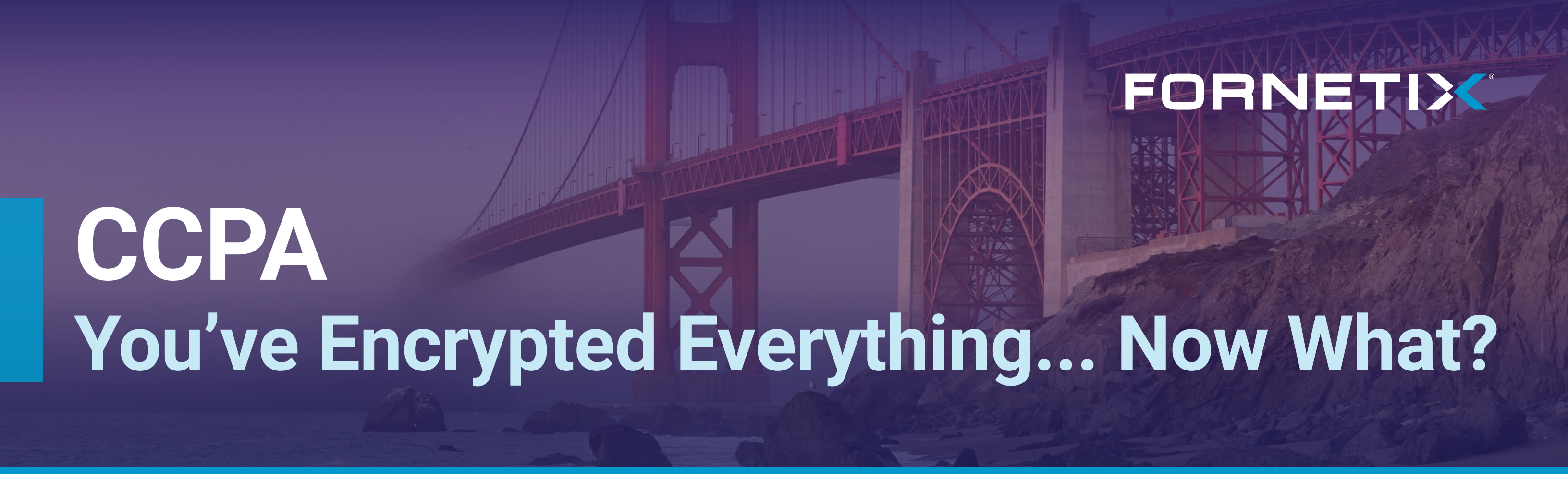


FORNETIX

CCPA
You’ve Encrypted Everything... Now What?

» HIGHLIGHT

The California Consumer Privacy Act (CCPA) aimed at securing sensitive consumer data from theft and misuse went into effect January 1, 2020. The Act’s stringent obligations, if not met, carry hefty per-name penalties starting at $2,500 per name, and as high as $7,500 if found “intentionally” in violation of the Act. At the core of CCPA is an organization’s responsibility to encrypt sensitive data, which has led organizations across the globe to ramp up encryption of their data at rest, in motion, and in the cloud.

» ABOUT FORNETIX

Fornetix’s VaultCore is helping organizations across the globe unleash the full potential of encryption by conquering the key management challenge and working to secure some of the world’s most vital secrets by automating the key lifecycle from enterprise to edge with groundbreaking precision, speed, and accuracy.

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

☎ 1-844-539-6724

5728 Industry Lane
Frederick, MD 21704

Encryption Key Management Is Saving Companies Struggling with California Consumer Privacy Act (CCPA)

» THE CHALLENGES

The encryption necessary to meet CCPA and adequately protect consumer data moves beyond generalized server-level encryption to include a more granular level of encryption down to the file level. This overall positive step in data security has had the unintended consequence of producing thousands or even millions of encryptions keys, that when left unmanaged or mismanaged, are leaving organizations and their data increasingly vulnerable to attack.

The more keys that are used, the higher the odds an attacker will find a way to compromise them. Just like passwords on our computers, encryption keys must be rotated as frequently as possible. The rotation of keys increases the complexity and expense of encryption and key management exponentially but greatly decreases the probability of a successful attack on your data.

For many organizations, CCPA has inadvertently created more key material than can adequately and successfully be managed without a dedicated key management solution. This has left organizations struggling to effectively protect their customer’s data and balance the burden of costs necessary to protect their customer’s data.

CCPA COVERS THE FOLLOWING PERSONAL DATA:

- Identifiers such as real name, alias, postal address, email address, IP address, and more
- Personal and commercial behaviors, as well as inferences from them
- Characteristics protected under California or federal law
- Commercial info including purchase records, personal property, and buying behavior
- Biometric information and geolocation data
- Internet and other network activity such as browsing and search history
- Professional, employment, or educated related information
- Audio, electronic, visual, thermal, olfactory, or similar information
- Inferences drawn from any of the above

> “Ultimately, protecting someone else’s data protects all of us.”
>
> *Tim Cook, CEO of Apple*

» THE SOLUTION

Historically, organizations have viewed key management as daunting and as a result have thrown additional manpower at the problem in an effort to manage it. Unfortunately, with the growth in regulations such as GDPR (General Data Protection Regulation), CCPA, and others, organizations are quickly realizing this mismanagement results in higher overhead costs and an increased risk from inevitable human errors. However, thanks to VaultCore™ by Fornetix, this antiquated approach is no longer necessary. Our modernized and compliant solution provides safer data, less chance for error, ***and*** a decrease in spend.

VaultCore is a patented, state-of-the-art, unified encryption key management system that gives organizations the power to meet the latest best practices in data security and help ensure CCPA regulations are met through:

1. Simpler, Enhanced Protection of Data

VaultCore's Mandatory Access Controls (MAC) provide a unique, hybrid combination of Attribute-Based Access Controls (ABAC) and Role-Based Access Controls (RBAC). This simpler, centralized approach to key management enables organizations to fully control their key life-cycle operations – generate, register, store, distribute, install, use, rotate, backup, recover, revoke, suspend, or even destroy keys – with extreme policy granularity.
This unprecedented power over the key lifecycle can be completely automated, and policy enforcement control can easily be exercised across all environments including storage, applications, virtualization, networks, and cloud services, providing the ultimate cyber defense to meet the stringent CCPA and truly protect personal data.

2. Separating Keys From the Data

This security best practice makes clear the need to separate encryptions keys from the device where the data resides. VaultCore works by enforcing separation of key material from the data source and further restricting access to the keys by providing an independent, reliable source for delivering key material over a secure channel. Incorporating VaultCore renders most any breach of any duration inconsequential and leaves the attackers with nothing more than gibberish instead of your valuable data.

3. Centralized Control and Streamlined Reporting

VaultCore streamlines audit reporting with a centralized control panel accessed via a simple web interface. Administrators have clear visibility of all encrypted devices utilizing KMIP, and are provided signed, validated audit log information on key management and key consumption. These logs include who accessed the key, the event time, and the success or failure of the operation. The hassles of collecting access reports, locating credentials, and organizing reporting from multiple locations become a thing of the past.

4. Positive ROI

With VaultCore, you're capable of setting a re-key schedule that matches your organization's desired policy – a simple "set it and forget it" 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.

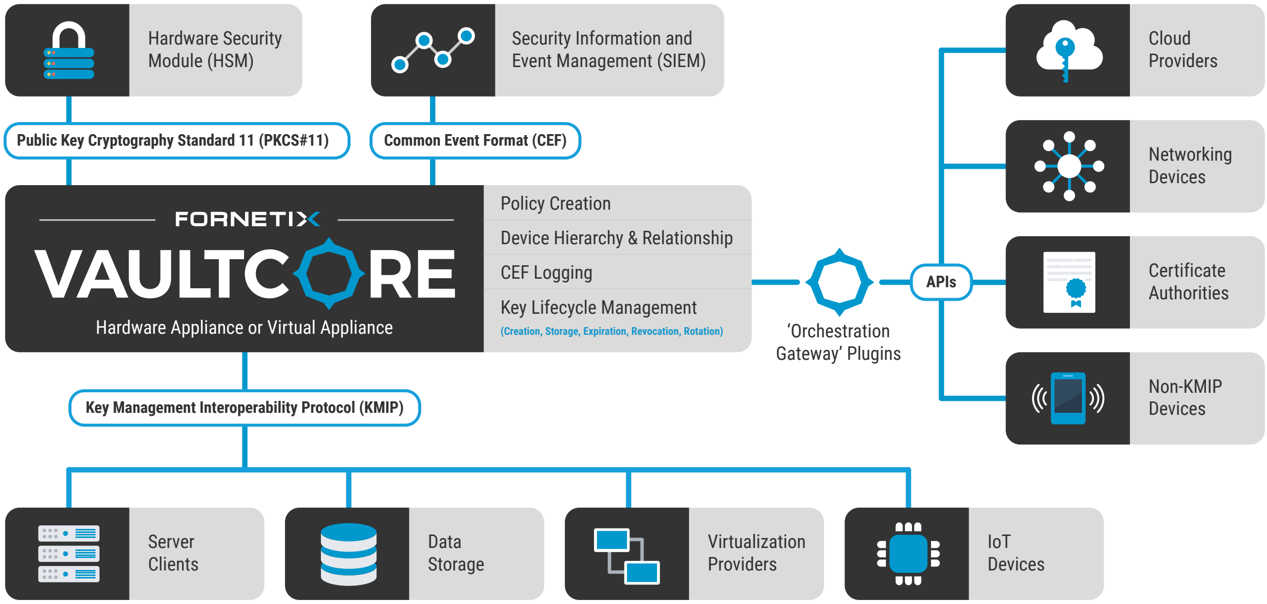
5. Swift Integration and Scalability

KMIP connectors and almost two dozen plugins that connect with non-KMIP technologies make integration with your existing systems and VaultCore quick and simple.

VaultCore's best-in-class capacity to manage over one hundred million encryption keys makes it the world's most scalable key management solution.

» SUMMARY

Securing data has become exponentially more complex as organizations struggle to meet CCPA. Additional encryption has created an overwhelming influx of keys that has left security and risk management leaders struggling to adequately protect customer data.
The number of keys have moved far beyond what a team of humans can manually oversee. VaultCore provides a simple key management solution that works with an organization's existing investments – whether the data is in the Cloud, hyperconverged, or on premise. VaultCore, through a simple KMIP connection, can provide enterprise level key management that fully protects sensitive data, reduces overhead costs, and diminishes inevitable human errors. Remember, any security strategy that does not include a centralized encryption key management solution is putting data at risk. At risk data becomes compromised and your organization is left paying the fine.


Hardware Security Module (HSM)
Security Information and Event Management (SIEM)
Cloud Providers
Public Key Cryptography Standard 11 (PKCS#11)
Common Event Format (CEF)
Networking Devices
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
Data Storage
Virtualization Providers
IoT Devices