FORNETIX™

KEY ORCHESTRATION™

PROTECT AND ACCELERATE YOUR ENTERPRISE

Data protection is a fundamental goal of cybersecurity. Current cybersecurity solutions attempt to do this in one of two ways:

1. Preventing bad actors from breaching network perimeters; and
2. Quickly detecting network breaches once the perimeter has been breached.

While important, these two approaches are not enough to secure your enterprise, as enterprises with strong perimeter protection and breach detection are still being compromised and millions of records containing sensitive, non-encrypted data are being stolen every day.

The hardware encryption market is growing almost four times faster than the cybersecurity solution market, as organizations are quickly realizing that current cybersecurity solutions are not enough and data needs to be protected at its source.

However, encryption is only as powerful as its implementation. Encryption needs to be applied to all sensitive data, whether at rest, in motion, or in use and it needs to be applied at granular levels that require highly scalable, fully automated encryption key management solutions.

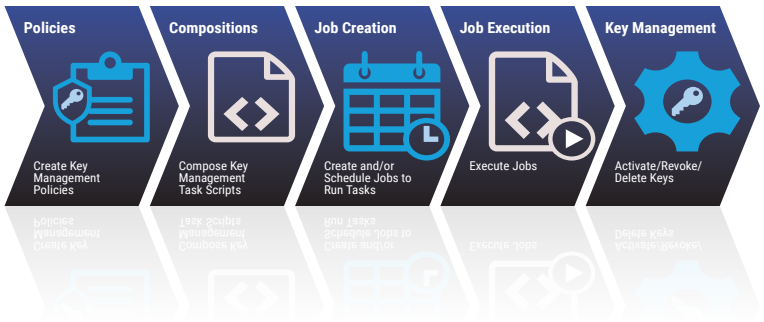
Most Electronic Key Management Systems (EKMS) cannot centrally manage all encryption or handle the scale required to fully secure the enterprise. Key Orchestration seamlessly integrates and scales with your enterprise, allowing fully centralized granular encryption key management through smart automation, standardization, and policy.

CENTRALLY MANAGE YOUR KEYS

Key Orchestration consists of four main components, which allow you to manage all encryption keys across all network devices, endpoints, and entities throughout your enterprise—on premise, in the cloud, on IoT devices, at rest, or in motion.

1. The Key Orchestration Appliance provides key management administration that is compliant with Key Management Interoperability Protocol (KMIP). Key Orchestration Agents can be used to manage non-KMIP compliant devices.
2. The Key Orchestration Client is installed on a server or device and can push or pull keys generated by KOA or any other KMIP compliant server.
3. The Key Orchestration Agent is used as a KMIP driven proxy to manage keys on devices where clients cannot be installed.
4. The Key Orchestration RESTful Services are used to integrate KOA with existing enterprise services aligning Key Orchestration with business needs.

Key Orchestration has standard HSM integration (PKCS#11), which provides added security and allows continued use of existing HSMs to manage keys they are assigned to.



KEY FEATURES

Interoperability: KO is highly compliant with OASIS Key Management Interoperability Protocol (KMIP), for maximum interoperability. This means that none of our protocols are proprietary allowing you to future-proof your organization with minimal investment.

Scalability: Scalable to hundreds of millions of keys, KO provides the ability to manage keys at IoT scale to manage encryption for all devices and entities that touch your enterprise. KO also provides full clustering capability with immediate, uninterrupted failover so your keys are always safe, secure, and available.

Ease of Use: Automate the entire encryption key management lifecycle through policy-driven rules automatically triggered by events or specific timeframes. KO's intuitive user interface and built-in workflows allow you to manage encryption keys across your enterprise without needing extensive cryptographic expertise in-house.

Security: KO's scalability and extensibility allows you to apply and manage separate keys at the device and/or entity level, rather than using the same key or pool of keys for everything, which presents obvious security risks. For high-value data, KO can rotate keys in seconds or minutes, rather than the days, weeks or months it would take to rotate these keys manually. In addition, the Key Orchestration Appliance is FIPS 140-2 compliant to ensure compliance with US government security standards.

 | www.fornetix.com

FORNETIX™