Assignment 3.1: Designing a Zero Trust Strategy for Third-Party Risk Management

Joshua A. Wortz

University of San Diego

CSOL-530

Cameron Carter, MS

05/26/2025

Introduction

Medium-sized healthcare networks increasingly depend on third-party vendors for IT support, cloud infrastructure, and supply chain logistics. With patient safety and data privacy at stake, these partnerships introduce significant cybersecurity risk. This report presents a tailored Zero Trust Security framework that enhances third-party risk management for a healthcare network with approximately 5,000 employees. This framework prioritizes access control, continuous monitoring, and regulatory compliance to uphold data confidentiality, integrity, and availability across the ecosystem (Rose et al., 2020; Kindervag, 2010).

Industry Context: Healthcare Network with 5,000 Employees

Our hypothetical organization, "Trinity Regional Health," includes multiple outpatient clinics, a centralized hospital, and administrative offices. The hybrid IT infrastructure consists of on-premise servers and cloud-hosted EHR systems. These services are supported by third-party vendors providing EHR hosting and backups, 24/7 IT support, medical device integration, and supply chain logistics for pharmaceuticals and equipment. The diverse digital supply chain amplifies attack surfaces, necessitating robust security measures grounded in Zero Trust principles (DISA & NSA, 2022).

Third-Party Risk Identification

Third-party relationships introduce several risks to healthcare systems. Vendors reusing passwords across systems can result in credential stuffing attacks. Unmanaged laptops and mobile devices may serve as attack vectors, while vendors with broad or permanent access can facilitate lateral movement across systems. Many organizations also struggle with vendor activity

visibility, and software updates from device vendors could contain vulnerabilities or malicious code that compromise patient safety or data integrity (CISA, 2023; Aliyu et al., 2021).

Zero Trust Application for Vendor Risk Management

Applying Zero Trust to vendor relationships requires technical and procedural safeguards. Role-based access ensures each vendor has permissions only for necessary tasks, such as allowing a network support contractor access to infrastructure tools but not patient records. Temporary access credentials that expire after task completion and privileged access tools like CyberArk reduce exposure from lingering credentials.

Authentication should incorporate multifactor methods, including biometrics or hardware tokens, and federated identity systems that allow vendors to use managed logins with restricted scopes. Device compliance should be enforced through endpoint management tools like JAMF or Intune.

Network segmentation isolates vendor traffic from core systems. A dedicated vendor DMZ can act as a gateway to internal services. Internal systems should be segmented by function —clinical (e.g., EHR), administrative (e.g., HR), and operational (e.g., HVAC and supply chain) —to contain potential breaches.

Finally, real-time monitoring through SIEM tools like Splunk or Sentinel, combined with XDR for endpoint visibility and SOAR platforms for automated response, enables the organization to detect anomalies such as off-hours access or abnormal data usage patterns. The session can be automatically suspended and reviewed if a vendor’s behavior deviates from expected norms.

Compliance Considerations

HIPAA protects electronic Protected Health Information (ePHI) in the United States and requires vendors to sign Business Associate Agreements. These agreements must enforce administrative, physical, and technical safeguards, including encryption, audit logging, and controlled access (Aliyu et al., 2021).

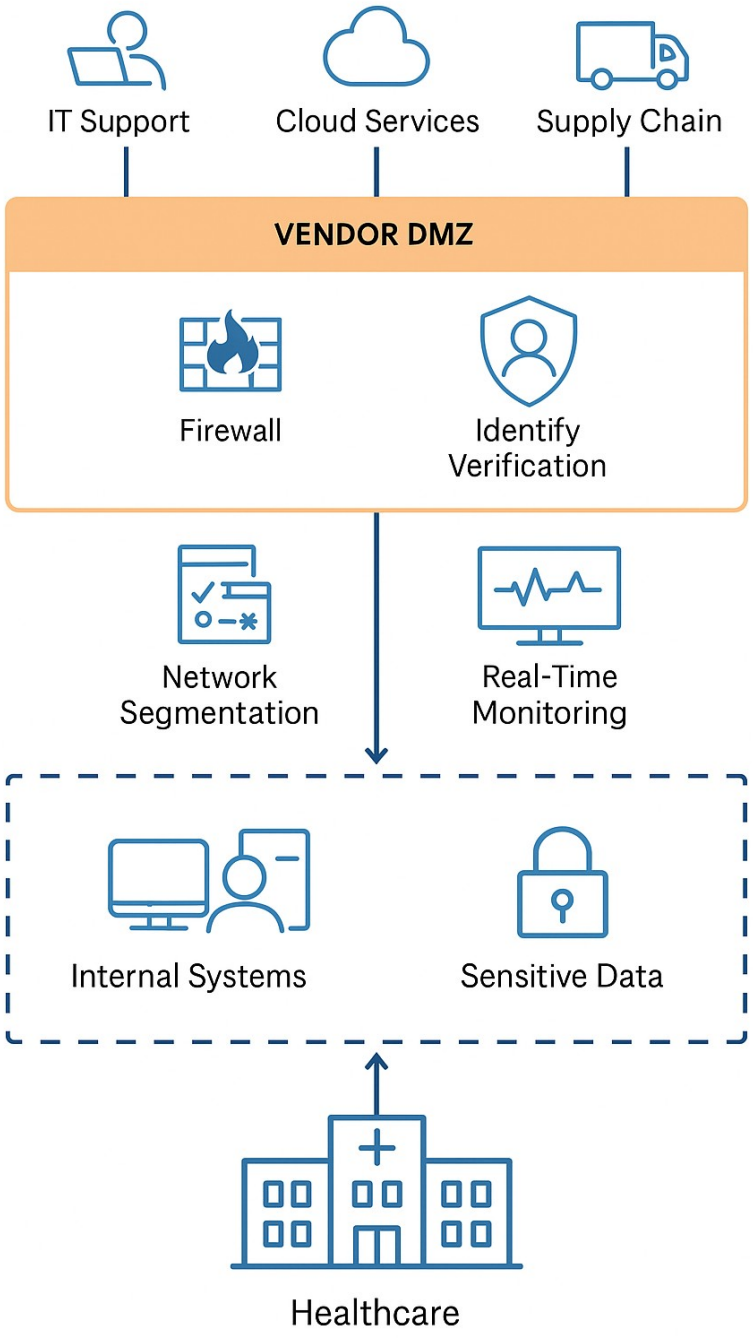
Although not legally required, SOC 2 Type II compliance is a growing expectation for third-party vendors. It ensures that vendors have been independently audited for security, availability, and confidentiality controls. Requiring SOC 2 compliance during onboarding offers assurance that vendors follow rigorous cybersecurity practices.

Zero Trust Network Diagram Description

Figure 1 illustrates a Zero Trust architecture designed for Trinity Regional Health. In this framework, employees and internal systems are protected by strong access control and identity verification mechanisms. Third-party vendors, which pose risks such as stolen credentials, insider threats, and unsecured devices, connect through a secure Zero Trust Gateway. Their activity is continuously monitored in real-time, and any suspicious behavior can trigger automated responses.

Figure 1

Zero Trust Architecture with Vendor DMZ for Healthcare Network



Note. This diagram illustrates how third-party vendors interact with a healthcare organization's internal systems through a dedicated Vendor DMZ. Security measures such as firewalls, identity verification, network segmentation, and real-time monitoring help isolate sensitive data and minimize third-party risk.

The architecture includes a Vendor DMZ that separates third-party access from internal resources. Core internal systems, including the EHR and sensitive data environments, are microsegmented based on their clinical, administrative, or operational functions. This segmentation minimizes lateral movement within the network. All components operate under the guidance of compliance standards such as HIPAA and SOC 2, ensuring the organization meets regulatory obligations while maintaining a strong cybersecurity posture.

Conclusion

Healthcare organizations must secure third-party interactions with a Zero-Trust mindset to reduce exposure and meet compliance demands. For a large network, scaling identity-based controls, segmenting internal resources, and leveraging real-time analytics enables precise, verifiable access control. Implementing this framework safeguards sensitive patient data and strengthens resilience across clinical and operational systems.

References

Aliyu, A., Santos, D., & McMillan, C. (2021). *Cybersecurity governance and compliance in healthcare: A systematic review*. Journal of Biomedical Informatics, 118, 103795. https://doi.org/10.1016/j.jbi.2021.103795

Cybersecurity and Infrastructure Security Agency. (2023). *Zero Trust Maturity Model Version 2.0*. https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

Defense Information Systems Agency & National Security Agency. (2022). *Zero Trust Reference Architecture* (Version 2.0). https://dodcio.defense.gov/

Kindervag, J. (2010). *Build security into your network's DNA: The zero trust network architecture*. Forrester Research.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207