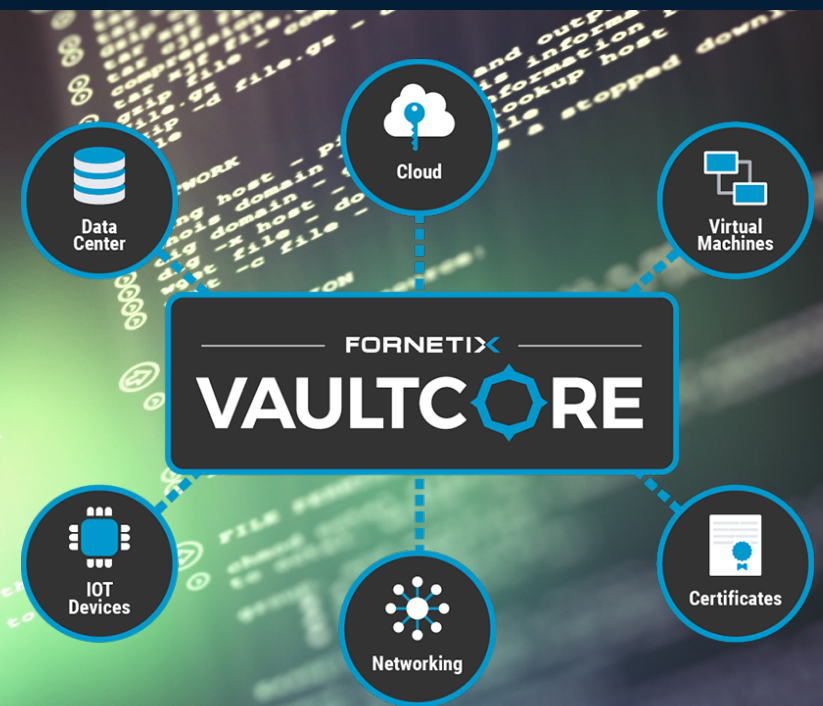


A CHAVE PARA A SEGURANÇA DE DADOS

O VaultCore foi desenvolvido para tornar a criptografia de dados contínua, rápida, flexível, escalável e econômica.



Nos conectamos com tecnologias líderes em todo o mundo para automatizar e orquestrar a criptografia em grande escala.

O controle simples e centralizado de políticas de segurança e acesso evita erros humanos, reduz custos operacionais, protege dados críticos e garante conformidade regulatória.

RESOLVENDO O MAIOR DESAFIO DA SEGURANÇA DE TI

Pergunte para qualquer pessoa que implementou criptografia em um nível empresarial e provavelmente ela dirá:
“A criptografia é fácil. O gerenciamento de chaves é difícil.”
É uma das tarefas mais complexas da indústria de segurança.

Muitas vezes, as organizações se confundem com as as tecnologias, quando todas falam diferentes protocolos e exigem processos altamente manuais para administrar. *O resultado final é um sistema que é ao mesmo tempo mais caro e menos seguro.*



Tarefas criptográficas de alta manutenção desviam tempo e dinheiro de um trabalho mais produtivo

Aumento do risco de violações de dados devido a erro humano e ataque interno

Falta de flexibilidade quando você está "preso" a um ecossistema proprietário

Pesadelo para auditoria e a conformidade regulatória



O maior valor do gerenciamento de chaves é uma estratégia de criptografia unificada e centralizada que automatiza fluxos de trabalho complexos e se integra perfeitamente com toda a sua infraestrutura, seja com tecnologia nova ou legada.

É aí que o VaultCore faz a diferença!



PODER DE AUTOMAÇÃO

Elimine o erro humano e reduza o impacto das violações de dados, automatizando tarefas complexas do ciclo de vida



CONTROLES DE ACESSO

O VaultCore fornece uma combinação híbrida única de controles de acesso baseados em atributos e funções



MOTOR DE POLÍTICAS

Ferramentas patenteadas organizam a empresa em uma hierarquia que garante a conformidade com os padrões de segurança



ESCALABILIDADE SEM IGUAL

O VaultCore oferece suporte a mais de 100 milhões de chaves para ambientes globais de grande escala



GATEWAY DE ORQUESTRAÇÃO

Biblioteca de plug-ins que traduzem APIs de sistemas não KMIP para viabilizar a utilização dos recursos do VaultCore



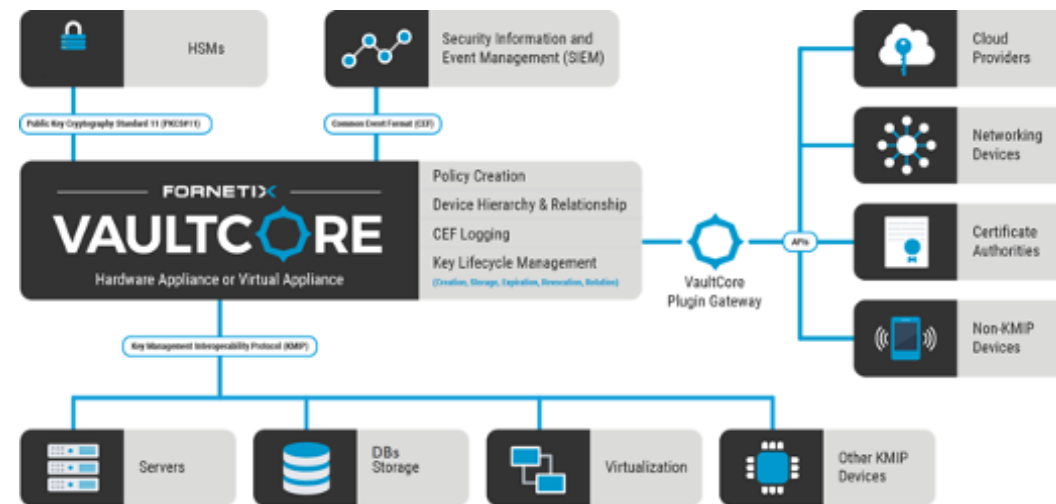
GESTÃO DE CHAVES

Gerenciar e aplicar a rotação de chaves em sistemas críticos, a partir de definições de políticas

O VaultCore oferece um amplo ecossistema de plug-ins, protocolos e arquiteturas para resolver os maiores desafios da segurança cibernética.

A biblioteca cada vez maior de ferramentas traz os recursos exclusivos do VaultCore para dados em repouso, dados em movimento e dados em uso.

Orquestrar e automatizar a criptografia de bancos de dados, máquinas virtuais, backups, serviços em nuvem, CASBs, SAN / NAS, endpoints de IoT, infraestrutura hiper convergente, hardware de usuário final, certificados, proxies, balanceadores de carga, servidores web, SSH, rede com / sem fio, PKI e muito mais.



Integração KMIP

O VaultCore se conecta a qualquer dispositivo ou serviço que use o Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP), o padrão da indústria para comunicação de operações de criptografia. A adoção do KMIP está aumentando rapidamente para incluir servidores, bancos de dados, endpoints, aplicativos, e-mail, nuvem e muito mais.

Plug-ins para integração não KMIP

Para sistemas que não falam KMIP, o Foretix Orchestration Gateway e seu ecossistema de plug-ins atuam como um tradutor que estende os recursos do VaultCore para esses sistemas. Estamos constantemente adicionando plug-ins do Orchestrator à nossa biblioteca de conexões.

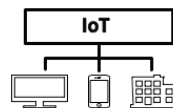
Multi-Cloud & containers, VMs

Gestão de chaves em Nuvens publicas e privadas, com uma única console



Big data

Viabiliza plataformas de dados, com segurança.



Internet of Things (IoT)

Sistemas integrados de ponta a ponta



Digital payments

Escalabilidade a Sistemas de pagamento



Applications

- MarkLogic
- MongoDB
- Mozilla NSS
- MS IIS
- MS SQL
- Oracle DB
- Oracle MySQL
- SSH Client

SIEMs (CEF)

- Elastic
- IBM Qradar
- Loggly
- Logrhythm
- Splunk

PKI / CA / Identity

- BeyondTrust
- DigiCert
- GlobalSign
- MS ADCS
- PrimeKey

HSMs

- Engage Black
- Entrust (nCipher)
- SafeNet Luna
- Securosys
- Utimaco

Cloud Services

- AWS
- Azure
- BitGlass
- IBM
- McAfee
- NetApp
- NetSkope
- Panzura
- Trend Micro
- VMware

Storage / Servers

- Cisco
- Cray
- DDN
- Dell
- Fujitsu
- Hitachi
- HPE
- IBM
- Linux
- NetApp
- Pure

Hyperconverged

- Nutanix
 - RackTop
 - VMware
- Internet of Things**
- ADDAX Meters
 - Micron Authentia

Networking

- Cisco
- F5
- Huawei
- Juniper
- Ruckus
- VMware

Encryption

- Zettaset





CLOUD



DATACENTER



DEVOPS



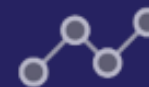
IOT / OT



VIRTUALIZATION



HSM

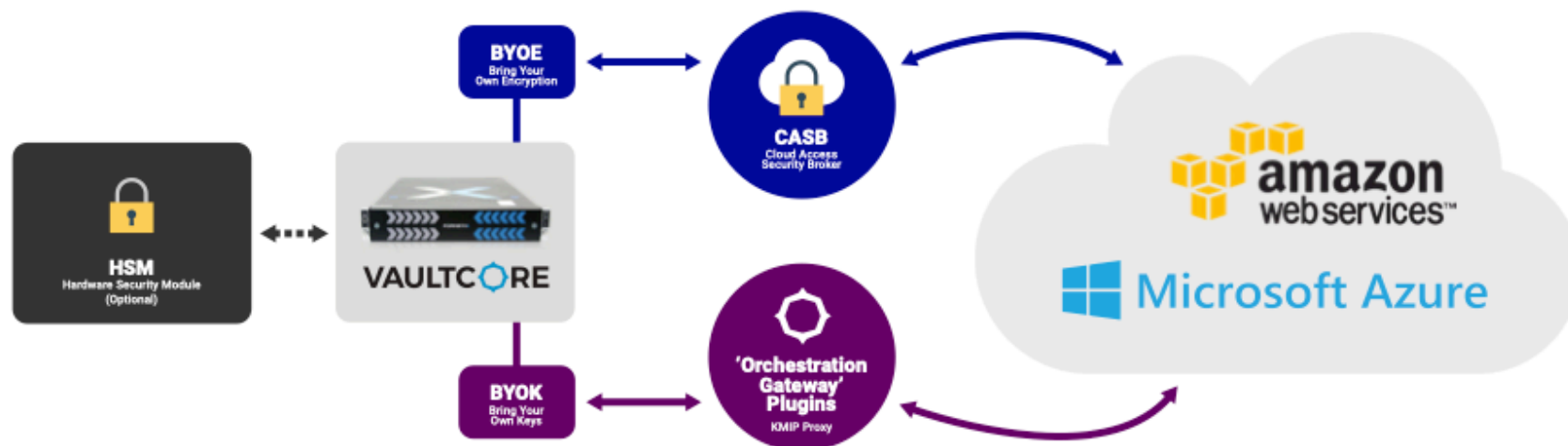


SIEM

VAULTCORE



O VaultCore está pronto para tornar a criptografia simples e perfeita para aqueles que adotam os serviços em nuvem em todo o mundo.



O VaultCore suporta 'Bring Your Own Key' (BYOK), Cloud Access Security Brokers (CASBs), ambientes de várias nuvens e pode ser totalmente implantado em um contêiner de nuvem por meio de VMware e AWS.

Conheça um Caso de Uso BYOK



CLOUD



DATACENTER



DEVOPS



IOT / OT



VIRTUALIZATION



HSM



SIEM

VAULTCORE



Os produtos de armazenamento emparelhados com o VaultCore criam uma solução de criptografia poderosa para datacenters, fornecendo gerenciamento de chave externa para criptografia de dados em repouso, integração simples com tempo de inatividade de rede zero e permitindo comando e controle centralizado com acesso total a relatórios de auditoria em um local.

Conheça um Caso de Uso de
proteção de dados





CLOUD



DATACENTER



DEVOPS



IOT / OT



VIRTUALIZATION



HSM



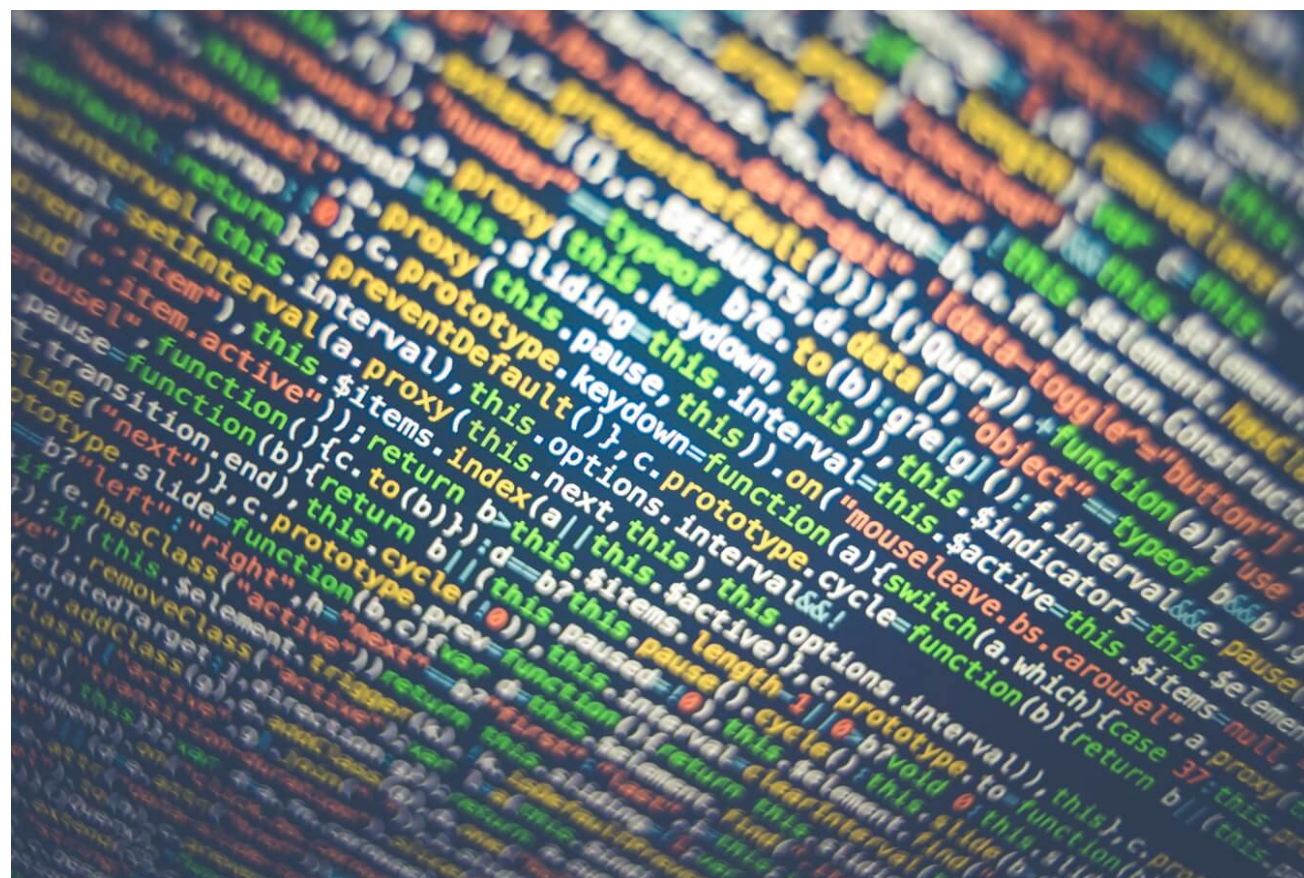
SIEM

VAULTCORE



As organizações podem proteger os dados do contêiner de maneira flexível em qualquer implantação local, na nuvem ou híbrida com criptografia rápida e transparente, permitindo:

- Concentrar esforços para impulsionar a inovação
- Reduzir drasticamente o risco de violações de segurança e roubo de dados
- Garantir de que os desenvolvedores não sejam mais obrigados a tomar decisões de segurança
- Fornecer consistência para gerenciamento de chaves de criptografia de carga de trabalho e contêineres em Desenvolvimento e Operações
- Criar um plano suave para a transição para DevSecOps





CLOUD



DATACENTER



DEVOPS



IOT/OT



VIRTUALIZATION



HSM



SIEM

VAULTCORE



A escalabilidade incomparável do VaultCore oferece uma base preparada para o futuro para gerenciar automaticamente a criptografia para milhões de sensores, dispositivos e terminais gerados por redes IoT massivas.

[Veja o White Paper](#)



CLOUD



DATACENTER



DEVOPS



IOT / OT



VIRTUALIZATION



HSM

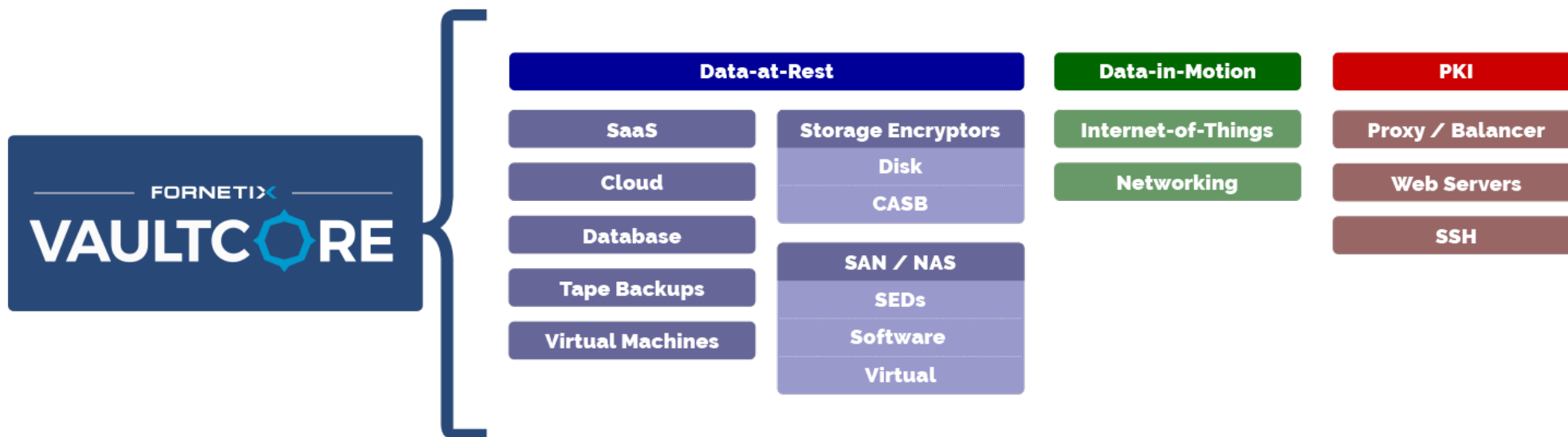


SIEM

VAULTCORE



Atenda aos requisitos de um gerenciador de chaves externo de forma rápida e contínua em ambientes VMware.



O VaultCore oferece uma abordagem unificada e escalável para criptografia em VMware, vSAN, vSphere e outras soluções virtualizadas.

Conheça o resumo da solução conjunta VMware



CLOUD



DATACENTER



DEVOPS



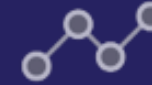
IOT / OT



VIRTUALIZATION



HSM



SIEM

VAULTCORE



A combinação do VaultCore com os Módulos de Segurança de Hardware (HSMs) líderes do setor, fornece gerenciamento de ciclo de vida de chave de criptografia unificado e recursos de automação apoiados pela certificação de segurança FIPS 140-2 Nível 3.





CLOUD



DATACENTER



DEVOPS



IOT / OT



VIRTUALIZATION



HSM



SIEM

VAULTCORE

O VaultCore tem a capacidade única de resposta instantânea bidirecional a alertas fornecidos por produtos de gerenciamento de informações e eventos de segurança (SIEM), como o Splunk, permitindo uma nova digitação rápida após a detecção de um incidente de segurança.

Além disso, o VaultCore fornece registro exaustivo em Common Event Format (CEF) para facilitar a auditoria e o monitoração.

Conheça o resumo da solução conjunta Splunk



De uma pequena empresa com apenas algumas chaves a empresas globais com enorme infraestrutura de IoT, sempre haverá uma opção de implantação do VaultCore que se adapte perfeitamente às suas necessidades exclusivas.



HARDWARE APPLIANCE

Disponível em dispositivos montados em rack 1U e 2U, capazes de suportar mais de cem milhões de chaves de criptografia.



VAULTCORE
VIRTUAL APPLIANCE

APPLIANCE VIRTUAL

Dispositivo virtual baseado em software, capaz de suportar dezenas de milhões de chaves de criptografia.



VAULTCORE
CLOUD APPLIANCE

APPLIANCE CLOUD

Variante do VaultCore que pode ser hospedado e implantado em instâncias de nuvem.



GATEWAY DE ORQUESTRAÇÃO

Arquitetura de plug-in personalizada que atua como um tradutor entre o e os sistemas que não falam KMIP.

No centro dessas regulamentações estão os problemas que podem ser resolvidos pela ampla implantação de criptografia.

O VaultCore tem as ferramentas de automação, mecanismo de política e escalabilidade incomparável para lidar com esse aumento repentino nas chaves de criptografia sendo geradas. À direita estão alguns exemplos das regulamentações que uma organização pode precisar considerar ao desenvolver sua estratégia de segurança.



- | | | | |
|---|----------|---|------------|
| ✓ | PCI-DSS | ✓ | GDPR |
| ✓ | CDM | ✓ | CCPA |
| ✓ | NIST 800 | ✓ | SHIELD Act |
| ✓ | LGPD | ✓ | HIPAA |