cognizant

Implementing zero trust in healthcare

A strategic blueprint for cybersecurity

Healthcare organizations can greatly improve system resilience against attacks by adopting the proven and practical zero trust approach to network, device, application and data security.

Healthcare continues to be an attractive and vulnerable target for cybercriminals. Even the largest healthcare organizations have suffered cyberattacks that have exposed millions of patient records and disrupted critical services.[1] Some have paid multimillion-dollar ransoms to restore access to their own systems.[2] That's understandable in an industry where system downtime can directly endanger patient lives.

Attacks continue. In 2024 alone, there were 181 confirmed ransomware attacks on healthcare providers, affecting more than 25.6 million patient records. The average ransom demand reached $5.7 million, reflecting the high stakes involved in healthcare cyberattacks.[3]

These incidents illustrate that healthcare organizations can no longer rely on implicit trust, flat networks or reactive defense models to guard against cyberattacks. The healthcare industry's security landscape is too complex. The average organization must protect a wide range of environments, from cloud-based electronic health records (EHRs) to legacy, premise-based systems to a variety of portable and unmanaged medical devices. All these likely hold highly sensitive personal health information (PHI), the unauthorized release of which puts organizations afoul of regulations such as HIPAA, HITECH and emerging data privacy laws. In short, healthcare organizations must evolve their security strategies toward proactive, risk-based frameworks. This is where adopting the zero trust approach to cybersecurity becomes not just relevant, but essential.

The case for zero trust in healthcare

Zero trust is not a product or a one-time initiative. It is a continuously evolving cybersecurity strategy that assumes no person, application, system, device, endpoint, etc., within or beyond the organization's network perimeter should be automatically trusted. In other words, every user, device, application and connection must be continuously authenticated, authorized and validated.

The modern healthcare delivery ecosystem has several inherent vulnerabilities that the zero trust concept helps address. First, healthcare computing is distributed by design across cloud platforms, telehealth services, third-party vendors, remote workers and a significant number of unmanaged Internet of Medical Things (IoMT) devices. Identity management across clinical, administrative and third-party actors tends to be fragmented, making identity validation more challenging.

Moreover, healthcare relies heavily on legacy systems. These systems may be nearing their end of life, be out of support, lack endpoint protection and/or be part of a monolithic architecture. These factors all create ideal conditions for lateral movement into other systems and applications once an attacker gains initial access. The combination of minimal or no network segmentation and limited real-time telemetry contributes to both the frequency and impact of healthcare breaches.

Zero trust addresses these pain points by enforcing least-privilege access, continuously verifying trust and minimizing the blast radius of a compromise. Rather than focusing solely on perimeter hardening, zero trust promotes a data-centric and identity-driven defense strategy.

While interpretations of the strategy vary slightly across frameworks (e.g., NIST, CISA, Microsoft), the core pillars of zero trust generally include the following:

Identity

Strong identity governance is the foundation of zero trust. Every clinician, staff member, third-party vendor and device must be strongly authenticated, continuously verified and governed through least-privilege access policies. In other words, users, apps, devices, etc., only have access to the specific data, apps and resources they require to carry out their function.

Device

With healthcare's mix of managed endpoints, unmanaged medical devices, bring your own device (BYOD) and contractor devices, a zero trust approach calls for rigorous asset visibility, posture assessment and segmentation to isolate risky devices from critical systems.

Network

Flat networks are a liability in healthcare. Network microsegmentation can prevent an intruder's lateral movement from a compromised endpoint to mission-critical systems like EHRs. In addition to microsegments, network policy enforcement must be dynamic and identity-aware.

Application

Applications, including EHRs, telemedicine platforms and third-party SaaS solutions, must be protected through context-aware access rules, runtime controls and secure software development practices. Zero trust ensures that only verified users and compliant devices can interact with sensitive apps.

Data

Patient records are among the most valuable and regulated data types. Zero trust data protection requirements include classification, encryption, access control and continuous monitoring of data at rest, in motion or in use. For example, continuous monitoring can immediately flag unusual data movement while encryption helps ensure data is unreadable if somehow accessed by an unauthorized user or device.

Healthcare organizations must invest in foundational capabilities to support a zero trust strategy. The required capabilities include the following:

Visibility and analytics

Continuous monitoring, behavior analytics and real-time telemetry are crucial for detecting malicious activities.

Automation and orchestration

Zero trust at scale requires automation to keep up with policy enforcement and remediation actions. This reduces response times and ensures consistency.

Governance

Strategic oversight ensures that zero trust initiatives align with clinical workflows, privacy regulations and business priorities. Governance also includes lifecycle management of identities, entitlements and exceptions.

Zero trust in action

To understand where zero trust delivers the most tangible impact in healthcare, it’s important to look at how its principles address key operational pain points. These include security gaps created by legacy infrastructure, the risks introduced by medical devices and the regulatory complexity of handling sensitive patient information. The following use cases illustrate how healthcare organizations can apply zero trust to improve resilience, manage risk and maintain compliance in their unique contexts.

Use case: Ransomware resilience

Ransomware attacks are among the top cybersecurity risks in the healthcare industry. A single infection of malicious code can shut down emergency rooms, delay diagnostics and force clinicians to fall back on manual processes.

Healthcare's vulnerability to ransomware attacks stems from a mix of technical debt and operational complexity, including:

- Legacy systems with components that are outdated and/or can't accept security patches
- Flat, permissive networks with minimal segmentation
- Fragmented identity governance and excessive administrative privileges
- Limited endpoint visibility and delayed threat detection
- Weak or incomplete backup and recovery processes

Zero trust does not eliminate ransomware risk but when implemented properly it can significantly reduce the potential damage, slow down attacker progression and support rapid recovery. Here's how:

Access and containment

Identity- and device-aware access controls restrict access based on role, context and device posture, limiting initial exposure. Network segmentation and microsegmentation prevent lateral movement, ensuring that a compromise in one zone doesn't spread to critical systems. Continuous telemetry and analytics detect abnormal behavior early, enabling automated containment of compromised accounts or endpoints.

Data security and recovery

Zero trust enforces strict policies around access to structured and unstructured data, including personally identifiable information (PII), PHI and other clinical records. Immutable backups and air-gapped storage are essential for ensuring that recovery points are not compromised during an attack.

Granular restoration strategies enable prioritized, staged recovery to minimize care disruption. Regular recovery testing and business continuity planning ensure that the implemented capabilities translate into actual service restoration during an incident.

Operational continuity

Service dependency mapping, that is, knowing which apps support surgical scheduling, medication dispensing or ICU monitoring, is critical to orchestrate functional recovery. Just-in-time access provisioning can re-enable critical roles after an incident without restoring excessive privileges.

Integrated incident response playbooks link zero trust policies with disaster recovery and business continuity processes (DR/BCP)—closing the loop between prevention and recovery.

Use case: Medical device security

Connected medical devices are indispensable to modern care delivery. But they also represent one of the most unprotected segments of the healthcare threat surface. These devices are often unmanaged, unpatchable and lack basic security controls, making them attractive targets and convenient entry points for threat actors. Unlike conventional IT assets, medical devices present a unique set of challenges:

- Many run proprietary or unsupported operating systems with limited or no patching capabilities
- Devices are often deployed in flat network segments, with little to no access control
- Clinical workflows demand 24/7 availability, limiting the feasibility of downtime for maintenance
- Security teams often lack a complete and current inventory of devices, let alone real-time health and risk posture data

These gaps not only increase the risk of compromise but complicate incident response, because even basic forensics or containment steps can interrupt patient care.

While traditional endpoint security models don’t work for medical devices, zero trust principles can be adapted to mitigate risk without disrupting care. These include:

Device discovery and classification

The foundation is visibility. Network monitoring tools can help identify devices, categorize them by type, vendor and function and assess baseline behavior—all without interfering with clinical use.

Network-based segmentation

Using software-defined networking (SDN) or other OT/IoT-specific segmentation solutions, healthcare organizations can logically isolate IoMT devices into tightly controlled segments.

Real-time behavioral monitoring

Zero trust requires ongoing validation. Anomalies in communication patterns—such as a diagnostic machine suddenly reaching out to an unknown external IP—should trigger alerts or automated isolation.

Risk-based policy enforcement

Devices with known vulnerabilities or unpatched firmware can be placed in restricted zones with limited communication paths.

Security controls nonetheless must align with clinical realities. Blocking device traffic arbitrarily can compromise care. To minimize the risk of service disruptions, security teams must cooperate with other parts of the organization to:

- Define acceptable communication patterns by device type
- Establish “safe isolation” procedures that preserve availability while limiting exposure
- Integrate zero trust policies with existing clinical risk assessments and device procurement standards

The role of AI

AI is rapidly reshaping the cybersecurity landscape. For security leaders, the question is not whether AI has a role, but how to integrate it in a way that supports both security and clinical reliability. Here are several areas in which AI can significantly improve zero trust outcomes:

Enhancing detection and response

Healthcare environments generate massive volumes of data across endpoints, networks, identities and applications. Traditional pattern-based systems struggle to keep up with this velocity and complexity. AI and machine learning can address these challenges by:

Analyzing behavioral baselines for users, devices and applications to detect subtle anomalies—for example, a nurse accessing unusual patient records or a diagnostic system exfiltrating data

Correlating signals across domains, including identity, network and data access, to provide high-confidence threat detections

Reducing noise and alert fatigue by prioritizing events based on context and risk scoring

Triggering automated policy enforcement, such as revoking access or isolating devices, in near-real-time

Supporting risk-based access decisions

AI can also augment access control frameworks:

- Dynamic risk scoring can be applied at the point of access, evaluating behavioral context (e.g., time, location, device health, historical patterns)
- AI-driven identity analytics can flag stale, orphaned or high-risk accounts that may violate least-privilege principles
- Natural language processing can support access governance by analyzing access request rationales or reviewing unstructured data for policy violations

Caution: AI-powered threats and operational risks

While AI offers clear advantages, it also introduces new cybersecurity risks. These include:

- **Adversarial AI.** Attackers are leveraging AI to craft convincing phishing content, evade detection and automate lateral movement
- **False positives.** Overreliance on black-box AI can erode trust if its alerts adversely affect clinical workflows without a clear rationale
- **Model drift and bias.** Healthcare environments evolve quickly; AI models must be retrained continuously or risk missing critical patterns

Healthcare organizations should apply the zero trust mindset to AI itself: Do not implicitly trust automated outputs. Ensure these are subject to governance, auditability and human oversight.

AI should be viewed as a force multiplier, not a standalone solution. When layered into a mature zero trust architecture, AI enhances both proactive defense and resilience under pressure. But its deployment must be disciplined, transparent and aligned with clinical imperatives, not just security goals.

From theory to practice: Strategic and tactical recommendations

For many healthcare organizations, zero trust may seem aspirational, an ideal model that's difficult to implement amid budget constraints, legacy systems and complex clinical workflows. But successful zero trust programs aren't built overnight. Instead, they are achieved through incremental progress, driven by clear priorities and business alignment.

Here are some practical tactics that can get organizations started on this journey:

- Conduct a zero trust readiness assessment, aligned to NIST or CISA guidance. Create a holistic zero trust strategy to guide the organization through a phased implementation.
- Inventory identities, assets, applications and data flows, starting with high-risk areas.
- Implement risk-based multifactor authentication (MFA) for high-impact user groups, such as users with remote access and/or privileged roles.
- Roll out network segmentation for at least one critical service area, such as picture archiving and communication systems (PACS) or pharmacy.
- Deploy visibility tools that can passively monitor medical devices without disrupting care.
- Define access baselines for key applications and use telemetry to enforce policies.
- Conduct tabletop exercises with scenarios combining ransomware, clinical downtime and zero trust controls.

The rise in ransomware attacks, the complexity of digital transformation and the criticality of patient care systems demand a security model that goes beyond traditional defenses. Zero trust offers a practical, risk-aligned approach to securing the healthcare enterprise. By focusing on identity, segmentation, continuous verification and resilience, healthcare organizations can reduce risk exposure, improve operational continuity and build trust.

Zero trust isn't a product or a certification, it's a culture shift. It requires cross-functional alignment among cybersecurity, IT, clinical operations and executive leadership. This journey requires investment and collaboration. But the cost of inaction is far greater. In a threat landscape where attacks are inevitable, zero trust is how healthcare stays functional, secure and patient-centered

References

[1] "Change Healthcare Attack Underscores Urgent Need to Strengthen Cyber Preparedness as Individual Health Care Organizations and as a Field," American Hospital Association, January 2025, https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and

[2] Capoot, Ashley. "UnitedHealth CEO tells lawmakers the company paid hackers a $22 million ransom," CNBC, May 1, 2024, https://www.cnbc.com/2024/05/01/unitedhealth-ceo-says-company-paid-hackers-22-million-ransom.html

[3] Alder, Steve. "2024 Was Another Bad Year for Healthcare Ransomware Attacks," The HIPAA Journal, January 15, 2025, https://www.hipaajournal.com/2024-was-another-bad-year-for-healthcare-ransomware-attacks/

Authors

Sudhakar Kamalanathan

Cybersecurity Strategy Leader

Stephen Martin Rajan

North America Markets Leader, Cybersecurity

Ferenc Spala

Zero Trust Practice Lead, CMT Cybersecurity

cognizant®

About Cognizant

Cognizant (Nasdaq-100: CTSH) engineers modern businesses. We help our clients modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast-changing world. Together, we're improving everyday life. See how at www.cognizant.com or follow us on @cognizant

World Headquarters

300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Toll Free: +1 888 937 3277

European/UK Headquarters

280 Bishopsgate
London
EC2M 4RB
United Kingdom
Tel: +44 (0) 20 7297 7600

India Operations Headquarters

5/535, Okkiam Thoraipakkam,
Old Mahabalipuram Road,
Chennai 600 096
Tel: 1-800-208-6999
Fax: +91 (01) 44 4209 6060

APAC Headquarters

1 Fusionopolis Link,
Level 5 NEXUS@One-North,
North Tower,
Singapore 138542
Phone: +65 6812 4000