CHECK POINT

セキュリティレポート

2024.1

Check Point SMB

YOU DESERVE THE BEST SECURITY

2023年振り返りと2024年予想

2023年振り返り

進化を続けるランサムウェア

深刻な脅威として再浮上したUSBデバイス

人工知能の悪用が拡大

2023年振り返りと2024年予想

✓ 断片的な暗号化

- ファイルの一部を暗号化
- 攻撃者にとって作業負担軽減とパフォーマンス向上
- アンチウイルスソフトにとって
  - 高速に一部を暗号化されるため検出が困難または手遅れの可能性

✓ イニシャルアクセスブローカ(IAB)

- 組織のネットワークへ侵入しログイン情報を盗取することに特化
- 盗取した認証情報をランサムウェア攻撃者へ販売
- ランサムウェア感染率向上に貢献している可能性

進化を続けるランサムウェア

身代金の支払い額の増加

Classic
“情報を暗号化していますが、
お金を払えば暗号化を解いてあげましょう ”

2013

二重恐喝型
$15M “お支払いいただけない場合は、御社の個人情報を外部に公開します”

2019

三重恐喝型
$40M “あなたがお使いのメーカーより
あなたの個人情報を盗みました”

2021

2023年振り返りと2024年予想

深刻な脅威として再浮上したUSBデバイス

国家関与型のグループおよびサイバー犯罪者のいずれも、世界中の組織を感染させる媒介手段として世界的にUSBデバイスを利用しています。

人工知能（AI）の悪用が拡大

多様な生成AIツールが、フィッシングメールやキーストローク監視マルウェア、基本的なランサムウェアコードの作成などに乱用されており、より強力な規制措置が求められています。

2024年予想

サプライチェーンによる重要インフラへの攻撃拡大

本支店間だけではなく、下請け・孫請け企業からの感染が非常に増えている

企業を悩ませ続けるフィッシング攻撃

ますます見分けのつかないフィッシングメール
メール受信後にテキストリンク先のHTTP書き換えによる感染拡大

ランサムウェアの更なる悪用化

チャットGPT等を利用した自動生成するマルウェアが出始めている
学会等によるUSBを利用した情報共有を悪用した手口の増加

2024年対策において

ゼロトラストという意識を持つ

予測・耐える・回復、適用する

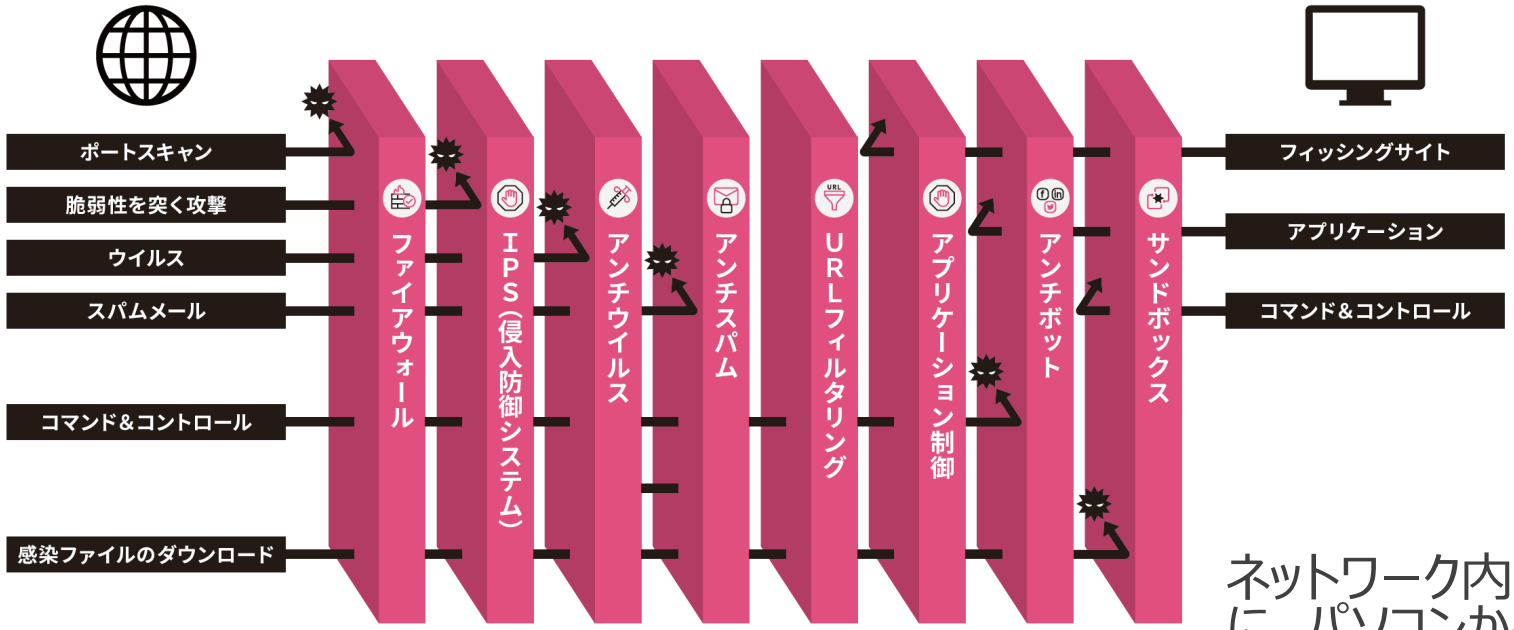
予測においては既知の脅威対策はもちろん、一歩先のことを考える
（自社の弱点やアタックサーフェスにおいて、どのような被害をうけるかをしっかりと考える）

耐えるにおいては実際の攻撃に対して如何にして最小の被害に抑えることができるか、ということが大事です
（自社の弱点を把握した上で、予めデータのバックアップは必須）
（取引先間でのセキュリティ情報共有をしっかりしておくことが大事）

回復、適用においては自動復旧が社内リソースを考慮して優先されると考えます
また、未知の脅威において未然に防ぐことが100%実施できないことを考えると、インシデント毎に内容を把握、回復を実施しながら取引先や関係各所に的確な情報共有を実施することが重要になると考えます

①オールインワンアプライアンス

複雑なサイバー攻撃を防ぐために必要な機能が1筐体に集約されたUTM！
（統合脅威管理：Unified Threat Management）



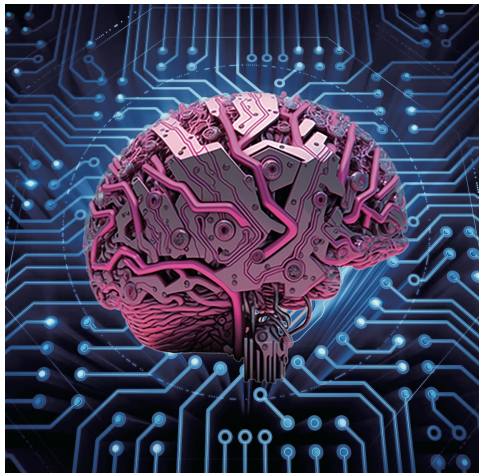
ネットワーク内にある、パソコンをUTMでブロックするとともに、パソコンからC＆C等へのアクセスを遮断します。

外部からの脅威と内部から実施するアクセスを

オールインワンで保護。

あらゆる脅威からの保護

様々なセキュリティ機能に関する脅威対策エンジン



THREATCLOUD

感染ホスト検出
サンドボックス静的解析
サンドボックス動的解析
メール静的解析
フィッシング対策AIエンジン
ネットワークAIエンジンアグリゲータ　などなど

◆世界中の約15万のセキュリティ・ゲートウェイを通過するトラフィックから日々脅威情報を収集
◆脅威情報を防御可能な情報に活用
◆リアルタイムに防御情報をアップデート

容易な導入と管理

クラウド管理によって導入から運用フェーズまでのコスト削減を実現

簡単デプロイ

- ✓ 事前定義された設定ウィザードにより数分でのセットアップが可能

モバイル・クラウド管理

- ✓ クラウドからの一括管理・設定変更が可能なため、保守運用のアウトソースが可能
- ✓ モバイル管理にも対応、インシデントをリアルタイムに確認可能

セキュリティレポート

- ✓ シンプルで直感的なレポートを標準で提供
- ✓ 通信量や検出したセキュリティ脅威等の情報を確認可能

Check Point1500Proシリーズラインナップ

10名規模の企業から400名まで幅広くサポート可能！

	1535	1555	1575	1595	1600	1800
参考ユーザー数 (NGTX全て有効時)	20	50	100	200	300	400
NGTX スループット ※エンタープライズトラフィック ※スマートアクセル有効	440Mbps	600Mbps	650Mbps	900Mbps	2.0Gbps	2.6Gbps
ファイアーウォール スループット ※試験環境トラフィック	1.5Gbps	2.0Gbps	4.8Gbps	6.4Gbps	8Gbps	17Gbps

※NGTX：サンドボックス含む全てのセキュリティ機能を有効にした状態

差別化ポイント！他社のUTMスループットは理想環境でセキュリティ機能を全て有効にしていない数値の場合が多いですが、チェック・ポイントのスループットは全てのセキュリティ機能を実環境で有効にした数値です

Summary

脅威に晒されそうな環境にならないために

確認・予測・対応策を

今一度お客様とご確認されてみてください!!

Thank You!

YOU DESERVE THE BEST SECURITY