illumio

INDUSTRY GUIDE

Zero Trust Segmentation for Healthcare Organizations

Healthcare providers can guard critical applications, medical devices and patient information from ransomware and other cyberattacks with Zero Trust Segmentation

Healthcare Has Become a Prime Target for Cybercriminals

Ransomware attacks and data theft have risen to record levels in the healthcare industry, resulting in billions of dollars in losses and threatening the quality of care — potentially creating life-or-death circumstances.

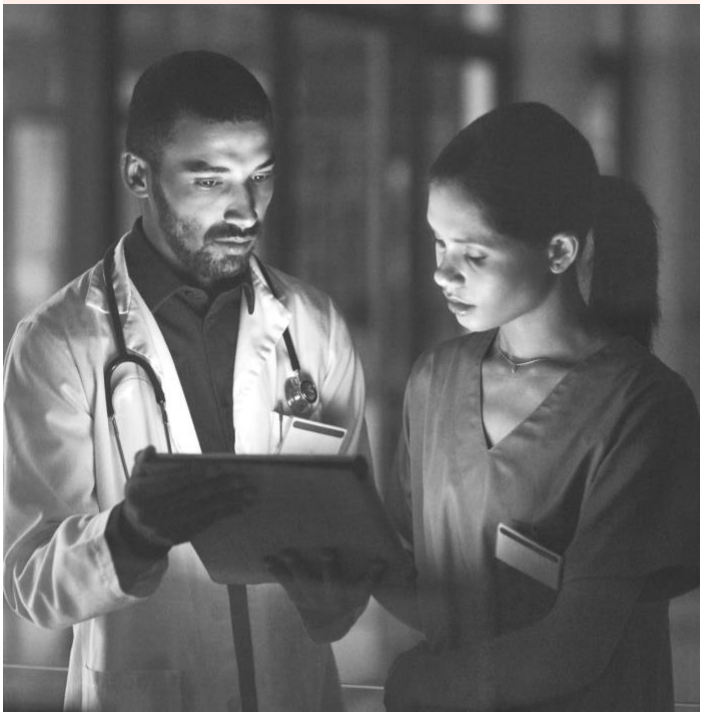
The increasingly hyperconnected healthcare landscape has become a prime target for cybercriminals. The risks to healthcare organizations continue to broaden as providers expand cloud systems, Internet of Medical Things (IoMT) devices, integrated patient care systems, wireless networks, and remote personnel.

This environment is precisely what cybercriminals exploit to infiltrate hospital data centers and medical device networks. A shift to remote access for some employees during the Covid pandemic has opened even more pathways to mission-critical systems and data.

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

In this guide, we explore the unique cybersecurity challenges facing healthcare providers. We look at how they can best respond with Zero Trust Segmentation to secure digital systems, protect medical records, and ensure patient care.

> "Given the increasingly sophisticated and widespread nature of cyberattacks, the healthcare industry must make cybersecurity a priority and make the appropriate investments needed to protect its patients."
>
> **U.S. Cybersecurity and Infrastructure Security Agency**



The Ransomware Threat to Quality of Patient Care

Cyberattacks on healthcare organizations 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.

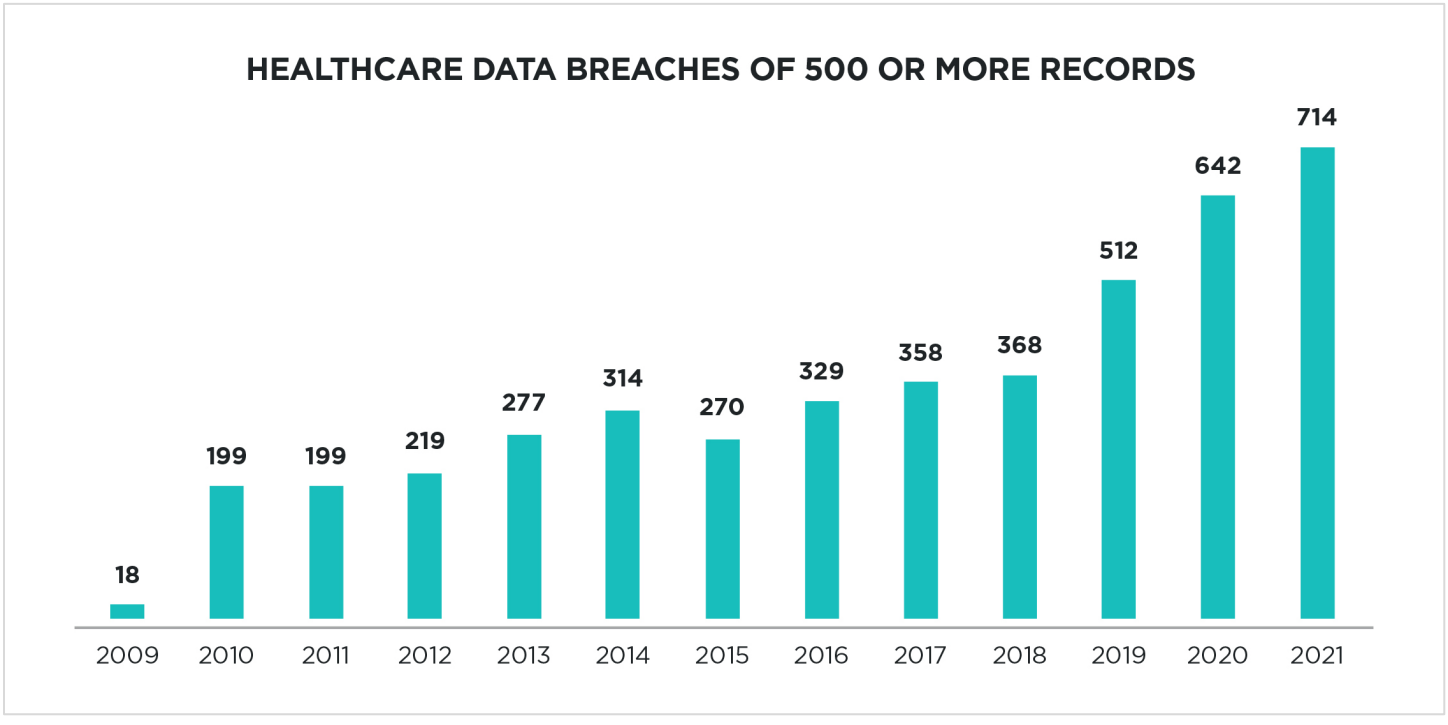
More than two-thirds (67%) of healthcare cybersecurity professionals say their organizations experienced "significant security incidents" in the preceding 12 months, according to the 2021 HIMSS Healthcare Cybersecurity Survey.

In particular, ransomware is harming the quality of patient care, according to a survey of nearly 600 healthcare IT and security professionals conducted by Ponemon Institute for Censinet, a healthcare-focused risk management provider.

The Ponemon Institute found that 43 percent of respondent organizations had suffered a ransomware attack, resulting in these impacts to patient care:

- 71% cited longer length of patient stays
- 70% cited delayed procedures and tests resulting in poor healthcare outcomes
- 65% cited an increase in patients transferred to other facilities
- 36% cited an increase in complications from medical procedures
- 22% cited an increase in mortality rate

Cybercriminals profit from the life-and-death stakes in healthcare — making the sector especially promising for swift and lucrative ransomware payouts. As a result, bad actors are targeting IoMT and operational technology (OT) devices critical to patient care, in addition to more traditional targets of financial data and protected health information (PHI) patient records.



Source: HIPAA Journal

IoMT Devices Broaden the Risk for Healthcare

Growing IoMT usage has expanded the scope of risks for healthcare providers from cyberattacks. Imaging equipment, patient monitoring, diagnostic systems, infusion pumps, and other medical devices are commonly connected to main networks and core systems, leaving healthcare organizations more vulnerable to attack.

Poor visibility across the IoMT landscape exacerbates the problem. The Ponemon Institute survey found that just 36% of respondents say their organizations are effective in knowing where all medical devices are; only 35% know when a device is at end-of-life or out-of-date.

Even as IoMT grows, legacy technology remains widespread and a top concern for chief information security officers (CISOs) at healthcare organizations, according to a survey conducted by the Healthcare Information and Management Systems Society (HIMSS).

One reason that legacy technology is such a challenge is because vendors typically stop supporting outdated systems. Patches and upgrades are unavailable for many end-of-life technologies.

The combined security concerns around IoMT, legacy technology, PHI, and financial data are prompting healthcare organizations to turn to Zero Trust security strategies such as microsegmentation.

> "Given the interconnected nature of the future with IoMT devices, augmented reality, robotics and more, it is clear that the current perimeter-based security model that most healthcare organizations use will no longer be effective.... healthcare organizations must continue to invest in the basics while making a fundamental shift from the castle-and-moat approach to a Zero Trust model."
>
> **U.S. Department of Health and Human Services, "Zero Trust in Healthcare"**

Illumio Zero Trust Segmentation in Healthcare

Illumio's Zero Trust Segmentation technology enhances traditional perimeter and firewall defenses to embed security at a far more granular level into the interior of networks and data centers. Instead of a single firewall protecting hundreds of applications and devices, security is applied at each asset individually.

This defense-in-depth model bars lateral movement of malware, even if it's able to infiltrate an asset, such as an application or device. It's like thieves breaking into a building, but they can't move beyond the first room they entered.

Illumio follows the Zero Trust principle that no application, device, or user can be trusted without verification and must therefore be restricted to least-privilege access. 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:

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

> "The appropriate implementation of Zero Trust solutions can lead to significantly heightened security postures for healthcare organizations."
>
> **2021 HIMSS Healthcare Cybersecurity Survey**

1. Secure critical assets and services

Illumio Zero Trust Segmentation ensures that access to any asset or application is secure and authenticated. It eliminates paths that allow lateral movement. It enforces and maintains policy within large, rapidly changing environments. With Illumio, you can:

- **Easily segment assets, environments, users, and groups.** Build Zero Trust access rules through data-driven policy design, automatic policy creation, and scalable enforcement using your existing network and device infrastructure.
- **Enforce policies dynamically to consistently secure evolving applications, devices, and networks.** Write simple rules. For example, "bedside care systems can talk to electronic health record (EHR) systems." Policies will automatically update as systems change.
- **Operate at the host level.** Manage existing host-based firewalls that scale easily — managed from from a single console, all without moving cables or changing your virtual infrastructure.

Illumio stops ransomware in ways that legacy security tools simply cannot. With Illumio, you will reduce your attack surface, limit the blast radius of a successful breach, and protect your most sensitive data, applications, and assets.

> "Zero Trust segmentation or microsegmentation is fine-grained control of application needs, user access, and data repositories. Tools help automate, orchestrate, test and implement granular policy across network security controls."
>
> **Forrester, Trusting Zero Trust**

2. Secure critical assets and services

Illumio immediately shrinks your attack surface by automating workflows — like policy discovery, authoring, distribution, and enforcement — that block communications on any high-risk port in your network. With Illumio, you can:

- **Pinpoint your critical sources of ransomware risk.** See all of your commonly exploited pathways, orphaned legacy connections, and data flows that are out of compliance with your existing security policies.
- **Proactively close and monitor high-risk pathways.** Close commonly exploited ports in your environment, while monitoring those ports that must remain open.
- **Create a reactive containment switch to stop in-progress incidents.** Develop a one-click solution that can precisely block communications down to the workload level, isolating and protecting unaffected systems during an incident.

Fortune 100 healthcare service ensures secure divestiture

At a Fortune 100 healthcare service, the IT team was concerned about exposing the organization's data center to unauthorized access as the company sold a portion of its business and associated infrastructure to an acquiring entity.

The IT team turned to Illumio to quickly understand system communication flows and then put segmentation policies in place.

The acquiring firm gained secure access to relevant assets, while the seller locked down systems access outside the scope of the divestiture.

Illumio's plug-and-play capabilities proved far faster, far simpler, and less costly than an alternative proposed by a consulting firm. The healthcare service avoided re-architecting (or even touching the network) while meeting contractual obligations of the divestiture within a tight timeline.

See the case study

"Zero Trust is an information security model moving from perimeter-based defense to minimizing trust by continuously verifying that access is secure, authenticated and authorized."

Forrester, Trusting Zero Trust

3. Visualize device and system communication

Illumio provides actionable insights by mapping all communications between assets, including applications, medical devices, clouds, containers, data centers, and endpoint devices. And it does this without touching or changing your network.

With Illumio, you can:

- **Build real-time network visibility.** Automatically map the internal communications and outbound Internet connections for each of your medical devices, applications, and workloads.
- **Lower operational risk by identifying unnecessary connections.** Build a clear picture of your vulnerable systems, noncompliant data flows, and excessive communications. You'll gain a better understanding of what's open and why.
- **Share a unified view of your communications for your teams and your SIEM/SOAR tools.** Create tight collaboration, offering customized views for Network Ops, Security Ops, DevOps, and DevSecOps. Feed real-time data to your SIEM or SOAR.

Unified and continuous visibility across a healthcare IT landscape reveals high-risk traffic and supports the implementation of Zero Trust Segmentation policies to minimize the impact of any breach.

Aligning With the NIST Cybersecurity Framework

The Illumio Healthcare Solution aligns with the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework and its five pillars of Identify, Protect, Detect, Respond, and Recover.

Widely used among healthcare providers, the NIST framework supplies a foundation for a holistic security strategy that utilizes modern Zero Trust Segmentation.

Illumio supports the framework with Illumio Core, Illumio Endpoint, and Illumio CloudSecure products. Illumio's technology partners and integrated solutions provide additional security capabilities and functionality specific for healthcare organizations.

The NIST Cybersecurity Framework is based on five steps of Identify, Protect, Detect, Respond, and Recover.

Illumio NIST Mapping

Illumio makes it far easier for healthcare organizations to implement the Cybersecurity Framework (NIST CSF), as well as support Zero Trust security practices. Together, these complementary initiatives greatly improve cyber resilience for healthcare organizations.

Illumio streamlines the adoption of the NIST framework and simplifies the path to Zero Trust security. In this section, we will look at each of the steps in the NIST CSF and explain how to use Zero Trust Segmentation to achieve them.

Identify

Identifying what to protect and when to do it can sometimes become the most complex and controversial part of any cybersecurity strategy. Budget and resource restrictions often limit the ability to protect everything to the same level and at the same time.

The first step is a simple audit to identify which systems will have the biggest impact on delivering health services. Intensive care, digital imaging systems (PACSs), patient monitoring devices, and operational facilities are likely to be at the top, with functions such as catering or car parking at the other end of the spectrum. Using a model that maps the likelihood of an attack with the impact of an attack will help pinpoint the relative risk of each area.

The second step is to understand your communications pathways — what is talking to what.

Illumio generates a simple graphical map to show devices and their communication flows with traditional IT systems, such as applications, servers, databases, the Internet, or even smart devices. It is important that this map includes any communication with workloads or services in the cloud. This is especially true for new EHR systems that share information through the cloud.

Illumio's application dependency map uses metadata from IT devices, as well as information gathered from OT and IoT security platforms such as Cylera and Armis. It can also be enriched with data from a CMDB (configuration management database) like ServiceNow.

The Illumio Core Services Detector will identify core IT services that need protecting like DNS, DHCP, etc. The need to perform this task is stated in the NIST CSF, and unlike many other solutions, Illumio provides real-time traffic flow information without impacting the operation of the network.

With this knowledge, generating the required security policies is a much simpler process.

Protect

Once you have identified what to protect, you then need to enforce that protection. The simplest first step to take is to deploy Zero Trust Segmentation.

Zero Trust Segmentation prevents communications except for those that are allowed and verified — enforcing the concept of "least privilege."

With least-privilege security controls consistently deployed across a hybrid network, healthcare organizations can stop a cyberattack at its first point of entry — preventing any further movement across the network.

With Zero Trust Segmentation, you can block specific traffic routes and ports that cyberattackers and ransomware typical use. Or you can block all traffic on a given pathway while allowing only traffic from specific sources.

This limits the lateral movement of an attack like ransomware that is trying to access high value assets. Ransomware will use popular existing protocols like RDP to move around the network.

By limiting this movement, you can contain ransomware and prevent it from reaching those high-value assets like PACS and the EMR system.

Zero Trust Segmentation helps ensure that a hospital can continue to deliver services even while undergoing a cyberattack.

Detect

Detecting an attack is key to neutralizing the threat — and the quicker the better.

Detection covers a number of technologies. Tools like EDR/XDR (extended endpoint detection and response) and NGAV (next-gen anti-virus) monitor your computing systems looking for "indicators of compromise" (IoCs).

IoCs raise the suspicion that a piece of code could be malware. Other security tools like NDR (network detection and response) and UEBA (user and entity behavior analytics) monitor for activities on the network that fall outside of normal baselines.

The final part of the puzzle is detecting any connections that should not be allowed (e.g. the imaging system communicating with the Internet). Illumio will generate an alert if a threshold for non-allowed attempts is breached to detect lateral movement of a potential attack.

Segmenting the network is shown to improve the performance of EDR systems by restricting the spread of an attack, thereby reducing the area required for detection.

Medical group blocks unauthorized access

At a large medical group, a network segmentation project became unmanageable (effort, cost, and maintenance) while failing to prevent lateral movement if a bad actor breached the system.

The medical group, with 400 physicians, turned to Illumio to establish baseline controls, confirm policy, and enforce authorized access across its IT ecosystem.

Illumio helps the medical group protect the personal information for 400,000 patients with its real-time application dependency map and easy-to-build segmentation policies.

"Illumio allows us to easily lock down communications at the server layer, and even the process layer," says the group's IT director. "If anything tries to go outside of what is approved, Illumio will alert you, and you can investigate."

See the case study

Respond

Once an attack is detected, you must respond instantly. As soon as an attack starts, it needs to be stopped.

Zero Trust Segmentation supports this essential security capability.

Illumio's incident response segmentation can be built as a manual response or automated within various incident response security systems, including SOAR (security orchestration, automation and response) and SOC (security operation center) tools.

Once any system detects an attack, the workflow within a management system can automatically trigger a lock down of all the relevant ports and protocols that an attack would use. Alternatively, entire sections of the network can be isolated.

With Zero Trust Segmentation, you can effectively lock down ransomware and attacks to help maintain services while the malicious code is removed from your computing systems.

Your response process and configurations should be planned and tested for efficacy, because any attack could be devastating with unknown consequences. Establishing a cyber resilience plan and practicing the response can make the difference between being able to maintain services and risking patient lives.

Restore

The last action is to restore services. If the attack is still underway, any premature repair work could create new risks.

With Zero Trust Segmentation, security and IT teams can set up protection around individual departments and systems, so they can resume operations, shielded from the attack.

Once the location of an attack is identified and contained, high-value systems like PACS or operations facilities can be released back to normal use.

EDR systems will be able to track and recreate the path of the attack to identify weak points and vulnerabilities in your network. Using the Explorer feature in Illumio Core, you can quickly identify and block any connections used by the attack.

Illumio Industry Alliances

Asset identification and mapping

Healthcare providers face the challenge of securing IT systems and life-saving medical assets. Mapping data flows between IT systems is simple, but it is more complex for medical devices.

Many organization utilize OT/IoT security solutions from Illumio partners such as Cylera and Armis to discover, identify, and map the communications flows among their devices and operational systems.

Illumio imports asset management and flow data from Cylera and Armis to provide visibility of all assets and communications across IT, Medical IoT, and OT networks.

Event management

To achieve real-time visibility into the progression of any breach — and to achieve earlier threat detection — healthcare providers are leveraging Illumio's native integrations with SIEM (security information and events management) platforms from IBM Security, Splunk, ArcSight, and Exabeam.

When an attack occurs, Illumio detects lateral movement attempts, aided by SIEM-based analytics and alerting. This complementary mix of security capabilities triggers earlier investigation and higher quality confirmation of possible threats.

Automated response

To automate a rapid response, Illumio has also integrated with the four leading SOAR platforms: IBM, Spunk, Palo Alto Networks, and Swimlane.

The Illumio integration supports a workflow that begins with the reduction of the attack surface, along with instrumentation of the network.

> Illumio compartmentalizes key assets and processes across a healthcare provider organization to provide fine-grained protection from attacks at the host level — without re-engineering the network.

The Illumio integration with SOAR platforms provides visibility into the ports and protocols being exploited by the attacker, so that those pathways can be rapidly and automatically blocked, stopping an attack in its tracks.

Remote access

Where healthcare workers need remote access to data, organizations are utilizing Zero Trust network access (ZTNA) tools.

However, ZTNA technologies lack visibility into the dynamic changes that occur within the internal network, e.g. when an application is assigned a new IP address.

Illumio and Appgate have integrated their technology to leverage the contextual-awareness and granularity provided by Illumio.

Healthcare providers can now achieve holistic, dynamic Zero Trust security in both their internal and perimeter networks by using Illumio in conjunction with Appgate.

Vulnerability management

If nothing, healthcare organizations must be constantly vigilant against growing cyber threats. Operating systems, applications, devices and everything across the network require the most current security protections. New vulnerabilities must be patched immediately.

But keeping up with this constant battle is challenging — even for the best IT organizations.

Illumio provides a key compensating control to help minimize the exposure of vulnerable systems.

Illumio integrates with vulnerability management platform including those from Tenable, Rapid7, and Qualys to import vulnerability data that is then used to prioritize risk and automate controls to reduce exposure.

Learn More About Illumio for Healthcare

Cyberattacks on healthcare organizations are likely to increase across rapidly changing ecosystems of IT, IoMT, and OT systems.

Healthcare CISOs committed to best-in-class security are turning to Zero Trust Segmentation to maximize the cyber resilience of their institutions, helping ensure the safety and privacy of their patients, clients, and partners.

To learn more about how Illumio can strengthen cybersecurity at your healthcare organization:

- Explore our products, including Illumio Core for workloads, Illumio Endpoint for user devices, and Illumio CloudSecure for cloud-native security.
- Schedule a demo and consultation with one of our healthcare security experts.
- Sign up for a virtual hands-on lab session.

About 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.