FORNETIX

Ensuring Sensitive Health Data Is Protected Throughout the Healthcare Ecosystem

» HIGHLIGHT

Every industry is vulnerable to data breaches, but healthcare has long been particularly susceptible to attack because of how personal data is stored and transferred within the healthcare ecosystem. The rise in medically necessary embedded IoT devices and integration of third-party suppliers, have increased vulnerability. Now, bad actors have more attack surface area for disrupting the delivery of lifesaving health services, and negatively impacting patient care.

Fornetix® VaultCore™ provides a critical layer of protection for cloud-based patient care, ensuring personal data remains secure. VaultCore's centralized encryption key management command and control works across the entire ecosystem including connected devices, data in transit and data at rest. The secure communication policy deployment control and robust device authentication is proven effective at securing sensitive patient data and mitigating the interruption of lifesaving services.

» ABOUT FORNETIX

Fornetix, a pioneer in encryption key management, understands that securing data in today's complex environment can seem like an impossible task. VaultCore™, by Fornetix, is a patented solution designed to simplify the encryption key management lifecycle across the entire enterprise through automation and policy enforcement. Scalable to over 100 million keys for data storage environments including multi-cloud and hyperconverged infrastructures, VaultCore allows you to leverage existing technology investments and take complete ownership of your keys ensuring that critical data is safeguarded no matter where it resides.

FREE TRIAL: www.fornetix.com/freetrial
FREE DEMO: www.fornetix.com/demo

☎ **1-844-539-6724**

5123 Pegasus Court, Suite X
Frederick, MD 21704

» THE CHALLENGES

Medical records contain valuable and sensitive personal data including social security numbers, insurance information, payment details, health records, and more. According to Experian, each individual patient's full medical record can sell for up to $1,000 – an irresistible, lucrative target for any attacker willing to take the risk.

The large amount of valuable information being stored, transferred, and used between healthcare providers, patients, and third-party vendors is increasing. This is particularly true now as hospitals are stretched to capacity due to COVID-19. The sheer volume of patient data that is being processed moment to moment has created a weak, interconnected chain that is vulnerable to breach.

The rising complexity of hospital technology systems has escalated known vulnerabilities. Medically necessary IoT devices can and are being compromised by cyberattacks capable of disrupting the delivery of lifesaving health services. With the projected acceleration in modernization of embedded IoT interventions such as ventilation, IV pumps, robotics, and patient monitoring expected to grow exponentially, the consequences could be devastating if critical security measures are not in place.

By 2021, the number of connected medical devices requiring security hardening will increase by 45%

Reference: *Gartner Focus Now on Digital Security Opportunities Within Connected Medical Devices Published 7 January 2019*

PROTECTED HEALTH INFORMATION (PHI) RISKS

Between HIPAA compliance and other privacy regulations, the often overtaxed healthcare network security administrators are faced with the daunting task of protecting a broad range of sensitive data that must be stored, readily accessed by a diverse group of users, and securely sent across multiple devices and varying platforms all while satisfying regulations. Data usage and storage requirements create multiple endpoints. These endpoints combined with the high value of stolen PHI records have resulted in the industry experiencing persistent and highly sophisticated attacks on sensitive data.

THIRD-PARTY RISK

While each healthcare provider may feel confident in their internal security strategy, network attacks typically originate from smaller, third-party vendor systems where security may not be as robust. Awareness of all third-party vendor vulnerabilities is improbable, yet this lack of knowledge and overt control over vendors' network architectures – outside the walls of the healthcare facility – continues to hamper even the best security practices implemented by most care providers.

RISKS TO IOT AND CLOUD SECURITY

The interconnectedness of hospital operations and communications with wireless devices such as tablet PCs, PDAs, and portable laptops, combined with the rapid increase in adoption of IoT embedded medical devices like IV pumps, anesthesia, automated glucose monitoring devices, or even internet-connected robots used in surgery have left security network administrators struggling to not only protect PHI but also the welfare of their patients.

"At least 82 percent of connected medical devices have been targeted in the past year, opening the potential for a variety of attacks, from highly sensitive information disclosure to denial of service (DoS) for critical devices"

Xtelligent Healthcare Media Survey

© 2020 Fornetix

» THE SOLUTION

One of the best security practices for protecting health information includes managing encryption across the enterprise. This can be achieved by utilizing a key management solution like VaultCore™, that is KMIP (Key Management Interoperability Protocol) enabled. While most Healthcare Security Administrators are mindful of the latest advancements in encryption, historically, there has been a dangerous lack of attention to the requirements of managing hundreds of thousands of encryption keys that are needed to ensure protection of PHI, networking communication devices used within the facility, and the embedded IoT appliances critical to patient care. **The bottom line is that managing encryption across the whole healthcare enterprise is a complicated and daunting task and, in some cases, best security practices are overlooked or simply ignored.**

VAULTCORE PROVIDES SECURE EXTERNAL KEY MANAGEMENT THAT SUPPORTS WIDE SCALE PROTECTION

VaultCore is a groundbreaking, state of the art cybersecurity solution that simplifies encryption key management. It provides a single-pane-of-glass view and access for deploying automated processes and enforcing key management across an entire organization, including connected devices, and the supply chain. This unified, centralized approach to key management allows storage and control of all encryption keys in all environments, whether data is on premise, virtualized, in the cloud, or hybrid.

As sensitive PHI data is stored or transferred between providers and/or patients, it remains encrypted and only appears legible to authorized users. However, for encryption to remain effective, it requires regular rotation and management of the encryption keys. VaultCore provides full lifecycle key management. This means you have complete control to generate, register, store, distribute, install, use, rotate, backup, recover, revoke, suspend, or destroy keys. This unprecedented power ensures only keys that comply with the most recent policy are deployed, only to the appropriate devices, and are enforced accordingly to the most granular level. Automation and policy enforcement control can easily be exercised across all environments, providing the ultimate cyber defense protection through VaultCore's Mandatory Access Control (MAC).

CENTRALIZED CONTROL PANEL AND STREAMLINED REPORTING

Capable of working with legacy devices or integrating seamlessly with newer KMIP-enabled devices, VaultCore streamlines control, visibility, and reporting through a centralized control panel accessed via a simple web interface. Administrators have clear visibility of all encrypted devices and are provided signed, validated audit log information on key management and key consumption. Transparent reporting includes who accessed the key, the event time, and the success or failure of the operation. The hassles of collecting access reports, locating client credentials, and organizing data from multiple locations for compliance purposes or internal reporting become a thing of the past.

LIFECYCLE CERTIFICATE MANAGEMENT

Certificate management plays a crucial role in security. The typical healthcare organization spends millions per certificate outage. With VaultCore, the request or renewal, approval, generation and deployment, and usage and monitoring of certificates can all be automated with a set it-and-forget it approach. A one-time setup process is all you need to automate what is currently an extensive, manual process, often complicated by human errors.

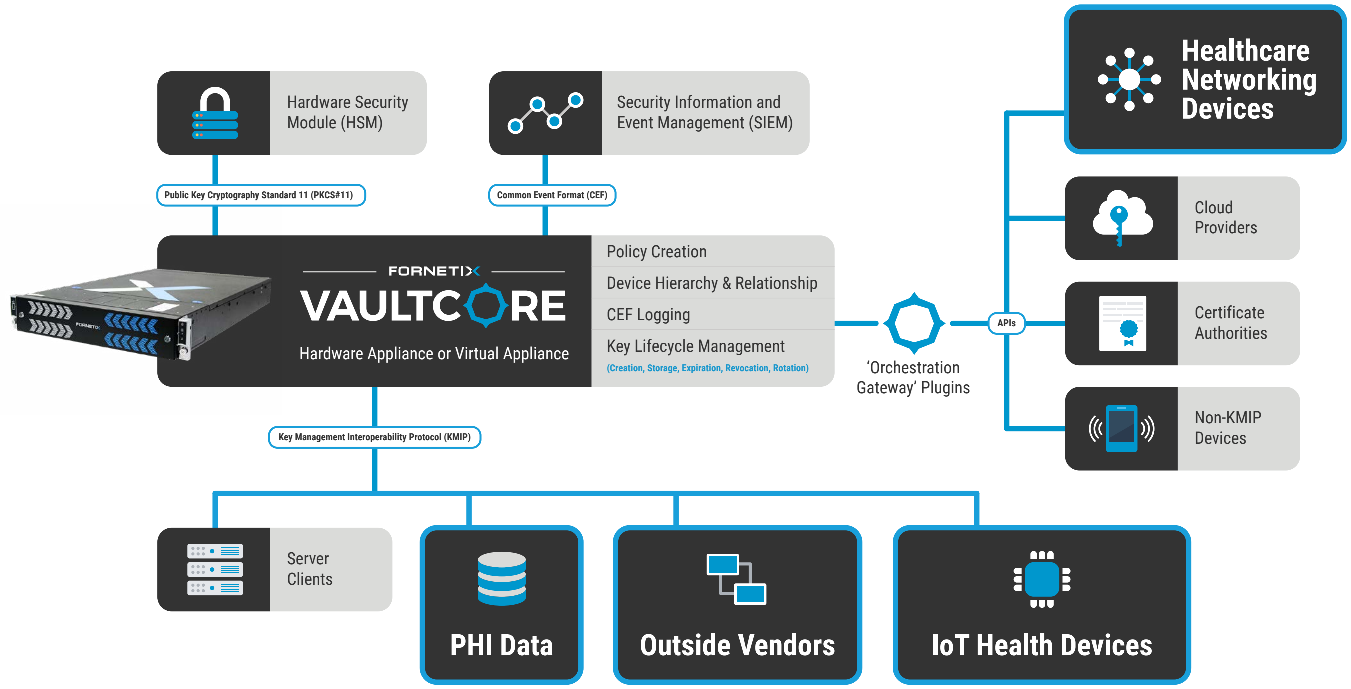
Delivered as a physical hardware or virtual appliance, VaultCore can also verify the cryptographic integrity of data to ensure critical code has not been tampered with between the facility and third-party vendors. This is a significant benefit in thwarting attack which can come from smaller, less secure partners. And with industry-leading capacity, VaultCore can manage over 100 million keys, more than adequate to serve the growing needs of the healthcare industry.

VAULTCORE = A RETURN ON YOUR SECURITY INVESTMENT

VaultCore is competitively priced and, on average, savings are recognized in two (2) years. With VaultCore, you're capable of setting a re-key schedule that matches your desired policy – an efficient approach – that ultimately saves tens of thousands of dollars (or more) by turning a manual process into a simple click of a button, removing known risks associated with human error, rotating keys, and deploying policy.

» SUMMARY

Securing sensitive data and patient care has become exponentially complex as the healthcare industry continues to migrate communications to wireless networks, store, and transfer the sensitive data of millions of patients, embrace modernization of IoT healthcare devices, and utilize third party vendors. As a result, security and risk management leaders struggle to support secure storage, access, and use of encrypted data while also meeting necessary speed, privacy, crypto-agility, HIPAA compliance, and business needs. Fornetix's VaultCore provides a simple and powerful, cost efficient solution that works with existing investments. It is also scalable to meet the growing demands of the healthcare industry through an enterprise level key management system capable of protecting both PHI and patient care.


Hardware Security Module (HSM)
Security Information and Event Management (SIEM)
Healthcare Networking Devices
Public Key Cryptography Standard 11 (PKCS#11)
Common Event Format (CEF)
Cloud Providers
FORNETIX
VAULTCORE
Hardware Appliance or Virtual Appliance
Policy Creation
Device Hierarchy & Relationship
CEF Logging
Key Lifecycle Management
(Creation, Storage, Expiration, Revocation, Rotation)
'Orchestration Gateway' Plugins
APIs
Certificate Authorities
Non-KMIP Devices
Key Management Interoperability Protocol (KMIP)
Server Clients
PHI Data
Outside Vendors
IoT Health Devices

© 2020 Fornetix