FORNETIX

VAULTCORE

“Sem a criptografia adequada, os dados podem ser comprometidos ou perdidos.

A criptografia é fácil. Gerenciamento de chaves é difícil".

Jon Oltsik

(Cybersecurity Analyst, ESG)

CRIPTOGRAFIA

AMEAÇA E O RISCO

Riscos para a criptografia segura

- Perda de conexão, perda de dados e performance
- Risco de erro humano, perda ou compartilhamento das chaves
- Tecnologias separadas gerenciadas por várias ferramentas diferentes
- Sobrecarga da equipe técnica para o gerenciamento manual de chaves
- Prazos não cumpridos e custos relacionados por gestão ineficiente

Não deixe a chave debaixo do tapete

FORNETIX
VAULTCORE

Como habilitar a criptografia dos dados, evitando erros básicos e o fator humano.

DESAFIOS

- Violações de dados são uma ameaça global
- A LGPD chegou!
- Os prazos são curtos e os recursos escassos

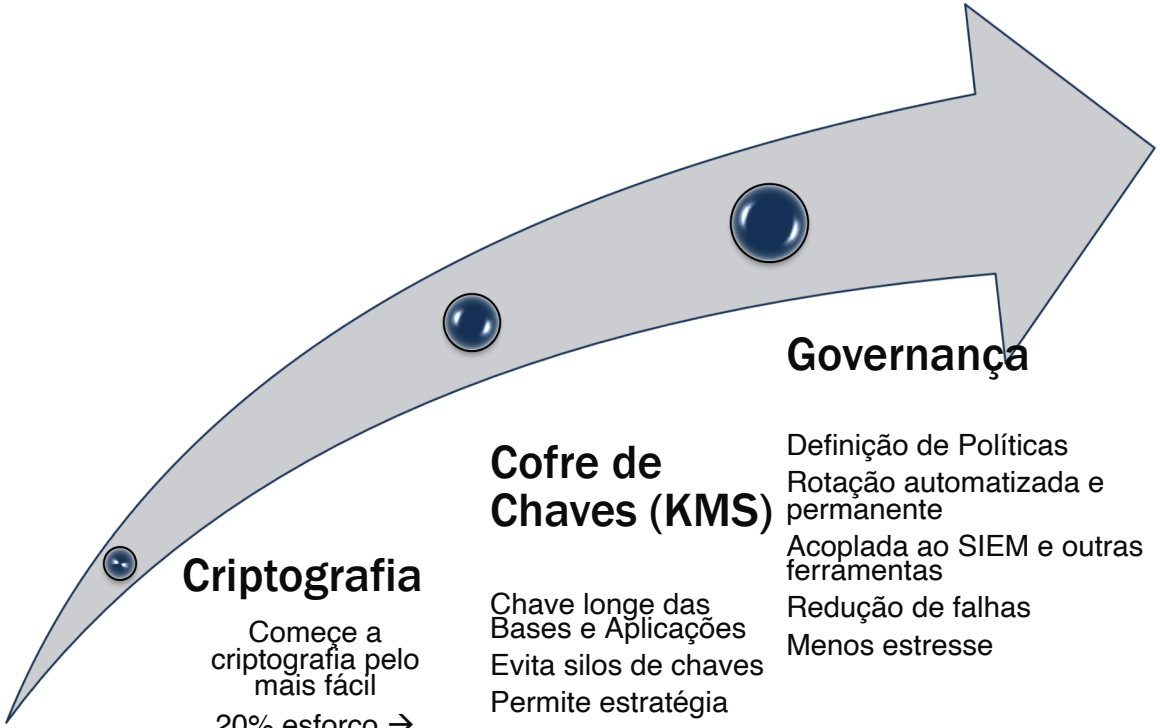
Como implantar uma estratégia regulatória de proteção de dados que não impacte os resultados do negócio, com orçamento reduzido e escassez de recursos?

Onde as chaves não podem ficar?

1. • Nos códigos
2. • Nas bases de dados
3. • Compartilhadas

FORNETIX

Chaves sob custódia e gerenciadas



Criptografia

Começe a criptografia pelo mais fácil

20% esforço → 80% resultado

Cofre de Chaves (KMS)

Chave longe das Bases e Aplicações

Evita silos de chaves

Permite estratégia

Interoperabilidde

Governança

Definição de Políticas

Rotação automatizada e permanente

Acoplada ao SIEM e outras ferramentas

Redução de falhas

Menos estresse

FORNETIX

Libere todo o potencial da criptografia com um avançado sistema de Gerenciamento de Chaves

FORNETIX
VAULTCORE

VaultCore ™ da Fornetix® é uma plataforma de cibersegurança hiper-escalável que automatiza a criptografia para proteção dinâmica de ativos.

Escalabilidade

Armazene centenas de milhões de chaves – capacidade superior às ferramentas equivalentes

Automação

Agende e execute operações criptográficas em milhões de chaves de uma vez

Compatibilidade

Integre perfeitamente o legado, otimizando os investimentos em tecnologia

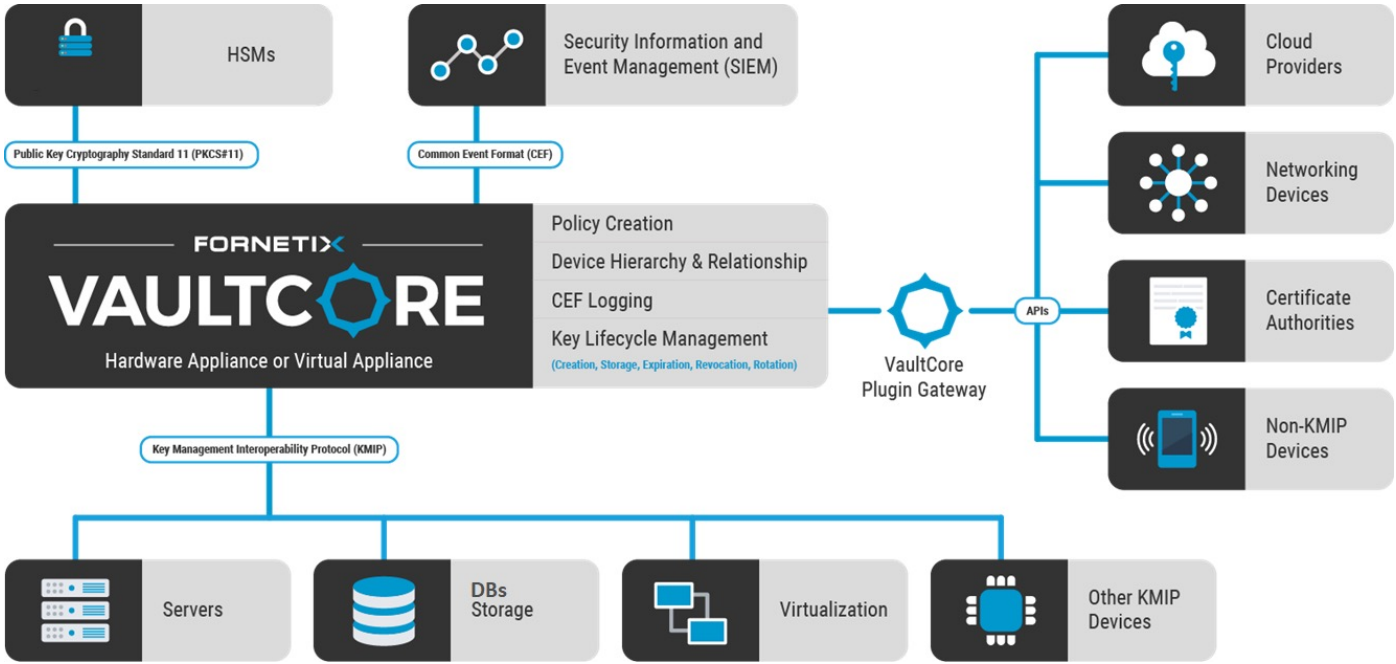
Compliance

Produza relatórios de auditoria completos, aderentes aos requisitos regulatórios atuais e futuros

COM AS VIOLAÇÕES DE DADOS SE TORNANDO UM OCORRÊNCIA QUASE DIÁRIA, É CRÍTICO PROTEGER AS INFORMAÇÕES QUE REQUEREM CRIPTOGRAFIA NA SUA CRIAÇÃO, EM USO, EM TRÂNSITO E EM REPOUSO.

PRINCIPAIS CASOS DE USO

ECO SISTEMA



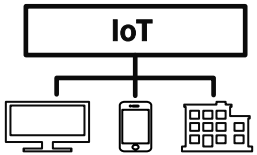
FORNETIX

PROBLEMA RESOLVIDO

Estratégia e gestão de criptografia

Multi-Cloud & containers, VMs

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



Internet of Things (IoT)

Sistemas integrados de ponta a ponta

Big data

Viabiliza plataformas de dados, com segurança.

Digital payments

Escalabilidade a Sistemas de pagamento

Eficiência

REDUÇÃO DE CUSTOS
AUTOMAÇÃO DOS CERTIFICADOS

Custódia

CUSTODIA SEGURANÇA E COMPLIANCE

FORNETIX

PROTEÇÃO

CICLO CRESCENTE

5

AUTOMAÇÃO CONTINUA,
CUSTÓDIA

1

INTEGRAÇÃO: Transparente e Nativa
TEMPO: 5 MIN por VM
PROTEÇÃO DE: arquivos dentro da VM, VSAN, VMotion.
PREVINE: RANSONWARE, ROUBO DADOS, Clear BACKUPS
CUSTO: Muito Baixo (Sem custo)

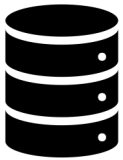
2

INTEGRAÇÃO: Transparente via conector
TEMPO: 30 MIN
PROTEÇÃO: SOBERANIA DE DADOS, BYOK.
PREVINE: Resoluções de cloud pública, perda de chaves
CUSTO: Muito Baixo (Sem custo)

4

INTEGRAÇÃO: NA APLICAÇÃO → chamadas REST
TEMPO: DIAS → exige desenvolvimento.
PROTEÇÃO DE: Dados granulares - máxima proteção independente da base, melhor performance.
PREVINE: Usuário DBA, acesso indevido ao arquivo das bases como um todo.
CUSTO: Alto, → envolve backlog projetos , alocação de desenvolvedores, tests

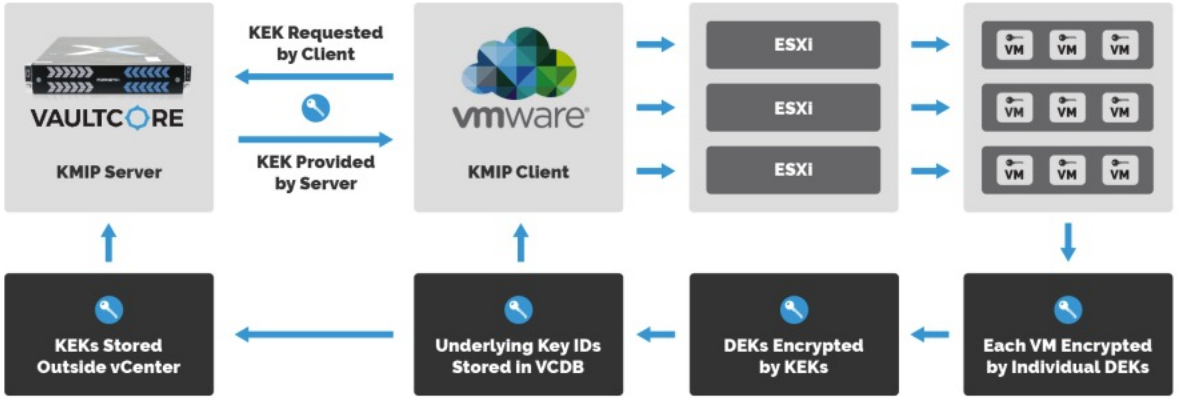
3



INTEGRAÇÃO: Transparente data encryption (TDE)
TEMPO: HORAS - pode ter downtime - depende da Base
PROTEÇÃO DE: Dados nas colunas, arquivos das bases, --> permissão controlada de usuários.
PREVINE Usuário DBA (alguns casos), acesso indevido ao arquivo das bases.
CUSTO: Baixo - Sem custo em alguns caso

PROTEÇÃO DO AMBIENTE VM

vmware | FORNETIX



Implementar Fornetix VaultCore com VMware vSphere 6.5 e mais recente é uma solução perfeita e segura:

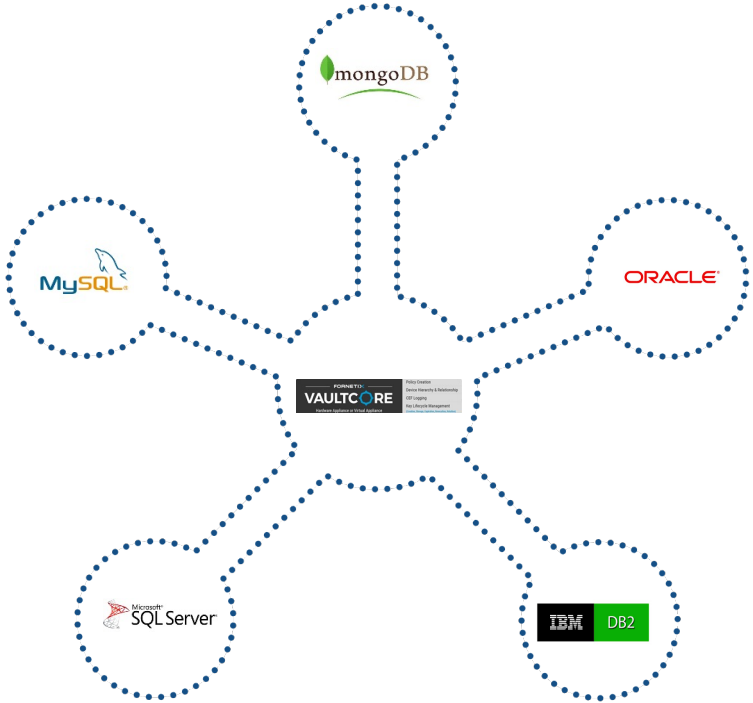
1. Quando uma máquina virtual nova ou existente é criptografada, o host VMware gera uma chave AES interna que é usada para criptografar a máquina virtual.
2. O servidor vCenter então solicita uma nova chave AES do VaultCore que é usada para criptografar a chave gerada internamente.
3. A chave do VaultCore usada para criptografar a chave interna não é salva no ambiente Vmware - apenas o UUID é armazenado.

CRIPTOGRAFIA DE BASE DE DADOS

TRANSPARENTE

- Integração nativa ou TDE transparente, para vários tipos de base de dados
- Client Less, livre de plataformas
- O Fornetix VaultCore é totalmente compatível com o KMIP, permitindo compatibilidade com a criptografia nativa para dados estruturados ou não.
- TDE, é a opção nativa para vários sistemas
- O VaultCore é a segurança que implementa a adequação aos privilégios para de acesso às chaves usadas no TDE, criptografando e controlando seu uso.
- Agora o DPO poderá ter uma console de gestão das chaves, adequadas às necessidades da LGPD.

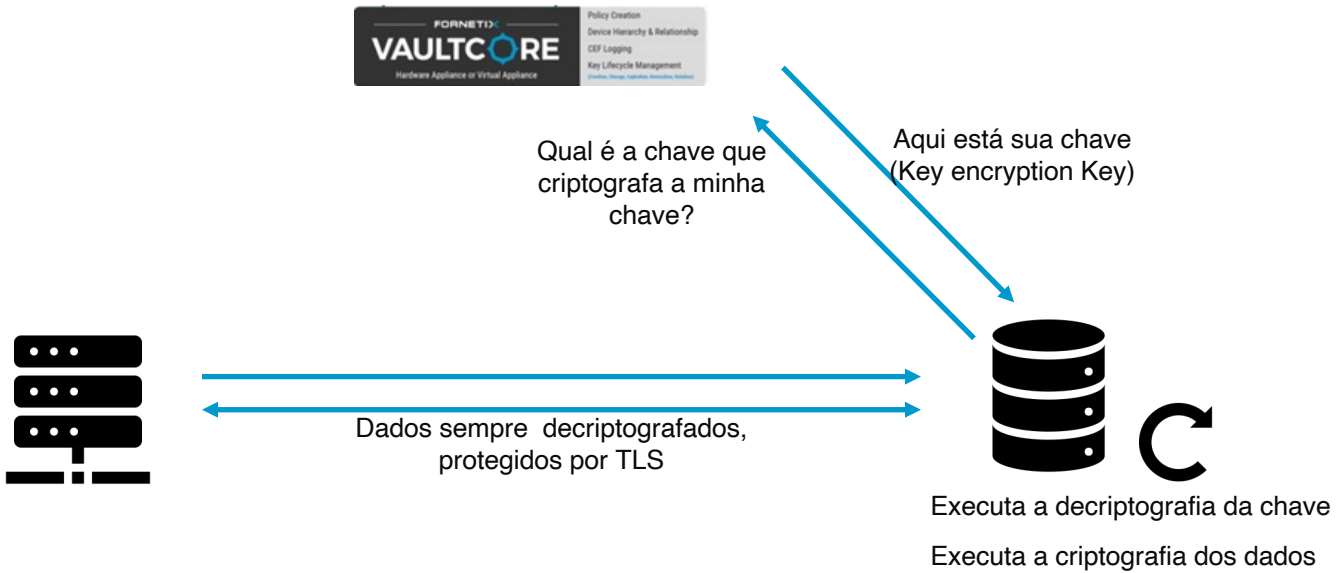
KMIP: Cofre das chaves



FORNETIX

TRANSPARENT DATA ENCRIPTION

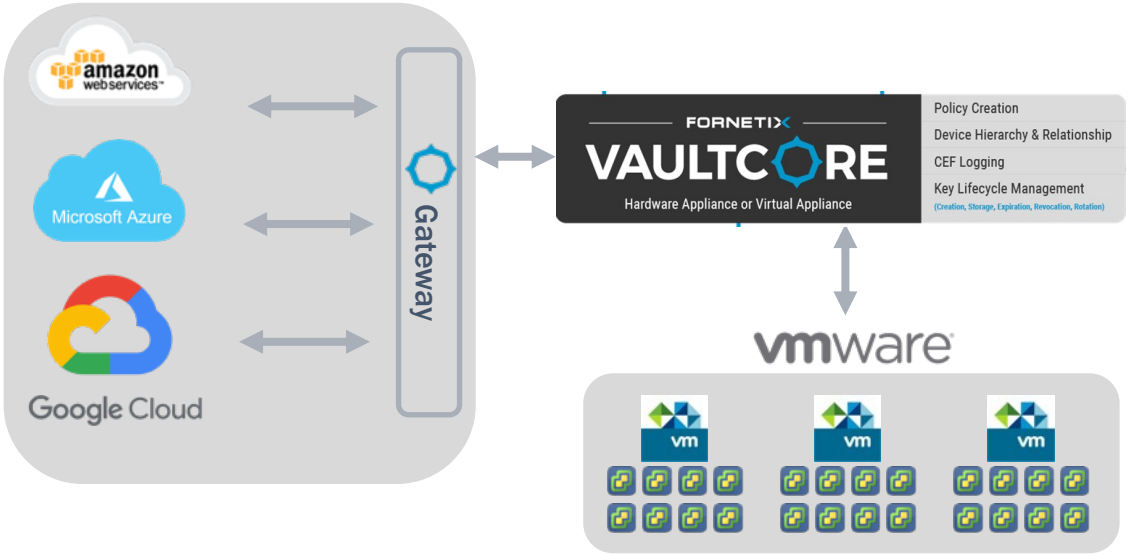
Criptografia de Base de Dados



FORNETIX

CRIPTOGRAFIA EM BASE DE DADOS NÃO ESTRUTURADOS

MULTI-CLOUD



PRIVATE CLOUD VMware

Integração via KMIP para controlar privilégios de criptografia em VM, VSAN e NSX

AWS

O VaultCore fornece gerenciamento das chaves mestras de clientes da AWS e outros requisitos de gerenciamento de chaves.

Azure

O VaultCore usa as APIs de orquestração para registrar as chaves no Gerenciamento de Chaves do Azure.

Google

O VaultCore se integra ao Google Cloud

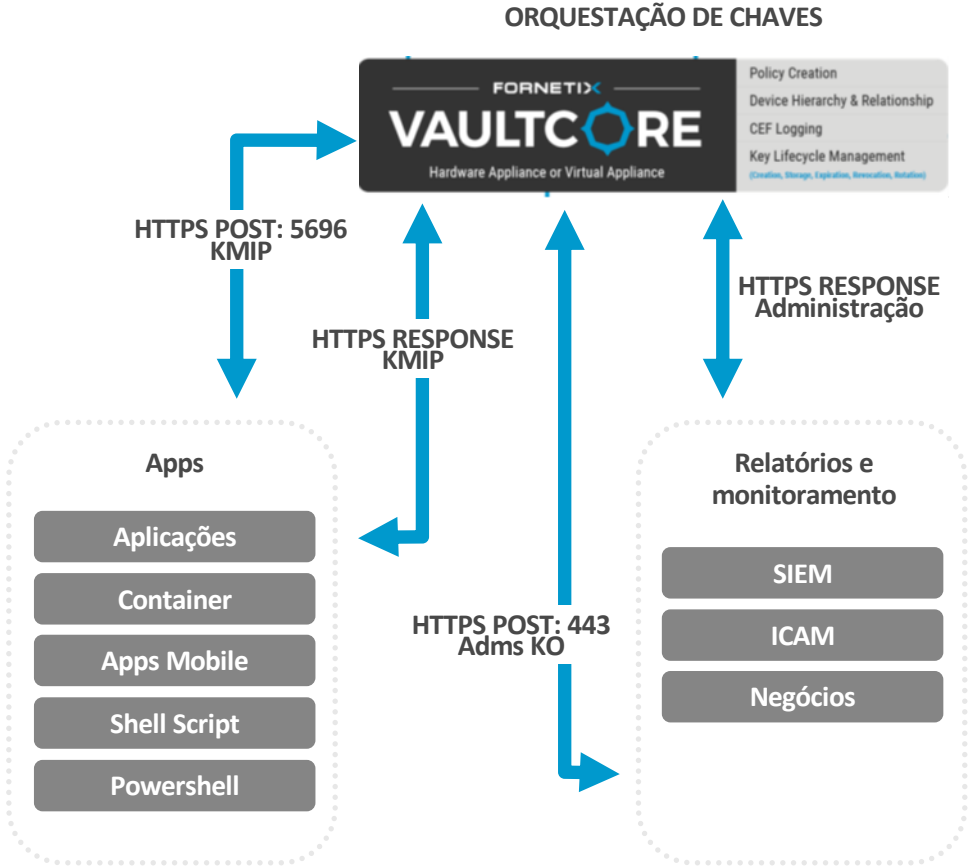
Storage

Via KMIP em produtos como.
Dell, HPE 3PAR, NetApp, Racktop, Cray

CRIPTOGRAFIA DE BASE DE DADOS

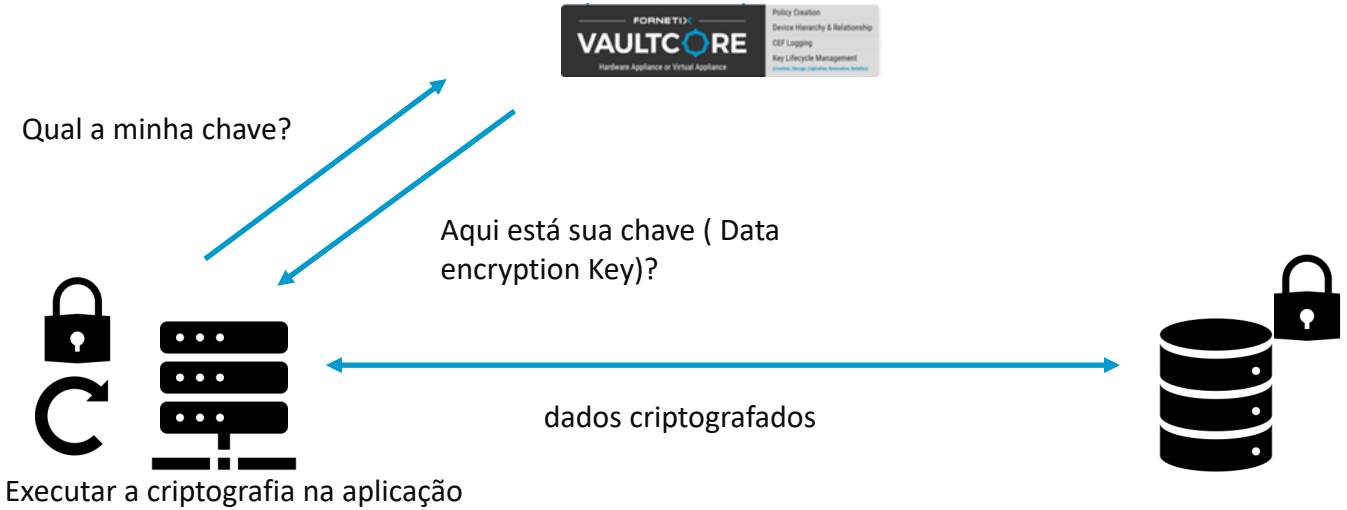
Integração via API

- Não há clientes, funciona Multiplataforma
- A API de gerenciamento de chaves e orquestração / VaultCore usa comandos baseados em JSON
- Os usuários podem fazer conexões de API com base na especificação KMIP ou REST para criar chaves, criptografar / descriptografar dados, dividir / unir chaves, ativar composições.
- Os usuários podem usar a API Key Orchestration / VaultCore para gerenciar clientes, políticas, tarefas e composições
- O appliance VaultCore registra conexões de API e as disponibiliza para SIEMs via Syslog
- A autorização da API é controlada pelo VaultCorepolicy



FORNETIX

Processo via API



VAULTCORE

Solução criada para rodar em qualquer plataforma

O KMIP é nativo em muitas soluções

Virtual Appliances			Cloud	Equipamiento Físico	
					
VCV-100	VCV-500	VCV-2100	VC-CLOUD	VCH-1000	VCH-2000
VaultCore Discovery Edition projetado para demonstrar recursos, mas limitado em capacidade e licenciado por um período de avaliação.	Até 250 mil chaves. Útil para nuvem híbrida e organizações com forte ênfase em mais virtualização política e automação. Software implementado.	Até 50 milhões de chaves. Útil para nuvem híbrida e organizações com forte ênfase na virtualização, além de política e automação. Software implementado.	Lançado em 2020. Versão do software VaultCore implantável como um contêiner nas principais plataformas em nuvem.	Capacidade para mais de 10 milhões de chaves. Equipamento de hardware de uma unidade de rack. Os usos incluem negócios, nuvem híbrida, pequenas redes IoT e redes móveis Ad-Hoc.	600 milhões de chaves, com módulo de expansão mais de um bilhão de chaves. Está em conformidade com FIPS 140-2 Nível 2, Nível 3 com HSM opcional. IoT massiva, redes móveis ad-hoc, computação de alto desempenho. Equipamento de hardware de 2 unidades de rack.

Ampla Gama Sem KMIP Plug-ins disponíveis

Plug-Ins

No KMIP

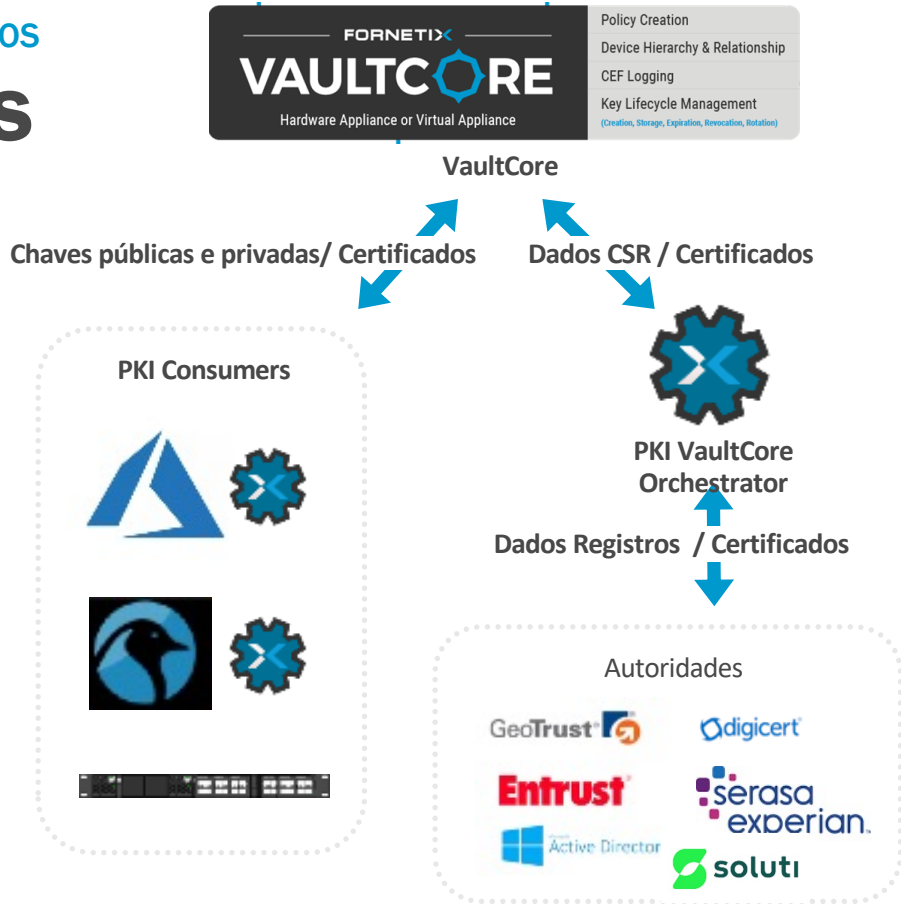
API Específica

FORNETIX

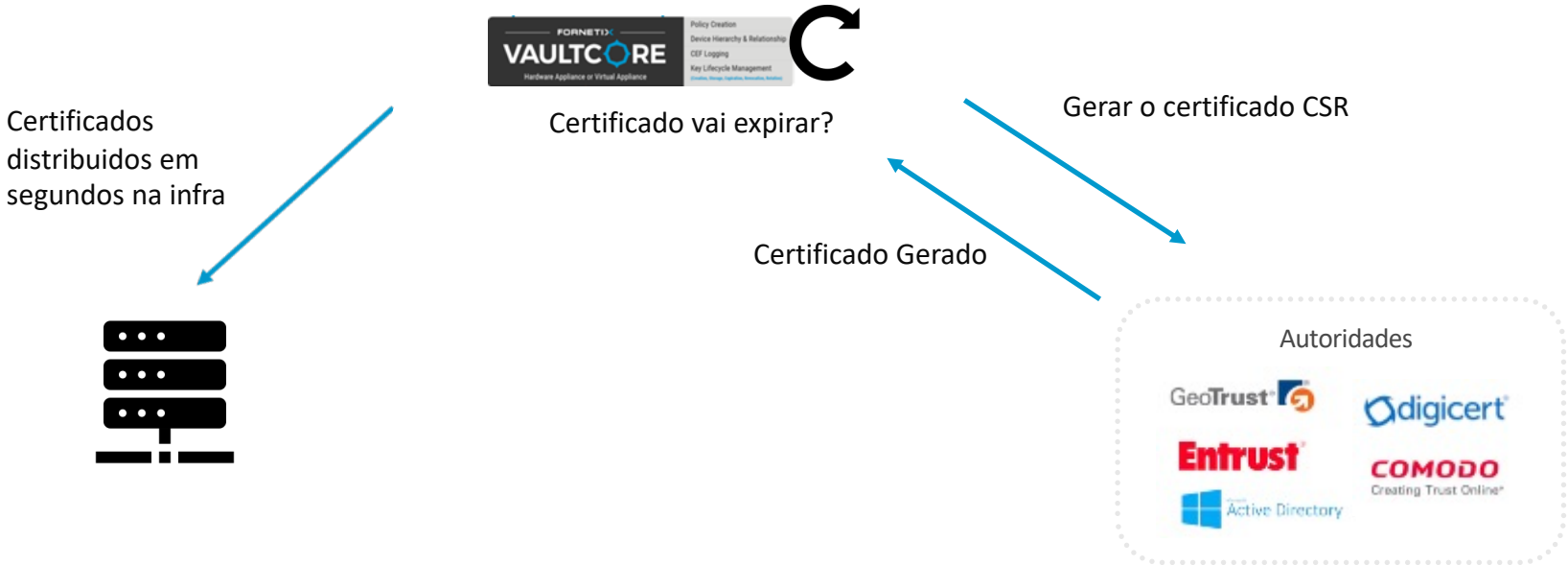
GERAÇÃO E INSTALAÇÃO AUTOMÁTICA DE CERTIFICADOS

AUTOMAÇÃO COM CAs

- Fornecer suporte para serviços públicos de certificação (CA) e do Active Directory
- O VaultCore acessa APIs específicas das autoridades certificadoras, sem interferência humana.
- Controla a expiração dos certificados digitais, sem queda de conexão. Programe sua renovação, automaticamente.
- O VaultCore pode gerar material de chave associado ao certificado e distribuir automaticamente na rede.
- O appliance VaultCore registra a execução da composição e o ciclo de vida das chaves e é disponibilizado aos SIEMs via Syslog.



Automatização do Certificado



FORNETIX

SOBERANIA DE DADOS

Office 365 Crypto

Criptografia para o Skype for Business, OneDrive for Business, SharePoint Online, Microsoft Teams e Exchange Online

- ✓ Todos os arquivos do cliente no SharePoint Online são protegidos por chaves exclusivas por arquivo que são sempre exclusivas para um único locatário. As chaves são criadas e gerenciadas pelo serviço do SharePoint Online, ou quando a chave do cliente é usada, criada e gerenciada por clientes.

- ✓ O armazenamento do Azure não tem capacidade de descriptografar ou mesmo identificar ou compreender os dados do cliente. A criptografia e a descriptografia acontecem nos mesmos sistemas que impõem o isolamento do locatário, que são o Active Directory do Azure e o SharePoint Online.

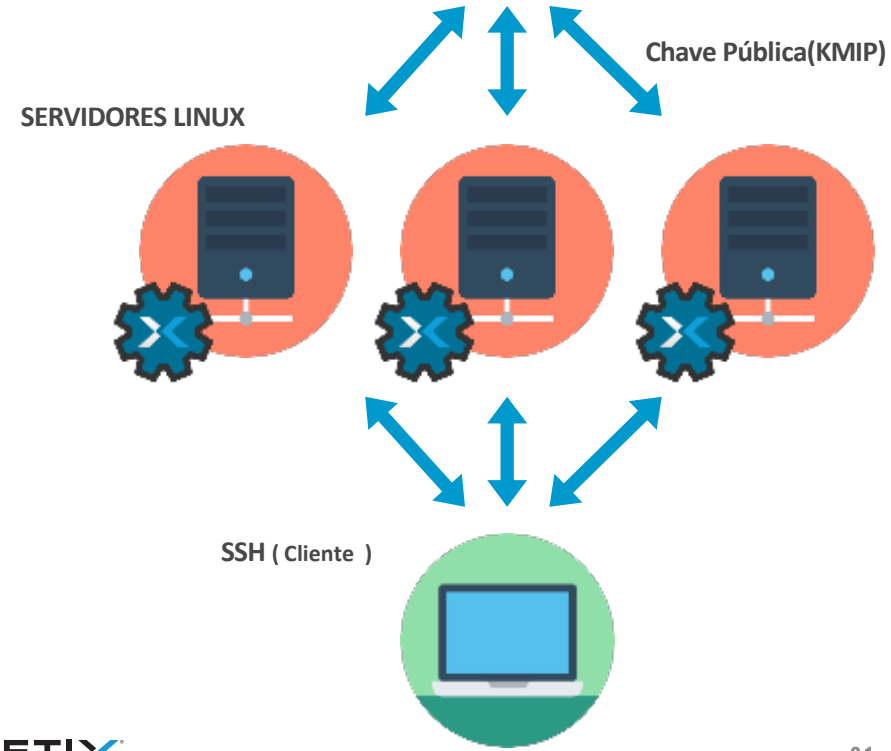
- ✓ Quando os clientes fornecem uma chave opcional, a chave do cliente é armazenada no Azure Key Vault, e o serviço usa a chave para criptografar uma chave de locatário, que é usada para criptografar uma chave de site, que é usada para criptografar as chaves de nível de arquivo. **Essencialmente, uma nova hierarquia de chave é introduzida quando o cliente fornece uma chave**

- ✓ https://docs.microsoft.com/pt-br/microsoft-365/compliance/office-365-encryption-for-skype-onedrive-sharepoint-and-exchange?view=o365-worldwide
- ✓ https://blogs.vmware.com/cloudprovider/2017/09/achieving-data-sovereignty-multi-tenant-service-provider-environment.html

VAULTCORE: OREQUESTAÇÃO DE CHAVES

CLIENTE SSH

- Fornece autenticação de chave SSH sem ter chaves públicas armazenadas localmente em servidores remotos: autenticação "just in time"
- A Segurança Posicional do VaultCore impõe quais servidores podem extrair chaves públicas para autenticação
- Os usuários criam seu próprio par de chaves SSH e registram a chave pública no dispositivo Vault Core
- O dispositivo VAultCore registra a recuperação de chaves públicas para autenticação e é disponibilizado aos SIEMs por meio do Syslog
- O VaultCore pode ser suspenso simplesmente movendo a senha do usuário



FORNETIX

VAULTCORE

Características

Hardware Appliances

POWER SUPPLY

VCH-1000	2-750w hot-swap
VCH-2000	2-1000w hot-swap

SHOCK

Drop test shock	12G, -3.75G

INTERFACES

6 1GB RJ45 copper ports
VCH-1000: 2 optional network upgrade slots
VCH-2000: 6 optional network upgrade slots
Graphical User Interface (GUI)
KMIP API
Command Line Interface
VaultCore Client, Agent, and RESTful Services
HSM (PKCS #11)

KEY CAPACITY

VCH-1000	10,000,000
VCH-2000	100,000,000+

CERTIFICATIONS AND INTEROPERABILITY

FIPS 140-2 compliant
KMIP 1.0, 1.1, 1.2, 1.3, and 1.4 compliant

SCALABILITY AND FAILOVER

Fully distributable
Clustering support
High availability / zero failover interruption
Backup / restore process

Virtual Appliances

VIRTUAL CPU

VCV-100 (Discovery Edition)	2 CPU
VCV-500	2 CPU
VCV-2100	2 CPU

VIRTUAL MEMORY

VCV-100 (Discovery Edition)	4GB RAM
VCV-500	4GB RAM
VCV-2100	8GB RAM

VIRTUAL STORAGE

VCV-100 (Discovery Edition)	16GB
VCV-500	16GB
VCV-2100	100GB

KEY CAPACITY

VCV-100 (Discovery Edition)	125,000
VCV-500	250,000
VCV-2100	50,000,000

CERTIFICATIONS AND INTEROPERABILITY

FIPS 140-2 compliant
KMIP 1.0, 1.1, 1.2, 1.3, and 1.4 compliant

SCALABILITY AND FAILOVER

Fully distributable
Clustering support — *EXCLUDING VCV-100*
High availability / zero failover interruption
Backup / restore process

INTERFACES

Graphical User Interface (GUI)
KMIP API
Command Line Interface
VaultCore Client, Agent, and RESTful Services
HSM (PKCS #11) — *EXCLUDING VCV-100*

FORNETIX

Monitoração e detecção de ameaças em tempo real

- Relatórios e monitoramento integrados através da interface do usuário Fornetix
- A integração com aplicativos SIEM populares permite uma inteligência mais ampla contra ameaças
- Outras ferramentas que falam formatos comuns de eventos. *(CEF Common Event Format).*