The Importance of Effective Encryption Management Across Network Boundaries

PROTECTING YOUR DATA WHEN YOU CAN'T PROTECT THE NETWORK

Chuck White
Chief Technology Officer

Extending the Protection Chain Across Multiple Perimeters

> *In recent years, the development of weapon systems and execution of service contracts have required multiple tiers of contractors performing work. This presents a distributed computing environment composed of multiple network perimeters. Security technology and solution providers continue to place an outdated emphasis on the perimeter instead of focusing security efforts down to a more granular scale and protecting what is actually valuable – sensitive data itself.*

With network boundaries becoming more skewed every day, protecting network architecture is no longer enough. The United States government must also protect against vulnerabilities and threats that exist outside of local networks – specifically, those that exist within the networks of partner nations and contractors. In modern networks, assets are regularly transferred from one organization to another where they can be exposed to threats in environments outside the data owner's control.

Breaches associated with the F-22, F-35, and other national programs are attributed to hostile foreign actors exploiting weaknesses across contractors and partner countries to access sensitive information. In almost all of these cases, attackers leveraged spear phishing and other user-initiated attacks to breach network perimeters, access other networks through trusted connections, and exfiltrate sensitive information. In other words, when multiple security perimeters are responsible for safeguarding sensitive data, the entire protection chain can be compromised by attacking a single link.

Protecting the Jewels by Incorporating Encryption and Access Control

Despite being useful in some security planning approaches, traditional network security concepts such as *defense in depth*, *perimeter protection*, and *dwell time* don't address specifics based on what is *valuable* to an organization.

Whether it's healthcare, financials, television shows, or military secrets, the access to valuable data must be governed by security concepts and metrics. Mechanisms must be implemented to protect the full breadth of an organization, from core to perimeter and even remote cloud resources. This begins with encryption and access control.

> *By determining what is valuable to a given organization and modeling the impact of compromises, there is an opportunity to assess security metrics based on actual impact rather than simple perimeter breaches and dwell times. In this revised model, security effectiveness becomes a decision based not on breach duration, but rather the effective time of protection provided by the controls securing any compromised information.*

Defense in Depth
A layering tactic that defends a system from attack using several independent methods.

Perimeter Protection
Refers to systems like routers and firewalls designed to tightly control access to networks from outside sources.

Dwell Time
The amount of time an attacker is able to act unchecked on a network or resource after the initial compromise or unauthorized access.

In the realm of cyber threats today, a consistent method of implementing security controls that protect critical resources across all links in a supply chain is needed to achieve a useful and practical defense.

For the sake of consistency, the lowest common denominator for systems security is encryption. Encryption impacts information security consistently by making information inaccessible without the appropriate key material. Key Management impacts the consistency and accessibility of encryption by providing a reliable source of key material delivered over a secure channel. Thus, a breach of any type and any duration becomes inconsequential so long as key material is consistently and safely protected.

With encryption comes the need to manage these keys to ensure that the key lifecycle is aligned with the content lifecycle. Additionally the implementation of Key Management introduces another logical step in regards to accessing information – adding complexity and increasing risk of exposure for a given breach. In a distributed supply chain, effective key management becomes an exercise in standards, such as Key Management Interoperability Protocol (KMIP), which allows for predictable behavior over known communications channels.

The responsibility of implementing and maintaining an encryption management strategy should be owned by the primary owner of the supply chain. In the case of the United States Government, responsibility for an encryption management strategy belongs to the government while authority can be delegated to Prime Contractors. The encryption management strategy must account for encryption use, secure key distribution, and effective key management across each link. In the case of a major weapon system such as the F-35 Joint Strike Fighter, the strategy from this point should take the distinct components of the chain into account, assuming that a prime contractor does not have the direct jurisdiction to control all aspects of perimeter security of its subcontractors. This effectively moves multiple steps beyond simple Digital Rights Management as orchestrated encryption and encryption management can support multiple methods of data-at-rest and data-in-motion encryption.

The strategy of consistently encrypting sensitive data shrinks the cross-section of vulnerable material to merely the keys themselves. What has an attacker gained if they have access to encrypted data but do not have the keys to decrypt it? They may as well have copied random static.

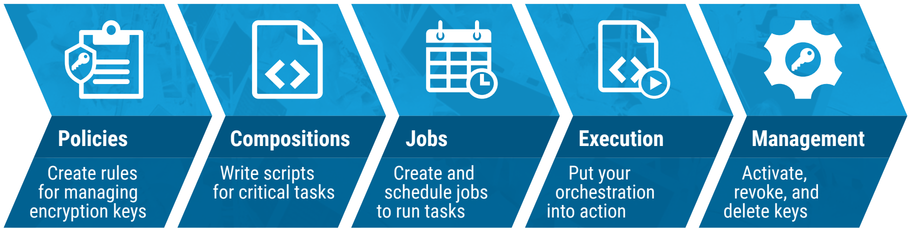
Thanks to their nature and size, keys are much easier to sequester than entire troves of data. Four things must be considered to make this effective:

1. Key Discretion

Discrete keys should be employed with as much granularity as the enterprise can manage. Is it better to encrypt an enterprise with one key set? Or, does it make sense to have a more granular approach based on systems component, classification, or location? Or, is a file or object-based approach more logical? Historically, manually-intensive Key Management techniques have limited the feasibility of highly-granular data encryption schemes. The use of single, long-lasting keys for large amounts of data suffered from a “keys to the kingdom” vulnerability. In the modern enterprise, new tools that are automated and policy-based can greatly improve the segmentation of data for discrete encryption.

2. Key Distribution

Key distribution has also been a difficult problem in the past. Specifically, the ability to deliver symmetric keys quickly and securely has proven daunting. Wide scale adoption of standards such as KMIP coupled with storage and authentication techniques for key protection communicating over TLS and other encapsulated key delivery mechanisms have alleviated most of this difficulty.


Policies
Create rules for managing encryption keys
Compositions
Write scripts for critical tasks
Jobs
Create and schedule jobs to run tasks
Execution
Put your orchestration into action
Management
Activate, revoke, and delete keys

Key lifecycle management workflow as part of Fornetix VaultCore.

3. Secure Key Storage

Key storage was once an intractable problem because keys are digital data and commonly stored in places that were vulnerable to attack themselves. Fortunately for most applications in the modern world, this problem has almost completely disappeared thanks to the rise and relative ubiquity of Hardware Security Modules (HSMs), Trusted Platform Modules (TPMs), and other dedicated cryptographic hardware components.

4. Key Lifecycle Management

The more keys are used, the higher the odds an attacker will find a way to compromise them. Using a single set of keys across a highly-dispersed environment can provide ample opportunity for successful attacks. Like granularity, the rotation of keys increases the complexity of key management exponentially. Manual techniques employed for decades cannot keep pace with increased encryption usage and prevent crypto administrators from effectively rotating keys regularly.

With the release of innovative new tools comes the ability to rapidly implement policy-based automation that can immediately provide the security-enhancing key lifecycle management so desperately needed by many organizations today.

Encryption Is the Lowest Common Denominator

Encryption and encryption key management form the lowest common denominators for production chain security. With proper encryption key management, content itself becomes less accessible as the keys change more frequently, regardless of the health and security of the overall enterprise.

Let’s consider an alternative scenario where Acme, a United States defense contractor implemented a production chain security strategy powered by encryption key management to protect the development of a next-generation anvil launcher:

Acme implements standards-based Encryption Key Management and provides a common software platform to their production chain, allowing for data-in-motion and data-at-rest encryption with short-life periodic key rotations. The key management system is tied to identity services, applications, and storage services used in development of the anvil launcher. This enables the release of encryption keys to process information for engineers, testers, machinists, procurement specialists, facility security officers, program managers, and others. Acme now has the visibility into when keys are created and requested, and has control over key rotations as governed by their policies, standards, and guidelines.

With the above in mind, even when the Krasnovians breach the perimeter of an Acme subcontractor, the Krasnovian attempts to access content now also require key material centrally controlled by Acme.

Let’s assume the Krasnovians obtain a credential that allows resource access to the anvil launcher development file system. After grabbing files, they hit their first problem: the files are encrypted. Furthermore, even if it is an insider attack and the Krasnovians recruited a spy who was an Acme employee who walked out the office with drives in hand, they are still encrypted.

This means the Krasnovians now have to pivot to a new attack vector and attempt to request that the Key Manager release the appropriate keys associated with the anvil launcher. This requires access to the Key Manager which is under Acme’s direct control and initiates a Mutual TLS request to the Key Manager. This leads to yet another pivot to attempt accessing Client TLS credentials, which may be stored on smart cards or other physical tokens rendering them completely inaccessible.

Each pivot executed by the Krasnovians increase the complexity of the attack. It increases the risk of discovery and counter-attack by requiring simultaneous access to more systems which are even more secure than the last. The situation becomes critical for the attacker as the Key Manager reports requests for key material to monitoring systems such as Security Information and Event Management (SIEM) providers.

When Acme notices the unusual activity from one of their subcontractors' networks, they can now temporarily or permanently disable access to the relevant encryption keys while the United States government confronts the intruder. The US may even use Acme's anvils in the response.

This ultimately gives the Krasnovians a harsh choice: Leave with unreadable data or risk discovery as they try to retrieve keys. The "easy" target is now virtually unassailable.

It becomes readily apparent that a protection-centric approach, bolstered by modern encryption technology, is the cost-effective and simple answer to truly successful information security.

Reducing Incident Frequency is Tough, Reducing Impact Doesn't Have to Be

In conclusion, encryption key management provides a consistent platform for extending the reach of encryption services and reporting information based on encryption use. Addressing the overall security of a supply or distribution chain with automated, policy-based key management tools allows for massive reductions to the impact of even the most complete network security breach.

How VaultCore™ by Fornetix® Can Help

Fornetix is helping organizations unleash the full potential of encryption by conquering the key management bottleneck. Our US-made VaultCore ecosystem automates the key lifecycle across the entire enterprise with groundbreaking precision and speed.

As global use of encryption rapidly expands, you can be prepared for the future with unparalleled scalability. Our commitment to standards-based interoperability ensures your existing investments in encryption are fully realized and will continue to integrate seamlessly as your organization grows. Policy-driven automation of the key rotation lifecycle reduces human error and empowers your organization to remain secure and avoid costly data breaches.

If you're ready to orchestrate your encryption key management, we'd love to hear from you. Please call 1-844-539-6724 or visit www.fornetix.com for more information.

Find Out More About Fornetix

Fornetix.com

Facebook.com/fornetix

Twitter.com/fornetix

Linkedin.com/company/fornetix

☎ **1-844-539-6724**

5728 Industry Lane
Frederick, MD 21704