aria CYBERSECURITY SOLUTIONS

APPLICATION NOTE

A Modern HSM for Enterprise-wide Data Encryption in the Healthcare Industry

Today, healthcare organizations are notoriously vulnerable to network-borne cyberattacks, including ransomware, malware, and data exfiltration. These attacks are becoming more frequent, increasingly sophisticated, and nearly impossible to detect. A successful attack can result in crippled operations, loss of data such as ePHI, and significant HIPAA fines.

Given healthcare's level of importance to society, it's important to understand why the healthcare industry is especially prone—and vulnerable—to cyberattacks:

- **A mix of environments and technologies result in applications being difficult to secure**: Today, most healthcare organizations have a broad threat surface, which is difficult to protect against intrusions and exfiltrations using traditional processes and tools. Additionally, they heavily rely on virtual machine (VM) environments, and are usually looking for ways to keep costs down, rather than increasing security and IT budgets.
- **Lack of security professionals and resources**: Many healthcare organizations simply don't have the teams or the expertise needed to perform effective threat detection and response. Even with adequate staffing, the typical investigative methods are not effective. Detailed understanding into how to architect, deploy, and optimize the most effective methods to protect data have been well beyond the capabilities of all but the largest organizations.
- **Past challenges protecting patient records and related personal data**: Healthcare organizations are under increasing scrutiny due to the large numbers of breaches of ePHI information over the past few years, breaches that have exposed nearly one half of all American's records. Due to high costs and complexity, encryption of such data has not been a prevalent practice in the healthcare industry. However, the surge in HIPAA privacy violations and a renewed industry focus on requiring conformance with the NIST Cybersecurity framework has put new pressure on healthcare organizations to examine how to best protect such data.

In March 2019, Columbia Surgical announced that a ransomware attack led to the compromise of **40,000** patient records, and in February 2020, PIH Health suffered the compromise of nearly **200,000** personally identifiable information (PII records) after a successful phishing campaign aimed at employee accounts.

Data security issues in the healthcare industry

How is encryption used in healthcare organizations? One common approach is to deploy a hardware security module (HSM), a physical appliance attached to the network that generates encryption keys and performs encryption/decryption functions. Data as generated/manipulated by healthcare applications is sent across the network to be encrypted before being returned and stored. These “black box” HSMs need to have secured rack space and be properly networked to avoid latency that can lead to application performance degradation.

The largest concern is the fact that traditional HSMs require specialized expertise to set up properly with the applications they are to perform the encryption operations for. The professional services needed to deploy these systems and the need to continuously engage with such experts every time the applications are updated can be extensive.

Additionally, there are known security vulnerabilities inherent in the Intel x86 chip architecture, which can be challenging for those looking for strong encryption techniques while running the encryption applications right on the host. The applications must run the keys in the clear when encrypting the data. Storing encryption keys in the open on an x86 host leaves them open to exposure if the server is hacked.

Finally, healthcare organizations have become increasingly porous, making them a high value/easy target for cyber attacks. A large number of devices are now networked, everything from the HVAC systems to medical equipment, devices, and patient IoT devices. Most of these don’t allow adequate security on the device and make them a target for hackers to use as an entry point into the healthcare network. As a result, healthcare organizations are one of the most successfully breached in the industry, and the reason for the need to protect critical information and patient data.

The solution: ARIA microHSM

The ARIA microHSM device, running the SvKMS application from StorMagic, is an ideal key encryption solution for healthcare providers. It delivers true plug-and-play enterprise-wide encryption using a low-cost approach that solves the challenges detailed above.

The ARIA microHSM is a SmartNIC-based HSM that is deployable in any standard PCIe slot found in commercial servers. Locating the key encryption functionality in-server, but off of the motherboard, offers several benefits:

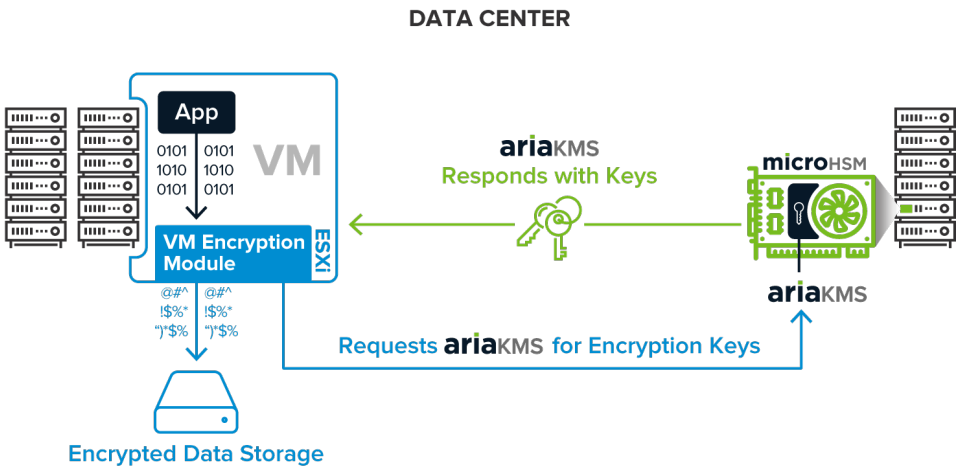
- The first is that it eliminates the need for a costly, standalone HSM appliance that consumes rack space.
- This also reduces power draw, improves application performance, and is deployable in a few minutes by untrained IT personnel, without the need to be re-tuned anytime there is a healthcare application update.
- The ability to locate the microHSM locally within the servers running the critical applications makes it much easier to plan for and then add such capabilities with higher reliability rather than rely on a networked standalone appliance.

The ARIA MicroHSM can be used in two types of encryption applications:

1. The first is most prevalent—it allows keys to be securely served into VMware's secure environment. This allows the data being produced and manipulated to be encrypted by the virtual machine before it is sent to data storage. Unique keys can be generated by ARIA microHSM on a per-application instance basis. This works for both local storage of data or for storing data on vSANs. Keys can be sent securely, locally across the PCIe Bus, to that server's virtual machines (VM), or out the SmartNIC's interfaces to other network connected VMs. High Availability is achieved by installing a cluster of just two or three ARIA microHSM devices which will assure keys are served properly to each VM.

   Key management is a strong suit of ARIA microHSM, as the proper keys need to be stored on it to be used as needed by the VMs to decrypt data. Data that has been stored for many months, or years, must have its proper keys securely archived. The ARIA microHSM provides this function.

   Best of all, this approach achieves the desirable separation of the key serving and management infrastructure, dictated as best practice by the industry, from the healthcare applications and VM environment. The svKMS also offers "Bring Your Own Key" (BYOK) support to send keys securely anywhere needed from the ARIA microHSM locally or even into public cloud infrastructure environments to encrypted those VMs or to provide the keys to be used by AWS, Azure, or Google Cloud Platform.

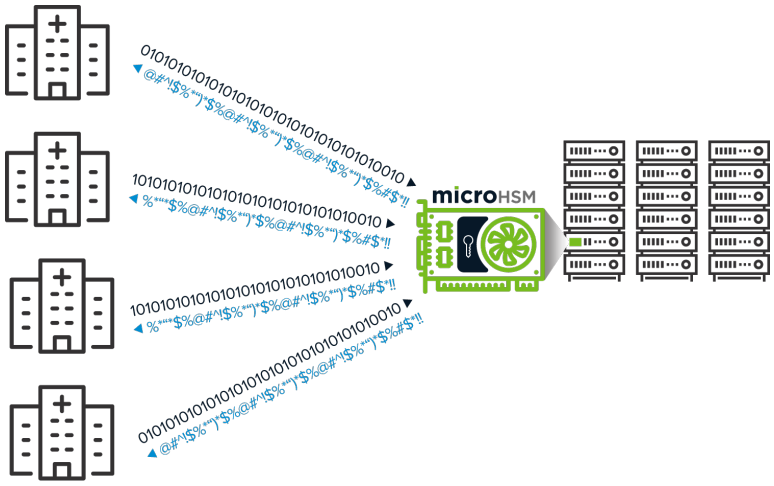


2. For other environments, the ARIA microHSM not only generates the keys but uses them to encrypt the data sent from the applications themselves. Using open industry-standard KMIP, it can communicate with compatible applications to perform encryption functions. This approach achieves the highest level of security as the encryption functions are all performed locally, but off the motherboard so that they can not be accessed if the server is breached.

The ARIA microHSM utilizes TrustZone on its ARM cores to shield the keys if the server is hacked. The ARIA microHSM offers high-availability, and performance as multiple SmartNICs can be deployed as needed, and it is also FIPS 140-2 level one compliant.

The Perfect HSM for the Healthcare Industry

In summary, the most significant benefit of the microHSM is the ease of deployment, set-up, and maintenance. It is a turn-key solution that plugs into existing servers and doesn't require any specialized tuning.ARIA microHSM is a low-cost fool-proof way for healthcare organizations--or companies in any industry—to adopt, deploy and manage encryption functions, to secure their critical data.



Critical Benefits of ARIA microHSM

- Can be installed in any standard PCIe server in minutes
- The simplest most secure approach to adding encryption capabilities to health care applications in any environment
- The industry's most flexible, but secure key management handling capabilities
- Open standard KMIP encryption with a large ecosystem of KMIP-capable applications
- FIPS 140-2 Level 1 compliance
- Provides plug-and-play high availability capabilities, unlike configurations available from legacy platforms
- Provides the lowest total cost means of adding and maintaining encryption functions

StorMagic

Contact Us Today: ARIAsales@ariacybersecurity.com or 800.325.3110

ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. Our solutions provide new ways to monitor all internal network traffic, while capturing and feeding the right data to existing security tools to improve threat detection and surgically disrupt intrusions. Customers in a range of industries rely on our solutions each and every day to accelerate incident response, automate breach detection, and protect their most critical assets and applications. With a proven track record supporting the Department of Defense and many intelligence agencies in their war on terror, and an award-winning portfolio of security solutions, ARIA Cybersecurity Solutions is committed to leading the way in cybersecurity success.

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA O1854

Connect with Us: ariacybersecurity.com • ARIAsales@ariacybersecurity.com • 800.325.3110

Follow Us: Linkedin • Facebook • Twitter • Blog

aria CYBERSECURITY SOLUTIONS ariaSDS nVoy SECURITY APPLIANCES Myricom NETWORK ADAPTERS