



Data Security Through Hardware-Based Encryption

SENSITIVE RECORDS EXPOSED**In the United States in 2016**

2016 set an all-time high in the number of data breaches according to the Identity Theft Resource Center.

4,281,000,000



Whether at rest on a server or in transit, our data is vulnerable to an increasingly diverse and sophisticated set of cyber threats.

INTRODUCING ENCRYPTION

With the growing online footprint that has become nearly unavoidable in everyday life, both corporations and individuals find more of their most sensitive information at risk than ever before. Whether at rest on a server or in transit, our data is vulnerable to an increasingly diverse and sophisticated set of cyber threats. The best counter to these threats is a method of enciphering data into an unreadable format by using encryption. Just as enterprise organizations spend vast amounts of resources on their products and services, they should also be investing in sophisticated encryption to prevent data breaches and the loss of sensitive information.



While the methods and mechanics behind encryption have no doubt changed over the centuries, the basic principle of the practice remains the same. Today, corporations can look to dedicated encryption devices, known as hardware security modules (HSMs), to provide all the encryption power needed to encrypt data traversing their network.

Futurex, a company with over 40 years of experience in data security, offers an advanced line of HSMs, key and certificate management solutions, and other encryption devices, all of which combine to form the Hardened Enterprise Security Platform. Futurex believes in a comprehensive approach to data security and incorporates common coding across their entire product line which allows for easy expansion and integration of Futurex products and services.

Futurex also provides a technology foundation to VirtuCrypt, a provider of cloud-based data security and cryptographic solutions. VirtuCrypt powers their cloud services with Futurex HSMs, which allows them to offer the power of hardened encryption to organizations that lack the resources or desire to maintain their own dedicated encryption hardware.

THE ROLE OF HSMs AND KEY & CERTIFICATE MANAGERS

Encryption was born out of a need to obscure sensitive data to the eyes of everyone except its intended recipient. While the methods of data transit have rapidly changed in the centuries since encryption was first used, the essential need to protect sensitive information has remained the same and encryption is still the most reliable method of doing so. Today, more and more companies look to new forms of automation and network connectivity to decrease operating costs and increase efficiency. Additionally, as more web-enabled devices join the ever-growing internet of things, the government, private organizations, and individual consumers find more of their sensitive data in transit than ever before.

At its core, encryption is a method of using algorithms to render data indecipherable to anyone without the correct encryption key, which is needed to decrypt the data into a readable form. Some organizations, especially those relatively new to encryption-based data security, see software-based encryption as the easiest, most accessible option. Software encryption uses computer applications, which require encryption keys to be physically typed into the computer to encrypt data. The downfall of software-based encryption is that it is only as secure as the system the software resides on and the security protocols used by those who input the keys. Simple keylogging software or a malware attack could potentially provide an unauthorized user with the encryption keys needed to decrypt an entire database of encrypted data.

HARDWARE-BASED ENCRYPTION

01


Hardware-Based Security
Cryptographic hardware represents the gold standard for data security.

Hardware-based encryption, using a dedicated cryptographic device known as a Hardware Security Modules (HSM), is the true “gold standard” for encryption-based data security. An HSM isolates the cryptographic processes onto a separate device, dedicated solely to encryption. HSMs are outfitted with a variety of environmental, logical, and physical security measures that not only make any physical tampering evident to the system administrators, but also delete any sensitive information if a tamper attempt occurs.

HARDWARE SECURITY MODULE

02


Hardware Security Module
Dedicated encryption hardware adhering to rigorous security standards

Another key benefit of HSMs not to be overlooked is compliance. HSMs typically fall under government regulations and must adhere to a variety of security standards. These standards require that these devices meet certain criteria established in the Federal Information Processing Standards (FIPS), the Payment Card Industry Data Security Standard, and various other regulatory bodies depending on the industry. The combination of physical barriers combined with compliant procedures make HSMs the most secure method of data encryption.

03



Enterprise Key & Certificate Management

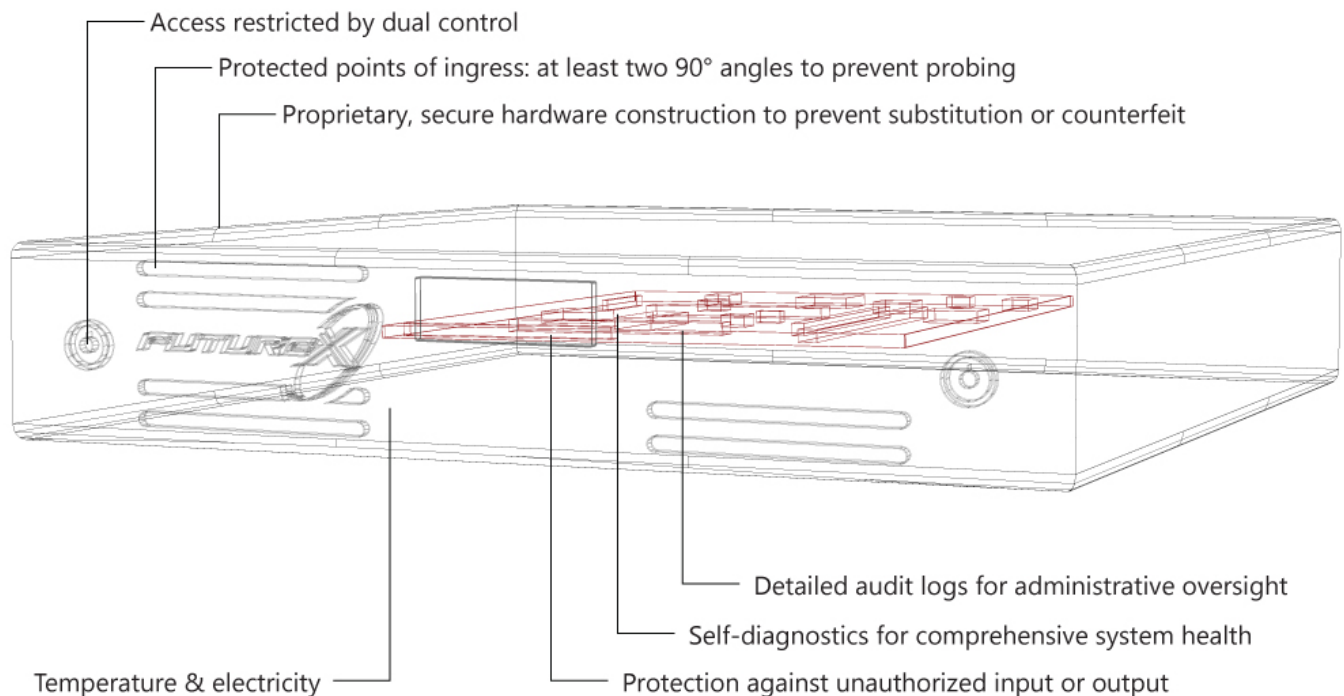
Full lifecycle key and certificate administration

One of the main cryptographic applications within the HSM is key and certificate management for Public Key Infrastructures. In terms of key management, the HSM is tasked with compliantly managing the encryption key throughout the key's lifecycle. This includes creating, managing, storing, distributing, and retiring keys. Sophisticated key management solutions are essential to any cryptographic operation because encrypted information is only as secure as the encryption keys. If the keys are compromised, then so is the encrypted data.

Certificate management is equally important. Just as individual users must verify their identities through passwords, smart cards, biometrics, and other methods, each networked device and user must also be verified using a digital certificate. Through a process known as certificate management, the HSM creates and issues a unique private key to for each user and device involved in the exchange of encrypted information. This private key is used as a digital certificate, which allows for mutual authentication among the various devices and users on an encrypted Public Key Infrastructure (PKI) network.

Hardware Security Module

Physical Security



Environmental Security

Logical Security

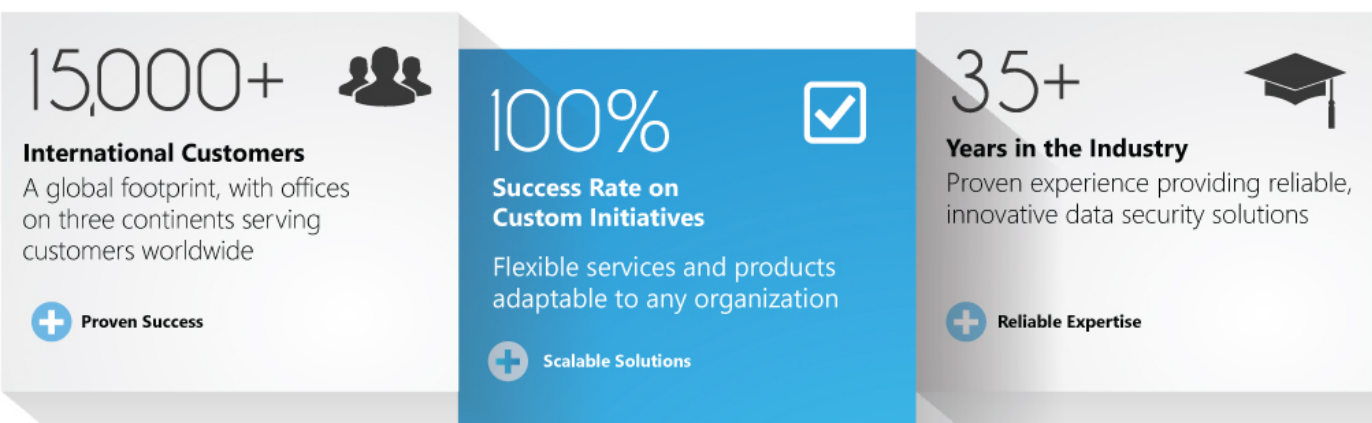
HOW FUTUREX SOLUTIONS FIT INTO THE DATA SECURITY LANDSCAPE

Futurex offers a variety of hardware-based data encryption devices, including HSMs, key management servers, crypto management technology, and secure storage solutions. Furthermore, what truly sets Futurex's Hardened Enterprise Security Platform apart from its competitors is the flexibility and scalability made possible by the Base Architecture Model shared across all devices.



The Base Architecture Model is a common code and functionality base that all Futurex devices operate from. This common code base allows for a high level of scalability and easy integration of new devices, which makes it easier for organizations to expand or reconfigure their cryptographic infrastructure as their needs grow. Additionally, the Base Architecture Model streamlines the process for firmware upgrades, system updates, and various functionality improvements, vastly reducing burdens on systems administrators. A single update can be pushed to all Futurex devices in a network, as opposed to updating the devices individually.

The diverse capabilities of Futurex's HSMs, along with the Base Architecture Model, assures that Futurex will be your first and last stop for encryption hardware. This offers your system architects and administrators the peace of mind in knowing that when they build a cryptographic production environment around Futurex's Hardened Security Platform, any additional Futurex products, now or in the future, will seamlessly integrate with their current Futurex hardware. When working with Futurex, your business will never need to overhaul or restructure your system in order to increase processing power, storage, or functionality.



HOW VIRTUCRYPT SOLUTIONS FIT INTO THE DATA SECURITY LANDSCAPE



New **Heights** in Enterprise Cryptography

While hardware-based encryption is the most secure, the most reliable, and the most compliant, it can also require a certain amount of expertise and time commitment to maintain. VirtuCrypt, however, provides another option. VirtuCrypt is a compliant, cloud-based cryptographic security service powered by Futurex hardware. VirtuCrypt customers can receive all of the security and compliance benefits of having their own dedicated cryptographic infrastructure, while never having to set foot in a data center.

Whether your organization maintains their own data center or rents rack space, maintaining cryptographic hardware can require significant resources. Furthermore, depending on your organization's security protocol, key holders will have to make periodic trips to the data center to upload new keys and perform other administrative functions. When using VirtuCrypt, the data center is maintained and audited for compliance for you, however you still have 24-hour access to your network through the VirtuCrypt Intelligence Portal (VIP) Dashboard. The VIP Dashboard is a web-based application that allows customers to connect to and manage their cryptographic infrastructure from their own computer, phone, tablet, or any other web-capable device.

Additionally, VirtuCrypt is customizable and flexible enough to fit the unique need of any organization. It comes complete with a full range of whitelabeling options and a robust API, which allows for organizations to integrate VirtuCrypt into their existing applications while maintaining their own visual branding.

VirtuCrypt tiers its offerings into three categories of services. VirtuCrypt Enterprise offers a comprehensive cryptographic service for organizations in need of large-scale security solutions. For those who only wish to implement certain functions through VirtuCrypt, VirtuCrypt Elements offers companies specific purpose functionality. Lastly, VirtuCrypt Plus offers a combined solution for organizations who own Futurex Hardened Enterprise Security Platform devices. This allows them to enhance the performance of their on-premises physical devices with cloud functionality from VirtuCrypt.

VirtuCrypt Plus was born out of a growing demand for a combined security approach that brings together both hardware and cloud-based security solutions. Large organizations, especially government organizations, find themselves in control of more proprietary data than ever before. This has led to a rise in demand for Crypto as a Service (CaaS). With CaaS, organizations can maintain their most sensitive data on their own devices, but can use cloud-based solutions to provide cryptographic applications for that data.



Many organizations simply prefer to own and physically oversee their own HSMs, but they also seek the accessibility and convenience of the cloud. VirtuCrypt Plus offers companies the ability to remotely monitor and view analytics or overall system health on their physical hardware using the VIP Dashboard. VirtuCrypt Plus also offers the ability to use the cloud to augment the scalability of their physical devices, or provide an off-site disaster recovery solution.



Futurex Engineering Campus

OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163