INDUSTRY GUIDE

AWS + Illumio: Helping Healthcare Modernize Their Cyberattack Response

Healthcare organizations must update their cybersecurity strategies to stop the spread of inevitable breaches and ransomware attacks.

Healthcare has become a prime target for cybercriminals

#1

The healthcare industry is the top target for cyberattacks.

$10M

The average cost of a healthcare data breach in 2023 is $10.93 million, nearly $7 million more than other industries.

231 DAYS

Healthcare data breaches tend to last 231 days before they're discovered, almost a month longer than other industries.

Ransomware attacks and data theft have risen to record levels, resulting in billions of dollars in losses, impacting quality of care, and potentially creating life-or-death scenarios.

The increasingly hyperconnected healthcare landscape has become a prime target for cybercriminals. The risks to healthcare organizations continue to broaden as providers expand cloud systems, Internet of Medical Things (IoMT) devices, integrated patient care systems, wireless networks, and remote personnel.

Such a diverse and hyperconnected environment is precisely what cybercriminals exploit to infiltrate a healthcare organization's and medical device networks. A shift to remote access for some employees during the last few years has opened even more pathways to mission-critical systems and data.

As it is, most healthcare providers have insufficient visibility into their IT network, and even less visibility into their growing inventory of IoMT and operational technology (OT) devices — including how those systems interact with one another.

Chief information security officers (CISOs) and other executives in healthcare are acutely aware of cybercrime threats such as ransomware. So are governments. Most governments around the world name healthcare as part of national critical infrastructure that, if incapacitated, could have devastating consequences. As a consequence, most regulators enforce specific legislation governing cybersecurity in this sector.

Guarding against ransomware and other attack vectors has become more than just a cybersecurity problem — it's now a business resilience challenge at the highest levels of a healthcare provider.

In this guide, we will explore the unique cybersecurity challenges facing healthcare providers and how securing your organization by integrating Illumio and AWS can provide an invaluable defense that protects both healthcare systems and patients across a rapidly changing landscape.

The top 7 cybersecurity challenges for healthcare

#1 Data breaches

Healthcare organizations are attractive targets. Cybercriminals exploit vulnerabilities and gain unauthorized access to data.

#2 Data sharing and interoperability

Secure data sharing, interoperability, and privacy is a significant challenge.

#3 Disaster recovery

Breaches can disrupt operations, compromise patient care, and expose sensitive data, costing healthcare organizations a significant amount of time and money to remediate.

#4 Insider threats

Employees, contractors, or third-party service providers who have authorized access to patient data may intentionally or inadvertently misuse or disclose sensitive information, leading to privacy breaches.

#5 Regulatory compliance

Ensuring compliance with regulations can be complex and challenging.

#6 Medical device security

The proliferation of network-connected medical devices introduces new security risks.

#7 Legacy systems and infrastructure

Existing technology often has security vulnerabilities or lacks up-to-date security measures.

INDUSTRY GUIDE

How Illumio + AWS helps protect against top healthcare security challenges

Data breaches

A data breach should not compromise a healthcare organization's ability to maintain services. Illumio will contain an attack and prevent it reaching critical systems that could compromise safety.

Data sharing and interoperability

AWS cloud services are HIPAA-ready and HITRUST compliant. They provide encryption at rest and in transit capabilities and enable secure and private data sharing.

Disaster recovery

Containing and securely recovering from an incident is key to cyber resilience. With Illumio, security teams can dynamically change security rules based on status, allowing them to create clean and dirty bubbles to migrate safe systems back into full service while quarantining infected systems until they are safe.

Insider threats

A healthcare organization is, by necessity, a very open environment. It needs to be accessed not only by patients and their relatives but by many suppliers, contractors, and service providers. Many of these will require access to the healthcare organization network, creating a potential danger of attack from the inside.

It's vital to be able to separate the traffic based on the requirements of each group. Trying to do this with traditional network-based models is often complex and very static. Using Illumio to segment at the individual asset creates a much more agile and secure model that can react to the needs of each individual group.

Regulatory compliance

Globally, healthcare organizations can come under critical infrastructure, medical, and privacy regulations.

The common aspect of each of these is the need to be able to separate data and systems from each other to protect each environment. Illumio is used by healthcare organizations and providers around the world to protect data, assets, applications, and systems, allowing them to comply with regulations.

Medical device security

Any medical device that is connected to the network is at risk of compromise. Security teams can use Illumio to follow some simple protective steps:

1. Map the data flows between all devices to understand what should and should not be communicating.
2. Put in place some simple rules to prevent the movement of ransomware from the IT to OT environment.
3. Create a Zero Trust approach to access based on only allowing verified and approved communication.

Legacy systems and infrastructure

Trying to keep the patch levels of systems up to date is a never-ending task. This is especially true of systems that have gone end-of-support and are not able to be patched. Organizations must be able to mitigate the threat posed to systems that may carry a vulnerability. By understanding the exposure of each system and applying compensating rules, Illumio can protect those systems until they can be patched or upgraded.

Start securing your healthcare organization

Contact Illumio today
illumio.com/contact

About Illumio

illumio

Illumio, the Zero Trust Segmentation Company, stops breaches from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.