Check Point UTM のメリットとは

Check Point 1500 シリーズ：UTM（競合脅威管理）

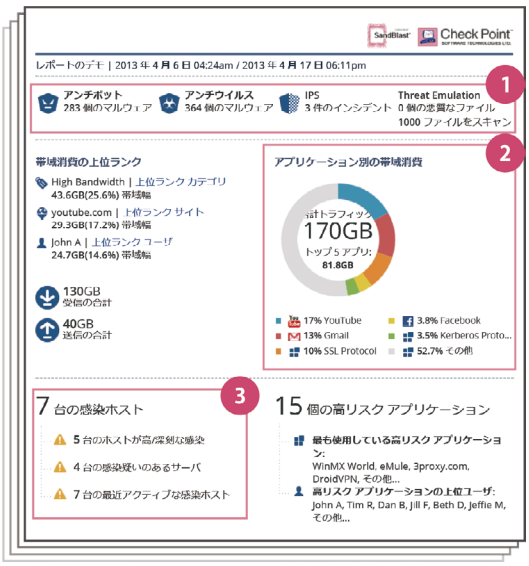
ここが他社よりスゴイ！

- 安定したスループット
- 充実したサポート
- 低コスト
- 見やすいレポート
  - 月次
  - 週次
  - 日次

見やすいセキュリティレポート

セキュリティ機器の導入効果は実感しにくいものです。しかしながら、レポートの自動配信で導入効果を可視化・見える化いたしました。
他社と比較してグラフィカルで細やかな日本語対応がされているところも Check Point レポートの魅力です。

- グラフィカルなレポートの自動配信でセキュリティを可視化
- 標準でレポート機能付与
- セキュリティの可視化を実現
- 月次・週次・日次で選択可能



1. 検出した脅威数がわかる！
2. 総トラフィックやアプリケーションの利用割合など、ネットワークの利用実態がわかる！
3. ウイルス感染している PC 台数がわかる！
   ※ 感染した PC の IP アドレスも詳細ページで確認可能

感染したホスト

レポートのデモ: 2013 年 4 月 6 日 04:24am / 2013 年 4 月 17 日 06:11pm

感染したホストの一覧

ホスト	深刻度	保護の名前	最後のインシデ...	インシ...
192.168.0.5 (host5)		Bot.b	9 10, 2017	35
192.168.0.2 (host2)		Bot.b	10 10, 2017	54
192.168.0.4		Bot.b	15 10, 2017	6
192.168.0.3 (host3)		Bot.c	16 10, 2017	1
192.168.0.1 (host1)		Bot.c	13 10, 2017	6
192.168.0.9		Bot.c	9 10, 2017	53
192.168.0.6 (host6)		Bot.c	14 10, 2017	77
192.168.0.7 (host7)		Bot.c	9 10, 2017	8
192.168.0.8		Bot.a	9 10, 2017	29
192.168.0.1 (host1)		Bot.a	10 10, 2017	12
192.168.0.10 (host10)		Bot.a	10 10, 2017	2

妥協しないセキュリティスキャン

パケットに対してフルスキャンを行うことで、パケットの後方にウイルスが存在しても見逃さない仕組みになっています。
Check Point はセキュリティに対して妥協いたしません。

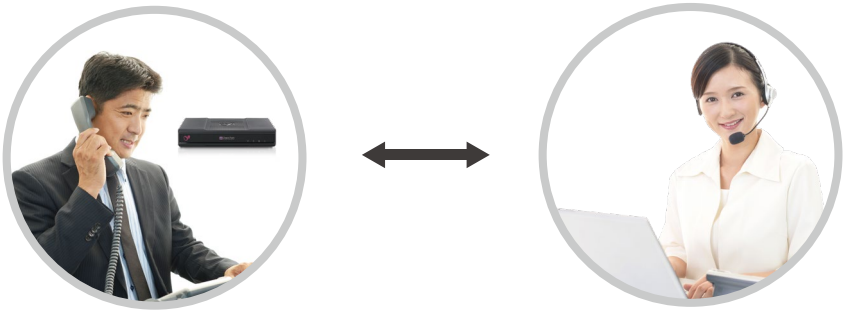
FORTINET　スキップ → 先頭スキャン

Check Point　フルスキャン

Fortinet は先頭スキャンに対して
Check Point はフルスキャンを行います。

便利なマネージメントサービス

機器はクラウドの管理下に入るため遠隔での設定変更に対応。
導入後に設定変更を行いたいお客様のニーズに合わせ、Check Point サポートセンターがリモート対応いたします。



リモートで機器の状態を確認

メールによるセキュリティレポートを定期配信
月次 週次 日次 より選択

設定の追加・変更をリモートで実施
(FW / Anti-Virus / IPS / アプリケーション制御 / URL Filtering)

障害時にリモートでログを取得し調査を実施

故障時の先出センドバック対応

ファームウェアアップデートをリモートで実施

2 種類のシンプルなライセンス体系

		Firewall	アンチウイルス	アンチボット	アンチスパム	IPS	アプリケーションコントロール	URL フィルタリング	サンドボックス
NGTP	セキュリティ基本機能	●	●	●	●	●	●	●	
NGTX	セキュリティ基本機能 ＋ **サンドボックス**	●	●	●	●	●	●	●	●

スループット

Check Point	1530	1550	1570	1590
	340Mbps	450Mbps	550Mbps	660Mbps

FORTINET	FG-30E	FG-50E	FG-60E	FG-80E
	150Mbps	160Mbps	200Mbps	250Mbps

Check Point の数値について
・Check Point 社 Enterprise Test 環境における実測値
・全ての機能を有効にした状態で計測

FORTINET の数値について
・データシート上の脅威保護パフォーマンスの数値
・脅威保護パフォーマンスはファイアウォール、IPS、アプリケーション制御、およびマルウェアに対する保護が有効な状態（Web Filtering Service は含まず）

なぜ Check Point を選ぶべきか – 4 つのポイント

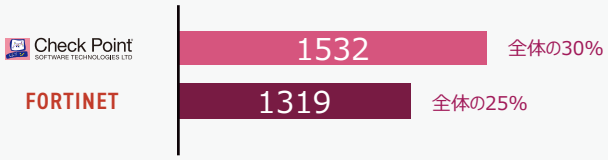
Check Point は顧客の情報を保護する最善のセキュリティ・ソリューションを提供することに尽力してきました。以下に第三者機関によって証明された、Check Point の優位性を示す 4 つのポイントをまとめました。

より詳細な情報は以下のリンクをご参照ください。

http://tiny.cc/rightarchitecture

1 正しい方向性

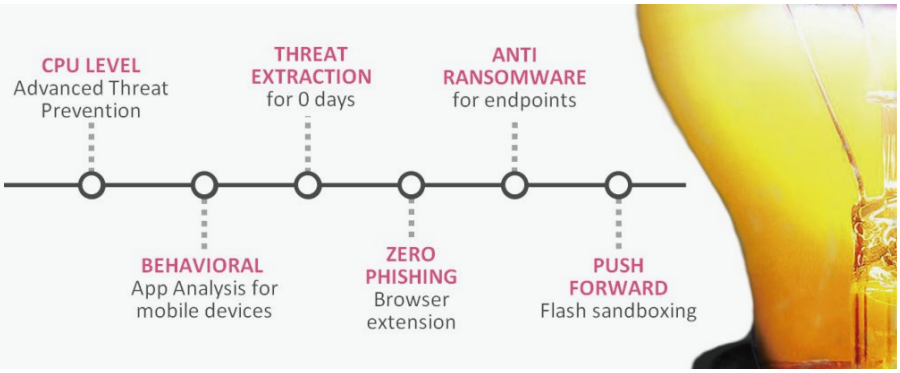
業界随一の研究開発に対する人的リソースへの投資



ソース：SEC Data: Palo Alto Form 10-Q I Fortinet 10-Q I Check point 20-F

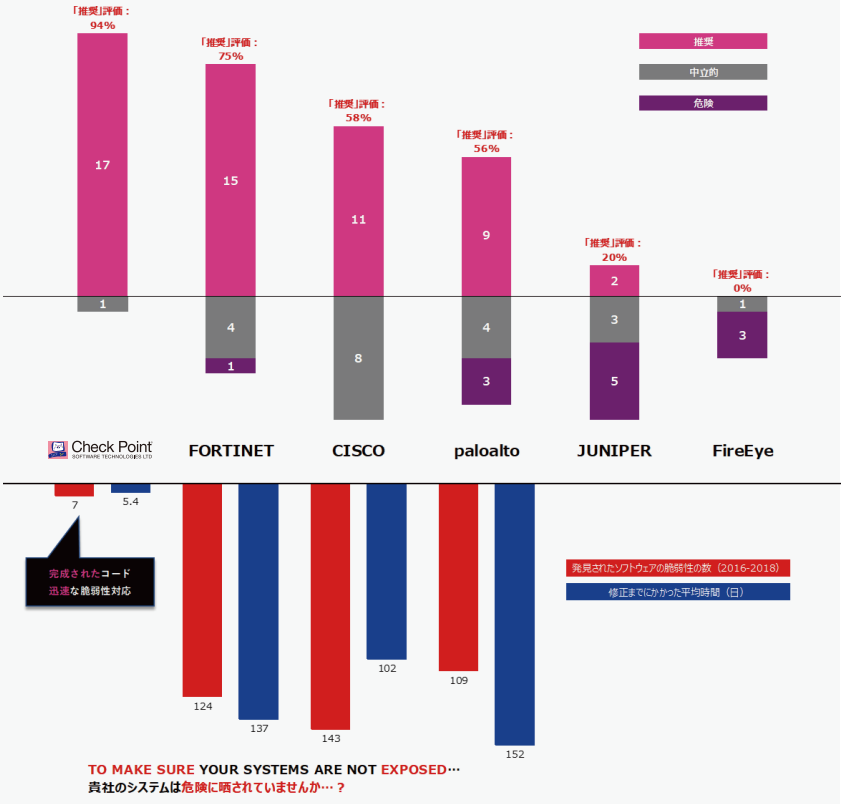
2 技術革新

CPU レベルのサンドボックスやランサムウェアからの復元など先進的かつユニークな脅威対策テクノロジー



3 証明され続けてきた確かな技術

業界最多の第三者機関による「推奨」評価（17 年連続）



4 危機管理に対する意識の徹底

最も安全なアーキテクチャと最速の脆弱性修正対応時間

TO MAKE SURE YOUR SYSTEMS ARE NOT EXPOSED…
貴社のシステムは危険に晒されていませんか…？

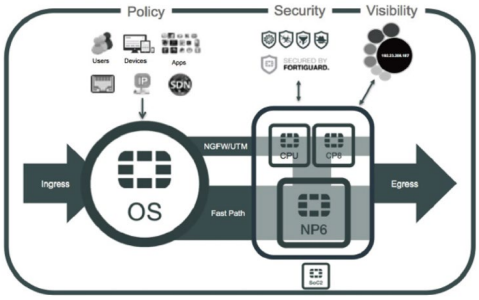
ソース：http://tiny.cc/nss_stats * ネットワークセキュリティにおける評価

Fortinet は ハードウェア に依存、Check Point は ソフトウェア技術を活用

Fortinet は ハードウェアに依存しているため全機能を ON にするとスループットが低下

SoC（System on a Chip）は、CPU と FortiASIC を統合したアーキテクチャです。

ASIC ベースのシステムは、開発元が初期設定を行った後、新手の攻撃に対処できるようにロジックを書き換えることができません。高速と低速という 2 つの検査パスがあり、低速パスの場合、処理速度はプロセッサの性能に依存します。またアプリケーション層の脅威に対処するにはパフォーマンスが不十分であることが少なくありません。



Optimum Path Processing (OPP)

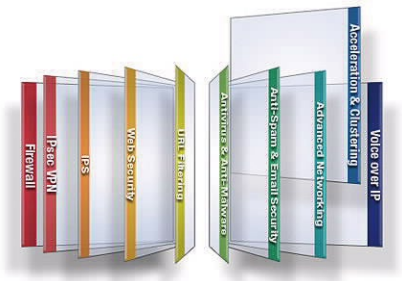
Check Point は ソフトウェア 技術で最適化処理を行い安定したスループットを実現

パフォーマンスを向上させるセキュリティとパフォーマンスを実現するフレームワーク（2 つの特許技術）があります。

SecureXL（セキュリティ・アクセラレーション）
ネットワーク・トラフィックがセキュリティ・デバイスを通過する際に生じる遅延を排除して、セキュリティ検査を高速化します。

CoreXL（マルチコア・アクセラレーション）
マルチコア・プロセッサをフル活用できるように設計された始めてのセキュリティ技術です。CoreXL は、セキュリティ検査の負荷をすべてのコアに分散します。

新しい攻撃手法が登場した場合でも ASIC からプロセッサへと検査パスを切り替えることに伴うパフォーマンス低下が生じません（SecureXL）。また、ディレクタ・コアにインテリジェンスを持たせることで、各コアへの負荷分散を可能にしています（CoreXL）。

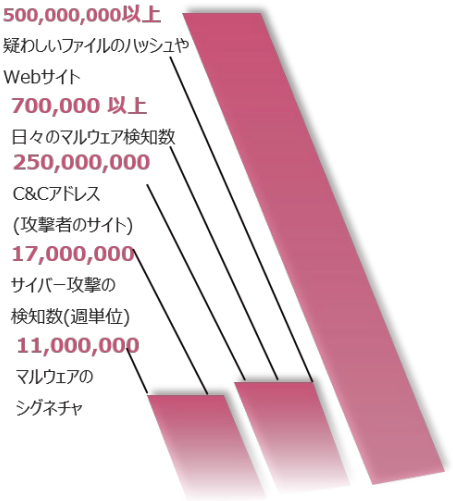


Acceleration and Clustering Software Blade

Check Point の優位点

- 妥協することなく最高レベルのアプリケーション・セキュリティとパフォーマンスを両立
- 新しいタイプの脅威が出現しても一定レベルのパフォーマンスを維持可能
- マルチメディア・アプリケーションやトランザクション指向アプリケーションのパフォーマンスを向上
- プロセッサ・レベルおよびシステム・レベルでの効果的な負荷分散

Check Point の頭脳である ThreatCloud



- 世界中の 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

お問い合わせ