Enterprise Strategy Group by TechTarget

SHOWCASE

OCTOBER 2023

How an HSM Provides a Secure Foundation for PKI and Data Security

Jack Poller, Senior Analyst

Abstract: As data has become ubiquitous within organizations, it has spread to the cloud, SaaS applications, data warehouses, relational databases, and more. Public key infrastructure (PKI) technology provides strong identities to users, network devices, and applications to protect sensitive data. However, organizations that try to manage their own cryptographic keys face many challenges, exposing them to risk. Hardware security modules (HSMs) offer organizations a secure root of trust for critical signing keys, based on a certified and protected hardware environment.

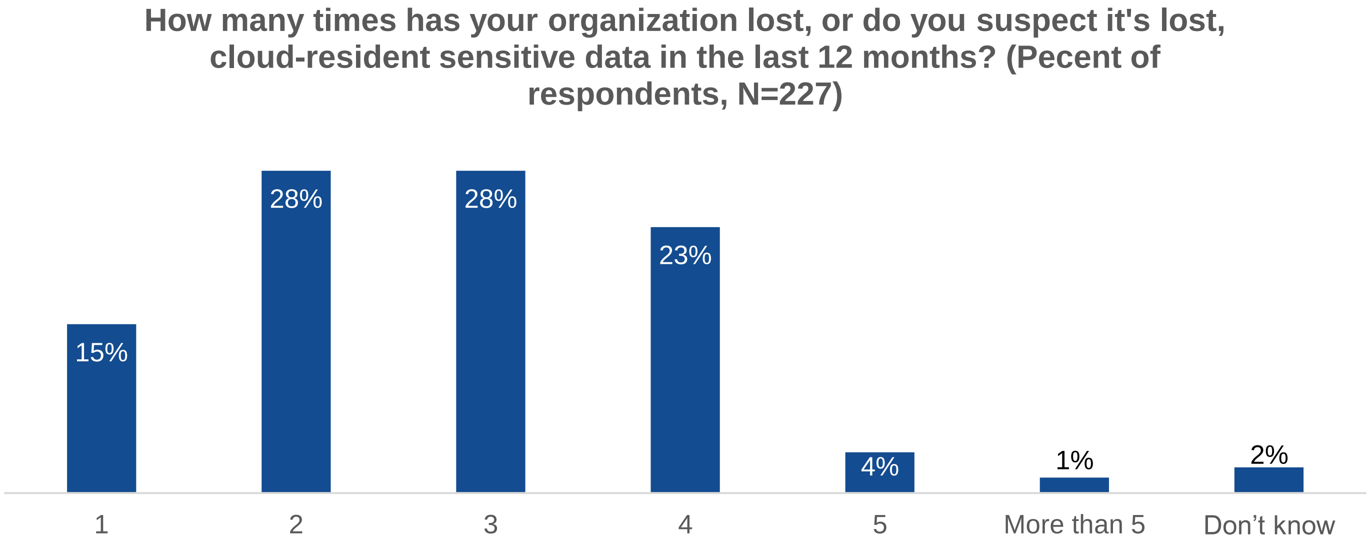
Protecting Data Is a Fundamental Concern for Businesses Today

Companies inevitably collect and create sensitive data as a part of doing business and data has become ubiquitous within organizations. According to research conducted by TechTarget's Enterprise Strategy Group, 86% of survey respondents say they have sensitive data stored within a data lake, data warehouse, or data lakehouse. Thirty-two percent say that sensitive data is critical to the business, and another 64% say the data is important to the business.[1]

Business data creates value by helping organizations find trends, better serve customers, measure business goals, and increase operational efficiency. However, sensitive data carries risks. Losing sensitive data can lead to regulatory penalties, damaged reputations, and lawsuits, proving costly to the short- and long-term health of the business. Despite the need to protect sensitive data, many organizations struggle to do so. Fifty-nine percent of companies surveyed suspect or know they've lost data from the cloud. Of those, 84% indicate they've had multiple data loss events in the past 12 months (see Figure 1). Businesses need help to protect their data.

[1] Source: Enterprise Strategy Group Complete Survey Results, *The Cloud Data Security Imperative*, April 2023. All Enterprise Strategy Group research references are from this survey results set.

Figure 1. Multiple Data Loss Events Are the Norm



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Businesses Turn to Encryption to Protect Their Data—With More Challenges

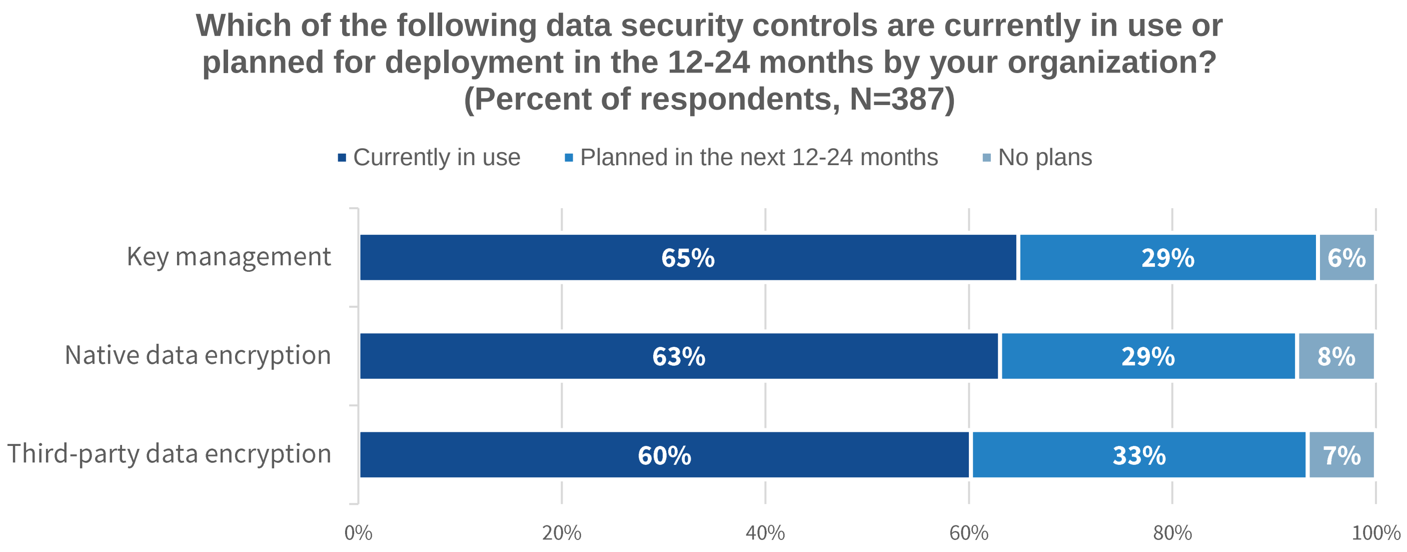
Public key cryptography has become a foundational technology, widely used to establish and verify identities of network users and devices and to protect the confidentiality and integrity of data in storage and transit within and across enterprises. The technology works by using a public/private key pair to sign digital certificates and encrypt data. This enables the issuance and validation of identities for enhanced authentication of users and systems and for the signing of documents and messages to attest to their integrity, authenticity, and provenance.

Public key cryptography depends on two critical components:

- A secure set of keys that sign the root certificate, proving the provenance of any digital certificates or identities created using that certificate. It’s like the signet ring of an ancient king, used to securely seal official documents and prove their authenticity.
- A key-management program to create, sign, revoke, rotate, and delete keys and certificates securely within a managed lifecycle.

Root keys underpin the security of the PKI and therefore must be given the highest level of protection to ensure the trust of the derived signing and encryption mechanisms used across the enterprise. Organizations may try to deploy a heterogeneous encryption strategy, including key management, sometimes using cloud key management services, as well as native data encryption (i.e., built-in encryption within vendor software) and third-party data encryption (i.e., using third-party services). According to Enterprise Strategy Group research, 65% of survey respondents are using key management to protect their data, with another 29% planning to take it on in the next 12-24 months (see Figure 2). Native data encryption and third-party data encryption were also cited by the majority as key initiatives now and in the future.

Figure 2. Use of Encryption Technology



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Some organizations take a “best tool for the job” approach, while others may organically create such an environment through departments that choose their own solutions for the problem. However, this strategy can lead to increased complexity and risk, as each solution requires its own keys, certificates, policies, and processes.

To combat this, some organizations create their own PKI for use by internal and third-party applications, where applicable, to provide greater control and define the security environment that best suits their needs. However, in the process, they also increase their burden and risk.

The critical keys used to sign the root certificate must be protected and managed. Stolen certificate-signing private keys or root keys enable malicious attackers to create forged certificates, granting them privileges and access to practically any data they want. Once discovered, all existing certificates must be revoked and reissued. When companies deploy new applications, mismanagement of certificate creation processes can lead to application downtime and business impact. Therefore, it’s important to consider how certificate encryption keys are being generated, safeguarded, and managed throughout their lifecycle.

Strong authentication and controls need to exist within the PKI to prevent misuse of the certificate authority (CA) and to make sure only those authorized can create root signing certificates. In addition to CA root keys, signing keys used for the certificate issuance process, as well as keys used for the certificate revocation process, need to be protected to prevent attackers from forging issued certificates and revocation lists. Protecting these PKI keys is also critical to safeguard against potential attacks that can compromise the PKI and lead to disruptions and outages.

Hardware Security Modules Provide the Needed Protection

Since all encrypted sensitive data depends on the keys used to sign the root and issuance certificates and revocation lists, the keys themselves have become the most important asset to protect. If an organization’s systems are compromised by an attacker, software-based encryption keys could easily be found and exposed. Further, malicious insiders could also compromise keys that are protected via software. Designed specifically for the purpose of generating and safeguarding critical cryptographic keys, HSMs provide the extra layer of protection needed to help ensure keys and the data they protect are kept secure.

HSMs provide practical benefits. The hardware device delivers a robust random number generation capability—a critical component of secure cryptographic key creation. Keys are stored within tamper-resistant hardware boundaries, out of sight from attackers that could easily detect keys in software registries. HSMs are designed and optimized to create robust keys quickly and securely. To ensure that no single individual or entity can subvert their operation, dual controls are also typically employed. As the linchpin for security, leading HSMs are independently validated and certified to be secure according to industry standards by internationally recognized bodies such as the US National Institute of Standards and Technology and the EU Common Criteria.

Introducing Entrust nShield HSMs

Entrust nShield HSMs are specifically designed to establish a root of trust, safeguarding and managing cryptographic keys and processes within a certified hardware environment. They provide enhanced key generation, signing, and encryption to protect sensitive data and transactions.

Entrust nShield HSMs are offered as an appliance deployed at an on-premises data center or leased through an as-a-service subscription. Entrust nShield as a Service is available across fully redundant data centers in Germany, the U.K., the U.S., and Australia. nShield HSMs are certified under Federal Information Processing Standard (FIPS) 140-2 and are undergoing certification to the new 140-3 standard; Common Criteria Evaluation Assurance Level (EAL) 4+; electronic identification, authentication, and trust services (eIDAS); and Singapore National IT Evaluation Scheme (NITES).

Entrust nShield Security World key management architecture enables organizations to combine different nShield HSMs to build a unified ecosystem that delivers scalability, seamless failover, and load balancing. Organizations can combine an on-premises HSM with nShield as a Service to extend their HSM capabilities in the cloud. This hybrid deployment model avoids additional Capex investment, while reducing data center footprint and the need for additional skilled resources.

Organizations that want to retain control, including the backup, of their cryptographic keys while using cloud provider services may consider adopting the bring your own key (BYOK) approach. With this method keys can be generated by an organization under their governance, assured in the provenance and veracity of the keys, and then securely exported to the cloud provider for use. nShield Cloud Integration Option Pack offers support for this method for the major cloud service providers. Customers leveraging the many services offered by the cloud service providers while seeking maximum control of their keys may wish to adopt the Hold Your Own Key (HYOK) approach. With HYOK, keys are always retained by the organization and never exposed to the cloud service provider. AWS, Google, and Microsoft all offer HYOK capabilities, which are supported by nShield HSMs.

Conclusion

Businesses inevitably collect and store sensitive data while doing their day-to-day work, whether that data belongs to their employees or to their customers. This data must be protected to prevent data breaches, which lead to regulatory penalties, lawsuits, loss of stock market value, and lost customer confidence.

Companies have turned to public key cryptography to help protect critical data and systems. PKIs provide the framework to create and sign certificates, which are then used to encrypt data, sign documents and messages to attest to their integrity and authenticity, or provide enhanced authentication for users and systems. Companies that choose to create an internal PKI face the challenge of managing the keys used to sign the root and issuance certificates and revocation lists, which provide the root of trust for all data and applications. Storing such keys in software exposes them to compromise if an attacker gains access to the network. Hardware security modules provide the means to protect these keys in a secure hardware environment.

Entrust nShield HSMs offer a protected, certified environment companies can use to establish a root of trust, safeguarding and managing cryptographic keys and processes. The HSMs are offered as an appliance or through an as-a-service subscription with fully redundant data centers across the world. Additionally, nShield Security World enables organizations to combine different HSMs, such as those on premises and in the cloud, to build a unified view of all keys with scalability, failover, and load balancing.

Enterprise Strategy Group believes the security of PKIs relies on best practices. The use of certified HSMs like Entrust nShield enables organizations to protect their PKIs from compromise in a world where data protection is core to business success.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

✉ contact@esg-global.com
🖥 www.esg-global.com