COMPLETE SECURITY, PRIVACY, AND COMPLIANCE PROTECTION FOR HEALTHCARE PROVIDERS

Protect patient data confidentiality and reduce the compliance cost and complexity associated with federal and state privacy laws, HIPAA, and other regulations through the automation of audits.

HP Enterprise Security Solutions Brief

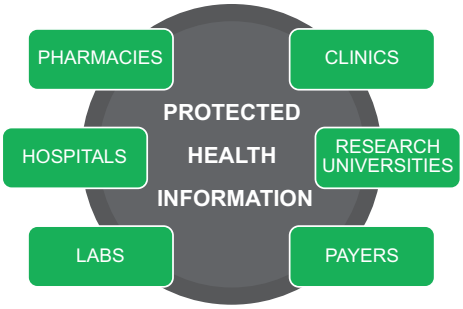
The HIPAA Act of 1996 has long emphasized the need for security and privacy of PHI (protected health information). Recent incidents of medical record breaches have further raised consumer awareness and regulatory oversight within the healthcare sector. In particular, state privacy laws and the ARRA-HITECH Act of 2009 have bolstered the objectives and the enforcement of HIPAA. These regulations also call for electronic health records (EHR) to reduce the administrative costs of delivering healthcare. However, along with the improvements in efficiency, electronic records have introduced greater accessibility and risk to patient data privacy.

As a result, healthcare institutions now face more PHI breaches, identity theft, frequent audits, and higher penalties for non-compliance, with the very real risk of civil lawsuits and potential loss of patient trust. Additionally these healthcare institutions are under significant consumer and governmental pressure to reduce the costs of healthcare. In response to these challenges, healthcare providers are investing in numerous security technologies, such as firewalls, encryption, provisioning, and identity management. While valuable, these investments further stretch limited IT security resources and provide only limited visibility into threats and breaches.

There is a clear need for visibility into all activities across users, applications, and data within provider networks. Automated and continuous monitoring of activities can address the goals of security and privacy, as well as meeting and demonstrating compliance. However, an effective monitoring solution must also address the unique challenges faced by healthcare providers.

Monitoring Challenges for Healthcare Providers

Monitoring healthcare provider networks for security threats and privacy violations is especially challenging because the processing of medical records spans a vast healthcare ecosystem including but not limited to hospital departments, insurers, clearinghouses, labs, clinics, consumers, governmental agencies, and research institutes.



This challenge is compounded by the numerous applications and users within any healthcare provider network. It is common for each department such as oncology, radiology, and billing to rely on a different application to support its unique requirements. Many providers are also launching online health and wellness patient portal applications which are targets of external attacks. Monitoring the spectrum of these applications and monitoring users including patients, physicians, nurses, contractors, and IT administrators for unauthorized access has become a significant challenge.

The open nature of hospitals introduces additional physical security threats by enabling easier network penetration and greater risk to the security and availability of hospital infrastructure, including critical and expensive medical equipment, pharmacy storage, research labs, etc. This makes physical infrastructure monitoring (badge readers, etc.) in context with network activity an important requirement.

In addition to medical records, healthcare providers need to protect many other kinds of data and comply with broader regulations. For example, most hospitals now accept credit card payments and therefore need to comply with the PCI Data

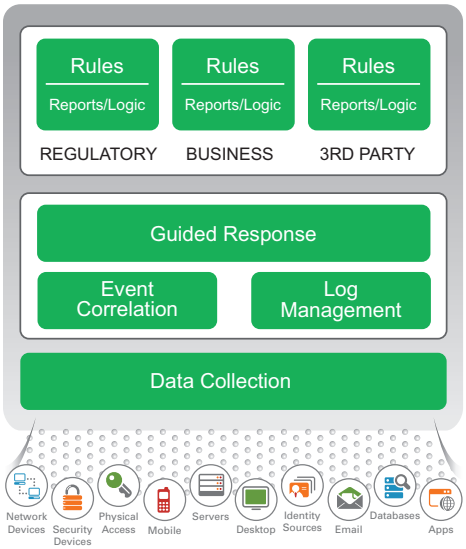
Security Standard. Similarly, healthcare providers that conduct research must also take adequate measures to protect against intellectual property theft.

The ArcSight SIEM Platform for Healthcare Providers

The ArcSight SIEM Platform for healthcare providers enables complete visibility into security threats and compliance violations through automated monitoring of all user, application, and system activity logs. The ArcSight SIEM Platform is used by leading healthcare providers as well as the United States Department of Health and Human Services which mandates HIPAA—to achieve the following goals and benefits:

- Reduce the cost of compliance with HIPAA, state privacy laws, PCI, and other regulations through automation of audits
- Protect proactively sensitive data such as PHI, PII, and R&D through continuous monitoring
- Eliminate expensive services by leveraging out-of-the-box best practices for security and compliance
- Mitigate the risk of non-compliance and disclosure along with associated fines, loss of customer trust, negative publicity, and class action lawsuits.
- Extract greater value from existing point security and identity-related IT investments
- Increase employee accountability of medical record access

The ArcSight SIEM Platform for healthcare providers is modular and can be deployed collectively or in phases.



Event Collection

ArcSight Connectors enable a non-intrusive approach for complete collection of all user, system, and application activity logs in provider networks. ArcSight Connectors provide extensive out-of-the-box support for physical devices, hosts, databases, security and network devices, as well as identity management sources. Additionally, ArcSight can easily be extended to collect logs from the wide array of applications common in hospitals and other provider networks such as Cerner, McKesson, GE, Siemens, Epic, and others. ArcSight Connectors normalize activity logs across sources into a common format, enabling simpler and faster monitoring.

Log Management

ArcSight Logger is designed to efficiently store, search, and report against large volumes of activity log data. A single appliance can efficiently store up to 35 TB of audit log trails in support of HIPAA, PCI, and other regulatory retention requirements. ArcSight Logger also enables rapid forensic searches to expedite breach investigations and comprehensive reporting to automate audit requirements for HIPAA, state privacy laws, PCI, and other regulations impacting healthcare providers.

Real-Time Correlation

ArcSight ESM delivers scalable, real-time correlation of logs across all systems, applications, and users for continuous detection of security threats and privacy violations in healthcare provider networks. Through a combination of trend analysis, statistical analysis, pattern discovery, and other techniques, ESM uniquely delivers an adaptive system that can detect both known and unknown threat vectors. ArcSight can also inject factors such asset criticality, user role, or user location to detect insider problems including unauthorized patient portal access and employee snooping. ArcSight ESM also offers tracking and escalation of threats along with inbuilt case management and workflow. Finally, as threats are detected, ESM supports a range of automated or approval-based remediation options.

Highlights

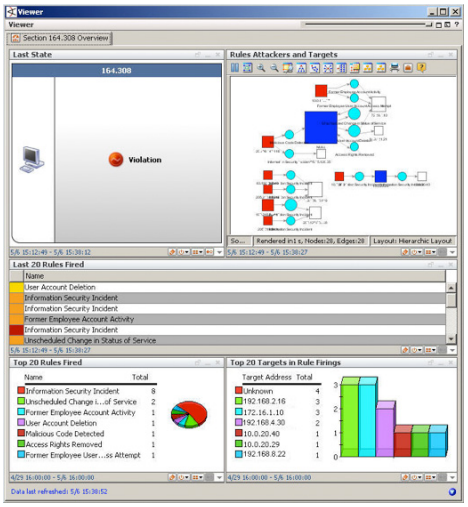
- Demonstrate compliance with HIPAA and state data breach laws
- Protect the integrity and confidentiality of PHI
- Reduce the risk of data breaches, negative publicity, and loss of patient trust

User Activity Monitoring

For threat detection, the ability to track activity back to users is critical, but logs often lack user context. Furthermore, a given user may have numerous identities across healthcare applications, making user-based analysis very challenging. ArcSight IdentityView is a specialized application that can associate users with network activity through a combination of session awareness and identity correlation. Through integration with leading identity management systems, ArcSight IdentityView enables detection of problems such as patient record snooping, identity theft, and medical data breaches by privileged users.

Compliance Insight Packages

ArcSight Compliance Insight Packages provide out-of-the-box monitoring reports mapped directly to the HIPAA Security Rule to automate and streamline compliance, while also reducing the need for in-house or third-party expertise. Providers subject to other regulations, such as Sarbanes-Oxley or PCI, can leverage similar focused-content packages to streamline cross-regulatory compliance efforts.



ESP-SLB017-080509-04, Created August 2011