Securing Hospitals, Enabling Patient Care

The problem

It is well known that healthcare systems have been the target of increasing cyberattacks. To put it in figures, JAMA researchers have reported [1] that the frequency of cyberattacks on health systems more than doubled from 2016 to 2021 and exposed the protected health information of nearly 42 million patients. Only one in five healthcare organizations reported being able to restore data from backups. Indeed, a ransomware attack on a hospital crosses the line from an economic crime to a threat-to-life crime. Hackers now specifically target medical devices, not only networks. They attack hospitals because even short disruptions in their IT systems can be catastrophic to the communities they serve, increasing the probability that the hospitals will be pressured to pay ransom or extortion.

CIOs and CISOs have myriad of challenges in responding to these cyberattacks, including but not limited to, budget pressures, shortages of skilled talent, acquisition integration, and many patchwork solutions with no enterprise-wide visibility of assets and traffic. Their security teams are responsible for securing a vast number of disparate third-party systems; the hospital's core EMR system, patient-facing portals, remote workers, and of course medical devices.

Building superior cybersecurity with Zero Trust

Today, an overwhelming number of organizations have been relying on mostly a patchwork of cybersecurity solutions, including firewalls, frequent patching, client anti-virus, IDS/IPS, SIEM, etc. They have been mostly blind to (a) East-West network traffic, and (b) OT or medical device traffic. Major attacks and ransomware have wreaked havoc by lurking in the data centers and organizations and took away billions of dollars of highly sensitive data or extracted ransomware money.

When a hospital implements zero trust microsegmentation, it makes it extremely difficult for unauthorized lateral movement on the network. Attackers will not even "see" most of the assets on the network which they could either target or use as an intermediary hop.

The same principles can be applied to host systems. A zero-trust host lock down will severely restrict what processes can execute on the host and what an attacker can leverage from what is already on it.

A critical attack vector for any organization is user access. Using principles of zero trust access, hospitals can granularly control users' access to sensitive patient data. User devices can be protected from lateral movement of ransomware.

Information security professionals have long recognized the value of zero trust implementations. Very few organizations have been able to successfully follow through on an implementation using traditional solutions. This is where ColorTokens brings unique value.

ColorTokens delivers protection and cyber resiliency for healthcare organizations

ColorTokens delivers a Unified Zero Trust Cybersecurity SaaS Platform that provides comprehensive security for hospital data centers, clouds, IoT/IoMT, and users.

Key benefits to hospitals

Epic System Protection

Epic Systems recommends that the application should be segmented to protect patient data. In a typical configuration, Epic can have over 15 related applications that are connected to it. ColorTokens creates dependency maps between Epic and ancillary components, and segments access and interactions between them using the concept of leastprivilege. This approach has been proven to protect Epic Cache. ColorTokens has out-of-the-box Epic security templates for organizations to customize and deploy for rapid time to value.

Medical Device Isolation

Medical devices and scanners are critical to patient care. Attacks on these devices can have significant impact to hospital operations, requiring critical care patients to be routed to other facilities. ColorTokens drastically reduces the attack surface and the chance of unauthorized access using a proprietary agentless approach.

Segmenting Devices and Access for Provider Workstations

Shared workstations and laptops used by nurses and doctors can pose a significant risk to hospitals. Malware and command and control executables downloaded via unsafe web browsing activities can quickly spiral into a ransomware attack. ColorTokens protects workstations and VDI instances using a three-pronged approach of host lock down, segmentation, and role-based access control.

Isolating/Ring Fencing Tier 1 Applications and Development Environments

With perimeter firewalls blind to over 80% of the hospital traffic within the data center, attackers stay under the radar while laterally moving from host to host.ColorTokens provides visibility to security teams that helps them either validate their controls or find controls that need to be further tightened (e.g., GPO policies). Security teams can ring fence groups of systems as large as an entire development environment or a single application, depending on their risk profile.

Legasy Systems Protection

Windows PCs or servers that are out of support can be critical to hospital operations, as they may be running critical applications. Hospitals looking to either support such applications for several years or decommission them in the future are at risk due to the vulnerabilities of these systems. ColorTokens provides a way to essentially ‘airgap’ legacy systems so that they cannot talk to servers in the data center.

Compliance

Several industry standards and compliance regulations require isolating systems that contain PII, PCI, or PHI data. ColorTokens collects detailed logs of every transaction on the network, providing auditors with the ability to validate conformance.

Third-Party Partner Protection

Hospitals require partners to connect to their networks and systems, often inheriting those partner organizations' cyber risk. While the hospital itself can't control their partner's security exposure, they can control their access to their own environment. ColorTokens doesn't put agents in a hospital's partner environment but can ensure that the assets they connect to only accept connectivity from the appropriate resources and users.

Making Zero Trust a reality, at scale

Without the right partner, the journey to zero trust can be incredibly difficult. In a recent survey conducted by Forrester on the state of zero trust [2], 83% of global large enterprises reported that they have committed their organizations to the adoption of zero trust. But a large majority don't know how to get started. And many organizations who started down the path have either deferred or abandoned the initiative.

Zero trust is a journey towards the goal of preventing data breaches and stopping cyberattacks from being successful by removing "trust" from digital systems. To enable this, ColorTokens has created a framework whereby security teams can make progress without burdening ancillary teams and disrupting business operations.

Some of our key innovations include:

Helping you get Started

- Automatically classify resources using attribute and tag discovery, programmatic tagging, and DevOps integration.
- Identify and visualize applications, 3rd party services (PaaS, SaaS, etc.), and data flows with detailed drill downs.
- Integrate with Active Directory and other SCIM-based identity providers to map user groups and data flows.

Achieving Progressive Enforcement

- Identify and lock down high-risk, unused ports and services.
- Define policies for Internet flows and enforce them while preserving internal communications.
- Create a comprehensive zero trust policy for internal, lateral (East-West) and user data flows.

Methodology for Success

- NIST Zero Trust Workflow in six implementation steps.
- Defined deployment process supported by a professional implementation team.
- Measurable security outcomes with defined metrics.

Maintaining Business Continuity

- Define policies and instantly view live simulation results without impacting users and applications.
- Enforce policies in “test mode” to measure performance and catalog any deviations prior to moving to production mode.
- Comprehensive role-based access and auditing to monitor and prevent unauthorized activity.

Expending Minimal Effort

- Zero trust makes the environment more resilient to cyberattacks and provides more time for analysis and remediation.
- Reduce alert fatigue by significantly reducing security events to the SIEM and SOC.
- Lower misconfiguration errors and troubleshooting calls due to centralized policy management with simulation and testing.

With a combination of agent/agentless, SaaS-delivered or on-premises deployment options, the ColorTokens unified zero trust microsegmentation and access platform enables organizations to deploy a zero-trust architecture via a modular and methodical approach.

[1] Journal of American Medical Association, Dec 29, 2022
[2] Forrester Security Survey 2022, Dec. 2022

Leading Cancer Center Selects ColorTokens to Strengthen its Cyber Resiliency and Reduce Risk

One of the leading, nationally ranked cancer and research centers in the U.S. with multiple data centers and campuses, witnessed an increase in ransomware attacks, specifically targeting backup administration control. With a network comprising of 10,000+ servers running a mix of modern and legacy applications, over 20,000 endpoints, and over 100+ petabytes of data, it had a clear need to control the processes during backup along with minimizing exposure to its environment.

The Challenges

- Secure its Epic system: The customer was using traditional tools (FW, ACLs) to secure its patient information and related systems. However, considering recent ransomware attacks, the customer wanted to adopt a zero-trust architecture to secure its patient data and systems. The customer had tried using virtual firewalls and found the process to be very time consuming, and it was looking for another approach.
- Safeguard legacy systems: The customer had numerous systems in the network that were no longer supported by the manufacturer, no patches were available, and hence these were left exposed to attacks.
- Block unauthorized traffic: over 60% of the healthcare provider's revenues are tied to its ability to perform diagnostic work in one department. The customer wanted to gain complete visibility into this application and quickly block un-authorized traffic without making significant changes to the network architecture.
- Limit lateral internal movement: Segment a flat data center network. With a flat network, even if one application is compromised it can be used as a launch pad to spread ransomware throughout the entire network.

Results and Benifits

> With ColorTokens Zero Trust solution, we were able to achieve the desired outcome we needed with surprising ease and zero disruption given the complexity of the task. This resulted in breaking down silos within our organization, creating agility, and driving decision-making using accurate data – we've seen amazing results with ColorTokens.
>
> Head of Infrastructure

About ColorTokens

ColorTokens is a leader in delivering innovative and award-winning cyber security solutions. It is a US corporation headquartered in Silicon Valley with offices in the US, the UK, Europe, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please go to **colortokens.com**