThreatLocker
62 Trustwave
63 tw-Security
64 Varonis
65 Veeam
66 Zscaler

Executive Insights

Cybersecurity Solutions for Healthcare 2025

A Look at Vendor- & Firm-Reported Capabilities

Cyberattacks continue to disrupt operations and care continuity for healthcare provider and payer organizations. Heavy use of third parties and medical devices makes cybersecurity a unique challenge for these organizations, and their security program needs are highly varied—requiring different software solutions, professional services, and internal culture and governance strategies to identify and protect against vulnerabilities. To help organizations in these efforts, this guide shares (1) a framework of cybersecurity software and services and (2) vendor- and firm-reported offerings in the cybersecurity space.

Report Methodology

This guide is based on vendor- and firm-reported claims about their cybersecurity offerings. The guide is intended to share currently available native cybersecurity capabilities; it is not an exhaustive list of all vendors and firms with cybersecurity offerings. 55 vendors and firms responded to a survey and self-reported their capabilities based on their interpretation of the survey. KLAS intends to share customer validations and feedback for these capabilities in the future. The guide also includes vendors and firms mentioned as top of mind for healthcare organizations in **KLAS' Cybersecurity 2025 report**. Those currently measured by KLAS are noted.

CYBERSECURITY MARKET OVERVIEW

Framework of Cybersecurity Software & Services for Healthcare

Note: Cybersecurity is a top investment priority for healthcare organizations, and the areas in this framework represent those most emphasized by healthcare organizations interviewed by KLAS. We expect this framework to continue to evolve over time. Other cybersecurity categories that may be added in the future include AI security, identity verification, network detection and response, security service edge, and zero-trust architecture.

Infrastructure	Identity	Governance, risk & compliance	Security operations	Data & application security	Proactive security	Managed services	Consulting services
Cloud security	Access management: multifactor authentication (MFA)	Healthcare safety, risk & compliance management	Vulnerability management software	Application security	Security training/ awareness	Security staff augmentation	Implementation/ configuration/ design of security technologies
Network security	Access management: single sign-on (SSO)	Risk management	Security orchestration, automation & response (SOAR)	Data loss prevention (DLP)	Attack simulation	Threat & vulnerability management	Security risk assessment
Endpoint security	Identity governance	Third-party risk management	Security information & event management (SIEM)	Data security posture management (DSPM)	Threat intelligence	Managed detection & response (MDR)	Healthcare IoT/ medical device security assessment
Email security	Privileged access management	Patient privacy monitoring	Endpoint detection & response (EDR)	Data governance/ classification		Incident response/ disaster recovery	Security program assessment/ development
Operational technology & industrial control systems (ICS)	Access management: electronic prescriptions for controlled substances (EPCS)		Extended detection & response (XDR)			Security operations center (SOC) or 24/7 monitoring	HIPAA privacy assessment
Healthcare Internet of Things (IoT)	Identity threat detection/response		Disaster recovery			Security software management (SIEM, DLP, IAM, etc.)	Social engineering & phishing
			Exposure management			Third-party risk management	Penetration/ vulnerability/network/ web application security testing
						Healthcare IoT management/ medical device security	Virtual/interim CISO
						Privacy management	
						Device patch management	

Third-Party Risk Management & Infrastructure Cybersecurity Are Top Provider Priorities; Organizations Look to Services Firms to Help Mitigate Resource Constraints

According to KLAS' Cybersecurity 2025 report, third-party risk management and infrastructure (particularly network security and segmentation) will be the top cybersecurity investment priorities for healthcare organizations over the next one to two years. **Infrastructure** solutions (particularly cloud and network solutions) are the most common offerings reported by vendors in this guide, demonstrating alignment with healthcare organizations' priorities. Fewer vendors offer **third-party risk management solutions.** This area represents an improvement opportunity for healthcare organizations, as noted in the 2025 Healthcare Cybersecurity Benchmarking Study published by KLAS, Censinet, and other partners. High-profile third-party breaches (e.g., the 2024 Change Healthcare breach) have highlighted the potential risks created by the interconnectedness between healthcare organizations, payer organizations, and vendors.

The 2025 Cybersecurity Benchmarking Study also shares that constraints in staffing resources and cybersecurity expertise are healthcare organizations' main barriers to improving their cybersecurity posture. One way that organizations navigate those constraints

is by using **managed cybersecurity services**. KLAS' Security & Privacy Consulting/Managed Services 2024 report shows that two-thirds of interviewed organizations are likely to expand their use of managed services in the next one to two years, especially for security operations center (SOC) monitoring and third-party risk management. Among the firms who participated in this guide, the most commonly reported managed services offering is security staff augmentation; SOC monitoring and third-party risk management offerings are less often reported.

CYBERSECURITY SOLUTIONS FOR HEALTHCARE

Cybersecurity Software Offerings: Vendor-Reported Capabilities

The capabilities charted below are self-reported by software vendors as being live and currently available to their customers. Links to relevant KLAS performance data are included where applicable, though measurement does not mean that KLAS has validated each capability the vendor reports to offer.

Vendor-Reported Cybersecurity Software Offerings

○ Vendor-reported offering ● KLAS-measured solution

Click vendor name for information about their cybersecurity strategies (if submitted)

		Cloud security	Network security	Endpoint security	Email security	Operational technology & ICS	Healthcare IoT	KLAS-measured solutions
Infrastructure	Armis	○	○			○	●	Healthcare IoT
	Asimily	○	○			○	●	Healthcare IoT
	AvePoint	○			○			
	Cisco	○	○	○	○	○	○	*Measured in other area*
	Claroty	○	○			○	●	Healthcare IoT
	Clearwater	○	○	○	○		○	*Measured in other areas*
	CloudWave	○	○	○		○	○	*Measured in other area*
	ColorTokens	○	○	○		○	○	
	Commvault	○		○	○	○		
	CyberProof	○	○	○	○	○	○	
	Cyderes	○		○	○			
	Cynerio		○			○	●	Healthcare IoT
	Darktrace	○	○		○	○	○	
	DigiCert	○	○	○	○	○	○	
	EY	○	○	○	○	○	○	*Measured in other areas*
	Forescout	○	○	○		○	○	
	Fortified Health Security	○	○	○	○	○	○	*Measured in other areas*
	GYTPOL	○	○	○		○		
	HadenGrey	○	○	○	○	○	○	
	Illumio	○	○	○		○		
	Imprivata						○	*Measured in other areas*
	ManageEngine	○	○	○	○			
	MorganFranklin Consulting	○	○	○	○	○	○	
	NCC Group	○	○	○		○	○	
	Netwrix			○				
	Nozomi Networks		○	○		○		
	Okta	○		○				
	Optiv	○	○	○	○	○	○	
	Palo Alto Networks	○	○	○	○	○	●	Healthcare IoT
	Ping Identity	○	○	○	○		○	
	Proofpoint	○		○	○			
	Radware	○	○					
	Rubrik	○			○			
	SailPoint	○	○			○	○	*Measured in other area*

Continued on next page

Vendor-Reported Cybersecurity Software Offerings, Continued

○ Vendor-reported offering ● KLAS-measured solution

Click vendor name for information about their cybersecurity strategies (if submitted)

Infrastructure

	Cloud security	Network security	Endpoint security	Email security	Operational technology & ICS	Healthcare IoT	KLAS-measured solutions
SANS Institute			○				
Splunk	○	○					
ThreatLocker	○	○	○		○	○	
Trustwave	○			○			
Varonis	○	○		○			
Veeam	○	○	○	○			
Zscaler	○	○	○	○	○	○	
Additional KLAS-validated vendors Note: These vendors didn't or weren't able to participate in the report survey, but within the past 12 months, KLAS has interviewed at least one live customer for the offerings listed.							
CrowdStrike			○				
Cylera						○	
ORDR						●	Healthcare IoT
Other vendors Note: These vendors didn't participate in the report survey, but healthcare organizations interviewed for KLAS' Cybersecurity 2025 report mentioned using or considering these vendors.							
Abnormal AI				○			
CDW	○						
Egress, a KnowBe4 Company				○			
Fortinet		○					

Identity

	Access management: MFA	Access management: SSO	Identity governance	Privileged access management	Access management: EPCS	Identity threat detection/ response	KLAS-measured solutions
AuthX	○	○			○		
AvePoint			○	○			
Cisco	●	●			●	○	Access Management
Claroty	○	○	○	○			*Measured in other area*
CloudWave	○	○	○	○			*Measured in other area*
Commvault	○	○	○				
CyberProof	○	○	○	○	○		
Cyderes	○	○	○	○			
DigiCert	○				○		
EY			○	○		○	*Measured in other areas*
Fortified Health Security	○	○	○	○			*Measured in other areas*
GYTPOL			○				
HadenGrey	○	○	○	○	○		
ID.me	○	○			○		
Imprivata	●	●		●			Access Management
ManageEngine	○	○	○	○	○	○	
MorganFranklin Consulting	○	○	○	○			
Netwrix			○	○		○	
Okta	○	○	○	○	○	○	
Optiv	○	○	○	○	○		
Ping Identity	○	○	○		○	○	
Proofpoint						○	
Rubrik	○	○	○	○			
SailPoint	○		●	○		○	Identity Management
SecureAuth	○	○			○		
ThreatLocker	○	○	○	○		○	
Varonis				○		○	
Veeam	○	○	○	○	○		

Continued on next page

Vendor-Reported Cybersecurity Software Offerings, Continued

○ Vendor-reported offering ● KLAS-measured solution

Click vendor name for information about their cybersecurity strategies (if submitted)

Identity

	Access management: MFA	Access management: SSO	Identity governance	Privileged access management	Access management: EPCS	Identity threat detection/ response	KLAS-measured solutions
Additional KLAS-validated vendors Note: These vendors didn't or weren't able to participate in the report survey, but within the past 12 months, KLAS has interviewed at least one live customer for the offerings listed.							
CyberArk				○			
Identity Automation	●	●			●		Access Management
Microsoft	○	○		○			
Other vendors Note: These vendors didn't participate in the report survey, but healthcare organizations interviewed for KLAS' Cybersecurity 2025 report mentioned using or considering these vendors.							
Saviynt			○	○			
SecureAuth	○						

Governance, risk & compliance

	Healthcare safety, risk & compliance management	Risk management	Third-party risk management	Patient privacy monitoring	KLAS-measured solutions
Armis	○	○	○	○	*Measured in other area*
Asimily	○	○	○	○	*Measured in other area*
AvePoint	○	○	○	○	
Censinet	○	○	○		
Claroty	○	○	○		*Measured in other area*
Clearwater	○	○	○	○	*Measured in other areas*
Commvault	○	○		○	
CyberProof	○	○	○	○	
Cyderes	○	○	○		
Cynerio	○	○	○	○	*Measured in other area*
EY	○	○	○	○	*Measured in other areas*
Forescout	○	○		○	
Fortified Health Security	○	○	○	○	*Measured in other areas*
GYTPOL	○	○			
HadenGrey	○	○	○	○	
Imprivata			○	●	**Patient Privacy Monitoring**
Intruno	○	○	○	○	
ManageEngine	○	○	○	○	
MorganFranklin Consulting	○	○	○	○	
NCC Group	○	○	○		
Nozomi Networks		○			
Optiv	○	○	○	○	
Origami Risk	●	○	○		**Healthcare Safety, Risk, & Compliance Management**
Palo Alto Networks	○				*Measured in other area*
Ping Identity	○	○	○	○	
Proofpoint	○				
Radware	○		○	○	
Rubrik		○		○	
SailPoint	○	○	○		*Measured in other area*
ThreatLocker	○	○	○	○	
Varonis	○	○	○	○	
Veeam	○				
Zscaler	○	○	○	○	
Additional KLAS-validated vendors Note: These vendors didn't or weren't able to participate in the report survey, but within the past 12 months, KLAS has interviewed at least one live customer for the offerings listed.					
Bluesight				●	**Patient Privacy Monitoring**
iatricSystems				●	**Patient Privacy Monitoring**

Continued on next page

Vendor-Reported Cybersecurity Software Offerings, Continued

○ Vendor-reported offering ● KLAS-measured solution

Click vendor name for information about their cybersecurity strategies (if submitted)

Governance, risk & compliance

	Healthcare safety, risk & compliance management	Risk management	Third-party risk management	Patient privacy monitoring	KLAS-measured solutions
Performance Health Partners	●				Healthcare Safety, Risk, & Compliance Management
RadarFirst				○	
Riskonnect	●				Healthcare Safety, Risk, & Compliance Management
RLDatix	●				Healthcare Safety, Risk, & Compliance Management
symplr	●				Healthcare Safety, Risk, & Compliance Management
Other vendors Note: These vendors didn't participate in the report survey, but healthcare organizations interviewed for KLAS' Cybersecurity 2025 report mentioned using or considering these vendors.					
Axio		○			
Bitsight			○		
Mitratech			○		
RiskRecon			○		
RSA Security		○			

Security operations

	Vulnerability management software	SOAR	SIEM	EDR	XDR	Disaster recovery	Exposure management	KLAS-measured solutions
Armis	○	○						*Measured in other area*
Asimily	○	○		○		○		*Measured in other area*
AvePoint	○		○			○		
Cisco	○	○	○	○	○			*Measured in other area*
Claroty	○							*Measured in other area*
Clearwater	○	○	○	○	○			*Measured in other areas*
CloudWave	○	○	○	○				*Measured in other area*
Commvault		○	○			○		
CyberProof	○	○	○	○	○	○	○	
Cyber Salus	○	○	○					
Cyderes	○	○	○	○	○			
Cynerio	○							*Measured in other area*
EY	○	○	○	○	○	○	○	*Measured in other areas*
Forescout	○	○	○		○			
Fortified Health Security	○	○	○	○	○		○	*Measured in other areas*
GYTPOL							○	
HadenGrey	○			○	○			
Intruno			○					
LevelBlue		○	○		○			
ManageEngine	○	○	○	○		○		
MorganFranklin Consulting	○	○	○	○	○	○		
NCC Group	○		○	○	○		○	
Netwrix						○		
Nozomi Networks	○			○				
Okta	○	○				○		
Optiv	○	○	○	○	○	○		
Palo Alto Networks		○	○	○	○			*Measured in other area*
Ping Identity	○	○	○	○	○	○		
Rubrik	○					○		
SailPoint	○						○	*Measured in other area*
Splunk		○	○					
ThreatLocker	○			○			○	
Trustwave	○							
Veeam						○		
Zscaler	○						○	

Continued on next page

Vendor-Reported Cybersecurity Software Offerings, Continued

○ Vendor-reported offering ● KLAS-measured solution

Click vendor name for information about their cybersecurity strategies (if submitted)

Security operations

	Vulnerability management software	SOAR	SIEM	EDR	XDR	Disaster recovery	Exposure management	KLAS-measured solutions
Other vendors Note: These vendors didn't participate in the report survey, but healthcare organizations interviewed for KLAS' Cybersecurity 2025 report mentioned using or considering these vendors.								
CDW	○							
Check Point Software Technologies				○				
Exabeam (LogRhythm)			○					
SentinelOne			○		○			
Tenable	○							
WatchGuard				○				

Data & application security

	Application security	DLP	DSPM	Data governance/ classification	KLAS-measured solutions
AuthX	○				
AvePoint	○	○	○		
Cisco		○			*Measured in other area*
CloudWave	○				*Measured in other area*
Commvault	○	○			
CyberProof	○	○			
DigiCert	○				
EY	○	○	○	○	*Measured in other areas*
Fortified Health Security	○	○			*Measured in other areas*
HadenGrey	○	○	○		
ManageEngine	○	○			
MorganFranklin Consulting	○	○			
Netwrix		○	○	○	
Okta	○	○			
Optiv	○	○	○	○	
Palo Alto Networks	○	○			*Measured in other area*
Ping Identity	○	○			
Proofpoint	○	○	○	○	
Radware	○				
Rubrik	○	○	○		
SailPoint				○	*Measured in other area*
SecureAuth	○				
Splunk	○				
ThreatLocker	○	○			
Trustwave	○				
Varonis		○	○	○	
Veeam	○	○	○		
Zscaler	○	○	○	○	
Other vendors Note: These vendors didn't participate in the report survey, but healthcare organizations interviewed for KLAS' Cybersecurity 2025 report mentioned using or considering these vendors.					
Digital Guardian		○			

Proactive security

	Security training/ awareness	Attack simulation	Threat intelligence	KLAS-measured solutions
Asimily	○		○	*Measured in other area*
Cisco			○	*Measured in other area*
Claroty	○			*Measured in other area*
Clearwater	○	○	○	*Measured in other areas*
Commvault	○		○	

Continued on next page

Vendor-Reported Cybersecurity Software Offerings, Continued

○ Vendor-reported offering ● KLAS-measured solution

Click vendor name for information about their cybersecurity strategies (if submitted)

		Security training/ awareness	Attack simulation	Threat intelligence	KLAS-measured solutions
Proactive security	CyberProof	○	○		
	Cyber Salus			○	
	Cyderes	○	○		
	Cynerio	○		○	*Measured in other area*
	EY		○	○	*Measured in other areas*
	Fortified Health Security	○	○	○	*Measured in other areas*
	HadenGrey	○	○		
	LevelBlue			○	
	ManageEngine	○	○		
	MorganFranklin Consulting	○	○		
	NCC Group	○	○		
	OnDefend		○		
	Optiv	○	○		
	Palo Alto Networks	○	○		*Measured in other area*
	Ping Identity	○	○	○	
	Proofpoint	○	○	○	
	Rubrik	○	○		
	SailPoint			○	*Measured in other area*
	SANS Institute	○	○		
	Security Compliance Associates	○			
	ThreatLocker	○	○		
	Varonis	○	○		
	Veeam		○	○	
	Zscaler		○	○	
	Other vendors Note: These vendors didn't participate in the report survey, but healthcare organizations interviewed for KLAS' Cybersecurity 2025 report mentioned using or considering these vendors.				
	AttackIQ		○		
	Cofense	○	○		
	Infosec	○			
	KnowBe4	○			

Cybersecurity Services Offerings: Firm-Reported Capabilities

The services charted below are self-reported by professional services firms as being live and currently available to their clients. Links to relevant KLAS performance data are included where applicable, though measurement does not mean that KLAS has validated each service the firm reports to offer.

Firm-Reported Cybersecurity Services Offerings

Click vendor name for information about their cybersecurity strategies (if submitted)

○ Vendor-reported offering
● KLAS-measured service

		Security staff augmentation	Threat & vulnerability management	MDR	Incident response/ disaster recovery	SOC or 24/7 monitoring	Security software management	Third-party risk management	Healthcare IoT management/ medical device security	Privacy management	Device patch management	KLAS-measured services
Managed services	Armis	○	○	○	○	○	○	○	○	○	○	*Measured in other area*
	Asimily	○	○	○			○	○			○	*Measured in other area*
	Censinet	○	○		○			○	○	○		
	Cisco	○	○	○	○	○	○	○	○	○	○	*Measured in other area*

Continued on next page

Firm-Reported Cybersecurity Services Offerings, Continued

Click vendor name for information about their cybersecurity strategies (if submitted)

○ Vendor-reported offering
● KLAS-measured service

		Threat & vulnerability management		Incident response/ disaster recovery			Security software management		Healthcare IoT management/ medical device security		Device patch management	
		Security staff augmentation	MDR	SOC or 24/7 monitoring			Third-party risk management		Privacy management			KLAS-measured services
Managed services	Clearwater	●	●	●	●	●	●	●	●	●	●	Security & Privacy Managed Services
	CloudWave	●	●	●	●	●	●		●		●	Security & Privacy Managed Services
	ColorTokens	○	○	○	○	○	○		○			
	Commvault		○	○	○		○					
	CyberProof	○	○	○	○	○	○	○	○	○	○	
	Cyber Salus	○	○	○		○	○	○	○	○	○	
	Cyderes	○	○	○	○	○	○	○	○		○	
	Cynerio		○		○	○			○		○	Measured in other area
	Darktrace	○	○	○	○	○	○		○			
	EY	○	○	○	○	○	○	○	○	○	○	Measured in other areas
	Forescout		○	○		○			○			
	Fortified Health Security	●	●	●	●	●	●	●	●			Security & Privacy Managed Services
	HadenGrey	○	○				○	○	○	○		
	Imprivata									○		Measured in other areas
	Intruno									○		
	LevelBlue	○	○	○	○	○	○	○		○	○	
	ManageEngine		○								○	
	Meditology Services	○										Measured in other area
	MorganFranklin Consulting	○	○	○	○	○	○	○	○	○	○	
	NCC Group	○	○	○	○	○	○	○	○	○		
	OnDefend		○									
	Optiv	○	○	○	○	○	○	○			○	
	Palo Alto Networks	○	○	○	○	○	○	○	○			Measured in other area
	Ping Identity		○	○		○	○	○	○	○		
	PwC	○	○	○	○	○	○	○	○	○	○	Measured in other area
	Radware	○	○	○	○	○						
	Rubrik				○							
	SailPoint	○										Measured in other area
	Security Compliance Associates	○										
	ThreatLocker	○	○	○	○	○	○	○			○	
	Trustwave	○	○	○	○	○	○	○	○	○	○	
	tw-Security	○						○				Measured in other area
	Varonis		○		○			○				
	Veeam				○							
	Zscaler	○	○	○	○		○	○	○	○		
	Additional KLAS-validated firms Note: These vendors didn't or weren't able to participate in the report survey, but within the past 12 months, KLAS has interviewed at least one live customer for the offerings listed.											
	Arctic Wolf	○	○	○	○	○	○					
	CrowdStrike					○						
	Deloitte	○	○			○						Measured in other area
	First Health Advisory	○	○	○	○	○	○	○	○			
	Secureworks					○						
	Other firms Note: These firms didn't participate in the report survey, but healthcare organizations interviewed for KLAS' Cybersecurity 2025 report mentioned using or considering these vendors.											
	CDW				○							
	Coalfire							○				

Continued on next page

Firm-Reported Cybersecurity Services Offerings, Continued

Click vendor name for information about their cybersecurity strategies (if submitted)

○ Vendor-reported offering
● KLAS-measured service

Managed services

	Security staff augmentation	Threat & vulnerability management: MDR	Incident response/ disaster recovery: SOC or 24/7 monitoring	Security software management: Third-party risk management	Healthcare IoT management/ medical device security: Privacy management	Device patch management	KLAS-measured services
Lumifi (Critical Insight)		○					
Cybersafe Solutions			○				
Expel		○					
Ivanti						○	
Mandiant			○				
Red Canary		○					
ReliaQuest		○					
Rule4				○			
SenseOn			○				
SentinelOne			○				
WatchGuard						○	

Consulting services

	Security risk assessment: Implementation/ configuration/ design of security technologies	Security risk assessment: Healthcare IoT/medical device security assessment	Security program assessment/ development: HIPAA privacy assessment	Social engineering & phishing: Penetration/ vulnerability/ network/web application security testing	Virtual/ interim CISO	KLAS-measured services
Armis	○	○	○	○	○	*Measured in other area*
Asimily	○	○	○	○	○	*Measured in other area*
AvePoint		○				
Censinet	○	○	○	○	○	
Cisco	○	○	○	○	○	*Measured in other area*
Claroty	○		○	○		*Measured in other area*
Clearwater		●	●	●	●	**Security & Privacy Consulting Services**
CloudWave	○	○	○	○	○	*Measured in other area*
ColorTokens	○	○	○			
Commvault	○	○		○		
CyberProof	○	○	○	○	○	
Cyber Salus		○	○		○	
Cyderes	○	○	○	○		
Cynerio	○	○	○	○	○	*Measured in other area*
Darktrace	○	○	○			
DigiCert	○					
EY	●	●	●	●	●	**Security & Privacy Consulting Services**
Forescout	○		○			
Fortified Health Security	●	●	●	●	●	**Security & Privacy Consulting Services**
GYTPOL		○				
HadenGrey	○	○		○	○	
Illumio		○				
Intraprise Health	●	●	●	●	●	**Security & Privacy Consulting Services**
LevelBlue	○	○		○	○	
Meditology Services	●	●	●	●	●	**Security & Privacy Consulting Services**
MorganFranklin Consulting	○	○	○	○	○	
NCC Group	○	○	○	○	○	
Okta	○					

Continued on next page

Firm-Reported Cybersecurity Services Offerings, Continued

Click vendor name for information about their cybersecurity strategies (if submitted)

○ Vendor-reported offering
● KLAS-measured service

		Implementation/ configuration/ design of security technologies	Security risk assessment	Healthcare IoT/medical device security assessment	Security program assessment/ development	HIPAA privacy assessment	Social engineering & phishing	Penetration/ vulnerability/ network/web application security testing	Virtual/ interim CISO	KLAS-measured services
Consulting services	OnDefend	○	○	○	○	○	○	○	○	
	Optiv	○	○	○	○	○	○	○	○	
	Palo Alto Networks	○	○	○	○	○		○	○	*Measured in other area*
	Ping Identity	○	○	○		○	○	○		
	Proofpoint	○					○			
	PwC	○	○	○	○	○	○	○	○	*Measured in other area*
	Rubrik	○	○							
	SailPoint	○			○					*Measured in other area*
	SANS Institute		○		○		○			
	SecureAuth	○								
	Security Compliance Associates	○	○	○	○	○	○	○	○	
	Trustwave	○	○	○	○	○	○	○	○	
	tw-Security	●	●	●	●	●			●	**Security & Privacy Consulting Services**
	Varonis	○	○							
	Veeam	○	○							
	Zscaler	○		○		○		○		
	Additional KLAS-validated firms Note: These vendors didn't or weren't able to participate in the report survey, but within the past 12 months, KLAS has interviewed at least one live customer for the offerings listed.									
	Chartis	●	●	●	●	●			●	**Security & Privacy Consulting Services**
	Deloitte	○	○	○	○	○	○	○		*Measured in other area*
	First Health Advisory		○	○				○		
	Guidehouse		●		●		●	●		**Security & Privacy Consulting Services**
	Impact Advisors	●	●		●	●			●	**Security & Privacy Consulting Services**
	Protiviti		○	○	○					
	Other firms Note: These firms didn't participate in the report survey, but healthcare organizations interviewed for KLAS' Cybersecurity 2025 report mentioned using or considering these vendors.									
	CDW		○							
	Coalfire		○							
	Rule4								○	
	Security Risk Advisors		○							
	Trace3				○					

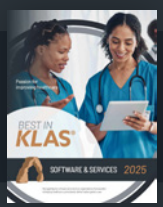
Cybersecurity Research from KLAS

Reports published in the last 6 months

Security & Privacy Consulting/ Managed Services 2024

Cybersecurity 2025

Best in KLAS 2025



Healthcare Cybersecurity Benchmarking Study 2025

Planned reports/areas of research

- Healthcare IoT Security 2025
- Third-Party Risk in Healthcare
- Best in KLAS 2026
- Validations of Vendor- & Firm-Reported Cybersecurity Capabilities (from this guide)

Report Information

Share your experience with peers.
Take a short survey about your cybersecurity technology and/or firm.

About This Report

This study is designed to give payer and provider organizations a clear picture of what capabilities software vendors and professional services firms offer to meet their cybersecurity needs. Most data in this study comes from **vendor- and firm-reported information**. 55 vendors and firms responded to the survey for this guide. Some insights from other KLAS research are also included.

In addition to asking participating vendors and firms to report their cybersecurity offerings, KLAS also asked participants the following questions:

1. How do you cater specifically to the needs of healthcare security and privacy?
2. How is your healthcare cybersecurity offering unique in this space?

Reader Responsibility

KLAS data and reports are a compilation of research gathered from websites, healthcare industry reports, interviews with healthcare, payer, and employer organization executives and managers, and interviews with vendor and consultant organizations. Data gathered from these sources includes strong opinions (which should not be interpreted as actual facts) reflecting the emotion of exceptional success and, at times, failure. The information is intended solely as a catalyst for a more meaningful and effective investigation on your organization's part and is not intended, nor should it be used, to replace your organization's due diligence.

CO-AUTHOR
Jaren Day
jaren.day@KLASresearch.com

CO-AUTHOR
Ciera Black Walker
ciera.walker@KLASresearch.com

WRITER
Natalie Hopkins

DESIGNER
Kath Spencer

PROJECT MANAGER
Sydney Toomer

KLAS RESEARCH

Our Mission
Improving the world's healthcare through collaboration, insights, and transparency.

365 S. Garden Grove Lane, Suite 300
Pleasant Grove, UT 84062

Ph: (800) 920-4109

For more information about KLAS, please visit our website:
engage.KLASresearch.com

Cover image:
© C Malambo/peopleimages.com / Adobe Stock

Vendor & Firm Insights

Note: Some vendors/firms who took the report survey did not answer the additional scoping questions and thus are not included in this section; these vendors/firms are HadenGrey, Nozomi Networks, and Origami Risk.

Based on vendor- and firm-reported information

Armis

KLAS-Measured Offerings

Healthcare IoT

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- **51%–75%**
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- **Payer/insurer**
- Post-acute care/home health/hospice
- **Standalone hospital**
- **Other**

How do you cater specifically to the needs of healthcare security and privacy?

Since the company's inception, Armis has provided specialized services for healthcare organizations, including a dedicated healthcare product—Armis Centrix for Medical Device Security. Armis Centrix offers complete visibility into and protection for every asset in the modern healthcare environment, from IoMT/IoT, IT, and OT assets. The platform compiles information (e.g., FDA recalls, MDS2) to provide a full picture of the risks associated with each asset and facilitate easier remediation and mitigation for assets involved in patient care. Real-time asset intelligence and network analysis monitor for exfiltration or transmission of unencrypted data in order to protect sensitive patient information. Medical device behavioral insights provide detailed security information that facilitates better patient flow, efficient device utilization, and accurate reporting to aid compliance with HIPAA, PHI, and additional privacy regulations. Floor map and location information streamline any remediation processes and allow clinical engineering teams to easily pinpoint assets and carry out updates with all the relevant information in one place.

How is your healthcare cybersecurity offering unique in this space?

Armis revolutionizes healthcare cybersecurity by addressing the unique challenges of protecting complex, sensitive medical devices and the broader healthcare environment. Designed for healthcare delivery organizations, the Armis Centrix Cyber Exposure Management platform seamlessly integrates with existing systems to deliver visibility and protection for not only medical devices but all assets in the healthcare environment. Comprehensive security of the attack surface and continuous real-time insights keep organizations protected against known and unknown threats. Armis' Early Warning detection allows organizations to take a proactive security stance with insights about potential risks that are being weaponized in the wild to facilitate action before the threats take hold. Armis prioritizes risks based on the organization's most critical assets, including information about when, where, and how they are used. Armis quickly assigns actions and resolves the top-priority findings and risks to patient care. Armis Centrix is powered by an AI-driven Asset Intelligence Engine that catalogs known good behavior baselines for over 6 billion assets. The solution prioritizes easy identification, classification, and asset context so that users have a true view of all risks for management, risk assessment, priortization, mitigation, and remediation.

Asimily

KLAS-Measured Offerings

Healthcare IoT

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- **51%–75%**
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- **Payer/insurer**
- **Post-acute care/home health/hospice**
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Asimily provides a platform for end-to-end cybersecurity for IoMT, as well as IoT and OT, in healthcare environments. The platform includes risk assessment, device security assessments, inventory management, vulnerability management, threat and response readiness, and more. Our goal is to meet all IoMT cybersecurity needs from pre-purchase to device retirement and disposal. This is accomplished through safe, passive listening to network traffic from IoMT/IoT. Unlike our competitors, we find quick targeted fixes (when possible) for security problems through vulnerability-by-vulnerability analysis. Further, our risk analysis considers the impact and likelihood of an attack to reduce the amount of work customers need to do to get the most risk out of their organizations. Additional unique features (e.g., IoT patching, configuration control/snapshots, packet capture) provide additional cybersecurity services to assist health systems. All PHI is kept out of Asimily's system and analyses, helping ensure patient privacy. It can be run entirely on premises or partially in the cloud, depending on customers' wishes.

How is your healthcare cybersecurity offering unique in this space?

Asimily provides vulnerability analyses (not just classification) to find out how an attacker can take advantage of a vulnerability for a given device in a given environment. These analyses result in dramatically easier fixes and better risk management. For remediation, Asimily's deeper research allows us to offer targeted fixes where possible to close out a risk vulnerability in addition to segmentation and micro-segmentation. Asimily also offers other capabilities:

- Ability to automatically capture packets in case of an incident to create a forensic trail in case of an investigation
- Ability to assess the device risk at procurement and provide recommendations for device hardening
- Configuration control: Ability to capture and store a good copy of device network configuration to recover better from ransomware, misconfigurations, or third-party errors; also provides the ability to detect a drift in configuration
- IoT patching: Automated that can quickly and centrally deploy patches to certain IoT devices (e.g., cameras, printers, switches) directly from Asimily portal to shorten exposure windows

AuthX

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- ○ 1%–25%
- ○ 26%–50%
- ○ 51%–75%
- ● 76%–99%
- ○ 100%

Current Client Base

- ● IDN/health system
- ● Outpatient/ambulatory
- ○ Payer/insurer
- ○ Post-acute care/home health/hospice
- ● Standalone hospital
- ○ Other

How do you cater specifically to the needs of healthcare security and privacy?

At AuthX, we redefine healthcare authentication—balancing security, efficiency, and compliance without disrupting patient care. Traditional login processes decrease the productivity of clinical workforce, risking both security and operational efficiency. AuthX eliminates these barriers with the following:

- Passwordless, adaptive MFA: Instant, secure authentication via passkeys, badge tap, biometrics, and AI-driven MFA
- Cloud-native & scalable platform: Rapid and effortless deployment across hospital networks with no on-premises overhead
- Seamless SSO: Federated secure access to all critical healthcare applications (e.g., Epic, MEDITECH, Oracle Health)
- Touchless, rapid authentication: Badge tap and facial recognition minimize login fatigue and maximize efficiency
- Compliance at the core: Platform is aligned to organizations' security and compliance needs

We secure access so that providers can focus on what matters most—patient care.

How is your healthcare cybersecurity offering unique in this space?

AuthX sets a new standard in healthcare cybersecurity with a cloud-first, security-driven approach that eliminates friction without compromising protection.

- Seamless EHR & app compatibility: Effortless integration with all clinical applications and configurable workflows to improve provider efficiency and outcomes
- Low TCO: No on-premises complexity; faster and seamless deployment across hospital networks
- FIDO & passkeys: Passwordless authentication for stronger security and a frictionless user experience
- Security-first design: End-to-end encryption, zero-trust architecture, adaptive authentication, and continuous risk assessment
- Device & environment agnostic: Secure authentication across all endpoints, from workstations to mobile devices; multiple operating systems
- One solution to secure all enterprise applications: A single solution to protect endpoint and application access across multiple mediums without the need for multiple vendors

AvePoint

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

The AvePoint Confidence Platform addresses healthcare organizations' security challenges through automated policies protecting sensitive information. The platform provides data governance ensuring compliance while maintaining confidentiality. For healthcare organizations using Microsoft 365, AvePoint offers controls and automation enabling secure team collaboration. The platform ensures only authorized personnel access critical information, managing data throughout its life cycle. AvePoint helps maintain operational continuity while adhering to HIPAA, HITRUST, and HITECH requirements.

How is your healthcare cybersecurity offering unique in this space?

AvePoint's healthcare cybersecurity solution stands out through its comprehensive approach to data security, governance, and resilience. Our platform uses automated policies to safeguard health information, preventing oversharing of sensitive data while ensuring compliance with stringent regulatory requirements. By implementing advanced controls, AvePoint supports secure cross-agency collaboration and decision-making. Our data governance capabilities streamline fragmented workflows, reducing operational costs, improving administrative productivity, and empowering teams to collaborate securely while maintaining patient confidentiality. Our platform also offers flexibility and scalability, helping healthcare organizations navigate digital transformation. By preventing potential data exposures that could disrupt patient care or business operations, AvePoint ensures comprehensive cybersecurity that supports both operational efficiency and patient safety.

Censinet

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Censinet RiskOps enables healthcare organizations to manage GRC and cyber risk at scale. Purpose-built for healthcare, Censinet enables organizations to assess, manage, and mitigate third-party and enterprise risks more efficiently and effectively in alignment with industry regulations and best-practice frameworks (e.g., HIPAA, NIST CSF).

Powered by Censinet AI infrastructure, Censinet delivers end-to-end process automation for third-party risk management (TPRM); strengthens AI risk management and governance; and facilitates enterprise-wide collaboration to reduce risk, strengthen resilience, and protect patient safety from cyber threats. The Censinet Digital Risk Catalog contains over 50,000 vendors and products, providing a centralized, digital inventory to manage all third parties supporting care operations—including software, services, medical devices, AI technologies, research and clinical trials, and nontechnical suppliers.

Censinet Systemic Risk capabilities automatically identify which third-party products and services support critical functions across care operations—including where AI influences clinical decision-making—enabling more effective prioritization of risks that directly impact patient care and minimizing potential disruptions to care continuity.

Censinet delivers enterprise assessments and peer benchmarking across NIST CSF 2.0, HPH CPGs, NIST AI RMF, HICP, and key organizational metrics.

How is your healthcare cybersecurity offering unique in this space?

Censinet RiskOps is the first and only cyber GRC platform purpose-built for healthcare, delivering a highly scalable, turnkey solution for third-party and Censinet RiskOps is the first and only cyber GRC platform purpose-built for healthcare, delivering a highly scalable, best-practice cyber risk management solution "in a box." Unlike pan-industry GRC solutions, Censinet is designed specifically to manage healthcare risks in alignment with industry regulations and best-practice security frameworks (e.g., HIPAA, NIST CSF).

Powered by Censinet AI, Censinet delivers end-to-end assessment automation out of the box—eliminating lengthy implementation delays while driving unmatched TPRM speed, scale, and risk visibility. Leveraging Censinet's network model, third-party vendors can share completed questionnaires and risk updates with a single click, accelerating assessment and reassessment workflows and creating a longitudinal risk record across the TPRM lifecycle.

Censinet Systemic Risk capabilities automatically identify which third-party systems support critical functions across care operations—including those where AI influences clinical decision-making—enabling risk teams to focus TPRM efforts on the vendors and products that directly impact care delivery and patient safety. These insights enhance strategic risk visibility across the enterprise and help cybersecurity leaders communicate in operational and clinical terms that resonate with non-technical stakeholders—enabling more informed, business-focused risk decisions.

Censinet also delivers the industry's first and only AI Governance & Risk Command Center, a unified solution that centralizes, streamlines, and strengthens the discovery, risk management, and governance of AI technologies in alignment with healthcare regulations and best practices (e.g., NIST AI RMF).

Continuous monitoring capabilities provide real-time breach alerts to expedite incident response and recovery. An integrated Censinet Risk Register centralizes all TPRM and ERM assessment findings and streamlines enterprise-wide collaboration to remediate risks. For organizations facing resource constraints, Censinet's on-demand managed services offer critical support to maintain TPRM program continuity.

Cisco

KLAS-Measured Offerings

Access Management

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Cisco enables thousands of healthcare organizations of all sizes to secure patient EHR, meet compliance and cyber liability insurance requirements, and provide secure access to critical applications used by medical practitioners. Our security solutions address threats healthcare providers face daily, such as ransomware attacks that are designed to steal patient medical records and take control of or shut down systems and devices. Features such as phishing-resistant multifactor authentication deliver strong security controls against these attacks while also helping organizations meet compliance with HIPAA, EPCS, cyber insurance, and other industry mandates. Cisco also addresses healthcare organizations' move to a hybrid model with single sign-on, which helps mitigate risks in local and remote environments where healthcare professionals are accessing applications and patient data hosted in the cloud or on premises. Our vendor-agnostic approach means hospitals can use any application, whether that is Epic, a telehealth program, or a custom app. Healthcare organizations can ensure only managed devices have access to sensitive patient information or extend that access to include personal, unmanaged devices through device trust policies.

How is your healthcare cybersecurity offering unique in this space?

Cisco has responded to the growing number of identity-based attacks with Continuous Identity Security (CIS), a unique AI-powered solution that stops sophisticated attacks that target users' identities and ensures a seamless authentication experience for every medical practitioner and staff member. CIS is composed of two services: (1) Cisco Identity Intelligence leverages data from a healthcare organization's entire identity ecosystem (e.g., IdPs, HRIS, CRMs, ticketing systems, etc.) to inform posture, detection, and response decisions. (2) Duo Passport improves the user experience and enhances security by minimizing the number of authentication prompts when accessing web applications, thick/thin clients, and browsers throughout the workday. In addition to CIS, Cisco has out-of-the-box integrations with critical EHR systems including Epic Hyperdrive and Hyperspace, as well as mobile apps like Epic Canto and Haiku, simplifying access to patient information for healthcare providers and administration for IT. Cisco also supports the industry's broadest range of authentication factors and operating systems to meet every use case required by healthcare organizations.

Claroty

KLAS-Measured Offerings

Healthcare IoT

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- **51%–75%**
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- Payer/insurer
- Post-acute care/home health/hospice
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Claroty xDome for Healthcare addresses the unique security and privacy challenges of healthcare by providing comprehensive visibility and protection for connected medical, IoT, and OT devices. It ensures real-time monitoring, identifies vulnerabilities in critical systems, and prioritizes risks to safeguard patient safety and operational continuity. xDome supports regulatory compliance with standards like HIPAA, HITECH, and NIST CSF by protecting devices that interact with electronic protected health information (ePHI) and streamlining audit readiness. Its proactive threat detection leverages a database of known signatures and behavioral analysis to identify anomalies and threats, like ransomware. Additionally, xDome continuously monitors device communications to recommend specific communication policies for medical devices based on known best practices in healthcare environments. By integrating seamlessly with existing IT security tools and focusing on privacy-centric data management, xDome enables healthcare organizations to defend against cyber threats without compromising patient care, ensuring resilience in an increasingly connected ecosystem.

How is your healthcare cybersecurity offering unique in this space?

Claroty xDome is a unique solution compared to other vendors on the market and has a robust data foundation that leverages industry-leading deep-packet inspection and other active scanning approaches. Healthcare organizations using our solution achieve superior inventory accuracy, sometimes increasing asset counts by up to 340% compared to other vendors.

Our broad solution set spans exposure management, network protection, threat detection, and operational efficiency use cases, providing detailed risk and exposure identification and scoring methodology. When measuring security postures, our risk assessments consider both exploitability and impact, adding a stronger level of accuracy. Claroty xDome offers industry profiling and benchmarking, leveraging one of the industry's largest connected-device databases to enable users to get a clearer understanding of their organizational risk.

Beyond technology, Claroty xDome for Healthcare is strengthened by a robust technical alliance program that integrates seamlessly with leading IT security vendors. Our solution is also backed by Team82, our industry-leading research team, which continuously drives innovation and shapes our road map.

Clearwater

KLAS-Measured Offerings

Security & Privacy Managed Services
Security & Privacy Consulting Services

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

We have account and delivery teams that are focused on serving the unique needs of different parts of the healthcare ecosystem, including IDNs and large health systems, regional and critical access hospitals, physician/ambulatory groups, and payers. Each has distinct challenges that require different solutions, and our go-to-market model is designed to ensure we are delivering the right solution to help the client move to a more secure, compliant, and resilient state so they can achieve their mission.

How is your healthcare cybersecurity offering unique in this space?

Clearwater provides the industry's deepest pool of experts across a broad range of cybersecurity, privacy, and compliance domains; purpose-built software that enables efficient identification and management of cybersecurity and compliance risks; managed cloud services; and a 24/7 Security Operations Center with managed threat detection and response capabilities. We provide the broadest portfolio of solutions focused on serving the needs of healthcare organizations, with offerings designed specifically for different segments of the ecosystem.

CloudWave

KLAS-Measured Offerings

Security & Privacy Managed Services

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

CloudWave delivers healthcare specific security and risk solutions that protect patient data, ensure compliance, and support clinical uptime. With 24/7 managed security services, HIPAA-aligned practices, and a private cloud built for healthcare, CloudWave addresses the unique risks hospitals face. We secure both IT and clinical systems, including biomedical devices, and offer proactive support through embedded advisors and healthcare focused incident response. Our approach combines technical expertise with deep industry understanding to help hospitals stay secure without disrupting care.

How is your healthcare cybersecurity offering unique in this space?

CloudWave's healthcare cybersecurity offering is uniquely designed to support hospitals with a deep focus on data protection, backup, and disaster recovery. Unlike general IT providers, CloudWave integrates security directly into its healthcare-specific infrastructure services, ensuring systems remain available, compliant, and resilient. With 24/7 monitoring, rapid threat response, and a strong understanding of clinical workflows, CloudWave helps healthcare organizations safeguard patient data and maintain continuity of care. The result is a purpose-built cybersecurity program that protects both IT operations and the clinical mission.

ColorTokens

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- **51%–75%**
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- **Standalone hospital**
- **Other**

How do you cater specifically to the needs of healthcare security and privacy?

Healthcare organizations are prime targets for cyberattacks. The complexity of healthcare IT, compounded by legacy systems, medical devices, and third-party integrations, makes achieving absolute security at the network perimeter nearly impossible.

Today, most significant cybersecurity investments focus on breach prevention such as firewalls, endpoint protection, and zero-trust network access. However, recent attacks have shown that breaches are inevitable, irrespective of advanced perimeter defenses. The question is no longer whether an initial compromise will occur—but how quickly and effectively organizations can contain the threat.

This is where microsegmentation changes the game. By enforcing granular access controls, it stops the lateral movement of malware and ransomware, preventing cyberattacks from becoming a crisis. Whether it is protecting EHRs, billing and coding applications, or segmenting medical devices such as infusion pumps, ventilators, telemetry devices and imaging devices, microsegmentation blocks cybercriminals from exploiting vulnerabilities and manipulating critical data—ensuring patient safety and operational resilience.

How is your healthcare cybersecurity offering unique in this space?

1. Comprehensive protection: ColorTokens' solution is unique because it secures hospital IT systems and networked medical devices in a single pane of glass. EHR systems, critical business applications, provider workstations, and medical devices are all protected from the spread of malware and ransomware with one unified tool.
2. Flexible visualization: ColorTokens lets you uniquely visualize your network assets and the traffic between them. Zero-trust policies are defined based on these views, which allow only authorized traffic, stopping the lateral movement of malware and ransomware.
3. Ease of implementation: Xshield can be quickly installed with only a lightweight agent for Windows, Linux, and Mac endpoints, or it can leverage existing EDR agents already installed in the enterprise. On-device simulation and testing before policy enforcement means there will be no disruption to the hospital's valid business processes.
4. Quick risk reduction: ColorToken's agile method for configuring policies, beginning with enterprise-wide controls on risky ports and paths, yields immediate security gains with ongoing improvement in the enterprise security posture.

Commvault

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- **76%–99%**
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- **Payer/insurer**
- **Post-acute care/home health/hospice**
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Commvault has a deep history of working directly with healthcare organizations, developing specific components to extend beyond backup and recovery to address security and privacy needs in this industry.

The platform is designed with stringent security standards and privacy protocols in mind, such as HIPAA, ISO 27001, GDPR, and SOC 2. We understand how healthcare systems and threat actors operate, so we have enhanced our security controls to provide notifications and escalations across systems where we leverage healthcare-specific protocols, like DICOM.

Ensuring compliance with regulations like HIPAA and the HITECH Act is crucial. This includes data encryption capabilities, even for post-quantum cryptography, to meet patient data privacy requirements. We also conduct risk analyses of live or protected data to identify data owners, access permissions, and potential exposure risks.

Implementing a zero-trust architecture with multifactor authentication, privilege access management, and role-based access controls helps limit the impact of any potential breaches, as data exfiltration is a significant threat in healthcare.

How is your healthcare cybersecurity offering unique in this space?

With our extensive experience in healthcare, our solutions are thoughtfully integrated into the platform, not just added as afterthoughts. The platform stands out by offering a broad range of options and capabilities across the entire threat landscape and toolchain.

Commvault intentionally operates within specific limits, but to add greater value, we build deep, bidirectional integrations with leading security tools and partners, ensuring comprehensive resilience. As environments and threats evolve, Commvault provides full adaptability and continuous protection so you don't have to choose between innovation and risk.

With double extortion becoming a service, healthcare organizations are particularly vulnerable. It requires continuous awareness, readiness, security, recovery, and compliance tools that integrate seamlessly with other top-tier security solutions to deliver true cyber resilience. Only Commvault offers this comprehensive platform to protect healthcare organizations and ensure compliance in an ever-changing landscape.

CyberProof

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- **51%–75%**
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- **Payer/insurer**
- Post-acute care/home health/hospice
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

CyberProof's focus is on the payer, provider, life sciences, and med tech specialties, covering healthcare automation and cybersecurity. Our significant relationships with Google, Microsoft, Wiz, and other key technology vendors, like Interpres Security, allow us to provide a seamless, correlated, and enriched data intelligence to our customers, starting with threat exposures to remediation. This intelligence allows for a hardened attack and defense surface, including OT/IoT, and unparalleled visibility into threats like ransomware.

How is your healthcare cybersecurity offering unique in this space?

CyberProof provides a seamless, correlated, and enriched data intelligence to our customers, starting with threat exposures to remediation. This intelligence allows for a hardened attack and defense surface, including OT/IoT, and unparalleled visibility into threats like ransomware.

Cyber Salus

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- **76%–99%**
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- Payer/insurer
- Post-acute care/home health/hospice
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Cyber Salus is dedicated to addressing the unique security and privacy challenges faced by the healthcare industry. With a deep understanding of clinical and regulatory complexities, we deliver specialized cybersecurity solutions tailored to protect sensitive patient data, medical devices, and clinical ecosystems from ever-evolving cyber threats. We align with frameworks like HIPAA, 405(d), GDPR, and NIST to ensure compliance while proactively managing risks. Our 24/7/365 monitoring services offer real-time threat detection and response, safeguarding healthcare delivery organizations (HDOs) against ransomware, data breaches, and system downtime. What sets Cyber Salus apart is our expertise in the intersection of technology, people, and processes within healthcare. We understand the operational nuances of medical IoT devices and electronic health records and offer end-to-end solutions from risk assessments to remediation services. This allows HDOs to focus on patient care, knowing their systems are secure. With a mission to enhance trust and resilience in healthcare, Cyber Salus empowers organizations to navigate the digital landscape with confidence, ensuring safety for patients.

How is your healthcare cybersecurity offering unique in this space?

Cyber Salus stands apart in the healthcare cybersecurity space by offering a fully integrated, end-to-end solution specifically tailored to the unique challenges of healthcare delivery organizations. Unlike generic IT security providers, we specialize exclusively in protecting clinical ecosystems, medical devices, and sensitive patient data, combining cutting-edge technology, regulatory compliance expertise, and deep industry knowledge. Our unique offering includes 24/7/365 SOC monitoring, proactive threat detection, and real-time incident response designed to address the operational and regulatory complexities of healthcare. We don't just secure IT systems—we focus on the medical IoT devices and clinical workflows critical to patient safety. Our solutions align with leading standards like HIPAA, 405(d), GDPR, and NIST, ensuring compliance while minimizing risk. What truly sets us apart is our holistic approach, encompassing risk assessments, vulnerability management, and boots-on-the-ground remediation. Our healthcare-first mindset and tailored strategies empower HDOs to not only defend against evolving cyber threats but also maintain uninterrupted patient care and trust.

Cyderes

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- **26%–50%**
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- Outpatient/ambulatory
- **Payer/insurer**
- Post-acute care/home health/hospice
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Every leadership position at Cyderes has in-field experience working with CE and BAs—our experience is not hypothetical. We have former CISOs for providers that run our various service categories, and we have a large healthcare CISO advisory board that reviews our road map, technologies, and the solutions that our clients are looking to implement. We are a true extension of our clients' teams, and we can provide the hands-on work needed to stop threats, while leveraging the existing investments and tools that our healthcare clients have in place today.

How is your healthcare cybersecurity offering unique in this space?

Cyderes builds and maintains playbooks and workflows that have been custom built by other health systems to deal with cyber threats. These playbooks are integrated into our service offerings and are reviewed by our healthcare CISO advisory board (comprising 20+ health systems) to ensure they are staying up-to-date with how threats are evolving. Cyderes provides actual remediation actions, not just alerts, and we leverage the existing tool sets (endpoint, SIEM, firewalls, DLP, etc.) to perform these actions. We do not need to deploy custom software to make this all work; we leverage the existing tool set, and if additional solutions are needed, clients can make a request to our advisory board for recommendations or referrals. This unique service model has worked very well in healthcare and has greatly shortened the SLA of stopping threats and performing other key tasks, such as resetting a user's password.

Cynerio

KLAS-Measured Offerings

Healthcare IoT

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- **51%–75%**
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- Payer/insurer
- Post-acute care/home health/hospice
- **Standalone hospital**
- **Other**

How do you cater specifically to the needs of healthcare security and privacy?

Cynerio is purpose-built for healthcare, consolidating full asset visibility, real-time threat detection, risk management, and automated remediation into a single, healthcare-specific security platform. Unlike traditional solutions focused only on IT security and data protection, we secure all connected devices—including medical device, IoT, OT, and IT—ensuring patient care and service availability are not compromised by cyber threats.

To address limited security resources and expertise, Cynerio provides automated risk prioritization, guided remediation, and real-time attack detection to reduce the burden on security teams. Our proactive risk management continuously assesses vulnerabilities, even for unpatchable legacy devices, while NDR-H (Network Detection & Response for Healthcare) stops ransomware and lateral movement before it spreads.

By integrating all devices and risks into a single pane of glass, Cynerio eliminates fragmented security views, giving hospitals complete visibility and control. Our automated compliance support ensures alignment with HIPAA, HICP, and NIST, helping healthcare organizations strengthen security while maintaining seamless operations.

How is your healthcare cybersecurity offering unique in this space?

Cynerio delivers both proactive and reactive security, ensuring hospitals prevent, detect, and respond to cyber threats without disrupting care. Our NDR-H provides day-one protection, stopping ransomware, lateral movement, and device misconfigurations in real time.

Our CynerioLive team—composed of leading healthcare security researchers—actively uncovers new vulnerabilities, such as JekyllBot:5, helping hospitals stay ahead of emerging threats. By focusing on security, not just visibility, Cynerio enables healthcare organizations to take action before incidents occur. Hospitals use Cynerio to set and achieve risk reduction goals, prioritize vulnerabilities, automate remediation, and track progress. Unlike fragmented solutions that focus only on IT or IoT, Cynerio secures all devices—medical devices, IoT, OT, and IT—in a single-pane-of-glass platform. With seamless SIEM, NAC, and firewall integrations, Cynerio maximizes existing security investments while ensuring continuous protection.

Darktrace

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

At Darktrace, we understand the unique security and privacy challenges that the healthcare sector faces. Our mission is to empower healthcare organizations with cutting-edge AI-driven cybersecurity solutions and ensure that sensitive patient data remains secure, critical systems stay operational, and compliance with regulations like HIPAA and GDPR is seamlessly maintained. Our Darktrace ActiveAI Security Platform prevents, detects, and responds to threats across digital ecosystems at machine speed. Our self-learning AI continuously adapts to the dynamic behaviors of users, devices, and systems, delivering unparalleled visibility and precision in identifying subtle indicators of cyber threats. By partnering with Darktrace, healthcare organizations can protect what matters most: their patients, their data, and their trust in a rapidly evolving digital world.

How is your healthcare cybersecurity offering unique in this space?

- Self-learning AI: Healthcare entity–centric, unsupervised ML for real-time anomaly detection
- Autonomous response: Precise, autonomous actions to contain threats without disrupting patient care
- Cyber AI analyst: Investigates every relevant alert like a human would, at the speed and scale of AI
- Proactive security: Proactively reveal and prioritize cyber risks to ensure a resilient business continuity of care
- Incident readiness: AI-powered preparation for incident management, response, and recovery

DigiCert

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Digital certificates protect healthcare organizations from cyberattacks by securing patient data, medical devices, and communications. As healthcare organizations integrate more connected devices and digital services, the implementation of comprehensive digital certificate infrastructure becomes critical for maintaining system integrity and patient safety. Essential security measures include:

- Deploying TLS/SSL certificates for web applications
- Utilizing client certificates for device authentication
- Implementing code signing for medical software
- Enabling email signing and encryption

These layered security protocols are essential for protecting sensitive healthcare data while ensuring operational continuity and regulatory compliance. Certificates provide essential security controls through authentication mechanisms, data protection, integrity assurance, and regulatory compliance. DigiCert helps healthcare organizations navigate complex security and privacy requirements, maintaining patient trust and minimizing cybersecurity risks. This combination of expertise, security features, and customer support sets DigiCert apart as a leader in healthcare TLS certificates.

How is your healthcare cybersecurity offering unique in this space?

DigiCert is one of the most trusted, most relied-upon certificate authorities in the world. DigiCert provides validation, invests millions in its infrastructure yearly, and continues to be at the forefront of post-quantum cryptography and IoT. DigiCert has extensive validation processes that ensure a higher level of trust than other vendors' processes. We differentiate ourselves from other TLS certificate vendors by offering solutions specifically tailored to the unique security and privacy needs of the healthcare industry. With a strong focus on HIPAA compliance, DigiCert ensures our certificates provide robust encryption to protect sensitive patient data. Our cloud-based certificate management platform simplifies deployment and renewal, reducing administrative overhead for healthcare organizations. DigiCert also prioritizes interoperability, ensuring seamless integration with healthcare systems like EHRs and medical devices. Unlike other vendors, DigiCert offers scalability, making our offering ideal for both small practices and large healthcare networks. Trusted for our reliability and exceptional 24/7 support, DigiCert helps healthcare organizations.

EY

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

At EY, we recognize that healthcare is one of the most targeted sectors and that cybersecurity is paramount to safe, seamless care delivery. EY Cyber is sector-led but business value-enabled; we collaborate with clients to enhance security and resilience and secure their ability to operate and derive value from their investments.

EY Cyber assets are powered by unique, relevant IP and asset development. Key solutions targeted at CISOs and privacy LOB owners include:

- **EY Assess (cyber program accelerator):** Proprietary assessment methodology to measure cyber exposure to risk with effective remediation tools.
- **EY Privileged Access Research and Inventory Systems (PARIS):** EY-developed privileged access management (PAM) tool offers built-in privilege identification rules/criteria, eliminating manual approaches.
- **EY.ai Cyber:** Collection of AI assets and proprietary accelerators for methods development and client engagement support, enhancing cyber offerings with AI/LLM capabilities.
- **EY Cyber Operations Platform:** Proprietary framework for delivery of operate/managed security services offerings.

Our global network of 18,000+ cyber and digital risk professionals in 150 countries invests deeply to build relationships with our clients and ensure our offerings fit their agendas, while bringing best-in-class expertise from across the firm. Our healthcare-specific insights ensure our services fit our clients' needs.

How is your healthcare cybersecurity offering unique in this space?

EY cybersecurity offers leading-edge breadth and depth capabilities across the full suite of services needed to support our clients, from the fundamentals to market-leading services. We support healthcare clients with their security and privacy strategy, support advisory projects, run full enterprise transformations and support ongoing operations. Our cybersecurity offerings for the healthcare sector are designed with humans, innovation, and agility in mind while keeping focused on regulatory compliance.

We are transforming our entire global & US cybersecurity practices with artificial intelligence (AI) embedded in our service offerings, and we recently announced a nearly $2 billion investment in EY.ai, our unified AI platform of assets, accelerators, and proven methodologies underpinned by GenAI/LLMs. This is further supported by a robust network of partner ecosystem and technology alliances, including Microsoft, Tanium, Saviynt, Zscaler, CrowdStrike, Splunk, Dell, NVIDIA, ServiceNow, SAP, and more.

At EY, we're passionate about helping health organizations make better decisions and improve people's lives. This is why we deliver world-class health care solutions with a human touch.

Forescout

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Forescout addresses the unique security and privacy needs for healthcare through a comprehensive platform that manages complex interconnected medical devices and networks. We leverage 30+ data collection and monitoring techniques tailored to each device type (IT, IoT, OT, and IoMT) to ensure security does not impact patient safety. The data is presented in a simple, intuitive UI that is accessible to clinical engineers with a limited security background. The resulting security and privacy outcomes include:

- Real-time inventory of all connected IT, IoT, OT, and IoMT devices (the entire attack surface)
- Visibility into all risk and exposure, with a prioritized list of recommended mitigation and remediation actions
- Compliance reporting/enforcement
- Ability to restrict access and limit blast radius of incidents via segmentation and network access control
- Real-time detection and response to threats
- Medical device lifecycle management, including recalls
- Tracking of devices handling ePHI and monitoring communication flows to ensure patient data security

Additionally, Forescout has an internal healthcare team that is focused on healthcare organizations and clinical teams and that listens to those customers' specific requirements and needs.

How is your healthcare cybersecurity offering unique in this space?

Our differentiators are:

- Broader protection: We protect IT, OT, IoT, and IoMT devices on a single platform; all other solutions focus only on a subset of devices (either IT or IoT and IoMT), leading to visibility gaps and missed threats.
- Segmentation and access control: We support zero-trust strategies, enabling the implementation of segmentation and access control policies to limit exposure, ensure compliance, and respond to threats. All other IoMT solutions show risks and threats, but they don't offer built-in mechanisms to take actual action and tackle them.
- Automated workflows: We define and automate policy-based workflows in orchestration with our 180+ ecosystem partners, streamlining asset, risk, and compliance management and incident response; reducing manual efforts; and improving mean time to resolution.
- Vulnerability research and threat intelligence: Our Vedere Labs team specializes in vulnerabilities and threats targeting IoT, OT, and medical devices; last year alone, 60% of the team's discovered exploited vulnerabilities were unknown by CISA. Vedere Labs tracks over 800 active threat actors and distributes intelligence freely to customers, security agencies, and ISACs globally.

Fortified Health Security

KLAS-Measured Offerings

Security & Privacy Managed Services
Security & Privacy Consulting Services

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- **76%–99%**
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- **Payer/insurer**
- **Post-acute care/home health/hospice**
- **Standalone hospital**
- **Other**

How do you cater specifically to the needs of healthcare security and privacy?

Fortified is healthcare's cybersecurity partner—protecting patient data and reducing risk across the healthcare ecosystem. As an award-winning managed security service provider dedicated exclusively to healthcare, we work alongside organizations to build customized programs that strengthen security while leveraging existing investments and processes. Healthcare security requires more than just cybersecurity expertise—it demands deep industry knowledge. Every organization faces unique risks, regulations, and technologies. Fortified's team includes experts in both cybersecurity and healthcare, ensuring our approach aligns with clinical realities, changing threats, and compliance requirements. With high-touch engagements and client-specific processes, Fortified delivers a scalable, actionable approach to managing cyber risk.

How is your healthcare cybersecurity offering unique in this space?

Our unified service delivery platform, Central Command, streamlines healthcare cybersecurity management, integrating advisory and threat defense managed services into one application. Users can view and interact with alerts, manage their risk register, gain insights from analytics, and react to real-time alerts on the desktop or mobile app. Central Command revolutionizes how healthcare providers, payers, and other healthcare entities oversee and interact with their managed services programs, enabling them to be more efficient in identifying risks, monitoring threats, and responding quickly to security matters of interest. The EscalationIQ module offers:

- Data-rich, tailored escalations: Actionable intelligence that fits seamlessly into operational workflows
- Upgraded insights: Context-driven threat analysis to support informed decision-making
- Enhanced visibility: A 360-degree view of potential threats, enabling faster, more effective responses
- Intuitive user experience: Simplified navigation and workflow optimization to empower security teams
- Robust feedback capabilities: Two-way dialogues that ensure continuous improvement and alignment with threats

GYTPOL

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Healthcare delivery organizations (HDOs) face complex IT environments, built over time with diverse systems and architectures. Managing security across these fragmented infrastructures is challenging, especially when patient care relies on system uptime. The constant trade-off between security and operations leads to delayed remediation, unaddressed risks, and compliance gaps. GYTPOL bridges these gaps by mapping IT/OT dependencies, enabling HDOs to make informed security decisions without operational disruption. By eliminating guesswork, GYTPOL ensures that security actions don't impact critical systems. With automated remediation and quick-win hardening, HDOs can proactively eliminate blind spots, maintain compliance, and strengthen their security posture—all with minimal resource consumption.

How is your healthcare cybersecurity offering unique in this space?

Healthcare is a prime target for cyber threats, yet traditional security approaches have relied heavily on vulnerability assessments and patching, leaving insecure configurations unaddressed. GYTPOL fills a critical gap by providing continuous security posture management across cloud, Windows, Linux, macOS, and server environments. Unlike conventional tools, GYTPOL enforces secure configurations dynamically, ensuring policies are correctly designed, implemented, and maintained without disruption. By automating configuration hardening at scale, healthcare organizations can rapidly mitigate risks, proactively defend against zero-days, and maintain compliance with minimal operational burden. GYTPOL empowers HDOs to close security gaps before they become breaches and before they impact patient care.

ID.me

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- **51%–75%**
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- **Payer/insurer**
- Post-acute care/home health/hospice
- **Standalone hospital**
- **Other**

How do you cater specifically to the needs of healthcare security and privacy?

ID.me is uniquely equipped to address healthcare security and privacy by providing secure, efficient, and compliant identity verification solutions. With a focus on fraud prevention, our platform ensures that only authorized users gain access to sensitive healthcare data, reducing the risk of data breaches. We leverage MFA, advanced identity proofing, and AI-driven fraud detection to maintain the integrity of patient and provider information. ID.me also enables seamless Kantara-certified. FedRAMP-approved, TEFCA-compliant interoperability, allowing healthcare organizations to exchange data securely and efficiently. By streamlining access, we reduce friction for patients while enhancing security for provider and payer organizations. Our solution is built to support compliance with HIPAA and other regulatory requirements, offering a trusted way to verify identities and protect patient privacy.

How is your healthcare cybersecurity offering unique in this space?

As one of the first identity providers certified by Kantara, the ID.me platform has over 141 million users, which equates to over 50% of the US adult population. Additionally, over 3 million healthcare providers leverage ID.me with a federated credential. The platform allows users to reduce friction when engaging in digital healthcare platforms, protect their identity, and share it only when and where they wish. For customer organizations, we provide not only compliant identity solutions but also a 24/7 US-based member support center. Customers can call that center and be helped by a live human agent, offloading help desk costs from our customer organizations. We also monitor fraud signals across our users, performing more fraud mitigation and network protection than an organization can do themselves. When fraudulent signals are detected anywhere on the network, we can lock that credential for the whole network, protecting ePHI, clinical systems, and security digital front door access.

Illumio

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Healthcare organizations have to balance the need to be open and accessible with the need to secure resources and patient data. This conflict makes designing a security system complex. The first and most simple use of Illumio is to fence the EHR to comply with regulations. The second is to identify potential risks within the infrastructure. If these risks are not fixed, they could provide a path for an attack to spread, ultimately causing a break in services. Illumio can mitigate risks by limiting access to the affected resources. The openness of public areas make it easy for a threat actor to gain access to a network. Attackers should not be able to move beyond what is authorized. But should an attack happen, Illumio can contain the attack, preventing it from reaching high-value assets that deliver primary medical services.

How is your healthcare cybersecurity offering unique in this space?

[Did not answer]

Imprivata

KLAS-Measured Offerings

Access Management
Patient Privacy Monitoring

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Imprivata delivers access management solutions that facilitate fast, simple, and secure access to all applications and information across every workflow—for every user and from any device. Imprivata's portfolio of solutions include SSO, passwordless MFA, EPCS, privileged access management (for both IT administrators as well as vendors and other third parties who need access), mobile and medical device security, advanced workflow analytics, patient privacy monitoring, and other access management capabilities. Together, these solutions enable healthcare delivery organizations to fully manage and secure all clinical, enterprise, and third-party digital identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

How is your healthcare cybersecurity offering unique in this space?

Imprivata solutions are purpose-built to help healthcare delivery organizations solve their unique and complex security, workflow, and compliance challenges. This includes providing fast, secure access for clinicians through deep integrations with EHRs and other clinical applications and workflows make authentication a seamless part of the task at hand. Imprivata offers the broadest set of authentication methods, providing flexibility to best meet user and workflow requirements, including using advanced passwordless approaches like FIDO and biometrics.

In addition, Imprivata provides unique user authentication capabilities for shared mobile devices, shared workstations, and connected medical devices, including by removing generic logins and enabling fast, secure access to applications on these shared devices.

Imprivata also leverages user access and workflow data to help organizations drive actionable insights and make informed, strategic security and operational decisions. This includes incorporating AI and ML as part of the strategy to continuously improve quality of the insights and to automate analysis to reduce the burden on IT staff.

In addition to technology solutions, Imprivata offers extensive services to ensure customer success. This includes an experienced team of nurses and physicians who help organizations optimize solutions to best meet clinical workflow specifications. It also includes managed services for day-to-day operations of Imprivata products to allow IT teams to focus on more strategic priorities.

Intraprise Health

KLAS-Measured Offerings

Security & Privacy Consulting Services

% of Unique Healthcare Cybersecurity Client Base That Is US Based

N/A

Current Client Base

N/A

How do you cater specifically to the needs of healthcare security and privacy?

Intraprise Health was formed in 2018 by combining the first healthcare HITRUST assessor with the world-class healthcare software development team that built the first HIE. Healthcare is all that Intraprise Health does. Our long-term healthcare expertise is critical to client success, as it requires deep knowledge of healthcare regulations, operations, and workflows to make decisions that enhance security without harming healthcare business. We have worked with organizations of all sizes and types, so we have knowledge that will apply to all participants in the industry. Lastly, combined with our security consultants, our automation software can address long-standing challenges faced by healthcare organizations with cost or resource constraints.

How is your healthcare cybersecurity offering unique in this space?

We are the only healthcare cybersecurity firm that offers automation software for third-party risk, HIPAA security, integrated risk management, NIST security as well as a complete range of consulting services that encompass V-CISO, HITRUST, NIST, HIPAA, 405(d) assessments, and other forms of security simulations and remediation. We can start anywhere in a client's security journey and fill in any part of their security portfolio. For organizations that have grown through M&A, our HIPAA One product dramatically shortens the SRA process. It also provides accurate tax ID statuses and the reporting required for MACRA/MIPS by automatically combining global parent security information with local security information. Many organizations are unable to do this work due to the manual effort. Our BluePrint Protect platform has a generative AI agent that reviews security data and evidence, which dramatically shortens the manual effort needed to manage large amounts of security data. Additionally, our platform effectively integrates all forms of risk data, including exceptions, to give security leaders a full picture of their risk program.

Intruno

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- **76%–99%**
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- Payer/insurer
- Post-acute care/home health/hospice
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Intruno addresses the unique demands of healthcare by offering AI-powered tools tailored for EHR systems. Our solutions detect and prevent privacy violations and data breaches using ML and unique digital fingerprints for real-time alerts to compliance, privacy, and security teams. With over five decades of healthcare expertise, our team understands the complexities of safeguarding sensitive patient data. Intruno aggregates data across platforms, enabling comprehensive monitoring without being tied to specific EHR systems. A quick implementation (30-45 days), a 7-year data retention policy with prebuilt migration tools, and customizable workflows ensure seamless integration into existing privacy programs. Features like rule-based alerts for high-risk activities, robust anomaly detection, and built-in investigations with detailed reporting streamline compliance and mitigate risks effectively.

How is your healthcare cybersecurity offering unique in this space?

Intruno's healthcare cybersecurity solutions stand out by combining advanced AI-driven privacy monitoring with unparalleled customization. Unlike competitors, we integrate data from diverse sources, offering centralized oversight for privacy teams. Our anomaly detection identifies deviations in user behavior, while preset alerts target specific healthcare risks, such as co-worker snooping or VIP record access. Our built-in investigation module simplifies the management of incidents with secure notifications and comprehensive reporting. Intruno also supports compliance with OCR audits, offering risk assessment tools and resources to align with regulations. Designed for rapid deployment and optimized workflows, Intruno empowers healthcare organizations to safeguard sensitive data efficiently.

LevelBlue

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

We serve as a trusted advisor who adopts a holistic approach to securing digital and business transformation. Our services are designed to make innovation faster and safer by addressing the unique security and privacy challenges faced by healthcare organizations. Our key services include:

- Cyber risk strategy: Tailored consulting for managing cyber risk and ensuring compliance
- Mobile devices: Unified endpoint management, mobile threat defense, and endpoint detection and response
- Network security: Managed edge appliances, including trusted access management services like SSE, SASE and SDWAN
- Cloud security: Assessments, application layer security, and threat detection and response for multi-cloud and SaaS environments
- Data security: Assistance with continuous compliance for HIPAA, HITRUST, and GDPR.
- DDoS & WAAP: Protection against DDoS and application/website attacks.
- Email & internet security: Managed email security, phishing defense, security awareness training and zero-trust network access for managing secure access to private/public applications and websites
- Firewall & microsegmentation: Managed next-generation firewall and FWaaS, paired with micro-segmentation

How is your healthcare cybersecurity offering unique in this space?

Our healthcare cybersecurity offering stands out due to our holistic approach and breadth of services to help organizations protect against top threats, ensure data protection and privacy, and maintain compliance. With a dedicated professional services and consulting team that has long advised major health and hospital systems, we tailor our services to the unique needs of individual customers. We focus on enabling digital transformation, including a zero-trust approach, while ensuring compliance.

ManageEngine

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- **76%–99%**
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- Payer/insurer
- **Post-acute care/home health/hospice**
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

ManageEngine AD360, an integrated IAM solution supports HIPAA and HITECH compliance by enforcing role-based access, multi-level approval workflows, automated provisioning and dormant account cleanup across EHRs and clinical systems. It leverages user behavior analytics, risk-based access control and identity threat detection to detect identity based threats and supports adaptive MFA and SSO to secure access to hospital, cloud, and remote apps—without disrupting clinical workflows. Self-service options for password resets and account unlocks reduce IT overhead while improving user experience for healthcare staff.

ManageEngine Log360, a unified SIEM solution protects ePHI through real-time monitoring of Active Directory, Exchange, and file servers. It detects ransomware, unauthorized access, and misconfigurations via ML-based anomaly detection and file integrity monitoring. It meets HIPAA log retention mandates and secures telehealth data via CASB and DLP tools.

ManageEngine Endpoint Central, a Unified Endpoint Management and Security solution supports diverse healthcare roles-nurses, physicians, telehealth professionals-by streamlining endpoint management and security. It enhances patient care workflows, prevents ransomware, strengthens facility security, ensures HIPAA compliance, supports EHR adoption, and helps meet HHS CPGs goals.

How is your healthcare cybersecurity offering unique in this space?

AD360 centralizes identity management enforcing security policies and compliance. It integrates with HRMS for automated user provisioning and real-time access adjustments across EHRs, scheduling platforms, and billing systems. Workflows ensure temporary, shift-based, and contract staff receive time-bound access without manual overhead. Granular delegation enables IT to restrict EHR and PACS access without escalating privileges. Built-in orchestration connects identity flows across pharmacy, telemedicine, and scheduling platforms. It has 150+ reports, ensuring quick response and compliance assurance.

Log360 combines SIEM, DLP, and CASB in a single console to protect hybrid healthcare environments—including on-prem IT and IoT medical devices. It uses ML-based anomaly detection and incident response workflows designed for ransomware, lateral movement, and privilege misuse—beneficial to hospital SOC teams.

Endpoint Central provides unified endpoint management and security for clinical workstations, shared devices, embedded PCs, barcode scanners, wearables, and more-all managed from a single console. Trusted by healthcare providers of all sizes, it streamlines infrastructure security.

Meditology Services

KLAS-Measured Offerings

Security & Privacy Consulting Services

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

We have conducted thousands of engagements for a wide variety of healthcare organizations, ranging from small, individual practices to large, complex national healthcare providers. Our staff includes prior CISOs and Chief Privacy Officers as well as directorate and other senior healthcare leaders. We have specialty services and assessments tailored to align with unique healthcare regulatory and business considerations above and beyond the standard approach to security, ensuring the balance between patient experience, safety, privacy, and business conditions can be met in a secure means.

How is your healthcare cybersecurity offering unique in this space?

Our subject matter expertise in the healthcare regulatory environment allows us to act as advisors on information security, privacy, and HIPAA compliance matters to the Office for Civil Rights (OCR), the U.S. Department of Health and Human Services (HHS), and the Office of the National Coordinator for Health Information Technology (ONC). We are an expert witness for the OCR, enabling a uniquely qualified perspective in the space to ensure clients are given the latest actionable insight and advisory guidance. Our firm is tailored to healthcare, and as one of the first dedicated security and privacy firms for the healthcare space, we have supported the largest names in healthcare alongside small municipal systems or independent hospitals. This broad spectrum of experiences and perspectives enables us to tailor our services and ultimately improve client outcomes.

MorganFranklin Consulting

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Our resources have technical security expertise, and some have been healthcare practitioners—increasing their understanding of the industry, the clinical and operational model, and the regulatory and compliance implications.

How is your healthcare cybersecurity offering unique in this space?

We don't have cookie-cutter offerings—we tailor our solutions to the problem that the specific client is experiencing. We have sat in the buyer seat before, and we understand the needs and expectations of our clients. Thus, we offer end-to-end solutions that support our clients holistically.

NCC Group

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- **51%–75%**
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- **Payer/insurer**
- **Post-acute care/home health/hospice**
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

At NCC Group, we bring deep healthcare experience to every engagement—rooted in regulatory expertise, real-time threat defense, and a partnership-first mindset. Our consultants work alongside providers, payers, and healthcare technology organizations to strengthen compliance with HIPAA, HITRUST, CMS, and state-specific mandates—while staying ahead of evolving privacy and security expectations.

We understand the urgency and complexity of healthcare environments, where uptime, trust, and patient safety are non-negotiable. Our work spans penetration testing for web, mobile, and APIs; risk assessments tailored to healthcare operations; HITRUST and HIPAA readiness; and third-party/vendor risk management—delivered with precision and urgency.

Whether you're preparing for an audit, responding to a breach, or securing devices across a distributed network, we tailor our approach to fit your infrastructure, workflows, and clinical goals.

We don't just consult—we execute. Our team integrates seamlessly into yours to deliver tangible, timely outcomes that support both security and care delivery. From hospital systems to ambulatory care, NCC Group helps healthcare organizations build cyber resilience with clarity and confidence.

How is your healthcare cybersecurity offering unique in this space?

NCC Group is a trusted cybersecurity partner for healthcare organizations seeking more than a check-the-box approach to risk. We offer an integrated suite of services—from compliance strategy and audit readiness to IoT risk reduction and 24x7 threat monitoring—led by experts fluent in HIPAA, HITRUST, CMS, and other healthcare-specific requirements.

What sets us apart is our hands-on, outcomes-driven approach. We don't stop at assessments—100% of our HITRUST clients have achieved HITRUST certification, thanks to our in-depth knowledge of the process and focused support every step of the way.

We embed ourselves into your team, offering practical guidance, rapid deployment, and clear communication—whether we're working with CISOs, compliance officers, or frontline IT staff. Our work aligns with the realities of healthcare delivery, helping organizations improve security without disrupting operations or patient care.

When you work with NCC Group, you get more than recommendations—you get results.

Netwrix

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Netwrix offers security solutions for data, identity and infrastructure regardless of the verticals. However, healthcare has consistently been one of the top performing market segments over the years. Netwrix provides guidance and mapping for industry and privacy regulatory requirements that help customers choose the right solutions for their security and compliance needs.

How is your healthcare cybersecurity offering unique in this space?

Netwrix is a vendor with the uniquely broad portfolio that covers multiple aspects of cybersecurity. This allows us to offer customers both end-to-end security solutions as well as separate products to adhere to the current priority.

Okta

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Okta helps leading healthcare organizations modernize and secure their digital identity across patients/members, providers, and partners in an integrated, easy-to-use way that mitigates risk, transforms user experience, and drives agility via both Okta and Auth0 platforms. With our products, Okta helps organizations take a modern, identity-based approach to kick-start their zero-trust journey. We seamlessly integrate identity solutions across entire tech ecosystems and partner with security leaders to unify approaches to zero trust. Beyond this, Okta and our partners offer a variety of services that can be delivered to enable delivery of security identity solutions.

How is your healthcare cybersecurity offering unique in this space?

Identity is the top attack vector, with healthcare being a prime target. As identity sprawl grows across the industry, detecting and protecting against these attacks is becoming increasingly critical. We enable the world's largest organizations to safely connect people to technology. Earning and keeping our customers' trust is at the heart of this effort. Okta's entire suite of products that sits on top of our orchestration layer was born and built in the cloud. This means our products are designed at their core to operate in a distributed, limited trust environment that healthcare is becoming. Our approach to identity offers the flexibility to offer secure services to a wide range of people in a wide range of scenarios. Our products are not inherently dependent upon existing identity infrastructure but rather enhance and integrate with legacy deployments with the modern zero-trust security that healthcare urgently needs. Three of our core pillars are Secure By Design, Always On—Resilience, and Built for Scale—which we demonstrate with initiatives such as the Okta Secure Identity Commitment and IPSIE.

OnDefend

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- **51%–75%**
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- Outpatient/ambulatory
- **Payer/insurer**
- Post-acute care/home health/hospice
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Healthcare organizations have implemented best-in-class threat detection tools and threat response solutions, but they don't have a way to continuously prove these investments are effectively protecting their company and providing a return on investment. Our Ransomware Defense Validation service, powered by our BlindSPOT breach and attack simulation system, provides a solution. We provide the following value:

- Operational assurance: Continuous testing ensures security controls are hardened against misconfigurations or changes and defenses are working, even as adversary threats evolve.
- Executive buy-in: Quantitative proof helps demonstrate ransomware readiness to executives and boards.
- Vendor accountability: Third-party vendors prove their performance against real-world threats and are held accountable to SLAs.
- Security ROI: Metrics-driven validation of current security investments justifies the budget and provides data to secure funding for additional resources.
- Proactive resilience: Gaps are identified before they can be exploited, moving from reactive to proactive security.

How is your healthcare cybersecurity offering unique in this space?

Ransomware Defense Validation is powered by our proprietary and patented BlindSPOT breach and attack simulation system. To our knowledge, we are the only vendor providing this managed service powered by our proprietary solution to the healthcare space.

Optiv

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

With former healthcare CISOs and more than 150 security consultants experienced in the healthcare industry on staff, Optiv is able to meet healthcare clients where they are in their cybersecurity journey and personalize their outcomes based on hands-on work, including client-side experience and expert guidance. Optiv's healthcare center of excellence is a collaborative team working across technologies and domains to bring to bear a unique, healthcare-specific perspective.

How is your healthcare cybersecurity offering unique in this space?

The top priority of healthcare and related industry organizations is ensuring the delivery of quality and safe patient care. Advancing medical technologies and the fast transfer of accurate information can improve outcomes and control costs, but only if medical devices and patient data are secure. That is where Optiv comes in. Our combination of technology partnerships and industry-leading advisory services will build a security program to secure an organization's environment so that they can focus on what matters: patients. Optiv melds advisory, deployment/integrative, and managed services around technologies, regulations, processes, and people and delivers them on a one-on-one basis to each individual healthcare client based on their desired outcomes.

Palo Alto Networks

KLAS-Measured Offerings

Healthcare IoT

% of Unique Healthcare Cybersecurity Client Base That Is US Based

N/A

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Palo Alto Networks is the largest global cybersecurity organization with $100+ billion in market capitalization and has a dedicated healthcare practice that includes architecture, engineering, incident response, support, sales, and marketing with industry experience across all healthcare sub verticals.

How is your healthcare cybersecurity offering unique in this space?

The combination of dedicated healthcare industry experience and complete product offerings across network, endpoint, security operations, identity, cloud, and incident response services positions Palo Alto Networks to help the largest and most complex healthcare organizations across the globe.

Ping Identity

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Ping Identity's healthcare cybersecurity solutions provide unified IAM, risk mitigation, and seamless integration to ensure security, privacy, and compliance. Ping Identity enables secure access to EHRs, portals, and third-party apps with decentralized identity, verification, and dynamic authorization while enforcing MFA, passwordless authentication, and zero-trust security.

Ping Identity offers a privacy and consent dashboard for data sharing and OAuth Scope, allowing users to manage access. End-to-end encryption, threat detection, and risk-based access controls protect sensitive data and prevent takeovers. Ping Identity supports FedRAMP High-authorized ICAM solutions for secure cloud, on-premises, and hybrid deployments.

With multimodal MFA and support for FIDO2, OAuth 2.0, SAML, SCIM, and LDAP/AD, Ping Identity delivers scalable identity management. A dedicated US healthcare team provides specialized security expertise.

How is your healthcare cybersecurity offering unique in this space?

Ping Identity's healthcare cybersecurity solutions provide enterprise-grade IAM with no-code orchestration, decentralized identity, AI-driven verification, and dynamic authorization. With deep investments in FHIR, SMART on FHIR, and EHR integrations, Ping Identity enables seamless identity synchronization and supports digital credentials for insurance, medical history, and licensure. Flexible deployment options let healthcare organizations modernize IAM at their own pace. Ping Identity ensures HIPAA, TEFCA, and zero-trust compliance with adaptive access, real-time threat detection, and multimodal MFA. FedRAMP High authorization and a dedicated US healthcare team provide expert support and compliance-ready solutions, making Ping Identity a trusted leader in digital health security.

Proofpoint

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

The company was a founding member of and a participant in the Cybersecurity Act of 2015 Section 405(d) Task Group, which works to enhance cybersecurity across healthcare with industry-led guidelines and practices. Proofpoint's Healthcare Customer Advisory Board plays a critical role in guiding the development of solutions such as Proofpoint Targeted Attack Protection (TAP) healthcare classifications, templates and modules for security awareness training, and the Healthcare Best Practices Technical Guide. Proofpoint pioneered the People-Centric Security Framework modeled on NIST standards, a comprehensive approach to protecting organizations. Proofpoint's Industry Solutions team regularly shares healthcare threat insights to help mitigate risks and respond to emerging threats. Proofpoint is an active member of prominent healthcare industry associations, including HIMSS and Health-ISAC. Additionally, Proofpoint has a dedicated healthcare sales and sales engineering workforce, focused on delivering solutions and support to healthcare organizations, ensuring that their specific security and compliance needs are met effectively.

How is your healthcare cybersecurity offering unique in this space?

Proofpoint Targeted Attack Protection (TAP) provides valuable insights into identifying and defending against attacks aimed at Very Attacked People (VAPs)—individuals or departments most at risk of becoming targets for cybercriminals. TAP allows healthcare organizations to pinpoint VAPs, enabling the organization to focus security efforts where needed most and improve defenses against email-based threats like credential phishing and business email compromise. By helping to identify high-risk users and tailoring defenses accordingly, TAP enables organizations to proactively protect sensitive patient data and reduce the overall risk of a security breach. There are 11 healthcare verticals in TAP to compare threat intelligence data, allowing users to see how their organization's threat landscape stacks up against others and providing an understanding of their security risks within their specific market segment. Healthcare modules and templates available in ZenGuide deliver specialized security awareness training designed to educate healthcare employees about the unique threats facing the industry, such as phishing attacks targeting medical staff or the misuse of patient data.

PwC

KLAS-Measured Offerings

Measured outside of cybersecurity

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- **26%–50%**
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- **Payer/insurer**
- **Post-acute care/home health/hospice**
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

We have 53 cybersecurity partners and over 410 practitioners aligned to support our healthcare payers and providers. In addition, there are thousands more that deliver technology and business transformational services specifically to this industry sector. Our group of about 500 healthcare cyber/privacy professionals is part of our broader cyber practice of over 7,000 practitioners. We leverage that breadth to bring a unique blend of specialized healthcare knowledge with the depth of specialization across the cybersecurity and privacy spectrum of focus areas. Although we deliver minimal software products as PwC branded, our joint business relationships and custom healthcare accelerators allow us to more quickly and sustainably implement and operate the technology of our partners. We also have unique and extensive relationships with our clients' C-suites and boards of directors, allowing us to embed business strategy into the work we deliver for CISOs, CIOs, and CPOs.

How is your healthcare cybersecurity offering unique in this space?

We have extensive experience in solving extremely complex cybersecurity problems for the largest organizations in the country. The majority of our time is spent with Fortune 500 and Fortune 100 organizations, often going through large transformations (e.g., payers building out their provider business, providers replacing EHRs or ERPs, payers replacing claims management systems, organizations moving from on-premises to the cloud, organizations responding to a breach or availability event). Additionally, much of our delivery is aligned to our sister platforms providing management and technology consulting for large organizational transformations (as outlined above). We bring a deep knowledge of cybersecurity and privacy coupled with expertise in our clients' business, strategy, obstacles, and technology landscape.

Additionally, we provide incident response and remediation services to some of the largest cybersecurity and privacy incidents in healthcare. This knowledge allows us to better inform the traditional consulting services we provide to our clients.

Radware

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- [x] 1%–25%
- [ ] 26%–50%
- [ ] 51%–75%
- [ ] 76%–99%
- [ ] 100%

Current Client Base

- [x] IDN/health system
- [ ] Outpatient/ambulatory
- [x] Payer/insurer
- [ ] Post-acute care/home health/hospice
- [x] Standalone hospital
- [ ] Other

How do you cater specifically to the needs of healthcare security and privacy?

Radware provides tailored cybersecurity solutions for healthcare institutions, focusing on service availability, data protection, and operational efficiency. Key features include:

- DDoS protection: Real-time detection and mitigation of DDoS attacks ensure healthcare networks remain accessible and resilient
- Data security: Protection against various attack vectors, including burst attacks and IoT botnets, helps prevent data breaches and ensures regulatory compliance
- Bot management: Prevents bots from scraping content, taking over accounts, and executing DoS attacks, thus safeguarding patient privacy and online portals
- Flexible deployment: Offers on-premises, cloud, and hybrid solutions, allowing healthcare institutions to choose the best fit for their needs

By addressing these areas, Radware helps healthcare providers protect patient data, ensure service availability, and maintain trust in a digital world.

How is your healthcare cybersecurity offering unique in this space?

Radware's healthcare cybersecurity solutions stand out due to their comprehensive approach to protecting sensitive patient data and ensuring the availability of critical services. Unique features include:

- Advanced DDoS protection: Radware offers real-time detection and mitigation of DDoS attacks, ensuring healthcare networks remain resilient and accessible. Our machine-learning algorithms minimize false positives by accurately distinguishing between legitimate and attack traffic.
- Multilayered security: Radware's solutions protect against various attack vectors, including burst attacks, dynamic IP attacks, SSL floods, and IoT botnets. This multilayered approach ensures robust protection for healthcare data and applications.
- Bot management: Radware prevents malicious bots from scraping healthcare content, taking over user accounts, and executing DoS attacks. This is crucial for maintaining patient privacy and the security of online patient portals.
- Flexible deployment options: Radware offers on-premises, cloud, and hybrid solutions. This flexibility allows healthcare institutions to choose the best fit for their specific needs and infrastructure
- Compliance and trust: Radware's solutions help healthcare providers comply with regulatory requirements and maintain patient trust by safeguarding sensitive data and ensuring uninterrupted access to medical services.

By addressing these critical areas, Radware's cybersecurity offerings uniquely cater to the evolving needs of healthcare institutions in a digital world.

Rubrik

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Healthcare faces constant cyber threats. Rubrik provides full cyber resilience with the ability to rapidly recover all critical data to a clean restore point, regardless of where an organization's applications run, while proactively surfacing cyberthreats to minimize future impacts. Rubrik DSPM discovers and classifies sensitive data (PII, PHI, PCI) across on-premises, cloud, and SaaS environments. This helps organizations document data locations and permissions for HIPAA and PCI-DSS compliance. Key features include customizable policy templates and automated violation alerts that strengthen security and protect patient information. Healthcare organizations benefit significantly from implementation. For example, California Department of State Hospitals recovered 160 days of productivity, while St. Luke's Health System achieved 73% cost savings over three years. Rubrik delivers both enhanced security and operational efficiency, providing the visibility, classification capabilities, and access controls healthcare organizations need to maintain regulatory compliance while improving productivity.

How is your healthcare cybersecurity offering unique in this space?

Rubrik automates protection for healthcare IT systems, including Epic, MEDITECH, Oracle Health, PACS imaging, and NAS data. Our Data Security Posture Management (DSPM) discovers and classifies sensitive information (PII/PHI/PCI), documenting data location and permissions to support HIPAA/GDPR compliance. As the only enterprise solution with a true single-pane SaaS-based control plane, Rubrik offers workload-agnostic backup across on-premises, cloud, and SaaS environments. Our purpose-built architecture reduces administrative overhead by 90%.

Rubrik's native immutability ensures resilience without additional firewalls and extra equipment to protect the backup data. Rubrik identifies compromise indicators within backups without exposing data to third-party scanners, accelerating investigation while reducing recovery time and reinfection risk. Our unique ability to instantly scan backups and perform threat hunts for hash values, YARA rules, and file pattern IOCs ensures organizations can reliably find clean restore points. Additionally, Orchestrated Recovery automates recovery of complex applications, speeding recovery after attacks and minimizing operational disruption.

SailPoint

KLAS-Measured Offerings

Identity Management

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- **26%–50%**
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- **Payer/insurer**
- **Post-acute care/home health/hospice**
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Hospitals and healthcare organizations are struggling to quickly enable their staff while securing against targeted cyberattacks. Organizations need to find ways to reduce their risk and simplify meeting complex compliance requirements. Healthcare identity management is no small task and cannot be handled through manual processes. Healthcare is uniquely challenged with securing individuals with one-to-many roles with multiple authoritative sources within complex user populations. However, healthcare organizations can increase their security posture and gain operational efficiencies through AI-driven identity security:

- Assign only the right level of access
- Prevent friction between clinicians and IT security staff
- Reduce IT burden managing manual tasks
- Simplify audit readiness and easily demonstrate compliance

How is your healthcare cybersecurity offering unique in this space?

SailPoint is the largest free-standing identity security solution provider who has a dedicated healthcare vertical. Over the past 14 years, SailPoint has invested in building our platform to align with some of the most important and complex uses cases required by healthcare providers and payer organizations. In addition, SailPoint has invested in building direct clinical integrations between our identity platform and leading applications to include Epic, Oracle Health, and MEDITECH. SailPoint's committed focus has enabled healthcare organizations to more effectively manage the access for employed and contracted clinical staff, granting staff day-one access so that they can focus on providing patient care. Processes that were once manual, burdensome, and the root cause of delays are now secured, automated, and enhancing the ability of clinical staff to rapidly care for patients.

SANS Institute

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- **76%–99%**
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- **Payer/insurer**
- Post-acute care/home health/hospice
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

SANS Institute provides a broad spectrum of cybersecurity and leadership courses that cater to all critical cybersecurity needs. SANS approaches training with a two-pronged approach; theory & hands-on keyboard practice. SANS offers many types of trainings, from deep dives and technical courses to executive-level simulations. With the unique challenges that healthcare practitioners face, SANS offers a healthcare-focused cyber solution to safely practice threat simulations and real-world cybersecurity scenarios, such as preventing ransomware, EHR theft, or medical device tampering.

How is your healthcare cybersecurity offering unique in this space?

At SANS, we partner closely with healthcare organizations to deliver cybersecurity training that is not only comprehensive but also purpose-built for your unique environment. From frontline staff to technical teams, we assess your current capabilities and design customized learning paths that close skill gaps and build resilience.

In today's healthcare landscape—where patient safety, regulatory compliance, and data integrity are constantly under threat—a well-trained workforce is your strongest line of defense. Our mission is to help you cultivate a security-first culture—one where every employee plays a role in protecting sensitive information and critical systems.

Organizations that embed security into their operational DNA don't just reduce risk—they gain the confidence to innovate, scale, and serve patients without compromise.

SecureAuth

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

In today's landscape, healthcare organizations face escalating cyber threats. Over 82% of ransomware attacks now target companies with fewer than 1,000 employees, and 80% of hacking incidents involve stolen credentials—yet only 20% of small businesses use multi-factor authentication (MFA).

Identity and access management is critical, but many security solutions disrupt productivity. Healthcare organizations report that 20%–50% of help desk tickets relate to access issues. SecureAuth eliminates friction by pioneering risk-based authentication, using over 20 identity signals to ensure security while maintaining seamless access.

Our continuous facial authentication ensures system access only when the registered user is present. In fast-paced healthcare settings, doctors can securely access patient records while moving between rooms, and sessions lock automatically when they step away. Patients also benefit from frictionless access to their medical records, with confidence that their sensitive data remains protected from unauthorized users.

How is your healthcare cybersecurity offering unique in this space?

SecureAuth delivers a healthcare-specific approach to identity security by balancing frictionless access with advanced protection:

- Seamless access: Healthcare professionals frequently move between patient rooms and need instant access to records. Continuous facial authentication ensures system access remains active only while the authorized user is present—eliminating unnecessary logins while maintaining security.
- Risk-based authentication: Using 20+ behavioral and contextual signals, we dynamically assess identity risks, minimizing unauthorized access while reducing friction for verified users.
- Patient confidence in data security: Patients require secure, easy access to their medical records. We simplify authentication, ensuring protected access while maintaining compliance with privacy regulations.
- Tailored for healthcare's unique challenges: These critical industry needs are addressed—quick access, stringent compliance, and high-risk data security—all without slowing down care delivery.

By providing adaptive security that keeps systems protected without disrupting workflows, we empower providers to focus on patient care while safeguarding sensitive information.

Security Compliance Associates

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Expert knowledge of HIPAA, HITRUST, and healthcare security challenges to all size healthcare organizations. We understand our clients' needs and limitations and work with a hands-on approach to ensure they are compliant with state and federal regulatory requirements, as well as the evolving cyber threat environments. Our team provides expert guidance and clear, thorough reporting to identify the current cybersecurity posture and a road map to enhance that posture, with prioritized recommendations.

How is your healthcare cybersecurity offering unique in this space?

- Our offerings are customized to each individual client's environment, delivered in a humanistic manner by highly skilled professionals
- Clear and concise communication throughout our relationship
- Guaranteed compliance if our recommendations are followed
- We are focused on client satisfaction and helping organizations deal with the evolving cyber threat and regulatory landscape

Splunk

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

N/A

Current Client Base

N/A

How do you cater specifically to the needs of healthcare security and privacy?

Splunk Observability is a combination of two integrated products, Splunk Platform and Splunk Observability Cloud. Splunk Enterprise, with Splunk IT Service Intelligence (ITSI) built in, provides comprehensive log analytics and management, centralized event correlation for alert noise reduction, and high-level business service monitoring to achieve AIOps. Splunk Observability Cloud is a unified, integrated product that seamlessly uses any log data that is available on Splunk Enterprise, together with metrics and trace data, and provides DevOps teams with capabilities such as application performance monitoring, infrastructure monitoring, network monitoring, real user monitoring, synthetic monitoring, point-and-click log analysis, and incident response. These capabilities can also be purchased à la carte. Splunk Enterprise can be consumed through a SaaS model (Splunk partners with several cloud providers and does not maintain any private network) or through an on-premises deployment. Splunk Observability Cloud is available through a SaaS model only.

How is your healthcare cybersecurity offering unique in this space?

Splunk Observability provides full-stack visibility and awareness across infrastructure, applications, and business services to improve customer experience, innovate faster, and run services with greater scale and efficiency. Whether an organization is cloud-native, on-premises, or anywhere in between, Splunk Observability cuts through silos of data—no matter the scale or complexity—and delivers real-time, context-rich insights to IT operations, SREs, and application developers so they can answer any question about the performance and reliability of their applications and infrastructure. With this insight, companies can build better experiences, deploy more than 8x more frequently and with greater confidence, and accelerate mean times to detect, investigate, and remediate service interruptions by up to 90%.

ThreatLocker

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- **26%–50%**
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- **IDN/health system**
- **Outpatient/ambulatory**
- **Payer/insurer**
- **Post-acute care/home health/hospice**
- **Standalone hospital**
- Other

How do you cater specifically to the needs of healthcare security and privacy?

ThreatLocker addresses the unique security and privacy needs of the healthcare industry by providing robust solutions tailored to protect sensitive patient data and ensure compliance with regulations like HIPAA. The platform offers application whitelisting, which prevents unauthorized applications from running, significantly reducing the risk of ransomware and malware attacks. Additionally, ThreatLocker's storage control secures access to critical data by blocking unauthorized devices and controlling file transfers, safeguarding EHRs.

Granular policies allow healthcare organizations to enforce least privilege access, ensuring that staff can only access the tools and information necessary for their roles, minimizing potential breaches. Real-time auditing and reporting provide visibility into all system activities, making compliance management and incident response efficient.

By focusing on proactive security measures and reducing attack surfaces, ThreatLocker ensures healthcare providers can protect patient data, maintain operational continuity, and meet stringent regulatory requirements.

How is your healthcare cybersecurity offering unique in this space?

What sets ThreatLocker apart is its ease of implementation and management. The centralized platform provides real-time visibility and auditing, empowering IT teams to monitor and respond swiftly to potential risks without disrupting critical healthcare workflows. Our cybersecurity offering also stands out by delivering a proactive, zero-trust approach to endpoint protection, uniquely designed to address the sector's critical needs. Unlike traditional solutions that rely on reactive threat detection, ThreatLocker employs application white-listing, Ringfencing, and storage control to block unauthorized applications and malicious behaviors before they are executed.

ThreatLocker's granular policy controls enable healthcare organizations to enforce least privilege access, ensuring that only approved applications and users can interact with sensitive systems and data. This level of control significantly reduces the risk of breaches, ransomware, and insider threats, which are especially critical for protecting EHRs and maintaining compliance with regulations like HIPAA.

Trustwave

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Trustwave's consulting services enhance cloud, network, and endpoint security while ensuring regulatory compliance. Our cyber advisory team helps healthcare organizations prioritize risks, maintain compliance, and leverage forensics with 24/7 threat detection for rapid breach response and recovery.

Trustwave offers virtual CISO (vCISO) services, providing strategic security leadership, policy development, and risk management. Tabletop exercises help organizations test and refine incident response plans. By utilizing expert-driven security solutions, healthcare organizations can reduce complexity, safeguard patient data, and confidently meet HIPAA and other security requirements.

Trustwave's managed security services deliver 24/7 threat monitoring, detection, and response, ensuring continuous protection for critical assets in hybrid healthcare environments. Additionally, Trustwave's DFIR provides proactive incident response readiness and emergency breach response to major incidents like ransomware. These services help healthcare organizations mitigate risks through forensic analysis, evidence chain of custody for litigation support, board and C-suite reporting, and structured recovery efforts.

How is your healthcare cybersecurity offering unique in this space?

We differentiate with our vendor-independent approach, deep industry expertise, and integrated security solutions. Leveraging best-of-breed and best-of-platform technologies, we implement gold-standard configurations and a global security operations infrastructure for robust protection.

Our cyber advisory team strengthens security programs with risk management, compliance support, and vCISO services, ensuring alignment with HIPAA, HITRUST, and other regulations. With our co-managed security operations model, expert advisors provide continuous optimization and strategic guidance for long-term resilience.

Our SpiderLabs delivers global threat intel, offensive security, and forensic analysis, equipping healthcare organizations with proactive threat detection and rapid breach response. We enhance security readiness through tabletop exercises, incident response planning, and 24/7 managed detection and response. A seamless onboarding and transition process accelerates time to value, reducing risks when adopting new technologies or switching providers. By integrating proactive security operations, expert advisory services, and advanced threat intel, we help minimize risk, strengthen resilience, and safeguard data.

tw-Security

KLAS-Measured Offerings

Security & Privacy Consulting Services

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

tw-Security provides information security and privacy advisory services exclusively to the healthcare industry. Our customer base spans small rural clinics and critical access hospitals to very large academic medical centers. We understand how to scale services based on a customer's size. We frequently work with numerous legal firms having security and privacy specialties, whose clients need our services.

How is your healthcare cybersecurity offering unique in this space?

tw-Security only employs senior-level consultants; no junior consultants are on staff. All consultants have held roles or currently serve in the role of CISO, privacy officer, or compliance officer in the healthcare industry. We also have consultants with higher education experience, who are well-versed in academic medical environments. Business associates engage tw-Security to assist with their security and privacy programs and help meet their customers' expectations.

Varonis

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

N/A

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Varonis secures PHI by automatically identifying and classifying PHI across cloud and on-premises data stores and limiting who can access it. We can implement access changes automatically without interrupting day-to-day operations. Varonis helps customers achieve HIPAA compliance through monitoring how PHI is accessed or shared to ensure confidentiality, prevent unauthorized access, and protect against cyberthreats. A full audit log of data activity helps satisfy auditors and meet breach notification requirements. Varonis automatically detects early signs of ransomware with behavior-based threat models. Alerts can trigger automated responses, like ending affected users' sessions or changing passwords, to stop an attack in its tracks. Varonis helps customers lock down sensitive data, right-size permissions, and monitor prompts to safely deploy AI copilots. We limit sensitive data access, monitor Copilot prompts, and detect abuse in real-time.

How is your healthcare cybersecurity offering unique in this space?

Varonis data discovery and classification scans for and classifies sensitive data, such as HIPAA-regulated data and PHI, across cloud and on-premises data stores. The Varonis data security platform continuously monitors data, creating a detailed audit trail of data activity that captures every action on data. The platform enforces automated least privilege access and uses behavior-based threat models to detect early signs of ransomware. Automated remediations can be triggered to stop an attack, such as ending affected users' sessions or changing passwords. Varonis offers a classification library with expert-built patterns spanning global compliance regulations. Out-of-the-box and customizable reports enable customers to easily share compliance reports with auditors and compliance officers to meet regulatory requirements. Our posture dashboard maps an organization's current app configurations against common compliance standards, such as HIPAA. We also offer a managed data detection (MDR) service that combines our threat detection technology with our team of elite threat hunters, forensics analysts, and incident responders who triage, investigate, and respond to alerts.

Veeam

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Veeam protects over 18,000 healthcare organizations worldwide. From patient data protection to compliance, we ensure healthcare data is secure, resilient, and recoverable from threats like ransomware. Solutions that cater to the needs of healthcare organizations include:

- Regulatory compliance support: RPO and RTO dashboard, automated DR documentation, and zero-impact tests
- Ransomware defense: Encrypted and immutable backups, cyber incident response, AI driven analytics, and proactive threat assessment
- EHR system coverage: Epic-validated fast backup of cache and agentless backups
- M&A support: Data migration, failover, and segmentation
- Cost-efficient backups for unstructured data: SMB, NFS, Windows, and Linux file shares

How is your healthcare cybersecurity offering unique in this space?

The Veeam Cyber Secure program is an elite offering that provides architectural design and implementation services, along with onboarding services before an incident, the best incident response services (via Coveware by Veeam), and robust recovery solutions to ensure resilience against cyber threats to healthcare organizations.

Zscaler

KLAS-Measured Offerings

N/A

% of Unique Healthcare Cybersecurity Client Base That Is US Based

- 1%–25%
- 26%–50%
- 51%–75%
- 76%–99%
- 100%

Current Client Base

- IDN/health system
- Outpatient/ambulatory
- Payer/insurer
- Post-acute care/home health/hospice
- Standalone hospital
- Other

How do you cater specifically to the needs of healthcare security and privacy?

Zscaler addresses the unique security and privacy challenges of healthcare organizations, protecting providers, payers, pharmaceutical companies, and medical device manufacturers. We ensure secure, compliant access to critical systems and sensitive patient data while meeting stringent regulations like HIPAA and defending against threats such as ransomware and breaches.

As healthcare digitizes, Zscaler simplifies security by replacing outdated, hardware-based solutions with a cloud-delivered zero-trust model. This reduces the attack surface, secures workflows like EHR access, and ensures reliable telehealth and cloud app performance. As the only certified cybersecurity partner for Imprivata, Zscaler integrates seamless authentication and access controls to enable secure clinician workflows without sacrificing efficiency.

Zscaler helps healthcare organizations do more with less by simplifying infrastructure, lowering costs, and reducing operational overhead. Teams spend less time managing security and more time on patient care. Our platform enables healthcare providers to protect critical assets, modernize IT, and build a scalable, secure foundation for digital transformation.

How is your healthcare cybersecurity offering unique in this space?

Zscaler's healthcare solutions stand out with a cloud-native approach that redefines security for highly regulated and fragmented environments. Unlike traditional static perimeter defenses, Zscaler's Zero Trust Exchange enables secure, identity-based access to EHRs, cloud apps, and telehealth platforms without exposing networks to threats.

Our solutions are tailored to the healthcare ecosystem, supporting providers, payers, pharmaceutical companies, and medical device manufacturers. A key differentiator is our partnership with Imprivata, where Zscaler is the only certified cybersecurity partner, delivering seamless integrations to secure authentication workflows while preserving clinician productivity.

Zscaler modernizes IT while driving cost efficiency. We replace legacy hardware with a cloud-delivered model that reduces complexity and operational overhead while improving security. We also support digital innovation on a large scale by securing IoT devices, telemedicine, and cloud collaboration tools. By combining security, simplicity, and innovation, Zscaler enables healthcare organizations to reduce cyber risk, lower costs, and embrace digital transformation without compromise.