COLORTOKENS

CASE STUDY

# How a Leading Academic Medical Center Strengthened Breach Readiness Across Its Epic Environment

Achieving scalable microsegmentation without disrupting clinical operations.

ABOUT THE ORGANIZATION

# A Leading Academic Medical Center With Statewide Impact

This case study features a nationally recognized academic health science center that operates hospitals, clinics, research institutes, and academic schools. The organization delivers healthcare services, medical education, and biomedical research across a wide regional network.

As a large healthcare and research institution, the organization manages highly sensitive patient data and supports mission-critical clinical systems that are essential to patient care and operational continuity. Protecting these environments while maintaining security, compliance, and system availability is central to its commitment to safe, uninterrupted healthcare services.

Ransomware and lateral movement techniques increasingly target healthcare environments. Strengthening cyber resilience across clinical systems has become both an operational and strategic priority for organizations like this one.

THE CHALLENGE

# Driving SEER Compliance with Easy-to-Implement Microsegmentation

Like many healthcare organizations, this medical center faced growing exposure to ransomware and lateral movement targeting critical healthcare environments. Strong perimeter defenses were already in place. Leadership recognized that protecting systems such as the Epic electronic health records system required a more proactive breach containment strategy.

The organization needed to isolate sensitive workloads quickly, reduce unnecessary communication paths, and limit the blast radius of a potential attack, all without disrupting clinical operations.

At the same time, the organization worked to align with Epic's SEER (Security Evaluation and Enterprise Readiness) framework. Updated SEER guidelines placed greater emphasis on microsegmentation as part of security scoring, prompting IT leadership to accelerate its segmentation strategy to strengthen cyber resilience and maintain compliance posture.

The organization first evaluated a network virtualization-based segmentation platform. As deployment progressed, the team encountered real limitations. The approach required specialized expertise, added architectural complexity, and demanded significant time to operationalize at scale. Extending segmentation policies across hundreds of critical workloads created ongoing administrative overhead that the clinical and IT environments could not sustain.

These limitations slowed progress and reinforced a familiar lesson for healthcare security teams: microsegmentation only reduces risk if it can be deployed and managed without adding operational burden. Without a more practical approach, the organization would likely have continued to rely on manual network controls and traditional perimeter security, limiting its ability to advance broader Zero Trust and breach containment goals.

# How the Organization Evaluated Microsegmentation® Solutions

Given the complexity of its healthcare environment, the organization set strict requirements for evaluating microsegmentation solutions. Security improvements needed to be achieved without impacting Epic workflows, introducing operational risk, or increasing administrative overhead for IT teams.

## Key Evaluation Criteria Included:

1. Deploy rapidly across complex healthcare environments without disruption
2. Maintain uninterrupted Epic and patient care workflows
3. Provide comprehensive visibility into workload communication patterns to identify lateral movement risk
4. Scale across large Epic environments spanning hundreds of servers and applications
5. Simplify policy creation and management to reduce operational overhead
6. Integrate with existing security infrastructure
7. Align with Zero Trust architecture and breach containment objectives

Beyond functionality, the organization prioritized how quickly and safely each solution could deliver measurable security improvements in a live healthcare environment.

ColorTokens emerged as a strong fit. The platform demonstrated rapid time-to-value, simplified operational management, and the ability to deliver granular visibility and segmentation at scale without adding complexity.

# A Proactive Microsegmentation Approach to Breach Readiness

Following earlier challenges with a more complex segmentation approach, the organization sought a solution that could strengthen its security posture without adding operational complexity or disrupting systems such as Epic.

The organization learned about ColorTokens through peer discussions within the healthcare security community, including reference deployments at other academic medical institutions. Based on its reported ease of deployment and rapid visibility, the organization initiated a proof-of-value engagement.

During the evaluation, the team also assessed alternative microsegmentation approaches, prioritizing solutions that could deliver rapid visibility, scalable policy enforcement, simplified management, and minimal operational disruption. Given the critical nature of Epic systems, the proof-of-value engagement was designed to validate both operational safety and technical effectiveness in a controlled environment.

Within hours of deployment, the ColorTokens Xshield™ Enterprise Microsegmentation Platform provided detailed visibility into the organization's Epic test environment, including workload communication paths, open ports, and network traffic flows. This visibility helped the team identify segmentation opportunities and validate early value.

Over a four-week evaluation period, the platform demonstrated ease of use, scalability, and compatibility with the organization's infrastructure. The results gave the team confidence to advance segmentation without introducing operational risk.

A key outcome of the engagement was the ability to implement a modern breach containment approach for Epic systems by progressively restricting unnecessary communication between workloads. This reduced the potential attack surface and improved the organization's ability to limit lateral movement while maintaining uninterrupted clinical access.

THE SOLUTION JOURNEY

# From Proof-of-Value to Enterprise-Wide Deployment

The organization began with a focused proof-of-value engagement targeting Epic test environments and supporting infrastructure. Early results demonstrated real-time visibility into workload communication patterns, enabling rapid identification of segmentation opportunities.

Following initial validation, the evaluation expanded to include policy enforcement workflows, operational integration, and scalability testing. Regular collaboration between the organization and ColorTokens helped refine deployment priorities and align technical and security teams.

After validating performance and operational simplicity, the organization proceeded with broader deployment across its Epic environment.

## Key highlights of the implementation



**Granular network visibility**

The critical need for enterprise-wide traffic visualization to identify lateral movement risks across disparate systems, like payment gateways, Hadoop big data clusters, and mediation layers.



**Agent-based coverage**

Xshield agents provided consistent enforcement across Epic infrastructure with minimal operational overhead



**Collaborative execution**

continuous engagement between the organization and ColorTokens supported alignment, accelerated rollout, and built stakeholder confidence

> **The organization segmented more than 238 Epic servers, completing a large-scale initiative without clinical downtime.**

# Strengthening Zero Trust and Breach Containment

Adopting ColorTokens produced measurable improvements in the organization's security posture and established a more structured, scalable approach to Zero Trust.

### Improved Compliance and Security Posture

The organization aligned its Epic environment with SEER framework expectations while strengthening breach readiness through scalable microsegmentation. This improved visibility and reduced exposure across critical systems.

### Enhanced Operational Efficiency

The platform integrated with the organization's existing security infrastructure, allowing teams to operationalize segmentation without added complexity. This reduced administrative overhead and improved policy management efficiency.

### Accelerated Stakeholder Confidence and Adoption

Real-time visibility into workload communication patterns improved transparency between security and application teams, helping accelerate alignment and adoption.

### Scalable Foundation for Zero Trust Expansion

Following successful segmentation of Epic environments, the organization established a repeatable model for microsegmentation and expanded its Zero Trust roadmap to additional applications.

**The organization's Breach Impact Score decreased from 100 to 20, reflecting the impact of scaled microsegmentation deployment across its Epic environment.**

*ColorTokens enabled us to implement a practical microsegmentation strategy across our Epic environment without disrupting clinical operations. The visibility and simplicity of the platform gave our teams confidence in strengthening breach containment while maintaining operational efficiency."*

Associate Director of Innovation and Artificial Intelligence, Customer Organization

# A Practical Path to Breach Readiness for Healthcare Organizations

Healthcare environments face a familiar tension. Security teams need to contain lateral movement quickly, but clinical systems cannot tolerate disruption. This organization's experience shows that microsegmentation does not have to force a trade-off between the two.

The path forward starts with visibility. Understanding how workloads actually communicate, before writing a single policy, is what makes segmentation safe to deploy in a live clinical environment. From there, containment can be introduced progressively, validated at each step, and scaled without adding operational burden to already stretched IT teams.

For healthcare organizations weighing their own microsegmentation strategy, the questions worth asking are the same ones this organization asked. Can the approach scale across hundreds of critical workloads without specialized expertise? Will it align with frameworks like SEER and broader Zero Trust goals? Can it deliver measurable containment without slowing down the people who keep patient care running?

***Learn how ColorTokens can help your organization become breach ready. Contact us.***

---

**About ColorTokens:**

ColorTokens, the premier enterprise microsegmentation provider, specializes in making organizations "breach ready" by halting the lateral spread of ransomware and malware within intricate network infrastructures using its innovative ColorTokens Xshield™ platform. The platform visualizes traffic patterns between workloads, devices, and users, enabling organizations to enforce granular micro-perimeters, swiftly isolate critical assets, and respond to breaches effectively. Recognized as a Leader in the Forrester Wave™: Microsegmentation Solutions, Q3 2024 evaluation, ColorTokens safeguards businesses by thwarting ransomware and malware attacks, ensuring significant savings in potential disruptions

Copyright 2026 © ColorTokens ®. All rights reserved.