illumio

INDUSTRY BRIEF

Securing Healthcare Organizations

Contain ransomware and malware to continue to deliver services during a cyberattack

Healthcare: A prime target for cybercriminals

Ransomware attacks have risen to record levels in the healthcare industry, resulting in billions of dollars in losses and threatening the quality of care.

The increasingly hyperconnected healthcare digital landscape has become a prime target for cybercriminals. As healthcare organizations expand their networks with cloud systems, including Internet of Medical Things (IoMT) devices and new digital record (EHR) systems, they increase their cyber exposure.

Cybercriminals only need to find one open door to infiltrate an entire network of IT, OT, and IoT systems.

And a huge surge in telemedicine and remote work during the pandemic has opened even more pathways of attack for bad actors looking to cause harm to healthcare organizations.

The threats are increasingly great, and healthcare cyber resilience has become a strategic issue.

Cyberattacks on healthcare have soared in recent years. For example, hacking and IT incidents more than tripled from 2017 to 2021, reaching a record high of 528, according to HIPAA Journal's analysis of data breach statistics from the U.S. Department of Health and Human Services' Office for Civil Rights.

More than two-thirds (67%) of healthcare cybersecurity professionals say their organizations experienced "significant security incidents" in the preceding 12 months, according to the 2021 HIMSS Healthcare Cybersecurity Survey.

Security Challenges Facing Healthcare

The growth in digital technology to improve healthcare services has also increased the cyber risks for healthcare providers.

The integration of medical systems
Including the connectivity to EHR applications is creating new attack vectors and pathways for the spread of malware.

Legacy technology
This can be unsupported and highly vulnerable, leading to potential weak spots in the security infrastructure.

Lack of visibility into IoMT devices
How they are connected to IT systems makes planning for a potential attack complex and difficult. Mapping all communications is vital to identifying the risk of an attack.

A ransomware attack
This could stop hospital services leading to disruption and potential health implications. Healthcare has become one of the top targets for ransomware gangs.

Expanding supply chains
This can create opportunities for cyberattacks launched from partner organizations that have been compromised.

Cybercriminals profit from the life-and-death stakes in healthcare — making the sector especially promising for swift and lucrative ransomware profits.

How Illumio Helps

Ensuring Service Continuity

Stop attacks in their tracks

Zero Trust Segmentation contains breaches to prevent the propagation of a cyberattack through interconnected healthcare systems.

Though traditional hackers have looked to acquire and sell patient data, new attacks focus on compromising medical systems or management infrastructure to disrupt or gain control of operations.

Regardless of motive, cybercriminals want access to as many systems as possible and the highest-value assets (PACS, EHR, bedside care, etc.).

To do so, they need to move through networks, data centers, clouds, and devices to reach critical applications and their data. The greater number of computing assets compromised, the more damaging the attack.

Unchecked, ransomware and other cyberattacks can cause increasingly serious reputational harm and threaten patient care.

Illumio Zero Trust Segmentation

By using Zero Trust Segmentation from Illumio, healthcare operators can stop cyberattacks before they spread to cause significant damage.

Illumio restricts the movement of traffic to only verified sources using allowed protocols. This prevents ransomware from stowing away on communication pathways to move across hybrid computing environments.

Illumio provides a simple map of the communication between your systems and applications, offering a detailed view of any potential risks, open ports, or firewall misconfigurations.

Critically, Illumio can map and segment communication among traditional IT data centers and clouds as well as devices on IoMT and OT networks, such as admin systems, bedside carts, X-Rays, etc.

With this information, simple security policies can be applied with a click of the mouse.

These Zero Trust Segmentation policies will contain breaches and prevent malware from spreading to a healthcare organization's critical systems, ensuring business resilience and operational continuity.

As a result, healthcare providers can protect critical assets and stop malicious actors from reaching critical systems and data, guarding against a major operational failure or loss of patient and financial data.

Named a Leader in The Forrester New Wave™: Microsegmentation, Q1 2022, Illumio's core capabilities equip healthcare providers to:

- Secure critical assets and services, even in the event of a breach.
- Stop the spread of ransomware across networks, data center servers, and applications.
- Realize comprehensive visibility across applications, devices and networks.

"We've gained so many benefits from Illumio we weren't really expecting. We set about doing segmentation and we got so much more."

– Information Security Manager, ACH Group

To learn more

Read our in-depth guide Zero Trust Segmentation for Healthcare Organizations.

About Illumio

illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.