Solution Brief

THALES
CYBERSECURITY

imperva

Imperva Cloud WAF + CipherTrust Cloud Key Management

アプリケーション脅威の防御

cpl.thalesgroup.com

THALES
CYBERSECURITY

アプリケーション脅威の防御とクラウド鍵の管理

エッジから暗号化までを網羅するエンタープライズセキュリティ

現代の組織は、成長とともに顕在化するセキュリティのジレンマに直面しています。**Imperva Cloud WAFがアプリケーションを外部脅威から保護する**一方、多くの組織は依然としてクラウドプロバイダーが管理する鍵に依存してデータの暗号化を行っています。**83%の組織が懸念を示しており**、クラウドセキュリティ侵害が急増する中、アプリケーション保護と暗号管理の間のギャップはビジネス上の重要な課題となっています。ImpervaCloudWAFと**CipherTrust Cloud Key Managementの組み合わせ**は、このギャップを解消し、アプリケーションからデータまで包括的なクラウドセキュリティを実現します。これにより、悪意のあるトラフィックを監視・フィルタリング・ブロックすると同時に、タレスの統合ソリューションを通じて業界をリードする暗号技術を適用します。

クラウドセキュリティの足りない要素

アプリケーション保護だけでは、包括的なクラウドセキュリティは実現できません。Cloud WAFはOWASP Top 10の脅威やボット攻撃などを防ぎますが、クラウド環境に保存されたデータを保護する暗号鍵の制御が十分ではありません。

従来の手法には戦略的な制約があります。クラウドプロバイダーが管理する鍵は、顧客による暗号鍵の管理権限やデータ主権を制限し、マルチクラウド戦略に不可欠な、クラウドに依存しない柔軟性を損なうことになります。

83%
データ主権に関する懸念を抱えている組織 (1)

35%
2024年のクラウドセキュリティ侵害の増加率 (2)

変化を促す市場要因

マルチクラウドの現実：69%の組織が3社以上のクラウドプロバイダーを利用しているが、クラウド上の機密データの80%以上を暗号化している組織はわずか8%にとどまっている。

ベンダー独立性：89%のITリーダーが「企業は単一のクラウドプロバイダーに依存すべきではない」と回答しており、クラウド非依存型ソリューションの需要を後押ししている。

コンプライアンス期限：PCI DSS 4.0は、2025年3月から自動化されたWebアプリケーション保護を義務付けるとともに、包括的な鍵管理を要求している。

侵害コストの増大：クラウドセキュリティインシデントは平均で数百万ドル規模の損害をもたらし、78%の組織が少なくとも1件のインシデントを報告している。

Webアプリケーションファイアウォール　＋　**クラウド鍵管理**

アプリケーション保護と暗号管理の間にある重大なギャップに対応します。 Cloud WAFにより外部脅威からアプリケーションを防御し、またCipherTrust Cloud Key Managementにより信頼できる顧客管理の暗号鍵でアプリケーションが稼働することを保証して、クラウドプロバイダーが管理する鍵サービスへの依存を軽減します。

包括的なセキュリティの利点

業界をリードするImpervaのWAFとタレスのCipherTrust Cloud Key Managementを組み合わせることで、組織は下記を実現できます。

多層防御戦略

リアルタイムのアプリケーション保護と顧客管理の暗号鍵の組み合わせにより、エッジからデータ層まで包括的なセキュリティを確保します。

マルチクラウド鍵管理の一元化

CipherTrust Cloud Key Managementは、AWS、Azure、Google Cloud、Oracle Cloudにわたり、ネイティブ、BYOK、HYOKの各導入モデルをサポートし、統合的な管理を実現します。

暗号主権

Cloud WAFによるアプリケーション保護と併せて、暗号鍵の完全な保管と管理を維持することで、クラウドプロバイダーが外部からの圧力に直面した場合でも、データにアクセスできない状態を保持します。

運用効率の向上

複数のクラウドKMSインターフェースを習得する必要なく、すべてのクラウドにわたるネイティブ、BYOK、HYOK鍵を管理できます。自動化された鍵ローテーションとポリシー同期により、管理オーバーヘッドを削減します。

業界をリードするアプリケーション保護

Imperva Cloud WAFは、ほぼゼロの誤検知率でエンタープライズクラスの保護を提供し、組織が導入初日からブロックモードで運用できるようにします。

OWASP Top 10対策：SQLインジェクション、XSS、リモートファイルインクルージョン攻撃のリアルタイム遮断

高度なボット防御：機械学習による高度な自動化脅威の検知

APIセキュリティ：RESTおよびGraphQL APIの包括的な保護

DDoS軽減：大規模攻撃およびアプリケーション層攻撃に対する統合的な防御

幅広いコンプライアンス対応

アプリケーション保護と暗号鍵ガバナンスの両面で、PCI DSS、HIPAA、GDPR、NIS2の要件に同時対応します。

マルチクラウドの自由度

クラウド非依存の鍵管理により、アプリケーションがどこで稼働していても柔軟性を維持できます。ベンダーロックインを排除し、すべての環境で一貫したセキュリティポリシーを適用します。

単一ベンダーによるアプローチでベンダー管理のオーバーヘッドを大幅に削減します。外部からのアプリケーション攻撃と鍵ガバナンス一元化の課題を同時に解決することで、潜在的な侵害コストを低減します。

94%

導入初日から
ブロックモードで運用した顧客

ほぼゼロ

誤検知により
即時保護を実現

始める準備はできましたか？

暗号管理なしでアプリケーションを保護している場合や、アプリケーションの可視性なしで鍵を管理している場合でも、この多層的なソリューションは実証済みの技術によって包括的な保護を提供します。

「Imperva Cloud WAF + CipherTrust Cloud Key Management」が、お客様固有のコンプライアンス要件とセキュリティ目標にどのように対応するか、当社のセキュリティ専門家にご相談ください。

規制への適合性

業界を問わず、組織はアプリケーション保護と暗号鍵ガバナンスによって有効に対処できる、共通のコンプライアンス課題に直面しています。

PCI DSS 4.0

自動化されたWeb
攻撃防御 + 鍵
管理プロセス

HIPAA

ePHI（電子保護医療情報）の
技術的保護策 + 必要に
応じた暗号化

GDPR

インシデントに対するシステムの
レジリエンス + 個人データの
暗号化

NIS2

リスクに応じた適切な
セキュリティ対策 + 暗号
ポリシーと暗号化

導入により得られる価値

Cloud WAFをすでに導入しているお客様は、マルチクラウド環境全体にわたる鍵の一元管理を追加することで、セキュリティ投資をシームレスに拡張できます。これにより、確立されたタレスとの関係を活用して導入を加速しつつ、暗号主権を実現できます。また**CipherTrustをすでにご利用のお客様**は、既存の暗号化管理を補完する包括的なアプリケーション層防御を獲得し、アプリケーション脅威と鍵管理運用の両方に対する可視性を得られます。さらに**クラウドセキュリティをゼロから完全に構築するお客様は**、両ソリューションを同時に導入することで、単一ベンダー戦略によるエンドツーエンド保護を実現し、運用の複雑性を低減するとともに、すべてのクラウド環境においてアプリケーションからデータ暗号化まで一貫したセキュリティポリシーを維持できます。

業界からの評価

KuppingerColeは、タレスを2025年のデータセキュリティプラットフォーム部門で「総合リーダー」に選出しました。Forresterは、タレス傘下のImpervaをWebアプリケーションファイアウォールソリューションのリーダーとして位置付けています。Gartner Peer Insightsでは190件以上の顧客レビューでImpervaが星4.5の評価を獲得しており、複数のFIPS 140-3レベル3認証がエンタープライズセキュリティアーキテクチャの有効性を実証しています。

タレスについて

タレスは、サイバーセキュリティのグローバルリーダーです。世界中の企業、政府機関、そして高い信頼を得ているさまざまな組織が、重要なアプリケーション、機密データ、ID、ソフトウェアを、あらゆる場所で包括的に保護し、最高のROIを実現できるよう支援しています。タレスのソリューションは、世界148カ国でFortune Global 500企業の58%を含む30,000社以上で導入されています。革新的なサービスと統合プラットフォームを通じて、リスクの可視化、サイバー脅威の防御、コンプライアンスギャップの解消を可能にし、毎日数十億の消費者に安全で信頼性の高いデジタルエクスペリエンスを提供しています。

cpl.thalesgroup.com

お問い合わせ先 – 連絡先情報につきましては、cpl.thalesgroup.com/ja/contact-usをご覧ください。