Protecting Healthcare Organizations with Akamai Guardicore Segmentation

Cybersecurity for Healthcare
New technologies in healthcare offer life-critical services while improving treatment and patient care. However, their vulnerabilities are a target for malicious cyber activity. The healthcare industry experiences more breaches than any other sector, with hospitals accounting for **30% of all large** data breaches.

The causes for initial infection vary from credential stealing malware, malicious or non-malicious insider threat, or loss of computer devices.

Target: The Healthcare Sector
Personal Health Information (PHI), is personal health history, including but not limited to, ailments, illnesses, and surgeries. According to the **Center For Internet Security** (CIS), PHI has a high value on the black market. It can be leveraged in scams that take advantage of the victim's medical conditions or create fake insurance claims. ***It has been estimated that lost or stolen PHI may cost the US healthcare industry up to US $7 billion annually.***

Cybercriminals are more likely to target medical databases because they can be sure of the data's high value, whereas targeting credit information or social security numbers has become less lucrative.

A US government report has revealed the health care sector as the ***" sector worst-affected by data breaches".***

*According to the US Department of Health and Human Services' **2020 Healthcare Breach Report**, security incidents in hospitals and medical clinics resulted in* ***losses of $13 billion.***

Guardicore Helps Healthcare Organizations Defend Against Cyber Attacks
Akamai's Guardicore Segmentation (formerly Guardicore Centra) solution is relevant to every stage of dealing with an attack: From preparation to remediation and recovery.

Despite the best perimeter defenses, breaches are inevitable. This is why a defense strategy that minimizes the impact of an attack and stops the spread within your network is essential.

ordr MEDIGATE by Claroty ARMIS

Sensor-enabled interconnectivity in Health Delivery Organizations (HDO) enables efficient data collection and elevated patient care. Since it isn't possible to secure these devices with a typical endpoint agent, we recommend leveraging the integrated agentless security offerings from our IoT partners.

These solutions feed device information and risk scores into the Akamai Guardicore Segmentation platform, providing a single digestible interface for monitoring and securing all devices across your HDO environment.

KEY BENEFITS

Protect patients and their PHI data: by catching the attacker before they can extract patient records

Reduce costs: by avoiding third-party fees for investigations and incident analysis

Reduce time to detect, investigate and remediate attacks: with real-time breach detection and automatic trigger mitigation

Optimize resources: with automatic continuous monitoring of suspicious activity and automated analytic insights

Akamai Guardicore Segmentation provides visibility, breach detection, and response capabilities to catch and contain active breaches before they can do significant damage to the network.

- **Zero Trust Segmentation:** Ransomware attacks move laterally within the environment both before and after they begin encryption by taking advantage of inherent trust within the network. By leveraging Akamai Guardicore Segmentation, unnecessary connections both between and within network segments can be prevented, drastically reducing the risk and impact of ransomware.
- **Process-level Visibility:** A dynamic map of the network allows users to discover and track process-level activity across applications, allowing you to identify every application and asset running in your environment. This level of granular visibility allows you to quickly map critical assets, data, and backups to identify vulnerabilities and risks.
- **Real-time Breach Detection:** Instantly identify active breaches inside the data center to prevent propagating inside the network and minimize damage through both detection and high-interaction threat deception that lures attacks into an area where they can be contained and analyzed.
- **Automated Analytics:** Healthcare security teams often lack the necessary resources to manually investigate security incidents. Automated security analytics reduce false positives while providing comprehensive attack analysis. This includes detailed attacker footprints and discovery of all compromised assets, so security teams can quickly determine the right remediation measures.
- **Rapid Response:** Automated mitigation and remediation measures stop active breaches early in the kill chain for round-the-clock coverage. Automatic containment prevents breaches from spreading, while infected servers are quickly identified, isolated, and remediated.

Designed for the Modern Healthcare Data Center
As healthcare organizations embrace virtualization and cloud computing technologies, so must their security tools. Applications and data can reside almost anywhere, on any platform. Whether servers are virtualized or bare metal, or infrastructure is on-premises, in the cloud, or hybrid, Akamai Guardicore Segmentation offers protection across any environment.

Support for HIPAA Compliance
The Federal HIPAA Security Rule requires health service providers to protect electronic health records (EHR) using proper physical and electronic safeguards to ensure the safety of health information. Organizations are required to perform a risk assessment following any security incident that involves electronic patient records. The assessment is often a manual process using tools developed in-house, running the risk of erroneous findings.

With Akamai Guardicore Segmentation solution, organizations can determine the nature of an incident quickly and efficiently, using automation in a standardized approach.

The solution enables security teams to:

- Immediately distinguish real attacks from false positives
- Break down the attack footprint and determine the extent of damage, including whether data theft is the intent or has occurred
- Identify and quarantine all infected systems
- Generate analyses and reports to help determine the proper course of action

Protection across any complex environment.
Guardicore.com

About Akamai Guardicore
Akamai Guardicore Segmentation takes a simpler and more dynamic approach to security by using software-based microsegmentation. Akamai Guardicore Segmentation applies a policy of least-privilege to every enterprise data flow, ensuring only machines and software that are intended to communicate with each other can. This drastically reduces the threat surface, ultimately limiting the movement of malware through a system.