datavant

Secure by Design

At Datavant, we're on a mission to make the world's health data secure, accessible and actionable.

Our scale and impact

1T+
records tokenized and linked annually

100M+
patient records processed annually

1500TB+
data annually exchanged

Trusted by
20 of the top 20
life sciences companies

Largest ecosystem of
350+
real-world data partners

Integration with
80K+
Hospitals and clinics through the largest health data retrieval network

Who we serve

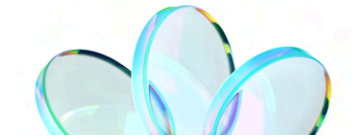
We provide solutions across key healthcare sectors:

Payer

Unlocking health plan operational innovation

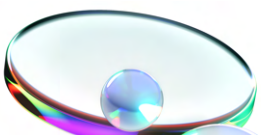
Provider

Activating data to power health delivery and outcomes



Life Sciences

Accelerating evidence for development, launch & safety



Legal & Insurace

Simplifying exchange and insights for providers and requesters

Our security commitment

Security is foundational to every Datavant offering. We align to industry-leading frameworks and certifications—including HIPAA, HITRUST, NIST, and FedRAMP—and operate under a rigorous security risk management process spanning all business units.

Datavant © Copyright 2025. All rights reserved.

Navigating Healthcare Cybersecurity

The evolving threat landscape.

Cyberattacks in healthcare are becoming more frequent and complex.

0101
0010
1010

Increasingly sophisticated phishing and multi-factor authentication bypass attacks

Malware that evades traditional endpoint tools

Supply chain vulnerabilities arising from third-party vendors and partners

Ransomware campaigns are increasingly targeting the healthcare sector

These threats are compounded by skills challenges related to cybersecurity workforce development and retention.

What's at stake?

These risks threaten more than just operations; a breach can lead to:

Erosion of trust

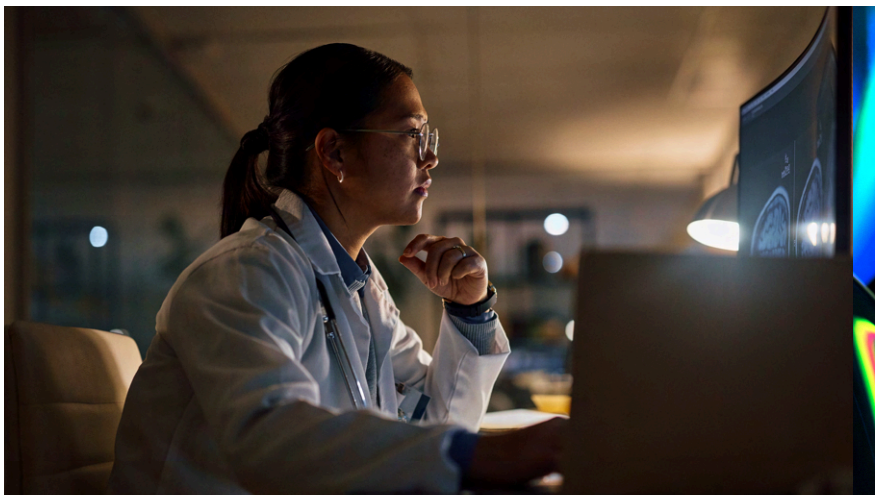
patients and partners may lose confidence in data handling practices

Compliance violations

non-adherence to regulations like HIPAA can result in sanctions

Financial Losses

costs associated with breach mitigation and legal penalties



An advanced security approach

Implementing advanced security measures is imperative to protect sensitive health information and maintain compliance. That's why we've doubled down on security investments to outpace the evolving threat landscape.

Datavant © Copyright 2025. All rights reserved.

Our Approach to Security Governance and Leadership

Security, privacy, and compliance—better together

Datavant's Information Security Program is tightly integrated with our Privacy and Compliance teams to ensure robust security standards, comprehensive risk management strategies, and consistent enforcement of policy and controls.

Business-integrated security

We leverage a Business Information Security Officer (BISO) model. Dedicated BISOs bring security leadership to each business vertical, improving risk management and customer-specific support.

Metrics-driven oversight

Our data-driven approach to security means we track and review key performance indicators (KPIs) and risk metrics to monitor controls, identify risks early, and guide remediation—ensuring clear oversight and accountability across teams.

Aligned with frameworks and standards

Datavant's security program is aligned with leading industry frameworks, including the NIST Cybersecurity Framework (CSF). This ensures our controls, processes, and risk management practices meet recognized standards and support regulatory, customer, and audit expectations.

Board-level reporting and engagement

Security and risk are regularly reviewed by executives and the board, with updates on key risks, controls, regulations, and program maturity to ensure alignment with business objectives and risk oversight.

Strong leadership and risk ownership

Our leadership team is committed to proactively managing risks through dedicated expertise and continuous improvement of security practices.

Datavant © Copyright 2025. All rights reserved.

Built to Defend — Our Security Measures in Action

Protect

Continuous configuration and vulnerability scanning

Cloud security posture management tools continuously monitor cloud environments for misconfigurations, vulnerabilities, and compliance gaps. This allows for real-time detection and rapid remediation of risks in our cloud infrastructure.

Penetration testing and dynamic application security testing

Regular internal and external reviews and tests help to identify vulnerabilities in external-facing and internal applications. Findings are quickly addressed and used to inform ongoing improvements in our security posture.

Secure access management

Our organization-wide enforcement of FIDO2.0 phish-resistant MFA strengthens secure access management.

Detect

24/7 threat monitoring

We've operationalized continuous threat monitoring to promptly detect and respond to potential threats.

Internet traffic governance

Our suite of perimeter and agent-based tools enhances internet traffic governance and strengthens web security.

Data loss prevention

We use next modern DLP tooling to monitor and protect sensitive data across endpoints, cloud services, and collaboration tools. DLP policies are enforced to detect unauthorized data movement and prevent accidental or malicious data leakage.

Respond

Email protection

We've enhanced our email security with stronger encryption and modernized detection capabilities.

Identity access management

We've implemented additional access reviews and termination improvement processes, as well as controls to proactively monitor leave of absence and inactive employees.

Security training

All users undergo improved phish training, including social engineering exercises, supplemented by continuous security communications.

Datavant © Copyright 2025. All rights reserved.

SECURE BY DESIGN

Built by Experts

Security isn't just a department at Datavant, it's a shared culture we cultivate across every team.

Meet our team

A multidisciplinary group of security architects, engineers and practitioners, driving innovation in healthcare data security.

Secure Product and Infrastructure

Proactively uncovering blind spots before they impact customers or patients. Partnering with engineering teams to build more secure software and systems using modern approaches.

Cloud-Native Security

Embedding security into every layer of cloud-native architectures. Collaborating with engineering, platform and infratructure teams to design, deploy, and operate resilient, scalable, and secure workloads from the ground up.

Attack Surface Management

Continuously mapping, monitoring, and reducing the organization's exposure. Leveraging detection engineering and rapid response to identify and neutralize threats before they escalate.

Identity and Access Management

Building automated, scalable IAM systems that enforce least privilege, streamline provisioning, and ensure secure, frictionless access for users, applications, and services.

Governance, Risk and Compliance

Modernizing compliance by automating controls, streamlining audits, and scaling governance frameworks. Partnering with stakeholders to ensure security and privacy requirements are met without slowing innovation.

End User Security

Protecting what matters most: Datavant's people. Our team designs and operates security measures across devices, email, and software, ensuring strong defenses and secure configurations at every level.

"Building a strong team is fundamental to any security capability. My job is to ensure the team is empowered and spending their time solving tough security problems."

– Dan Walsh, CISO

Datavant © Copyright 2025. All rights reserved.

Security Lifecycle Confidence

Secure-by-design architecture

1. Security is built into every layer of Datavant's products from the ground up.
2. The platform is architected with privacy by default: tokenization replaces personal identifiers with unique, irreversible encrypted tokens, ensuring sensitive data is never exposed in plain text.
3. Our technology ensures privacy by design: de-identified systems enable data linkage without raw PII exchange, while identified systems support secure, compliant sharing of sensitive data with strong protections. Together, they help you minimize risk exposure and enforce strong governance standards.

Verification and testing

1. Our security program uses layered verification and testing to ensure systems, applications, and processes remain resilient against evolving threats. Regular internal and external reviews and tests uncover vulnerabilities in both external-facing and internal applications, with findings promptly remediated and leveraged to strengthen our overall security posture.
2. We conduct continuous vulnerability scanning, configuration audits, code reviews, and automated static and dynamic analysis to identify risks early in the development lifecycle. These efforts are supported by ongoing security monitoring, incident and simulations.

Independent certifications and audits

Our dedication to information security excellence is reflected in the multiple independent certifications and accreditations we've earned.

FedRAMP · SOC 2 TYPE 2 · ISO 27001 · AICPA SOC · HITRUST

Customer assurance information is available via https://trust.datavant.com

Datavant © Copyright 2025. All rights reserved.

datavant