フォレンジック調査における
データセントリック・セキュリティ技術の
活用手法

Vormetric, Inc. 東京オフィス
池田克彦
kikeda@vormetric.com
Tel: 03-6717-4483

7万件のデータファイルの内、
ルール通りにパスワードがかけられていたのは実に7個

日経コンピュータ
2015.7.9号より

「守られないルールはルールではない。
人ではなくルールを疑い、見直しが必要」

「パスワードや暗号化を個人に任せるのは時代遅れ。フォルダ格納時にシステムで自動で暗号化するのがこれからの標準」ということだ。内部統制に詳しいプロティビティLLCの牧正人マネージングディレクタは「業務の効率上、基幹システムから情報をローカルのファイルサーバーに置くことは起こり得るが、システムで自動化できる今、人手に任せるのはリスクが高い」と話す。

Extensible Controls for Compliance

HIPAA security rule, which states data at rest should be encrypted unless it's not "reasonable and appropriate."

PCI DSS 3.0 covers a broad base of technologies and processes such as encryption, key management, access control, and auditing to offer a sound baseline of security.

In support of compliance with NIST 800-53 enables satisfaction of mandates and contractual obligations. Meets government requirements to encrypt data.

特定個人情報の適正な取扱いに関する ガイドライン（事業者編）
平成26年12月11日　特定個人情報保護委員会

d　情報漏えい等の防止

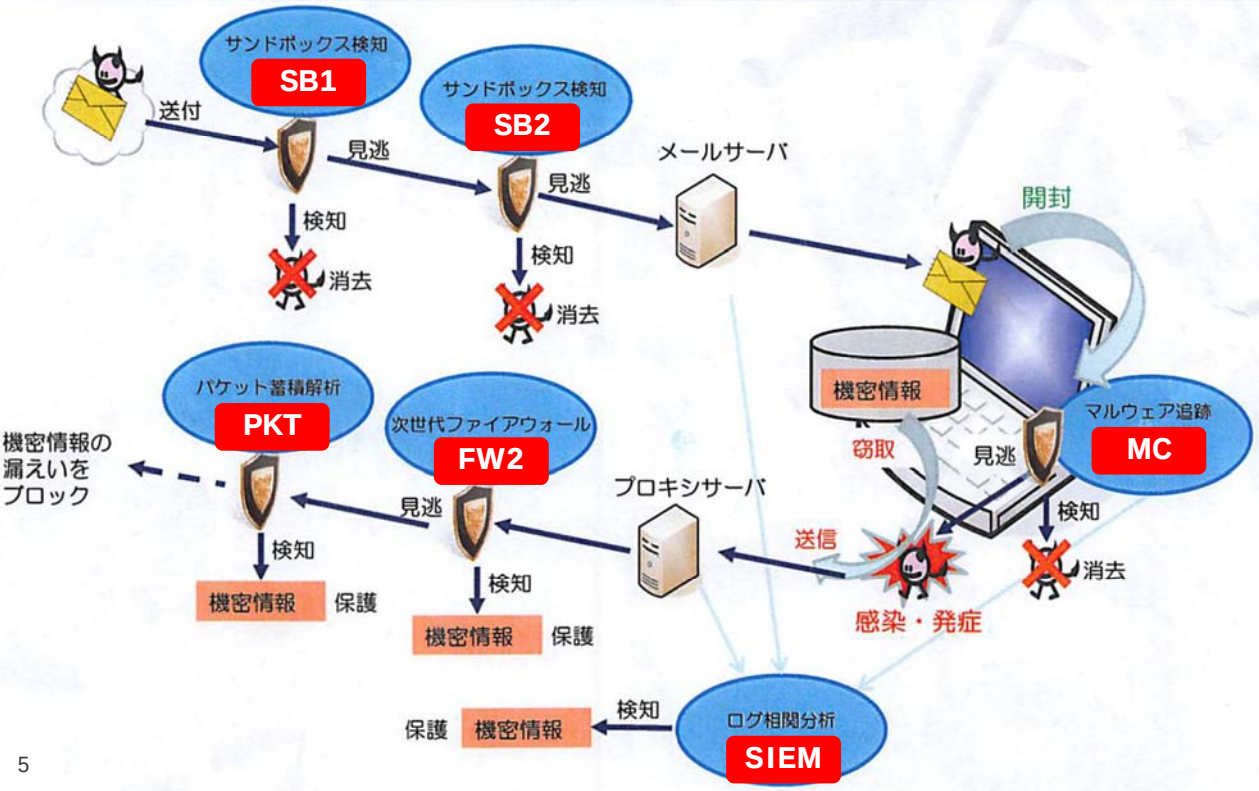
特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。

«手法の例示»

＊通信経路における情報漏えい等の防止策としては、通信経路の暗号化等が考えられる。

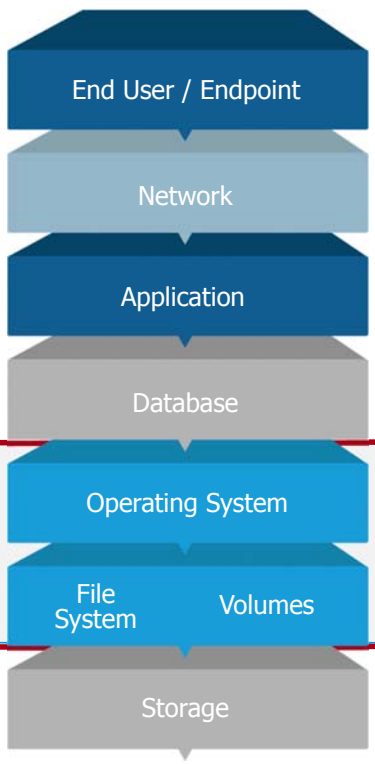
＊情報システム内に保存されている特定個人情報等の情報漏えい等の防止策としては、データの暗号化又はパスワードによる保護等が考えられる。

標的型ソリューション　リアルタイム検知の説明図



Vormetric Data Security

Vormetric Protects What Matters – The Data



Symantec. McAfee FireEye Next Generation Threat Protection

paloalto NETWORKS cisco

FORTIFY WhiteHat SECURITY

IMPERVA IBM Guardium

Perimeter Security

Vormetric

Data Security

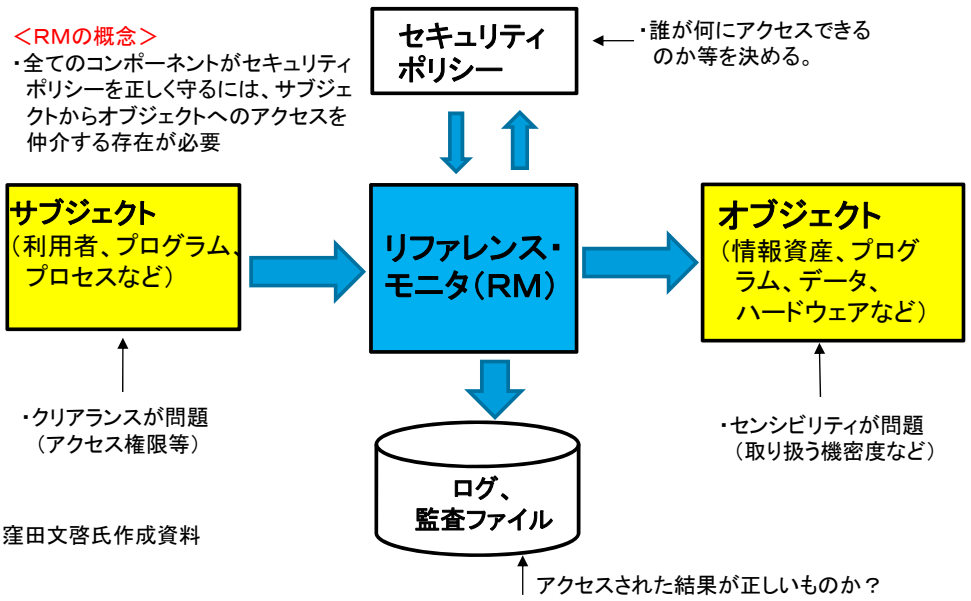
EMC² hp NetApp

Physical Security

Vormetric Data Security

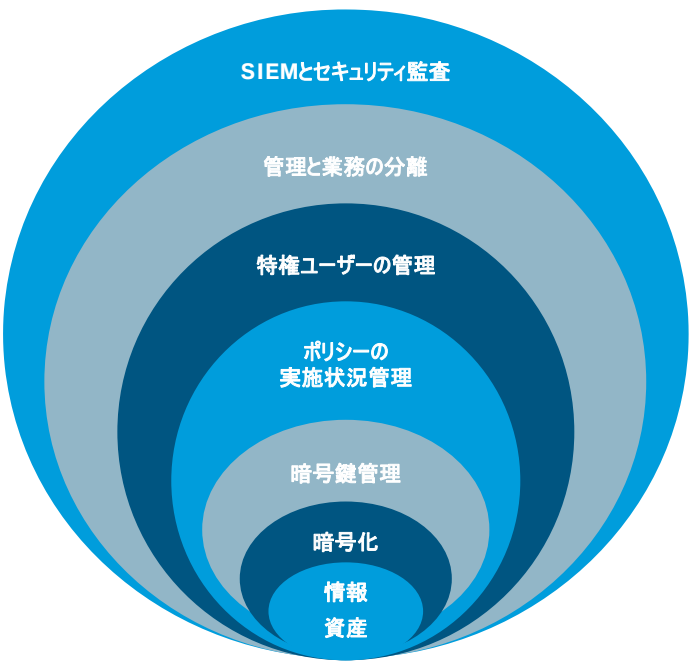
＜情報セキュリティの概念理解の重要性＞

・情報セキュリティのシステム上の基本機能はリファレンス・モニタ（RM）の機能で表現できる。
⇒情報セキュリティの機能を総合的に捉えるためには、下図のように、人（サブジェクト）がシステム（オブジェクト）に係る際のポリシーの役割、ログの役割を総合的に理解しつつ、個々のセキュリティ対策の持つ位置づけと十分性等のチェックをしていくことが重要である。
（これは、CISSPの教育でも最も重要な概念の一つ）



出典　窪田文啓氏作成資料

データ防衛の多層性



データセキュリティの実装基盤

Data Security Manager (アプライアンス or 仮想)

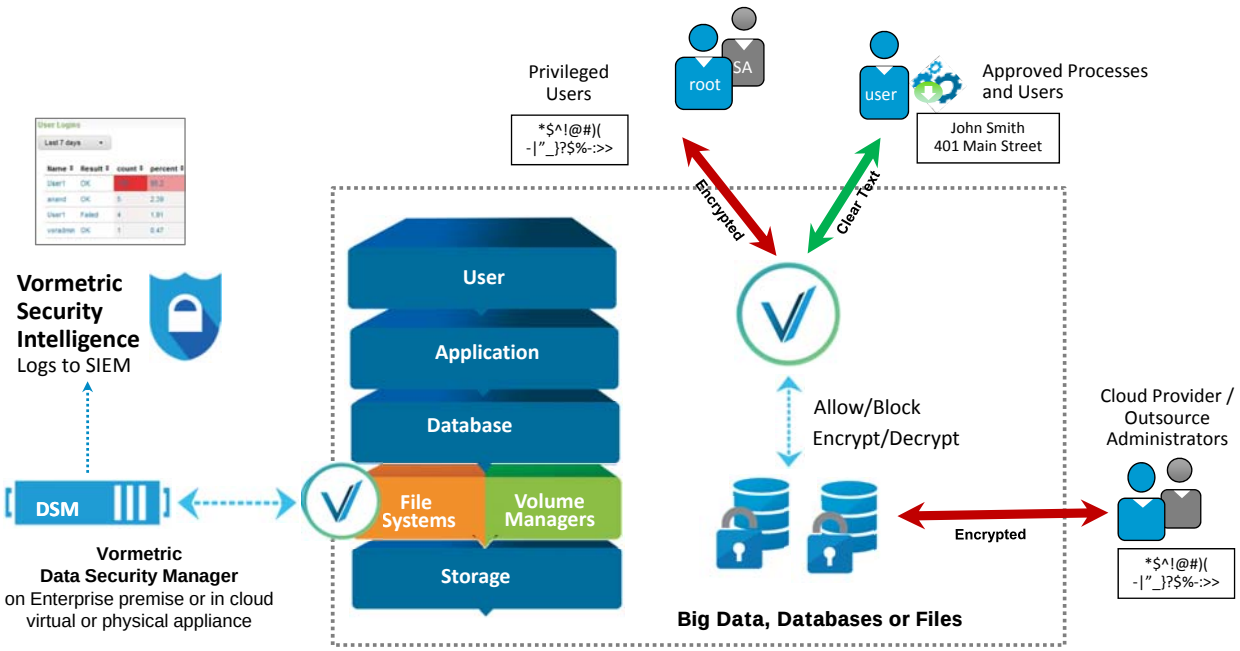
- 暗号鍵管理
- ポリシー配布
- 統合された監査環境
- ポリシーのテンプレ
- 権限の分散化

データのセキュリティと暗号化はファイル・DB・アプリを問わずどこでもどのようなデバイスにも

Encryption Expert Agent (ソフトウェア・エージェント)

- アクセス管理
- Read/Write 管理
- MetaClear Encryption
- 詳細な監査情報
- ポリシーベースの暗号化

煩雑な暗号化手法を簡易に、同時にアクセスをコントロールし、詳細なログを取得するするシンプルな仕組み

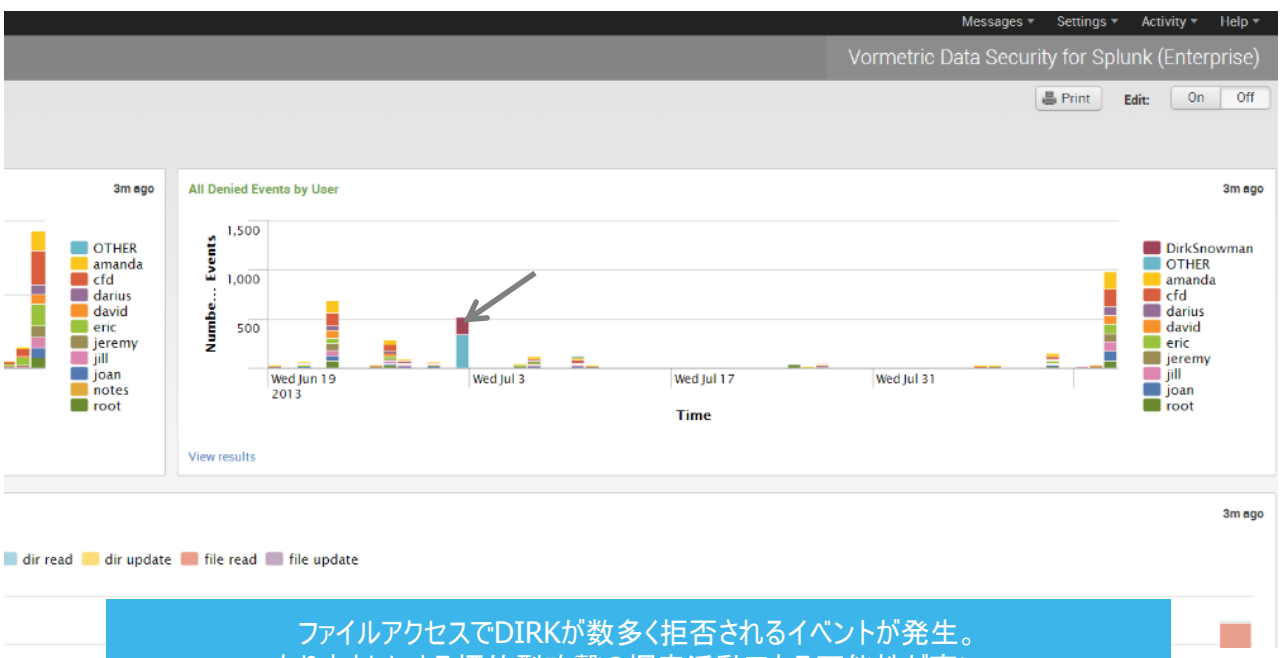


データセントリックセキュリティ
データに対するFirewall

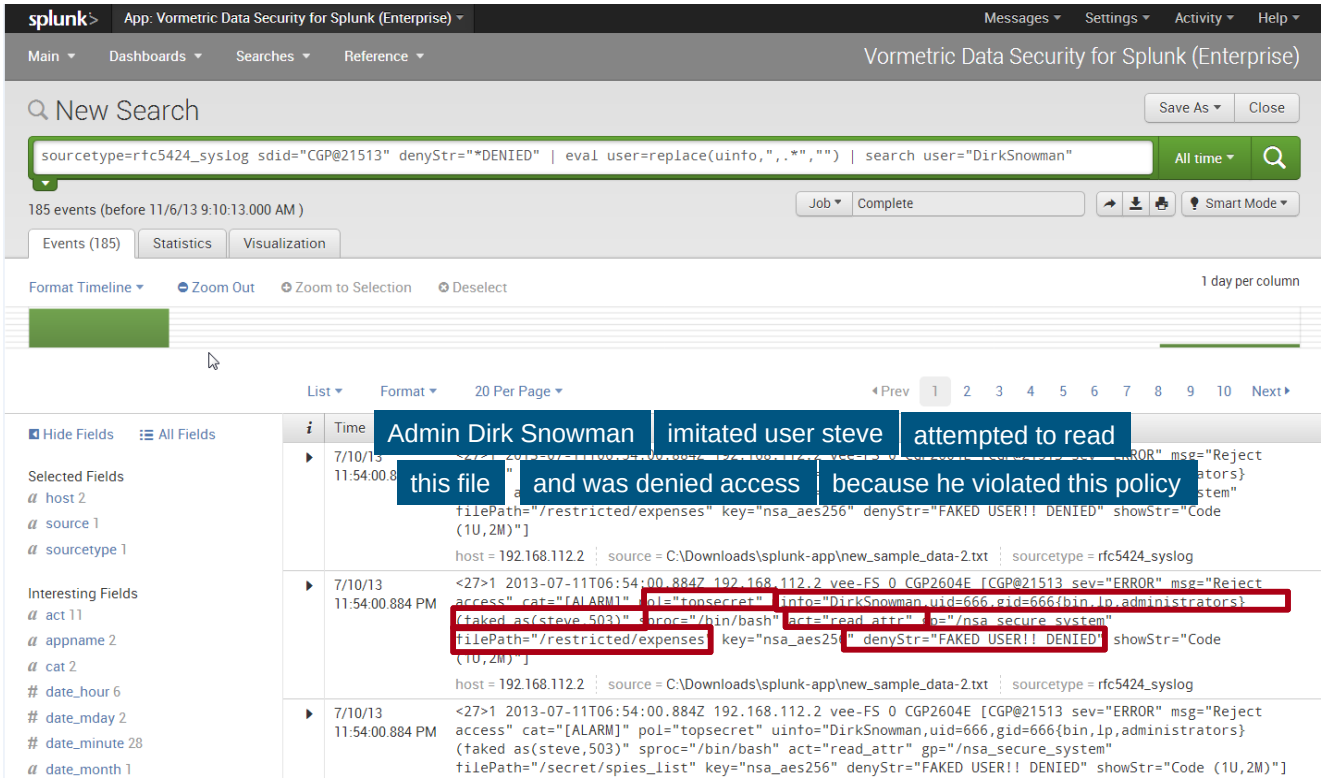
- ポリシー設定 ≈ Firewall ルール
  Criteria and Effect-based

#	User	Process	Action	Effects
1	oracle	oracle_binaries	any	permit, apply key, decrypt
2	root	admin_tools	read	permit, audit, view metadata only
3	any	any	any	deny, audit, view nothing

Security Intelligence, Detecting Abuse
Splunk での事例



ファイルアクセスでDIRKが数多く拒否されるイベントが発生。
なりすましによる標的型攻撃の探索活動である可能性が高い。



Vormetric Security Intelligence
内部犯行と標的型攻撃に効果

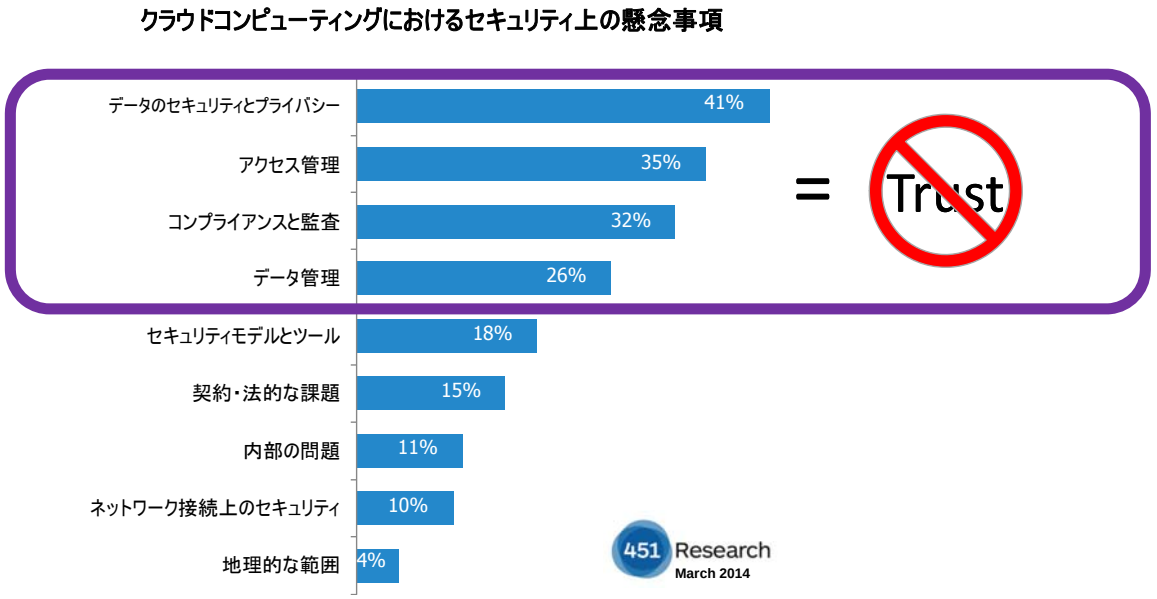
66%
OF BREACHES TOOK MONTHS, OR EVEN YEARS, TO DISCOVER.
VERIZON 2013 DATA BREACH INVESTIGATIONS REPORT

- データアクセスのログ監査
- 異常なアクセスパターンでのアラート
- なりすましなど、不正アクセスユーザーの特定
- 標的型攻撃や内部で活動しているマルウェアの検知
- コンプライアンスや契約で必要なレポート

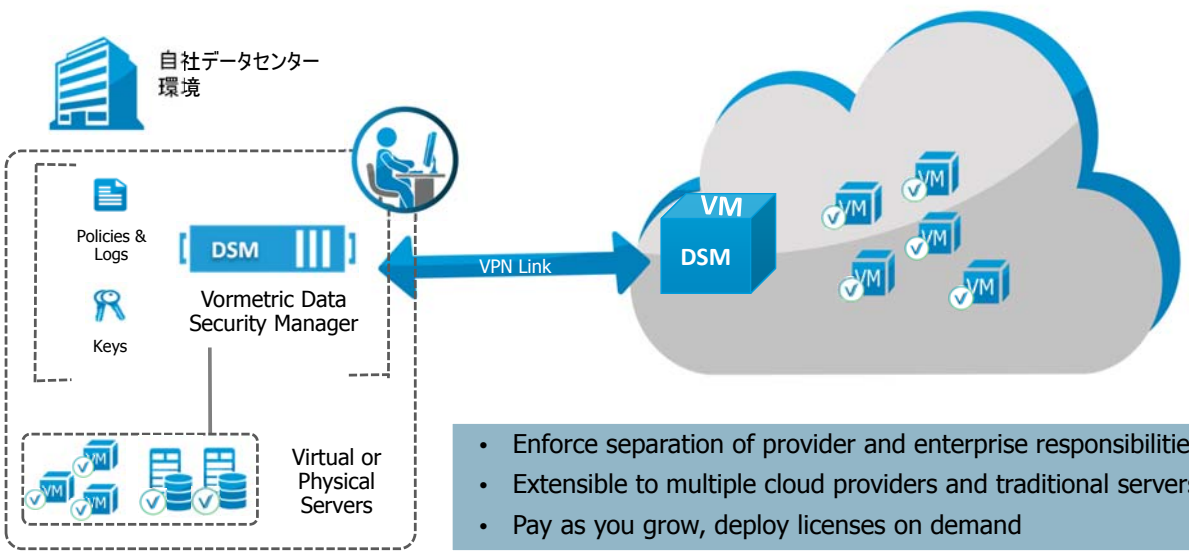
69% of breaches were spotted by an external party — 9% were spotted by customers.

splunk> McAfee IBM Radar hp ArcSight LogRhythm

クラウドセキュリティ上の懸念事項
「信頼性」の問題



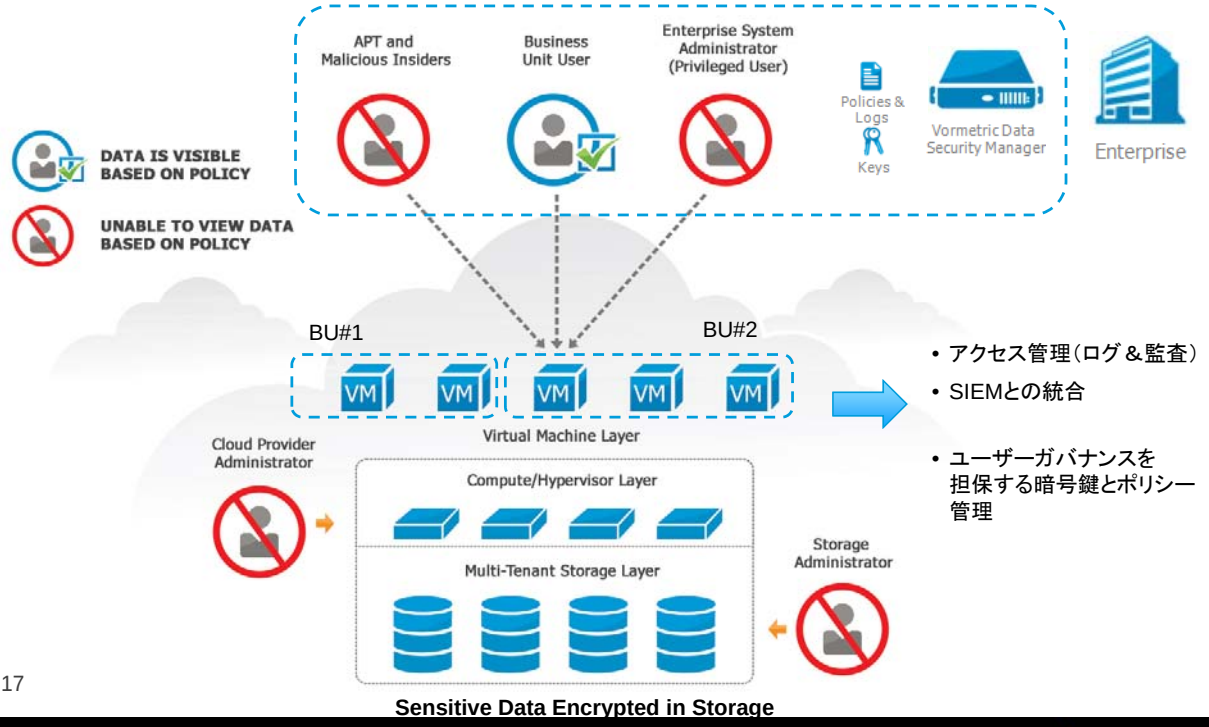
クラウド上データの安全確保と厳重な管理を実現
DSMをクラウド上にもオンプレミスにも配置が可能



- Enforce separation of provider and enterprise responsibilities
- Extensible to multiple cloud providers and traditional servers
- Pay as you grow, deploy licenses on demand

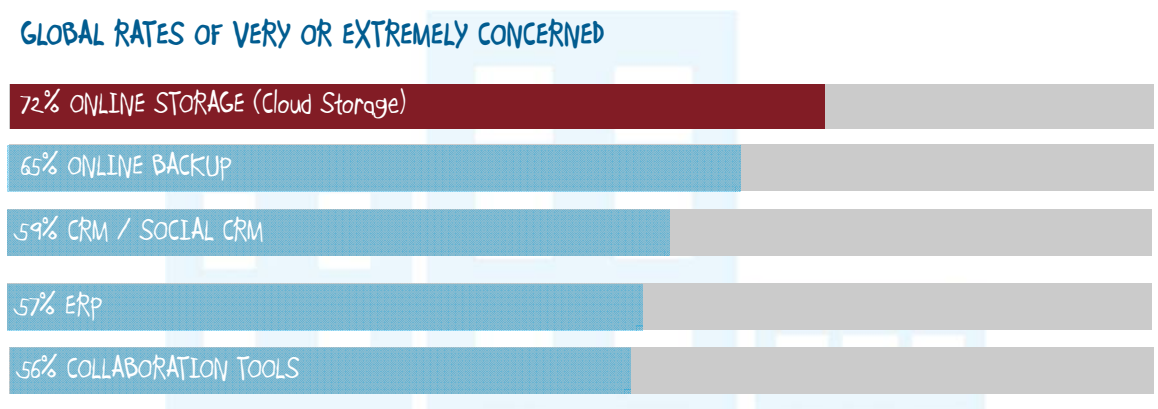
ポリシーと鍵管理を手元に置くことでユーザーガバナンスを実現

クラウド環境におけるデータを中心としたセキュリティ: 特権ユーザーにはアクセスを明確に制限



- アクセス管理（ログ＆監査）
- SIEMとの統合
- ユーザーガバナンスを担保する暗号鍵とポリシー管理

SaaS セキュリティの懸念事項
クラウドストレージが上位



OVUM

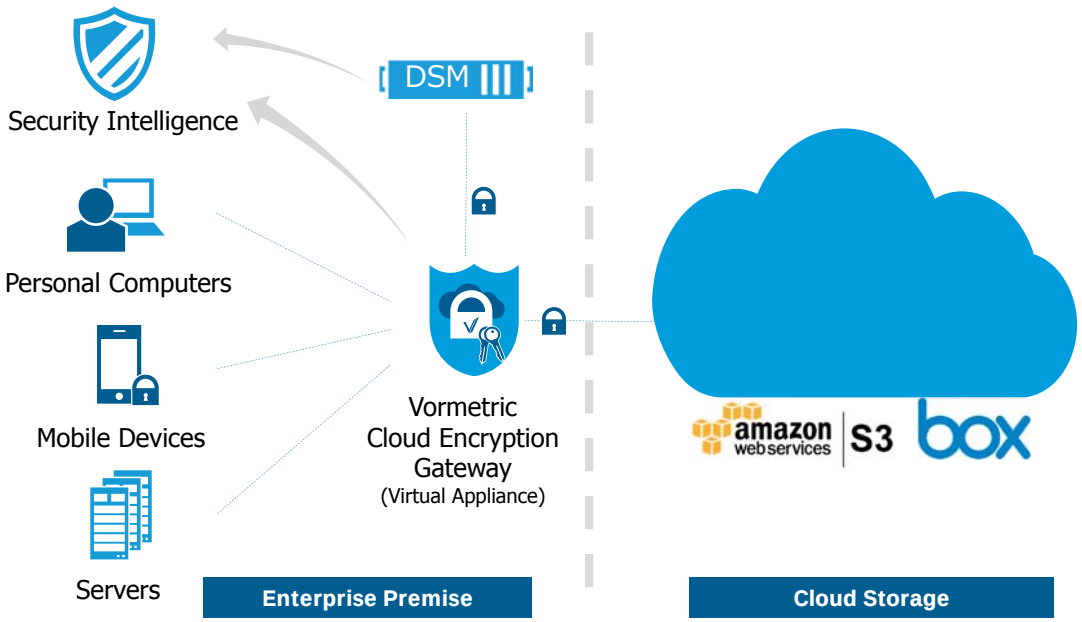
harris poll

"北米ユーザーの 83%、グローバルユーザーの72%が、オンラインストレージにセンシティブなデータを保管しても大丈夫かと重大な懸念を持っている。

- *2015 Vormetric Insider Threat Report – Cloud and Big Data Edition*

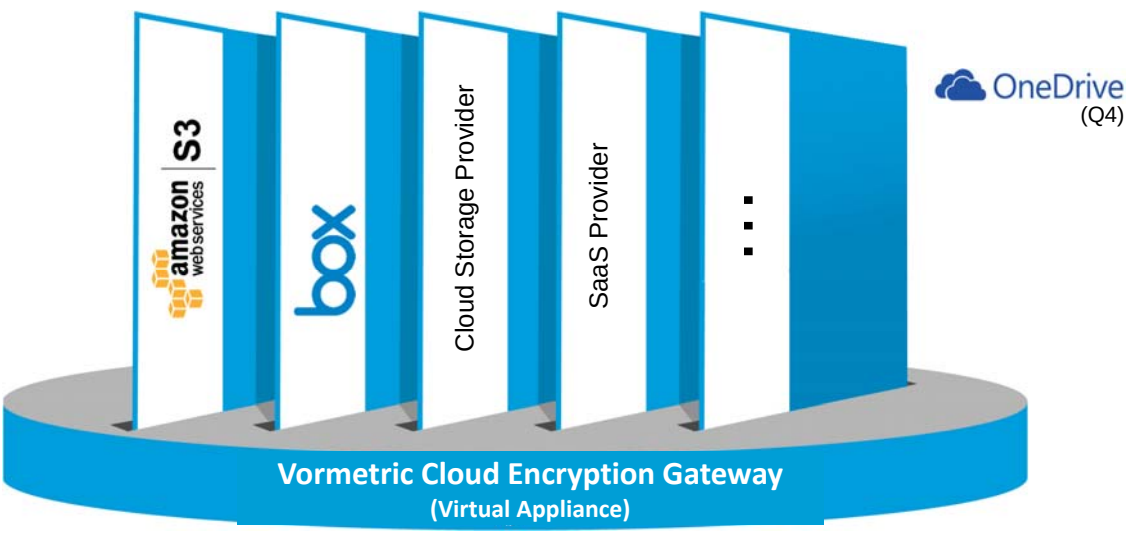
Vormetric Cloud Encryption Gateway

Encrypting and controlling files in cloud storage



Vormetric Security Blades

Modular service delivery with future expandability



Customers purchase licenses that enables new services

単一のプラットフォーム　シンプルな戦略
保存データのセキュリティ

- 物理的
- 仮想環境
- アウトソース

企業のデータセンター

VM VM

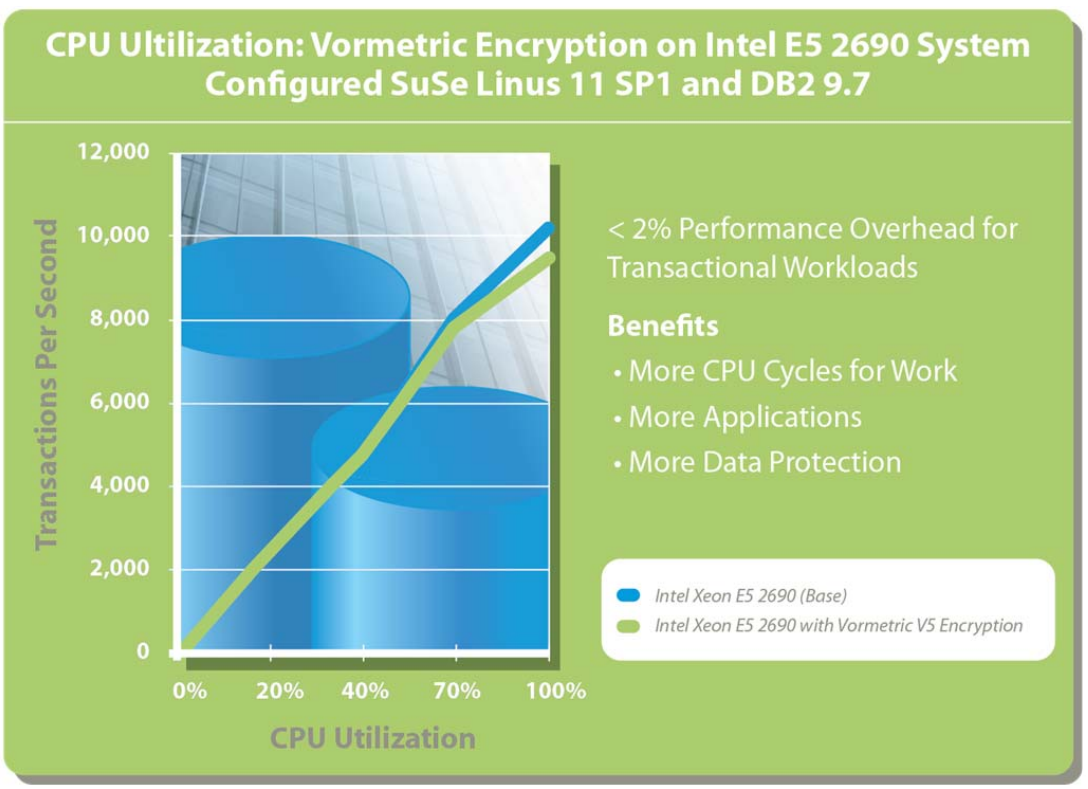
プライベート、パブリック、ハイブリッド
クラウド　SaaS, PaaS, IaaS

リモートサーバー

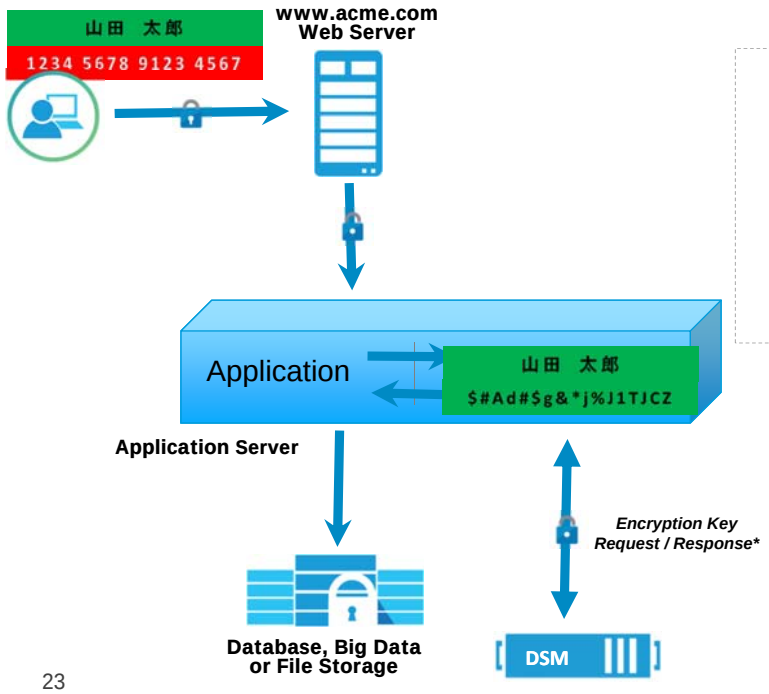
- ソース
- ノード
- 分析エンジン

ビッグデータ

暗号化による性能影響の現在



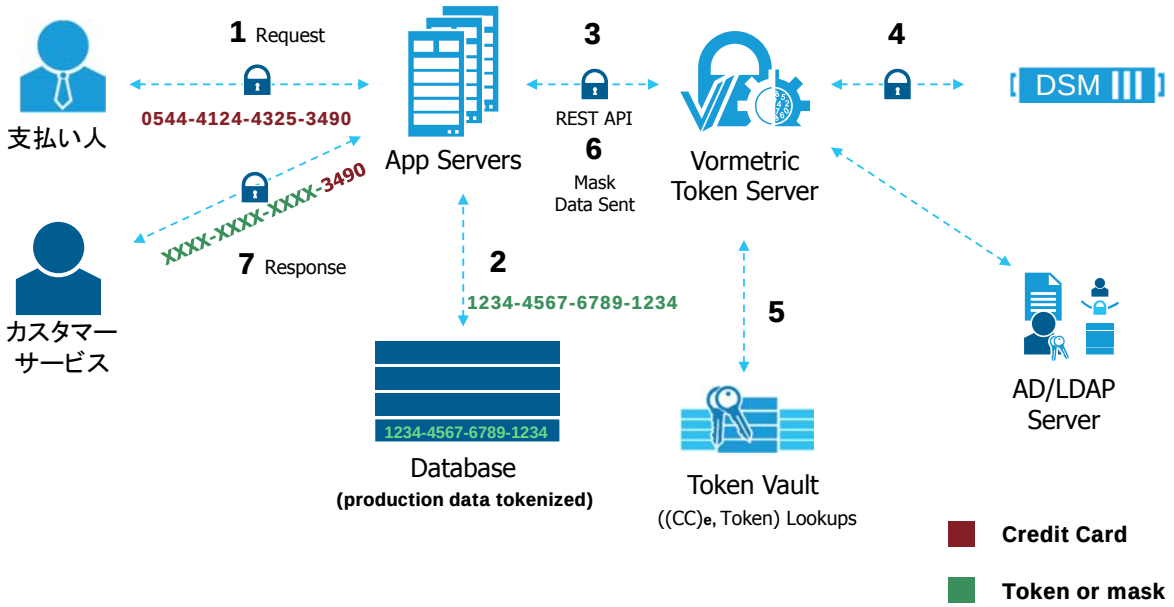
アプリケーションレベルでの暗号化



- Vormetric 暗号化と鍵管理の実績のある信頼性とパフォーマンスを拡張利用
- APIs、ライブラリ、サンプルコードを提供
  - Java, C/C++, .Net

*Key exchange at initial request or policy changes

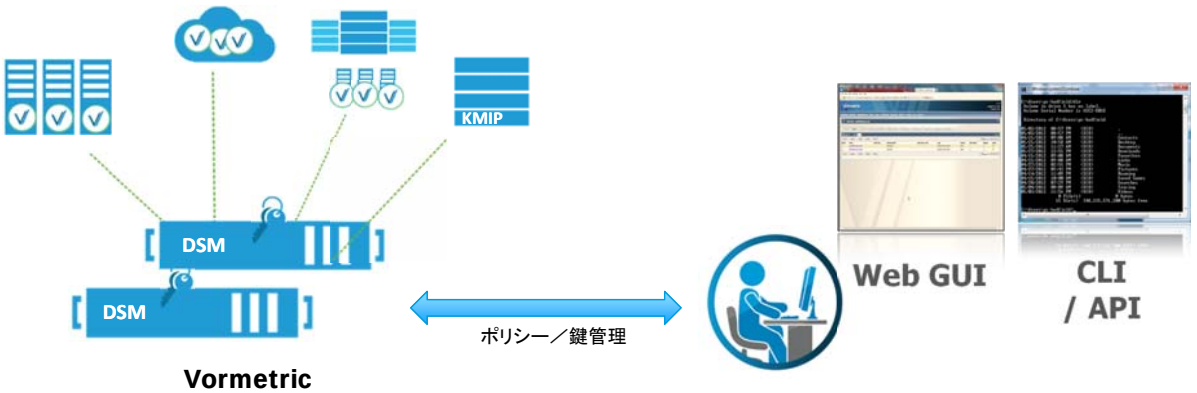
トークナイゼーションとダイナミックデータマスキングによる強度の高いデータセキュリティ



データセントリックセキュリティの実装例

効率的な一元管理

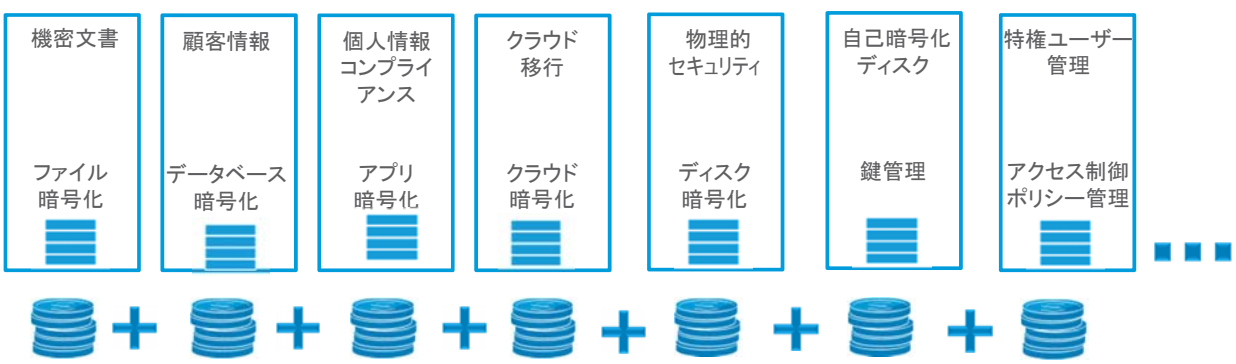
- 鍵とポリシーを集中管理
- 仮想アプライアンス／物理アプライアンス
- クラスターと高可用性
- マルチテナント及び職務分掌の強化
- 10,000以上のデバイスと鍵管理を実現
- Web, CLI インターフェイス
- FIPS 140-2 準拠（仮想レベル2／物理レベル3）



Vormetric
Data Security Manager

従来の暗号化・データのセキュリティ対策例

一貫性のない高価なポイントプロダクト集



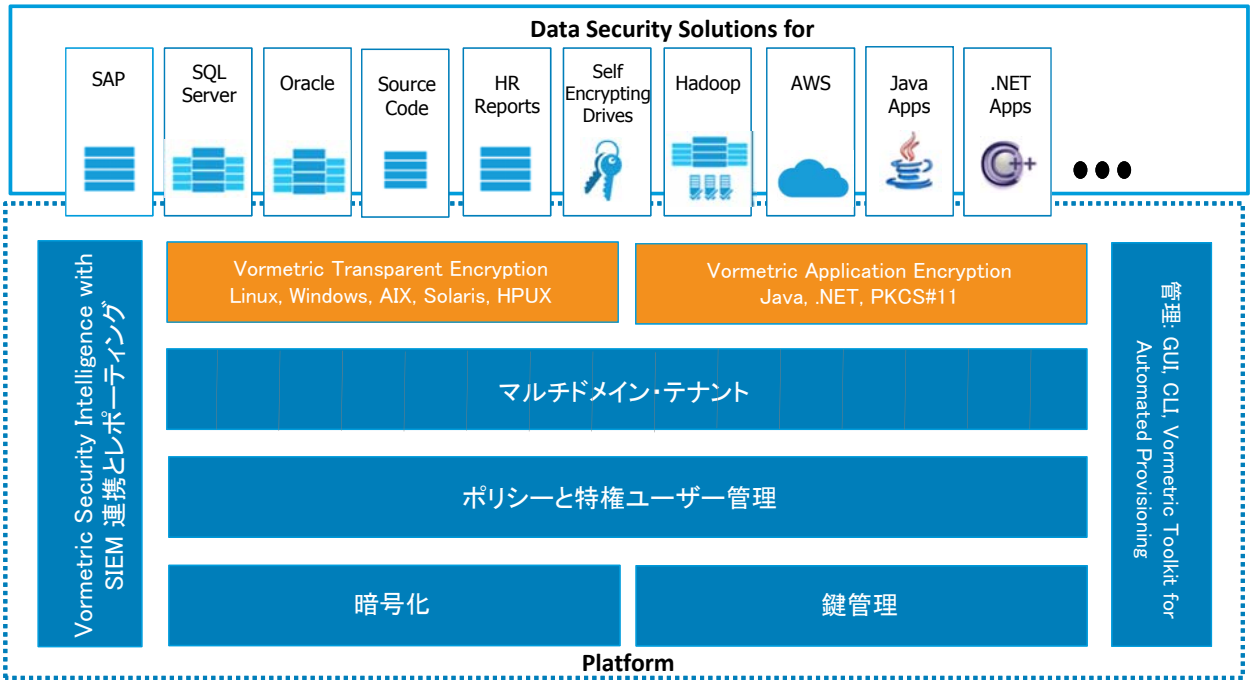
製品毎にインフラ、管理、コンソール、トレーニングなどが必要

- 製品習得
- インストール
- 設定構築
- 統合
- ポリシー設定
- ユーザー教育
- 本番稼働
- 監視
- 冗長化
- 保守
- 監査
- バックアップ …

複雑 • 非効率 • コスト高

新しいデータ・セキュリティ・プラットフォーム

拡張可能なオンデマンド・セキュリティとコンプライアンス対応



24 ヶ月

従来の暗号化手法で全社的な展開を見積もった所、導入完了まで24ヶ月必要

$2.4 MILLION

従来手法による導入費用

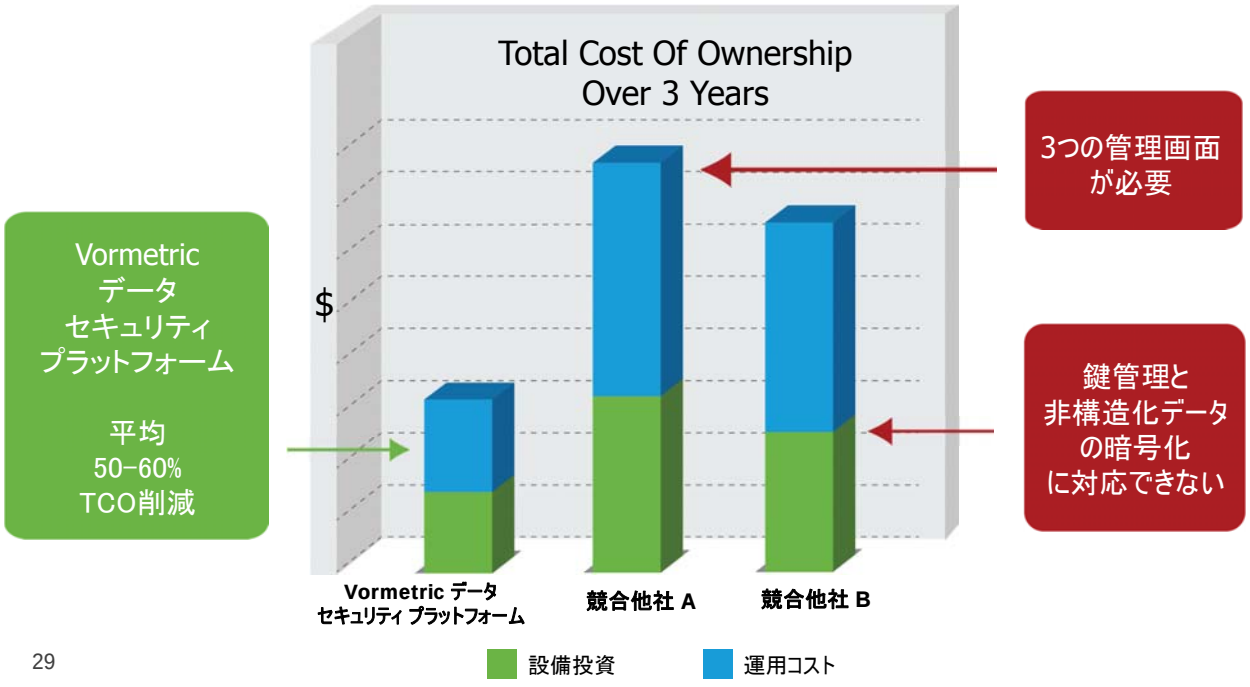
2.4 ヶ月

Vormetric Transparent Encryption (~160 Servers) 導入までに要した時間

Simple • Efficient • Lowest TCO

従来型との比較

コスト削減と複雑さを比較



Total Cost of Ownership 削減を実現

Vormetric データ・セキュリティ・プラットフォーム

- シンプル
  - 直感的で一貫した組織全体のポリシー管理でコスト、人的リソース及びエラーを削減
  - 必要なアプリケーションを透過的に導入
- 効率的
  - 同一プラットフォーム、容易な拡張性
  - SLA を維持し、最低限のサーバーで高性能な暗号化及び冗長化を実現
- セキュリティ強化と迅速なコンプライアンス対応
  - 監査ログとして暗号化、鍵管理、特権ユーザーのアクセス管理などのセキュリティ情報収集
  - インサイダー脅威や APT 攻撃の検知を加速

実演・デモンストレーション

Vormetric社について

- 設立　2001年
- 本社　米国カリフォルニア州、サンノゼ市
- CEO　Alan Kessler（アラン・ケスラー）
- データ保護のためのソフトウェア、ハードウェアソリューションの開発製品化にて2001年起業
- グローバルで1,400社を超えるユーザー
- 金融、公共、流通、製造　業種
- クラウドベンダー

  日本
- 2014年11月　AZM社と販売代理店（VAD）契約を締結
- 2015年　3月　Vormetric東京オフィスを開設

Vormetric データ・セキュリティ・プラットフォーム
世界中のブランドから信頼

グローバルに広がる顧客
- 顧客数1,500社以上
- Fortune 30社の内17社が採用

情報セキュリティに重きをおく企業
- 最大の金融企業
- 流通業最大手
- 大手製造業
- ビジネスサービスプロバイダー
- 連邦政府

OEM パートナー
- IBM
- Symantec

Cloud Service Providers Trust Vormetric

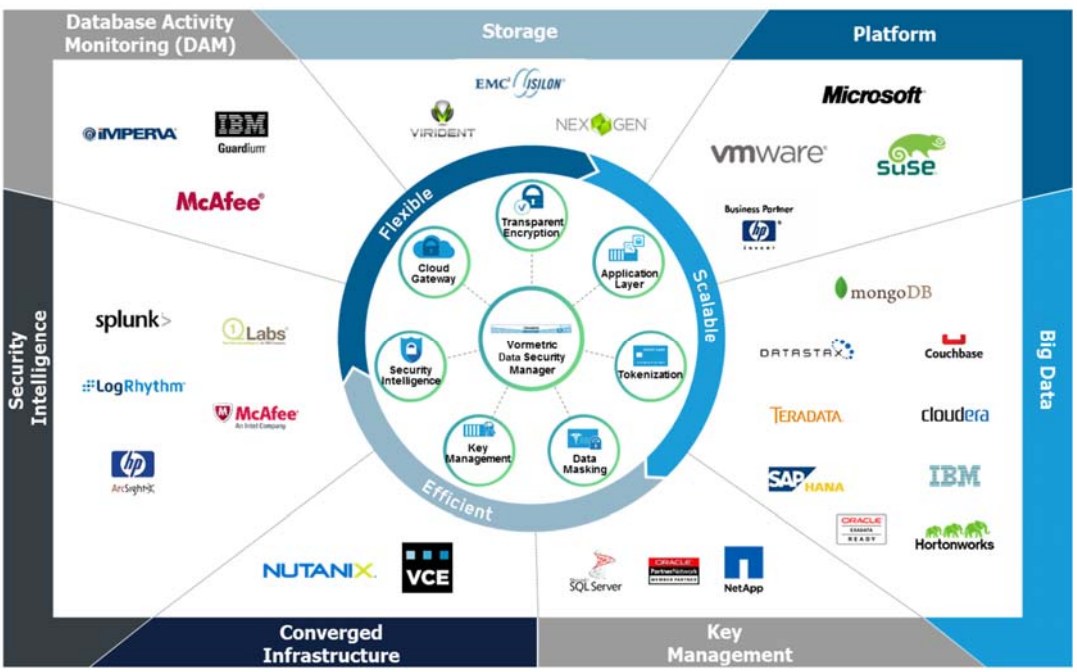
Cloud Managed Services

Microsoft Azure

Google Cloud Platform

amazon web services | Partner Network

主要な関連テクノロジーとのパートナーシップ
サイバーセキュリティソリューションとの緊密な技術連携



付録資料

個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
平成26年12月12日　厚生労働省・経済産業省告示第４号

(4)保管・バックアップ

①作業責任者の明確化

・個人データを保管・バックアップする際の作業責任者の明確化

②手続の明確化と手続に従った実施

・個人データを保管・バックアップする際の手続の明確化

※情報システムで個人データを処理している場合は、個人データのみならず、オペレーティングシステム(OS)やアプリケーションのバックアップも必要となる場合がある。

・定められた手続による保管

・バックアップの実施

・個人データを保管

・バックアップする場合の個人データの暗号化等の秘匿化

・暗号鍵やパスワードの適切な管理

・個人データを記録している媒体を保管する場合の施錠管理

・個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理

・個人データを記録している媒体の遠隔地保管

・個人データのバックアップから迅速にデータが復元できることのテストの実施

・個人データのバックアップに関する各種事象や障害の記録

府省庁対策基準策定のためのガイドライン
平成26年5月19日　内閣官房情報セキュリティセンター

第3部 情報の取扱い

遵守事項

(4) 情報の利用・保存

(a)行政事務従事者は、利用する情報に明示等された格付及び取扱制限に従い、当該 情報を適切に取り扱うこと。

【 基本対策事項 】

<3.1.1(4)(a)関連>

3.1.1(4)-1 行政事務従事者は、情報の格付及び取扱制限に応じて、情報を以下のとおり取り扱うこと。

：

：

f) 電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行う。

g) 電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化する。

データセキュリティサービスオファリング
Vormetricのクラウドパートナー

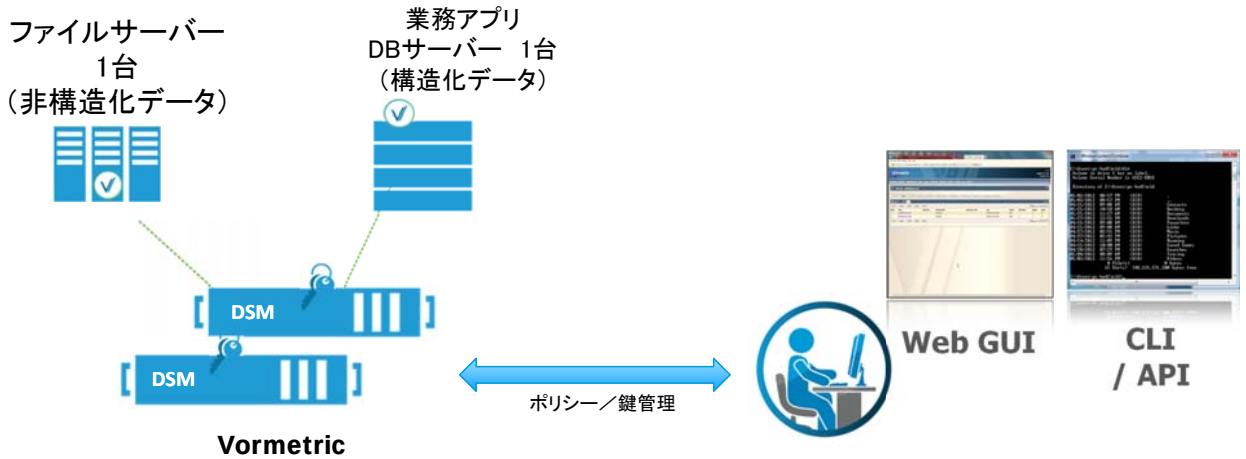
CenturyLink
rackspace
QTS
Microsoft Azure
firehost SECURE CLOUD HOSTING
at&t
CloudHesive
amazon web services | Partner Network
D+H
Pega
BAE SYSTEMS
virtustream
IBM SOFTLAYER
Google Cloud Platform
CIRRITY

“クラウド事業者が提供できる付加価値としてもっとも重要なデータセキュリティの機能を容易な形でVormetricは提供してくれる。重要なテクノロジーパートナーだ。”

John Engates
CTO
rackspace

スターターパック導入構成と参考価格

- 鍵とポリシーを集中管理
- 個人情報などを含むDBサーバー1台
- IPなど漏洩対策が必要なファイルサーバー1台
- DSM 2台HA構成　仮想アプライアンス／物理アプライアンス
- 合計約6百万円（参考価格）



Vormetric
Data Security Manager HA構成