SOLUTION BRIEF

Guardicore

Data Center Security for Healthcare

The healthcare industry is witnessing a surge in data breaches. Some 65% of healthcare organizations said they were victims of network-borne security incidents over the past two years, and more than 120 million patient records were compromised in 2015 alone. This onslaught is taxing the resources of organizations that are constrained in their ability to detect, analyze and mitigate live attacks.

Healthcare providers are stepping up their investments in security measures to defend against this onslaught. However, conventional security strategies typically focus on prevention at the network perimeter, leaving a security gap in detecting breaches within the data centers where Protected Health Information (PHI) records reside.

Guardicore catches active breaches inside the data center in real time

Guardicore fills a critical gap in security infrastructures. Focusing on providing visibility, breach detection and response for east-west traffic between applications within the data center. The Guardicore solution foils intruders through an integrated approach encompassing:

Process-level Visibility: Guardicore discovers and tracks process-level activity across applications and correlates it with network events, providing a dynamic visual map of the entire data center network. It detects and reports on suspicious activity and incidents, providing the security administrator with a quick view of all workloads.

Real-time breach detection: Guardicore instantly identifies active breaches inside the data center including insiders, advanced persistent threats (APTs) and malware. It employs high-interaction threat deception, creating a target that lures attacks into an area where they can be contained and analyzed.

Automated analytics: With in-depth semantic analysis, Guardicore helps security analysts cover more ground, automatically confirming authentic attacks, analyzing the details of attack methods and identifying the attack footprint, providing the security team with clear intelligence to determine the right remediation measures.

Rapid response: Guardicore triggers automated mitigation and remediation measures to stop active breaches in progress early in the kill chain. Automatic containment prevents breaches from spreading, while infected servers are quickly identified for quarantine and rapid remediation.

Benefits

- **Protect your patients, their PHI data – and your reputation**
  Catch attacks early, before they can extract patient records, and minimize the damage.
- **Detect breaches faster**
  Avoid sifting through months of historical data to identify breaches and determine the damage.
- **Accelerate incident response**
  Identify the source of attack and attacker tools in real-time and automatically trigger response.
- **Reduce costs**
  Avoid paying thirdparty providers for incident analysis and investigations.
- **Empower security teams to “do more with less”**
  Automatic monitoring and analysis enables analysts to focus on legitimate security incidents.

"Data breaches in healthcare continue to put patient data at risk and are costly. Based on the results of this study, we estimate that data breaches could be costing the industry $6 billion."

- Ponemon Institute, Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2015

Know when you're being attacked – as it's happening

Many healthcare organizations know they are under attack, but lack the resources to ensure they can detect and respond to a breach fast enough. Guardicore helps healthcare security teams to do more with less by delivering a powerful combination of deep visibility and visualization of their data center applications and workloads with real time breach detection and response. Guardicore enables security teams to know what's going on in their data centers and, most importantly, know when they are being attacked.

Guardicore covers all data center traffic, but focuses investigations only on genuinely suspicious activity, reducing false positives and dramatically cutting the time it takes to detect, understand and respond to all types of breaches.

Designed for the modern healthcare data center

Healthcare organizations have been embracing virtualization and cloud computing technologies to improve the quality of and access to care while controlling costs. And many healthcare applications today use a hybrid architecture. This means that any security solution is going to need to support virtually any kind of data center infrastructure, as applications and data can reside almost anywhere, on any platform.

At Guardicore, we can protect virtually any healthcare data center environment, whether servers are virtualized or bare metal and whether the infrastructure is all on premises, 100% in the cloud, or hybrid. Guardicore is integrated with leading data center and cloud computing infrastructure technologies, including Software Defined Data Center controllers and orchestration components, network and server virtualization platforms, containers, network security and management.

Support for HIPAA compliance

Under the HIPAA Omnibus Final Rule, organizations are required to perform a risk assessment following any security incident that involves electronic patient records. Its purpose is to determine whether the incident is a breach requiring notification of patients affected and the Department of Health and Human Services. However, the assessment is often an ad hoc, manual process using tools developed in-house, running the risk of erroneous findings.

With Guardicore, 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 genuine 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.

About Guardicore

Guardicore is a leader in Internal Data Center Security and Breach Detection. Developed by the top cyber security experts in their field, Guardicore is changing the way organizations are fighting cyber attacks in their data centers.

More information is available at www.guardicore.com

Guardicore