Solution Brief

PROTECTING HEALTHCARE ORGANIZATIONS FROM INTERNAL AND EXTERNAL CYBER THREATS

Secure medical records and research data for better patient engagement and stay ahead of competition
Secure Medical Records and Research Data for Better Patient Engagement and Stay Ahead of Competition

Overview

Hospitals and life science organizations are quickly evolving, due to the adoption of technological advancements. These advancements have led to widely used computer-based applications that manage an array of healthcare services that spam across hospitals, from admissions, discharges, transfer systems, various imaging systems, biomedical devices, diagnostic systems, robotic surgery, telemedicine, and laboratory systems. New frontiers of artificial intelligence, collaborative technologies, and predictive medicine are among the technological advances being rapidly adopted. While these advancements have significantly improved patient care, it also means that any vulnerability in the systems that support these technologies or malicious insider can compromise data integrity and disrupt patient care. Per a recent ransom-ware attack instance, the imaging servers were taken down, resulting in significant delays in critical patient care.

The cost of healthcare litigation has also become increasingly expensive, compelling healthcare providers to make investments in technologies to safeguard intellectual property and patient information. Per a recent survey conducted by the Ponemon Institute, the estimated cost of healthcare information is valued at $408/record – making it the highest across industries. With healthcare having the highest data breach costs, malware and insider attacks have become more rewarding in the healthcare industry as well. This ongoing struggle between patient engagement initiatives and securing medical data is giving healthcare security executives sleepless nights.

ColorTokens Unified Security Platform provides a software-defined security solution that takes a proactive approach towards security and assists healthcare executives in meeting compliance and audit standards. ColorTokens technology secures the vast computing infrastructure spread out across hospitals campus and the HIS workloads in the cloud data center against internal and external threats. ColorTokens Zero Trust architecture and intent-based security reduce CAPEX/OPEX by consolidating point security and point products.

Benefits:

- Provides an independent unified platform solution without any vendor lock-in headache
- Offers comprehensive security for both legacy and current endpoints, as well as for HIS applications in the data center
- Creates a Zero Trust network for securing electronic protected health information (ePHI), intellectual property and APT from healthcare malware and other unknown threats in compliance with HIPAA requirements
- Secures user, application workloads and endpoint without the need to invest in additional hardware
- Provides security posture visualization across applications, environments, workloads, users, and endpoints
- Protects even unsupported/unpatched medical legacy systems with signature-less endpoint security
- Provides rapid deployment in a matter of hours
| Security and Compliance Challenges in Healthcare |

- **Reactive Security**: Hospitals have a large number of interconnected devices, ranging from simple to highly sophisticated, mission-critical to patient-critical and from inexpensive to extremely expensive. Life science organizations and hospitals collaborate with universities, clinical research organizations, the pharmaceutical industry and medical experts across the world. Hospitals are increasingly adopting the cloud to share research information, store patient data and conduct routine business. The economic pressure due to rising healthcare costs is limiting the spending on IT security systems. In this environment, the IT infrastructure teams are forced to use multiple monitoring solutions resulting in a fragmented view of the hospital’s cybersecurity posture. These multiple monitoring systems generate a large number of false-positives events that need to triage. Unfortunately, the high costs of security systems and lack of budgets for them result in a reactive approach to security with a mentality that “Once breached, I’ll fix it, so it won’t happen again”.

- **Increasing Attack Surface**: A large number of hospitals are transforming to connected hospitals, primarily driven by two factors: (1) geographically spread hospital chains and (2) government funding for health information exchanges (HIE). Hospital in-patient care is extending from hospitals into long-term care organizations and home-care providers. This extension requires sharing of electronic medical record EMR between all of these entities for timely intervention to ensure that patients stay healthy and recover without being readmitted to the hospital after discharge. Modern multi-storied, multi-building hospital campuses are interconnected with complex wired, WI-FI and RFID networks. Personal mobile devices also access EMR for better patient engagements and staff efficiency. Data is even shared outside of the hospital environment for research and collaboration purposes. All these requirements result in an enormous attack surface where any leak point, whether malicious or by mistake, serves as an entry point for cyber-attacks.

- **Threats from Within**: Hospital staff and contractors need constant access to ePHI to do their job effectively. To gain access to this ePHI data, staff simply need to sign a release form in the hospital environment. There are very few ways to restrict who can see specified data inside a hospital environment which is further concerning. To compound this challenge, the processes for assigning access privileges are often ad hoc, and staff members continue to maintain their access privileges when they change departments. Contractors also often carry privileges even if they are not employed full time in the hospital. Further, staff or contractors may un-knowingly click on phishing emails that could act as an entry point to launch a cyber-attack. Healthcare providers need to continuously educate and train their personnel in cyber hygiene, which is time-consuming, expensive and still not 100% foolproof. As a result, it has become increasingly complicated for security teams to differentiate between malicious and legitimate users since not all threats are from rogue insiders or phishing attacks. Instead, simple human errors due to the complexity of network and security systems, e.g. misconfiguring an internal firewall, could leave applications in the data center exposed and vulnerable.

- **Vulnerable Endpoints**: Hospitals have hundreds of computer terminals used by their staff and third-party contractors. More and more medical devices are now Wi-Fi connected. However, most of these connected endpoints are vulnerable to internal and external cyber-attacks. The endpoints could be either un-patched legacy systems (thin terminals) or unsupported operating systems or applications.
Each of these poses a potential opportunity for a hacker to gain access to one or more hospital systems and spread laterally. All these endpoints are vulnerable to advanced persistent threats, malware, and ransomware. Many hospital systems worldwide get infected, spreading the malicious code to other endpoints across the network and eventually to the servers they are connected to.

**ColorTokens Healthcare Solution**

ColorTokens Unified Security Platform simplifies hospital and life science IT security and operations challenges. This solution locks down the endpoints and allows only “Known Good” applications to run, preventing any current or future threat from malware and ransomware through phishing attacks or malicious insiders. The networks are protected since only traffic from “Known Good” sources is allowed between endpoints and applications. “Known Bad” are prevented from execution and “Not Known” can be verified before allowing access. This activity is visible and controlled by a centralized control plane where visual representation makes it easy to see what is going on in the environment.

**ColorTokens Unified Threat Visibility and Analytics to Get Audit Ready**

ColorTokens provides micro visibility of computing assets which store, process and transmit ePHI information and their interaction with each other. Security operators can see all incoming and outgoing traffic across managed medical devices. ColorTokens provides holistic risk scoring built on a proprietary metric for critical resources. Risk mitigation strategies can be reviewed for impact on risk reduction prior to enforcement of the strategy. By reducing the risk score, the assets are better secured thereby aiding compliance and audit.

**ColorTokens Intent-Based Micro-Segmentation to Isolate ePHI, Intellectual Property and other High-value Assets**

ColorTokens visual policy authoring enables security administrators to isolate and control data flow, thereby fortifying critical healthcare applications. By securing point-to-point communication, ColorTokens product reduces the attack surface and blocks stealthy APT/lateral threats from propagating beyond the initial entry point. Micro-segmentation also reduces the scope of the audit, translating into cost savings.
Secure Medical Records and Research Data for Better Patient Engagement and Stay Ahead of Competition

Information security has become a boardroom discussion due to the frequency and sophistication of attacks, as well as the brand and revenue damage they can create. Healthcare providers, in their quest for modernization, should take a proactive approach to secure sensitive ePHI and intellectual property, irrespective of where that data is located. Healthcare providers may be short-staffed in IT or may lack the skilled personnel to protect the assets, but they must embrace a unified and platform agnostic security solution that will scale and grow along with their business. ColorTokens provides this solution and empowers healthcare providers through simplifying their digital transformation and security journey.

Conclusion

Information security has become a boardroom discussion due to the frequency and sophistication of attacks, as well as the brand and revenue damage they can create. Healthcare providers, in their quest for modernization, should take a proactive approach to secure sensitive ePHI and intellectual property, irrespective of where that data is located. Healthcare providers may be short-staffed in IT or may lack the skilled personnel to protect the assets, but they must embrace a unified and platform agnostic security solution that will scale and grow along with their business. ColorTokens provides this solution and empowers healthcare providers through simplifying their digital transformation and security journey.

About ColorTokens

ColorTokens is a Silicon Valley company, backed by legendary investors and advisors who have helped structure the IT industry over last 30+ years. ColorTokens core team brings deep and innovative industry experience from brands such as Cisco, Juniper, VMware, Microsoft, and Zscaler in domain areas including cybersecurity, networking, and infrastructure. With customers and partners worldwide, ColorTokens is headquartered in Santa Clara (Silicon Valley), CA, USA with a major center of development and sales in Bengaluru, India.

For more information about the ColorTokens solution email us at sales@colortokens.com
Call +1 (408) 341-6030 to speak to a ColorTokens security specialist.