Healthcare Should Leverage Unified Zero Trust Microsegmentation to Improve Security and Compliance

Healthcare organizations represent one of the most target-rich groups for cyberattacks due to the large amounts of personal data, which is highly valuable for criminal groups because they are easy prey. Additionally, they often aren't spending their security budgets on the right solutions or in an optimal manner, therefore making them an easy target for every type of cybercrime, from donation scams to ransomware attacks.

While cybersecurity is important to hospitals and other healthcare organizations, it's often not the highest priority. Typically, just enough security resources are applied to meet basic HIPAA compliance. When choosing between investing in security or new surgical equipment or research, the latter usually wins out.

As a result, IT teams face enormous security challenges, from ransomware attacks and data breaches, inability to secure legacy and unpatched endpoint systems, and ineffective risk prioritization, to compliance gaps and data theft by malicious insiders.

Consider the average cost of a healthcare breach in the U.S. is over $10M, according to **IBM's 2022 Cost of a Data Breach Report.** And this number has increased by over 42% in the past two years. In fact, the healthcare industry has had the highest average cost of a breach for 12 years in a row.

Healthcare organizations should focus on investing in managing the impact versus spending more on trying to prevent attacks from happening. A unified zero trust microsegmentation and access approach is an effective way to limit the scope, costs and complexities of security and compliance for healthcare organizations.

Protection and Compliance – key drivers for improving security

Protecting critical devices and data while meeting stringent HIPAA compliance requirements in healthcare can be enormously challenging for a multi-story and multi-building campus that has hundreds, even thousands of connected medical devices. Dozens of wi-fi zones and RF environments in connected hospitals pose significant security challenges. These locations also house vital assets, including electronic patient records (ex., EPIC systems), electronic protected health information (ePHI), healthcare information system (HIS) apps, Internet of Medical Things (IoMT) devices, and not to mention critical business and financial systems.

Additionally, cybercriminals profit from the life-and-death stakes in healthcare — making the sector especially promising for swift and lucrative ransomware payouts. As a result, bad actors are targeting IoMT and OT devices critical for patient care.

Unified zero trust microsegmentation and native access control can help keep medical devices secure, patient data safe, and enable healthcare providers to:

- Secure critical assets and services, even in the event of a breach, to ensure that access to any asset or application is secure and authenticated; this is achieved by granularly segmenting assets, environments, users, groups, and workloads.
- Stop the spread of ransomware across networks, data center servers and applications by shrinking the attack surface, restricting lateral movement, reducing the "blast radius," and automating workloads that block communications on any high-risk port.
- Realize comprehensive visibility across applications, devices, and networks by mapping the flows and communications between assets, including applications, medical devices, clouds, containers, data centers, and endpoints.
- Address HIPAA compliance requirements in three control categories and 21 sub requirements.

This unified approach reduces the attack surface while also reducing audit scope, cost, and management complexity, making the compliance audit process easier.

Conclusion: The healthcare industry faces strict compliance and regulatory requirements. Only a unified zero trust microsegmentation and secure, remote access control platform can help these organizations meet these requirements by enabling them to segregate sensitive data and enforce granular policies and access controls. As a result, they can demonstrate their commitment to protecting sensitive information and reduce the risk of non-compliance penalties.

A unified zero trust microsegmentation platform can help address 3 control categories and 21 sub requirements of HIPAA's privacy and security regulation

HIPAA Requirement	Sub Requirements Met w/Micro-segmentation and Remote Access	Example of How They Are Addressed
Administrative Controls (164.308)		
Security Management Process	164.308 (a)(1) 164.308 (a)(1)(ii)(A),(B),(D)	Map app flows, vulnerabilities and user access to get full view to cyber risk
Workforce Security	164.308 (a)(3) 164.308 (a)(3)(ii)(A),(B),(C)	Enforce policies to access healthcare apps based on roles and responsibilities
Information Access Management	164.308 (a)(4) 164.308 (a)(4)(ii)(A),(B),(C)	Access to apps based on network, user identity, and service
Security Awareness & Training	164.308 (a)(5) 164.308 (a)(5)(ii)(B),(C)	Allow only approved apps to run on workstations
Technical Controls (164.312)		
Access Control	164.312 (a)(1) 164.312 (a)(2)(i),(iii),(iv)	Provision to create unique user accounts and provide access to apps
Audit Controls	164.312 (b)	Network logs recorded with real-time/historical view to net comms
Person or Entity Authentication	164.312 (d)	Users can access apps only from authorized workstations
Transmission Security	164.312 (e)(1) 164.312 (e)(2)(i),(ii)	Enforce encryption and integrity for data transmitted
Physical Controls (164.310)		
Workstation Use	164.310 (b)	Use tags to identify workstations accessing ePHI

ColorTokens Inc. is a leading innovator in SaaS-based Zero Trust cybersecurity solutions providing global enterprises with a unique set of products and services for securing applications, data, and users across cloud and hybrid environments. Through its award-winning Xtended ZeroTrustTM Platform and context-aware machine learning-powered technologies, ColorTokens helps businesses accurately assess and improve their security posture dynamically. With a team of over 400 people, ColorTokens has global office locations in Santa Clara, California; New York; London; Copenhagen, Denmark; and Bengaluru, India. For more information, please visit **colortokens.com.**