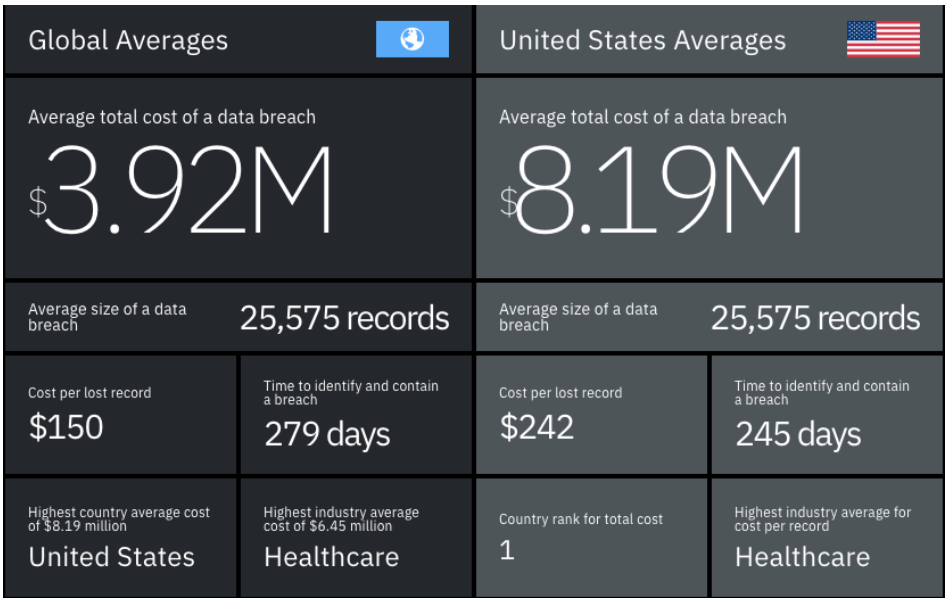
Seceon for Healthcare

Healthcare Industry Challenges

Healthcare providers operate under stifling regulations and within dedicated business processes. The healthcare industry is facing the growing challenges of today's cybersecurity environment with hospitals, nursing homes, clinics, and other healthcare providers being the valuable targets. Additionally, they have complicated infrastructure that's difficult to secure. According to the recent study "*2019 Cost of a Data Breach Report*" by *IBM Security and Ponemon Institute,*

- Healthcare organizations had the highest costs associated with data breaches at $6.45 million which is over 60 percent more than the global average of all industries.
- Data breach costs impact organizations for years after the incident. Healthcare organizations experienced higher than the average 3.9 percent rate of abnormal customer turnover.
- The lifecycle of a data breach grew noticeably by 4.9% in 2019. Healthcare took the most time of 329 days in the data breach lifecycle.



Source: IBM Security and Ponemon Institute 2019 Cost of a Data Breach Report

Top 5 Security Concerns in Healthcare Industry:

- Ransomware
- PHI/PII Data Exfiltration
- People (Insider Threats, Compromised Credentials)
- Unsecured and Unmanaged Legacy Devices
- IoT Exploits

Seceon Healthcare Solution

The main challenge with traditional point solutions is the residual vulnerabilities. Seceon aiSIEM Platform provides comprehensive coverage to proactively and fully protect you and your data. Furthermore, Seceon enables continuous compliance to help you comply with the regulatory compliance regulations.

With Seceon aiSIEM, the providers can enable large-scale and more robust data collection from cloud and other modern IT data sources, collect & analyze logs and data from networks & endpoints, incorporate threat intelligence feeds for correlation and enrichment, enhanced data analytics beyond rules, fast and scalable search over volumes of raw data and, most importantly, automated response.

Seceon Healthcare Use-Cases

Ransomware: In healthcare, ransomware accounted for more than 70% of all malware—"malicious software"—attacks, according to Verizon's 2019 Data Breach Investigation Report. Healthcare has been the number one targeted vertical for cybercrime since 2015. Ransomware attacks can come with a hefty price tag for their victims with hackers demanding large sums of money in exchange for decrypting an organization's computer files. These attacks hit critical medical systems like Electronic Health Records (EHR) or internet-connected medical devices bringing down hospital's IT systems and disrupting internal business processes. Seceon aiSIEM can detect ransomware at each stage of its development with unparalleled accuracy. The advanced correlation engine can help minimize the false positives, focus on real Ransomware attack and detect it at the earliest stage. The AI based actionable intelligence provides the recommendation to stop the attack and its proliferation. aiSIEM's auto remediation stops the threat before it causes irreparable damage.

Data Exfiltration (a.k.a. Data Raid, Theft, or Stealing): Attackers' primary goal is to go after Protected Health Information (PHI) and Personally Identifiable Information (PII) data since it's a high-value target. They consider healthcare providers with high volume of such important data as very lucrative targets. Some unexpected activities such as scans are always a pre-cursor to data exfiltration. Seceon aiSIEM can analyze security related data from multiple angles, such as, files, users, traffic, applications, and threat intelligence. It employs advanced machine learning and AI techniques to stay ahead of the attacker by continuously learning the context thoroughly and accurately with no pretext or presumptions. It proactively detects the data exfiltration and minimizes the damage by containing the attacker's actions as swiftly and as early as possible.

Insider Threats (Malicious Insider, Compromised Credentials, Privilege Misuse): According to 2019 Verizon Insider Threat Report, 46% of healthcare organizations were affected by insider threat in 2019 and is growing. Healthcare is the only industry where insiders were responsible for a higher percentage of breaches than external actors. Lack of employee education, unauthorized users and disgruntled employees present a serious security threat. The improper exposure of sensitive patient data can potentially put the entire business at risk with the regulatory liabilities. aiSIEM can detect the malicious insiders and compromised credentials to protect your PHI/PII data from unauthorized access by proactively detecting, eliminating and containing the bad actors in real-time.

Unsecured and Unmanaged Mobile Devices: Data breaches become more rampant with the use of mobile technology and unmanaged devices. The hackers steal patient records and information through the unsecured devices by installing malwares. Seceon aiSIEM can protect these mobile devices by detecting potential vulnerabilities on them as soon as the device is identified in its ecosystem. It can quarantine these devices in real-time within its ecosystem.

IoT Exploits: IoT plays a central role in digital healthcare ecosystem and its usage in healthcare industry is growing rapidly. The ecosystem includes: Patients & Healthcare Professional, Medical Devices, Surgical Robots, and Wearables & Wireless Sensors. Most of these devices have no inherent security exposing to several risks such as, Life & Death situations management, PII, PHI, Healthcare Delivery Process & 24x7 operations, and Healthcare Organization Viability. The type of IoT attacks include (but not limited to), IoT Botnet, IoT DDoS, Shadow IoT/Networks, Rogue Access Points, Airborne attacks via Bluetooth/ WIFI/ Other wireless protocol vulnerabilities, Air Gaped Devices, etc. Seceon aiSIEM helps with comprehensive visibility of all IoT interactions with context & situational awareness. It is an agentless solution best suited to protect IoT devices as they cannot be programmed to run agents. Built-in threat models driven by ML and AI are designed specifically to address IoT attacks in real-time with no additional operational expense to define rules and contains them through its built-in auto-remediation capability.

For more information and product demo, email to info@seceon.com

Seceon Inc., 238 Littleton Road, Westford MA 01886 USA | www.seceon.com | +1 (978) 923-0040 | © 2020