

仮想パッチによりレガシーOSの保護やゼロデイ攻撃などの脅威からサーバー環境保護を実現

Trend Micro Cloud One™ - Workload Security

昨今、サーバー環境へのサイバー攻撃は、さまざまな攻撃手法を組み合わせるなど巧妙な手口で行なわれています。場合によってはサポートが終了したOSをそのまま使わざるを得ないことがあるサーバー環境においては、物理・仮想・クラウド・コンテナといった利用環境にかかわらず、一貫した多層でのセキュリティ対策が重要となります。



課題 1

サポートが終了したサーバーOSにも、新たな脅威への対策を行ないたい

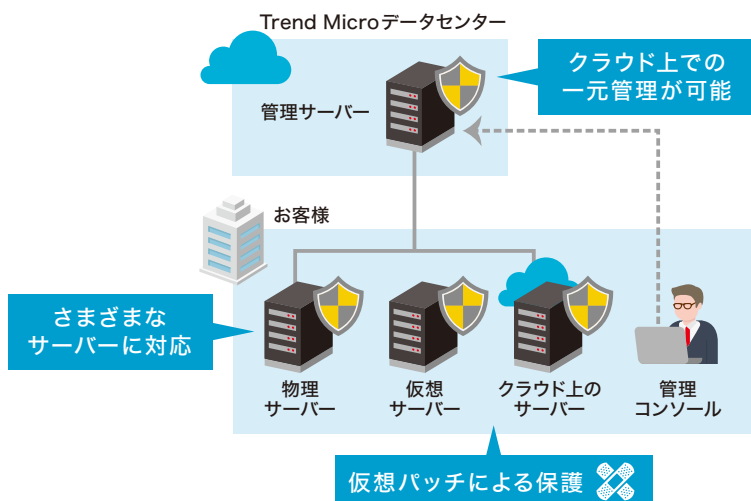
課題 2

サーバー環境のセキュリティ対策をコストをかけずに手軽に導入したい

課題 3

異なるサーバー環境に対しても、一貫したセキュリティ対策を実施したい

Trend Micro Cloud One™ - Workload Security はサーバーに必要なセキュリティ機能をオールインワンで提供します



- ✓ **不正プログラム対策**
リアルタイムにウイルスを検索
- ✓ **IPS/IDS (仮想パッチ)**
仮想パッチでOSやアプリケーションの脆弱性を保護
- ✓ **Webレピュテーション**
不正なURLへの接続を防止
- ✓ **ファイアウォール**
DoS攻撃など不正な通信を防御
- ✓ **変更監視 (改ざん検知)**
ファイルやレジストリなどの変更を監視
- ✓ **セキュリティログ監視**
OSやミドルウェアのセキュリティイベントを集中監視
- ✓ **アプリケーションコントロール**
ホスト上で実行されるアプリケーションを監視

仮想パッチにより 新たな脆弱性にも対策可能

メーカーのサポートが終了したサーバーOSに対しても、仮想パッチの自動適用により脅威への防御を迅速に実現。

コストを抑えた 短期間での導入が可能

SaaS提供のため管理サーバーも不要で、導入コストの削減を実現。サーバー1台分からのスモールスタートが可能。

一貫したセキュリティ対策が可能

物理環境、クラウド環境、Windows、Linuxなど、利用環境を問わず、同一のセキュリティレベルでの対策が可能。

Trend Micro Cloud One™ - Workload Securityの強み



仮想パッチによる脆弱性保護

IPS/IDSルールを用いて、ネットワークレベルで脆弱性を突いた攻撃からOSやアプリケーションを保護。仮想パッチにより、メーカーのサポートが終了したOSであってもセキュリティ対策が可能。



さまざまなセキュリティ機能による多層防御

不正プログラム対策、セキュリティログ監視、ファイアウォール、IPS/IDSなど、サーバーに必要なさまざまなセキュリティ機能をまとめて搭載しているため、1つの製品で多層防御を実現。



さまざまなサーバー環境に対応

物理環境、仮想環境、クラウド環境、コンテナ環境など、さまざまなサーバー環境に対応しているため、各環境の一元管理が可能。



無駄のないスモールスタート

サーバー1台分から購入可能なため、無駄のない投資が可能。また、月額利用のため、初期コストを抑えた利用を実現。

ライセンス別提供機能

提供機能	Workload Security Enterprise	Workload Security Essential
不正プログラム対策	○	○
IPS/IDS (仮想パッチ)	○	×
Webレピュテーション	○	○
ファイアウォール	○	×
変更監視 (改ざん検知)	○	×
セキュリティログ監視	○	×
アプリケーションコントロール	○	×
保護対象サーバーサポートOS	Windows、Linux、Solaris/AIX	Windows、Linux、Solaris/AIX
管理サーバー	サービス提供*	サービス提供*

*トレンドマイクロ社がクラウド上で提供する管理サーバーをご利用いただくことが可能です。

※本カタログ中の会社名、商品名は各社の商標、または登録商標です。※本文中および図中では、TMマーク、®マークは表記しておりません。※製品の仕様は、改良のため、予告なく変更する場合があります。※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。※本カタログ中の情報は、カタログ作成時点のものです。

 株式会社 日立ソリューションズ

www.hitachi-solutions.co.jp



本カタログ掲載商品・サービスの詳細情報

www.hitachi-solutions.co.jp/dsaas/

S21S-06-00

2022.03