radware
availability | performance | security

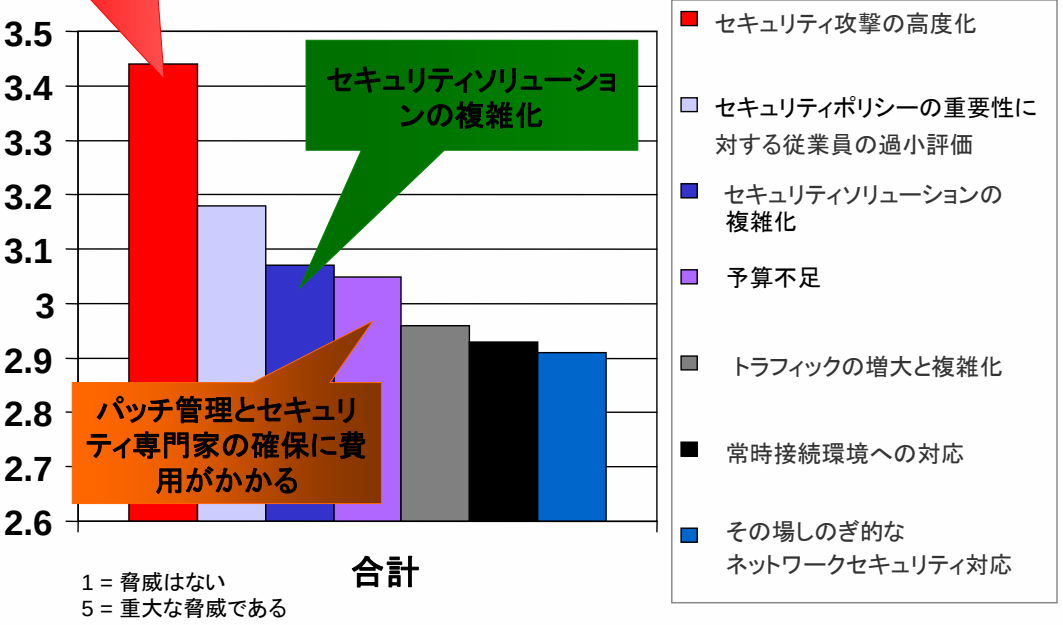
ラドウェアの次世代型　侵入防御技術

DefensePro 3.10

Smart Network. Smart Business.

radware | セキュリティの課題

Smart Network. Smart Business.



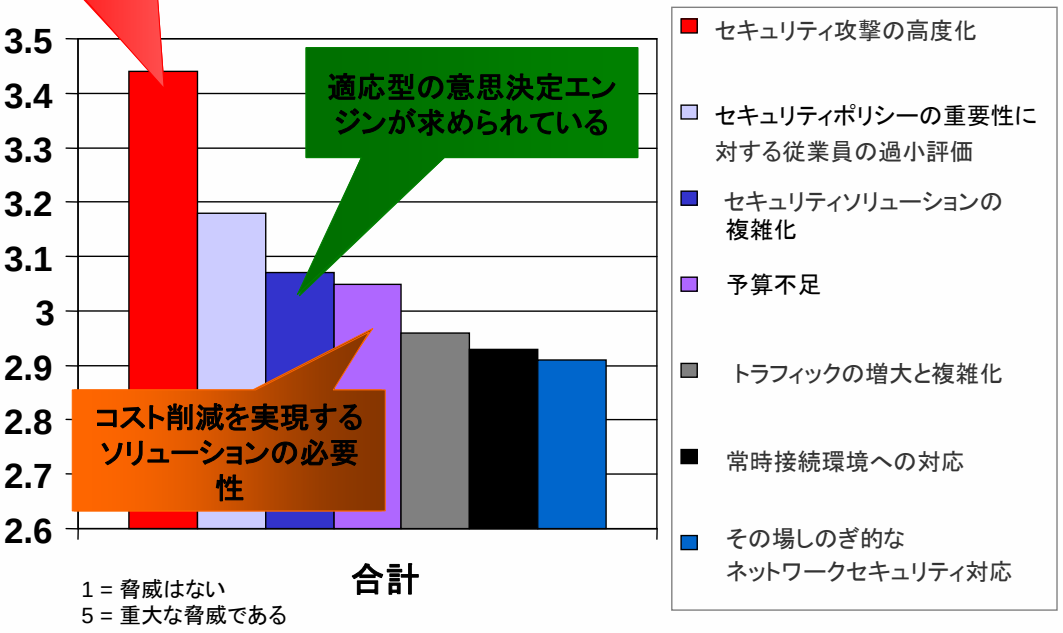
1 = 脅威はない
5 = 重大な脅威である

出典：IDC 企業セキュリティ調査（2005年12月）

radware | セキュリティの課題

Smart Network. Smart Business.

より「スマート」な
セキュリティ技術が
求められている



合計

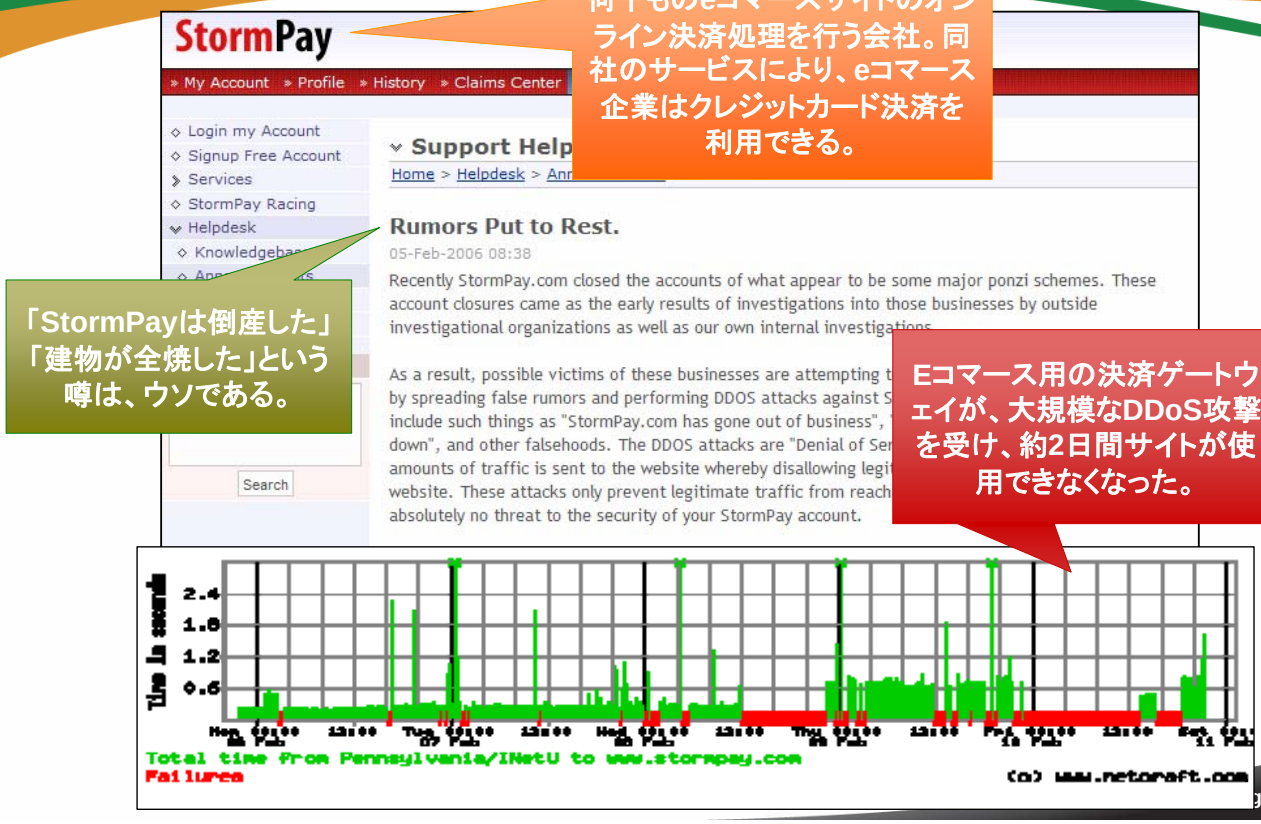
1 = 脅威はない
5 = 重大な脅威である

出典：IDC 企業セキュリティ調査（2005年12月）

radware | DoS攻撃：“建物が全焼した”

Smart Network. Smart Business.

何千ものeコマースサイトのオンライン決済処理を行う会社。同社のサービスにより、eコマース企業はクレジットカード決済を利用できる。



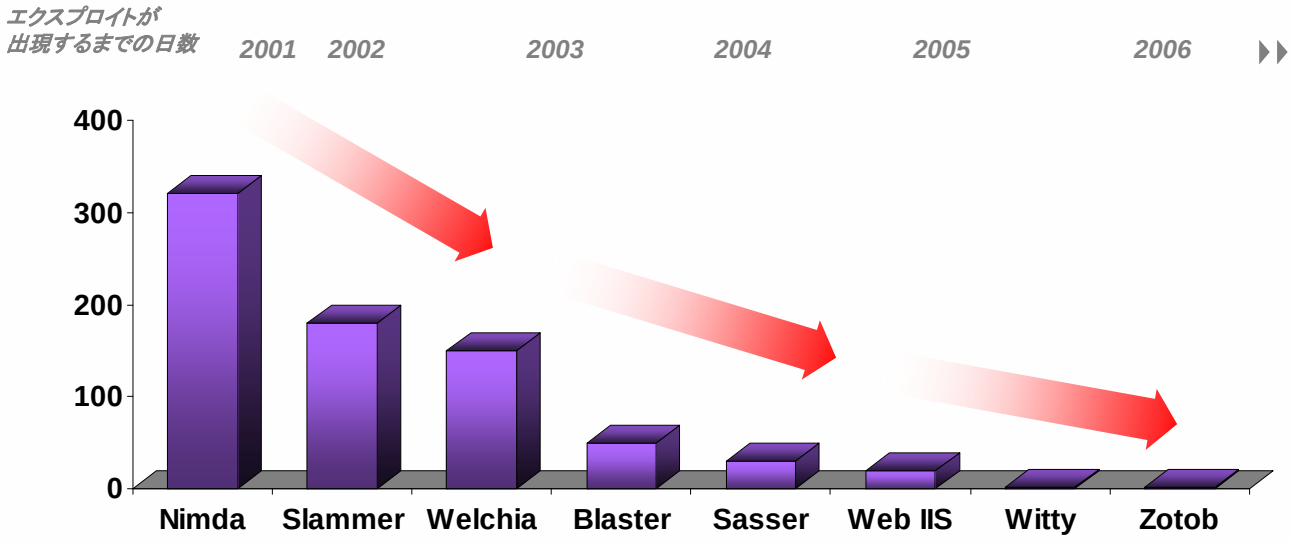
「StormPayは倒産した」「建物が全焼した」という噂は、ウソである。

Eコマース用の決済ゲートウェイが、大規模なDDoS攻撃を受け、約2日間サイトが使用できなくなった。

radware | ゼロデイ攻撃は実際に起きています

Smart Network. Smart Business.

エクスプロイトが出現するまでの時間は、短くなっています



radware | VoIPセキュリティの傾向

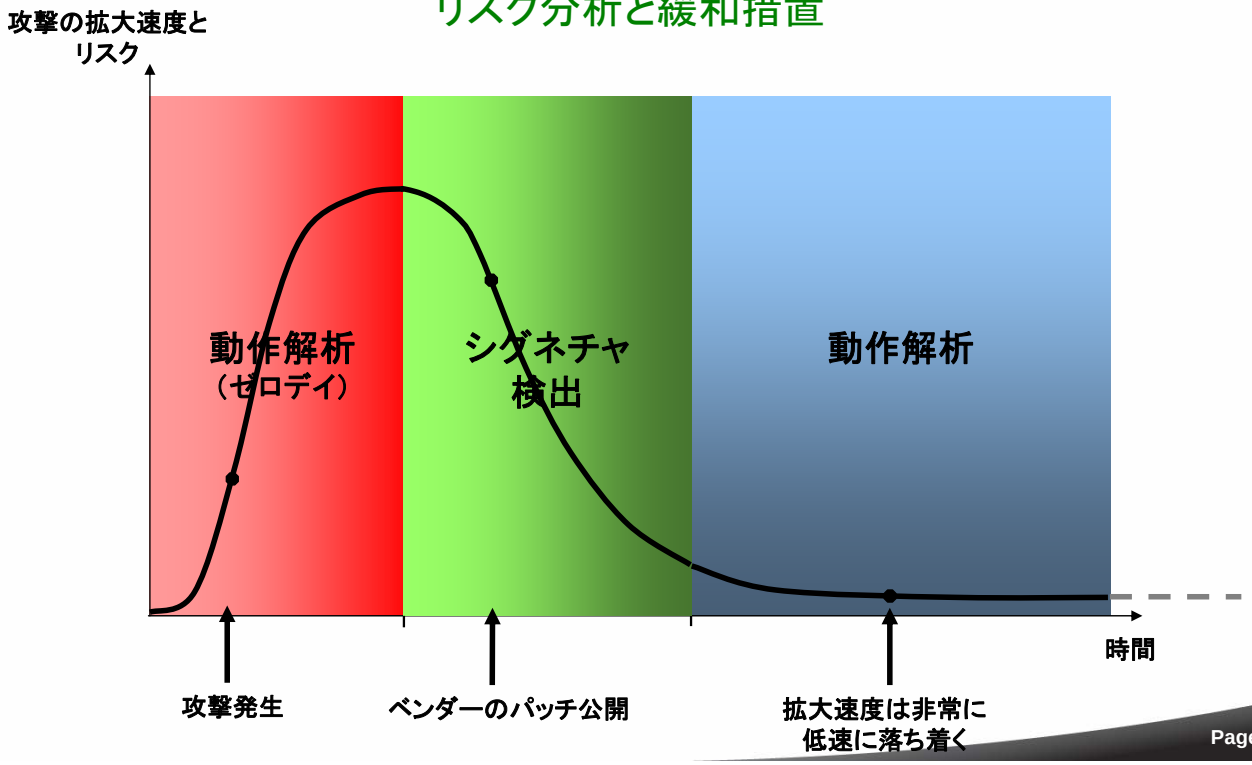
Smart Network. Smart Business.

身近な電話にも脆弱性の問題が迫っています

- 2007年までに、VoIP は世界の音声サービスの75%を占める見込み（「Communications Convergence Magazine」調べ）
- VoIPは、DoS攻撃など、IPベースの攻撃に対して脆弱
- 不十分な音質では、ユーザに受け入れられない
  - VoIPのリアルタイム性が、より脆弱性を高めている
  - VoIPパケットは遅延すると意味がない

- サービス拒否（DoS）攻撃、分散型サービス拒否（DDoS）攻撃
  - ネットワーク上のほぼすべての要素が、DoS攻撃の対象となりうる。
  - VoIPネットワークに対するDoS攻撃には、ネットワーク層におけるものと、アプリケーション層におけるものがある。

リスク分析と緩和措置



- 脆弱性の傾向
  - 毎月平均40件の新たな脆弱性が報告されています
    - 出典: US-Cert（**重大な**脆弱性のみ掲載）
  - 年間では、500件もの**重大な**脆弱性が新たに報告されています
- TCO（総所有コスト）の課題
  - シグネチャデータベースの継続的な**拡大**
  - パフォーマンスの**低下**
  - 高額なメンテナンス費用

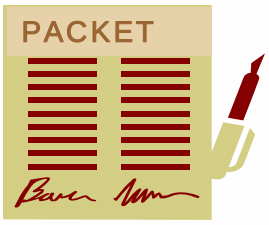
*結論: シグニチャベース **だけの** IPS エンジンでは、現在のセキュリティに関する脅威に対抗できません。*

- 効果的なIPSソリューションは、将来起こりうる次の脅威に対応する必要があります:
  - ✓ DOS/DDoS攻撃 – 既知の攻撃とゼロデイ攻撃
  - ✓ ネットワークワーム – 既知の攻撃とゼロデイ攻撃
  - ✓ アプリケーションの既知の脆弱性を利用した攻撃

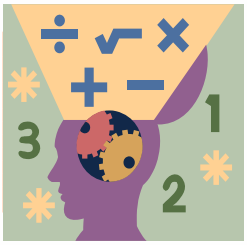
- ✓ 解決策:バランスのとれた、スマートなハイブリッドテクノロジ
  - ✓ 適応型の動作解析
  - ✓ シグネチャベースの検出
  - ✓ 帯域管理(トラフィックシェーピング)

利用可能なソリューションのタイプ

- **コンテンツベースのIPS**
  - シグネチャベース
  - プロトコル異常に基づくルール
  - アプリケーション層に対する単発の攻撃に対応

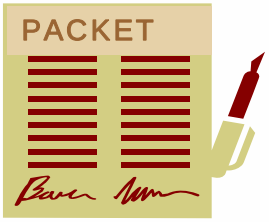


- **レートベースのIPS**
  - トラフィックの閾値は時間ベースで設定
  - 手動設定
  - 高度な専門知識が必要
  - 攻撃の緩和(レートの制限)

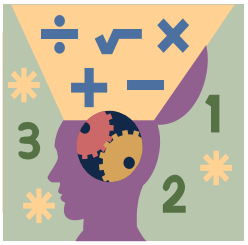


利用可能なソリューションのタイプ

- **コンテンツベースのIPS**
  - シグネチャベース
  - プロトコル異常に基づくルール
  - アプリケーション層に対する単発の攻撃に対応



- **適応型動作ベースのIPS**
  - 動作解析（ゼロデイ攻撃）
  - 自己学習機能
  - 自己修正機能
  - “ハンズオフ”型



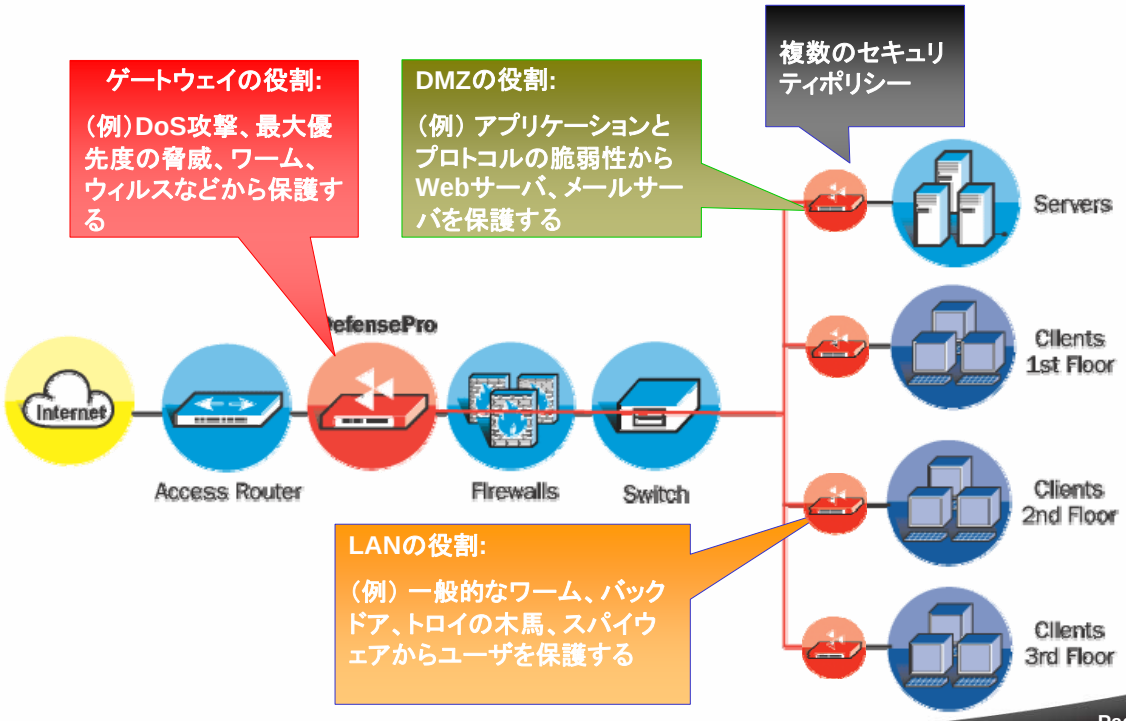
Radwareのハイブリッドアプローチは
相互に補完し合い
より完全なソリューションになります

DefensePro は、マルチギガビットの侵入防御とDOSプロテクションを兼ね備えた、統合型IPSです。先進的な自己認識対応とコンテンツベース、帯域制御をひとつにまとめた、拡張性の高いアプライアンスベースのマルチレイヤセキュリティソリューションです。

Tolly Verified
NSS approved
“With a range of innovative technologies under the hood, we found the V-100's detection and mitigation capabilities to be excellent.” Bob Walder, Director of the NSS Group and author of the report.
WINNER BEST OF INTEROP NETWORLD INTEROP 2005

radware | 企業への展開例

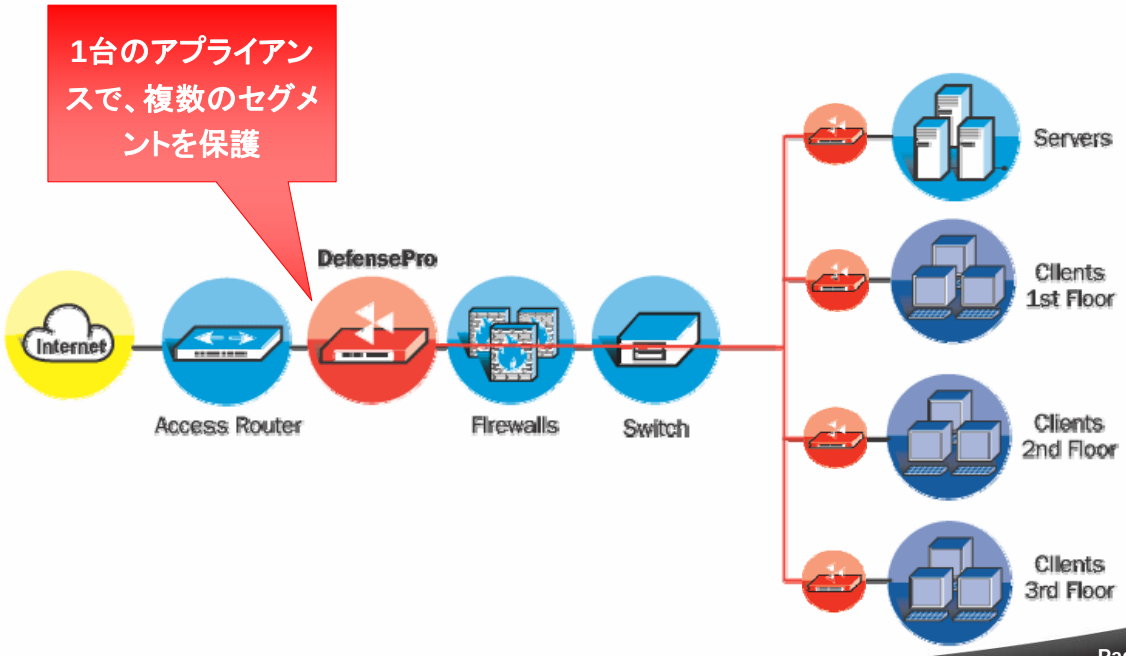
Smart Network. Smart Business.

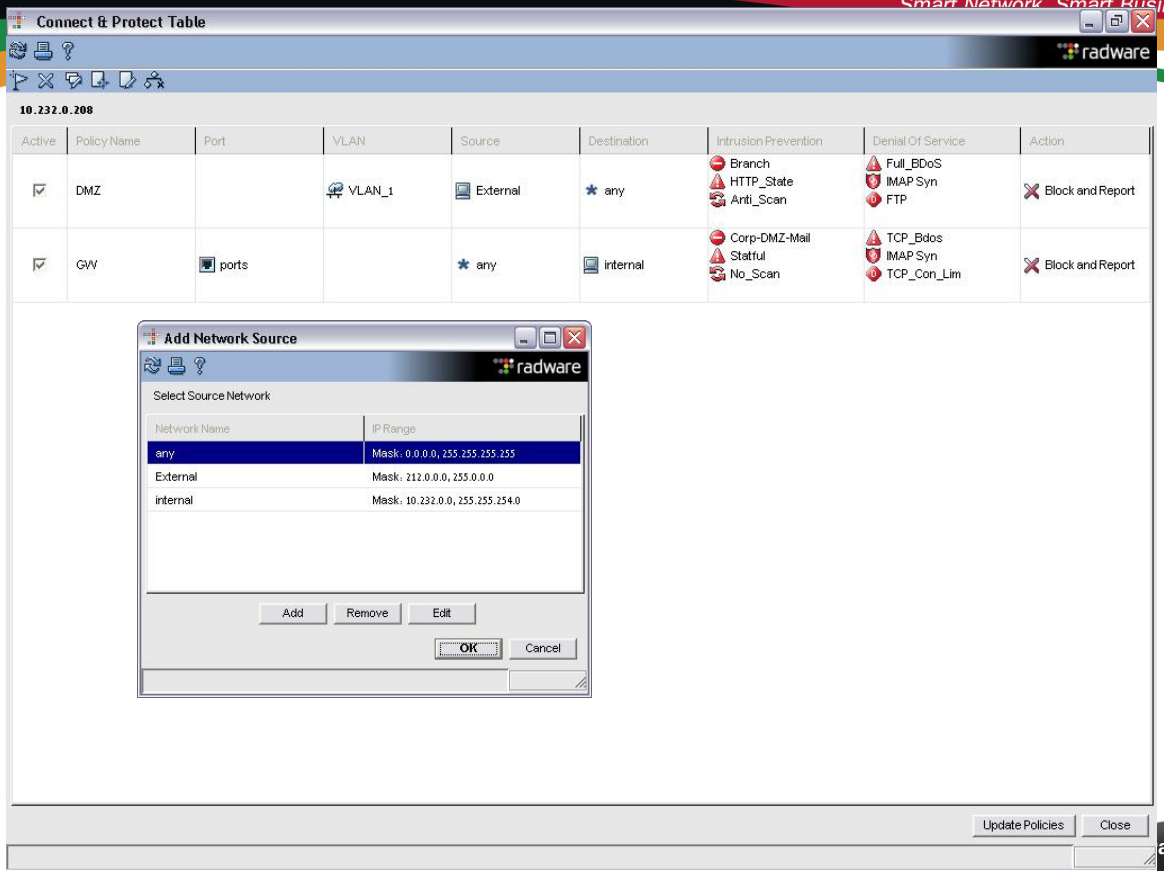


radware | 企業への展開例

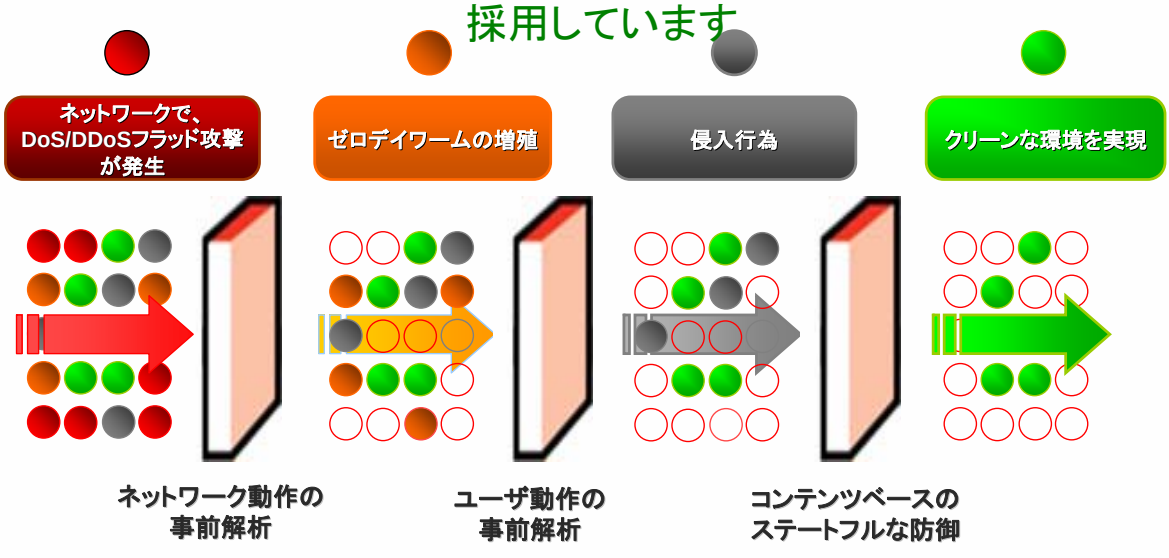
Smart Network. Smart Business.

1つの筐体に仮想的な侵入防御システムを構築



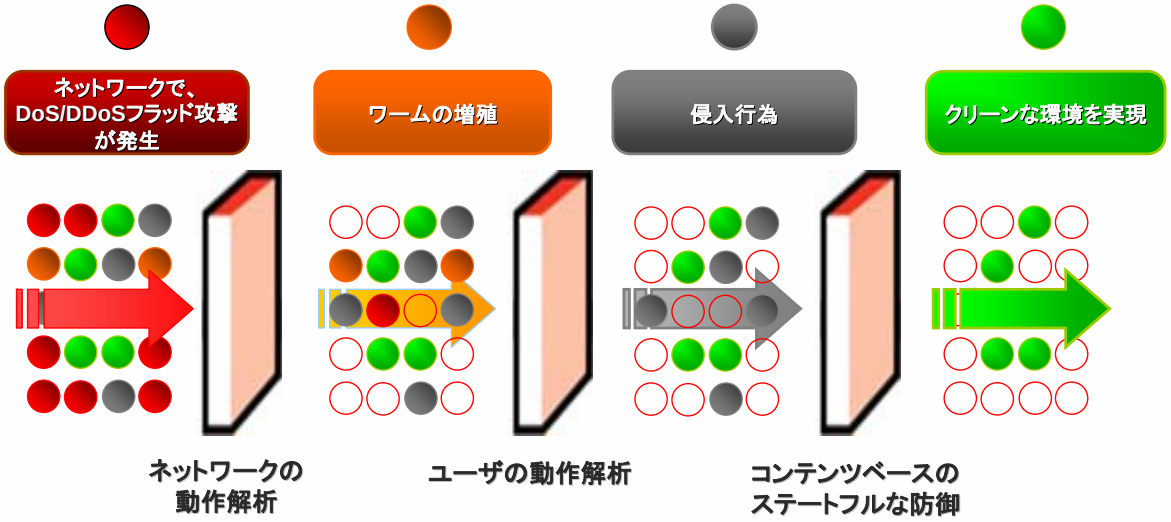


DefenseProは積極的なセキュリティアーキテクチャを採用しています



radware | “スマート”な適応型のマルチレイヤフィルタ

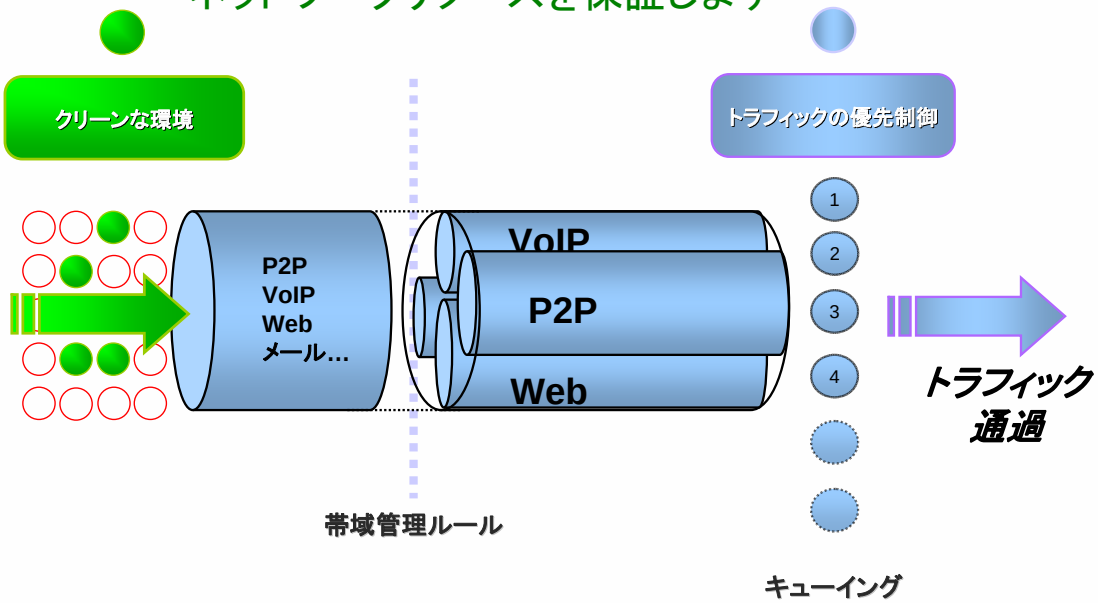
Smart Network. Smart Business.



radware | 効果的なトラフィックシェーピング

Smart Network. Smart Business.

帯域管理ルールの採用により、
ネットワークリソースを保証します



キューイングアルゴリズム（CBQ、WFQ、wRED）や階層的な帯域管理、
その他の機能により、100以上のアプリケーションに対応します。

radware | マルチギガビットの侵入防御システム

Smart Network. Smart Business.

- ネットワーク動作に基づき、ゼロデイ型のDoS攻撃を防御
- ユーザ、ホストの動作に基づき、ゼロデイ型のワームやボットを防御 新機能
- 双方向スキャンによる、ステートフルなコンテンツベースの侵入防御

- サーバへの侵入
  - Webの脆弱性
  - メールサーバへの侵入
  - FTPサーバへの侵入
  - SQLサーバへの侵入
  - DNSサーバへの侵入
- ワーム、ウイルス
- トロイの木馬、バックドア
- 水平、垂直スキャン

- クライアント側の脆弱性
- SIP 新機能
- IRCボット 新機能
- スパイウェア
- プロトコル異常
- IP/TCP層での回避攻撃
- IPv6でのトラフィックスキャン 新機能
- SSLベースの攻撃 (*)

*** AppXcel が別途必要です**

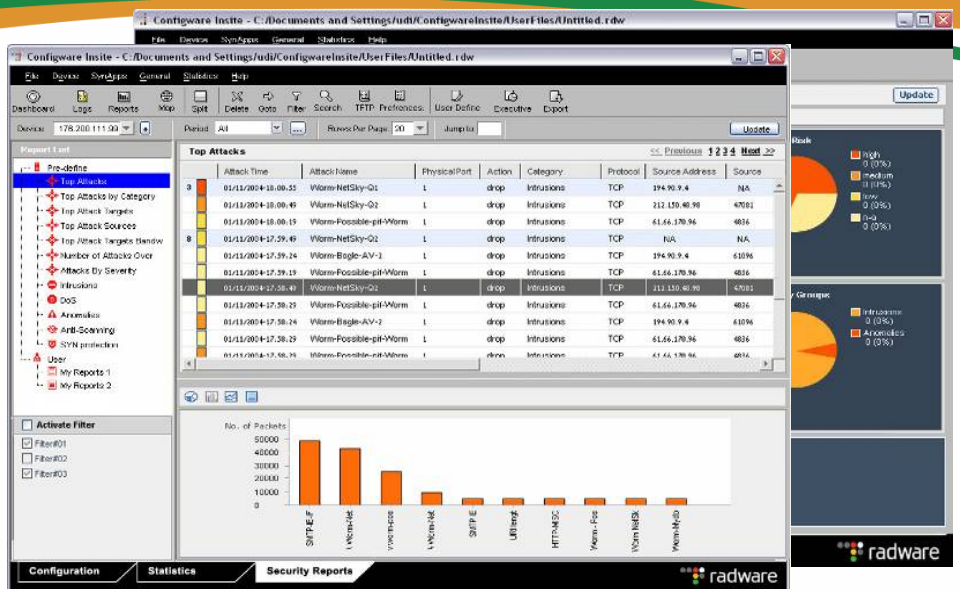
radware | 集中管理型のセキュリティレポート

Smart Network. Smart Business.

監視:ネットワーク全体で、すべての悪意ある行為をリアルタイムに監視

radware | 集中管理型のセキュリティレポート

Smart Network. Smart Business.

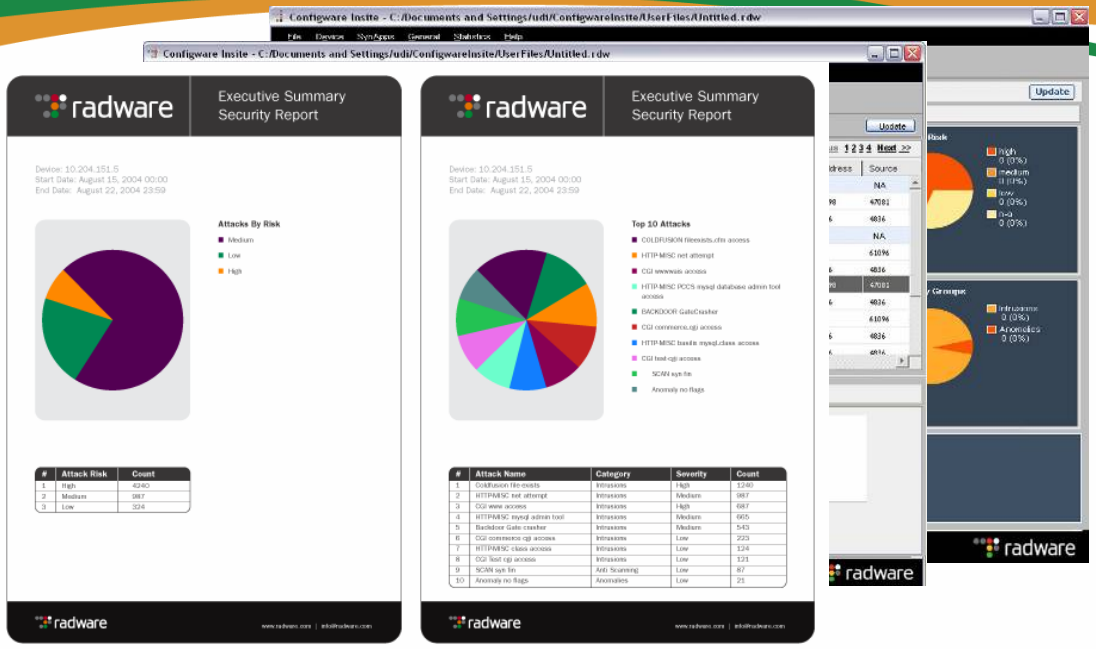


監視:ネットワーク全体で、すべての悪意ある行為をリアルタイムに監視

カスタマイズレポート: 管理者向けにビット単位での解析報告、フォレンジックにも対応

radware | 集中管理型のセキュリティレポート

Smart Network. Smart Business.



監視:ネットワーク全体で、すべての悪意ある行為をリアルタイムに監視

カスタマイズレポート: 管理者向けにビット単位での解析報告、フォレンジックにも対応

エクゼクティブレポート:ネットワークセキュリティ全般をサマライズ

radware | DefensePro 製品ラインアップ

Smart Network. Smart Business.

DefensePro 6000

- 大企業や大規模な通信事業者におけるゼロデイ型のDoS攻撃やワーム を防御
- 最大6Gbpsのスループット
- 10のGEポートを含む9つのセグメントに対応

DefensePro x20 シリーズ

機能拡張

- 本社部門、データセンタでの防御に最適
- 9つのセグメントを保護
- ソフトウェアによるスケーラブルなパフォーマンスのアップグレード

  600 → 1000 → 3000 Mbps

DefensePro x02 シリーズ

新製品

- 企業のゲートウェイ、支店、遠隔地のオフィスに最適
- 1つのセグメントを保護
- ソフトウェアによるスケーラブルなパフォーマンスのアップグレード

  100 → 200 → 500 Mbps

radware | DefensePro 3.0 と 3.10 の主な機能

Smart Network. Smart Business.

- 適応型のDoS攻撃防御
- 適応型のワーム防御
- VoIP (SIP)セキュリティの確保
- IRCボットからの保護
- スパムボットからの保護
- IPv6への対応

最適な機能を
ハイブリッド

動作とシグネチャ
ベースの意思決定

- 新製品ラインアップ (DefensePro x02、x20)
  - 100Mbps～500 Mbps – ライセンスのアップグレードのみで対応
  - 600 Mbps～3 Gbps – ライセンスのアップグレードのみで対応

radware | 主な差別化ポイント (1)

Smart Network. Smart Business.

- **ハイブリッドテクノロジ** – 適応型の動作解析、プロトコル異常、シグネチャベースの技術と、帯域制御機能のバランスが「スマート」に取れたテクノロジ
- 業界トップクラスの**ゼロデイ**攻撃防御機能:
  - 内部および外部からの**ネットワークワームの増殖**を積極的に防御
  - ゼロデイ型の**DoS/DDoSフラッド攻撃**を18秒以内に防御
  - **ネットワークスキャン**と、ネットワーク層、アプリケーション層における攻撃前の偵察行為を積極的に防御
- **ポート密度**とIPSポリシーの仮想化
  - Virtual IPSを以下の識別子により設定可能
    - vLAN、MPLS、IPv6、L2TPなど

radware | 主な差別化ポイント (2)

Smart Network. Smart Business.

- **ビジネスの成長に応じた対応** – スループットに応じてライセンスをアップグレードできる、スケーラブルなプラットフォームを品揃え – 最大のROI(投資収益率)と投資保護を実現
- マルチレイヤでの**VoIP (SIP)**保護機能
- IPv6の保護 – **シグネチャと動作**ベースの保護機能(ゼロデイ型)
- 携帯・固定電話事業者における防御の最前線として、**トンネリングプロトコル**に対応
- 帯域管理により、**エンドツーエンドのトラフィックシェーピング**を実現

- **低い総所有コスト(TCO)**
  - "ハンズオフ"なセキュリティ機能:適応型の侵入防御機能により、「ハンズオフ」でセキュリティを実現します(最低限の設定、メンテナンス作業でOKです)
  - シームレスな統合:ネットワーク環境にシームレスに統合できるため、ネットワーク設定の変更が不要です(透過的なデバイスです)
  - スケーラブルなプラットフォーム:ソフトウェアライセンスのアップグレードだけで、プラットフォームの拡張が可能です
- **容量** – 既存のインフラとサーバの有効容量が飛躍的に拡大します
- **社内のセキュリティ専門家** – マルチレイヤのVoIP保護、IPv6、IRCボット、動作ベースの検出手段などを提供します
- **SLAレポート** – 貴社の顧客に対し、価値を証明できます

radware
availability | performance | security

Smart Network. Smart Business.