CHECK POINT™

YOU DESERVE THE BEST SECURITY

# 最新のエンドポイントセキュリティ

## Harmony Endpoint のご紹介

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

# アジェンダ

- チェックポイントについて
- セキュリティ・ソリューションマップ
- エンドポイントにおけるサイバーセキュリティの脅威について
- Harmony Endpoint について
- よくある質問
- サマリー

# チェックポイントについて

YOU DESERVE THE BEST SECURITY

# 会社概要

## Check Point Software Technologies Ltd.

設立　1993年（1997年日本法人設立）

**IT業界初のステートフルインスペクション型ファイアウォールであるFireWall-1を開発**

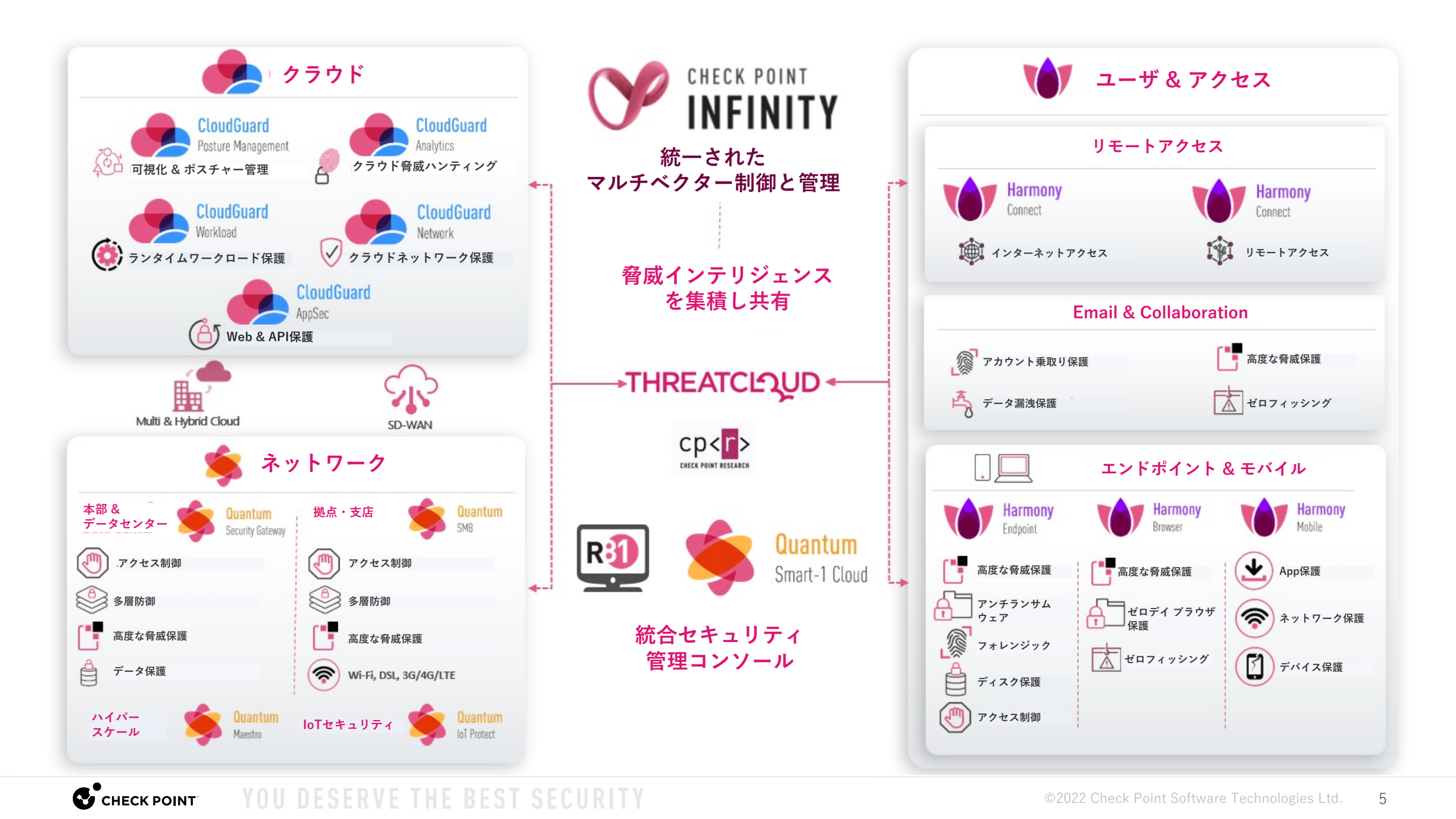
本社　インターナショナル本社：イスラエル　テルアビブ
米国本社：カリフォルニア州サンカルロス　日本法人：東京都港区虎ノ門

代表者　会長 兼 CEO　Gil Shwed（ギル・シュエッド）

**2019年、初のイスラエル技術賞を受賞**

従業員数　約5,400名 – R & Dスタッフ 30%以上

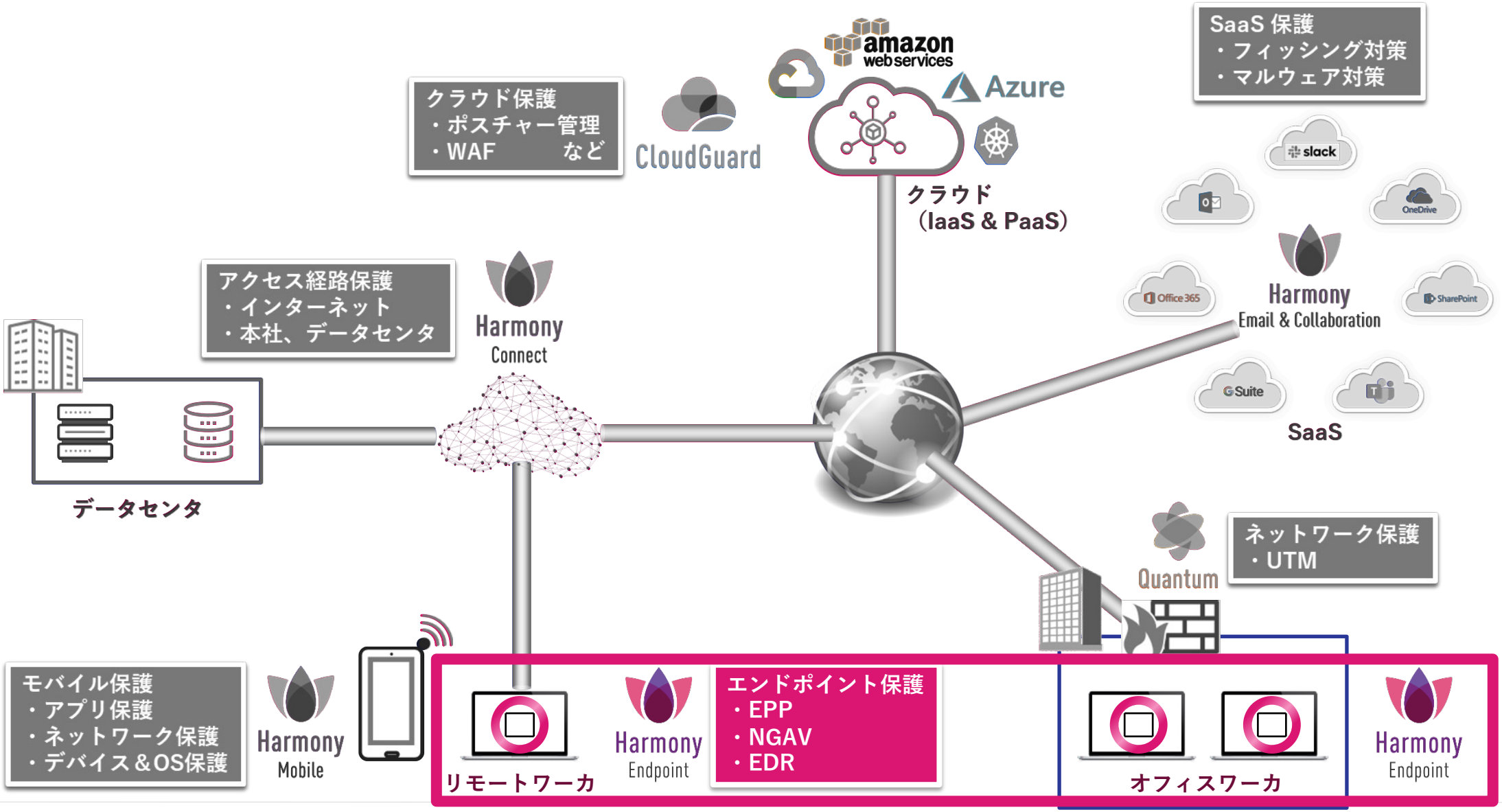
年間売上　20億0,065万ドル（2020年度）



# セキュリティ・ソリューションマップ

YOU DESERVE THE BEST SECURITY

# セキュリティ・ソリューションマップ



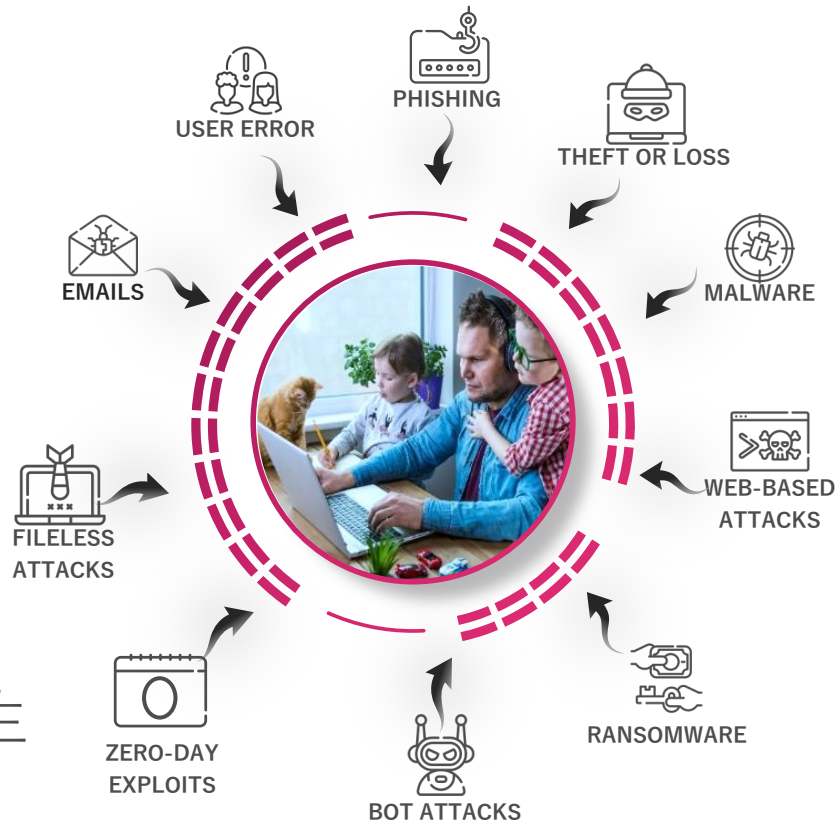
# エンドポイントにおける
# サイバーセキュリティの脅威について

YOU DESERVE THE BEST SECURITY

# エンドポイントに差し迫る脅威

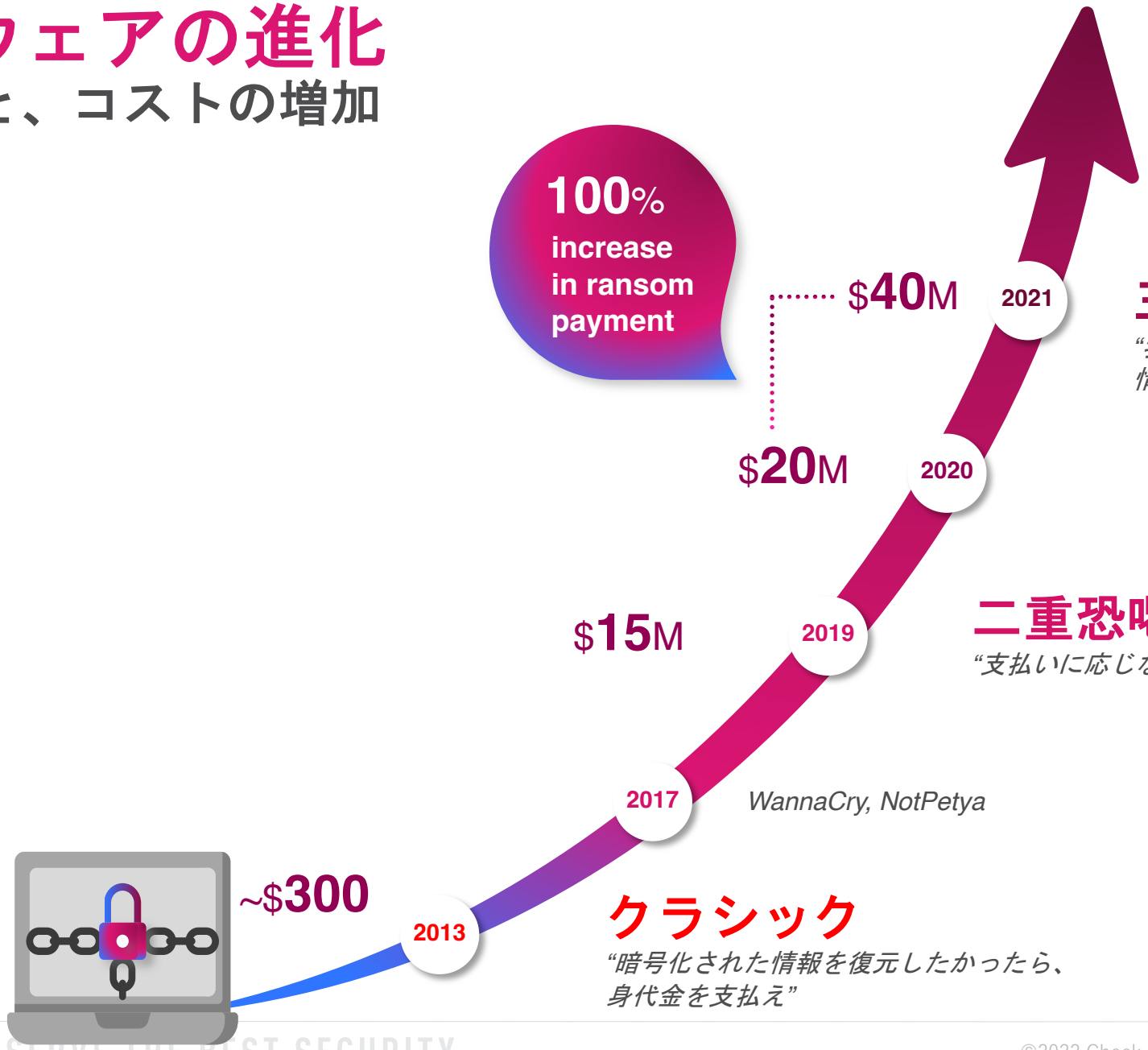
**エンドポイントをターゲットとした攻撃が、かつてないほど増加**
**直接的な金銭被害やビジネス停止に繋がるケースも発生**

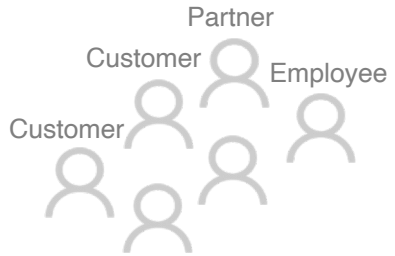
- コロナ禍におけるテレワーク増加
  - 保護が十分でない環境からの社内へのアクセス
  - リモートワーク中にウイルス感染し、社内へ感染拡大
- サイバーパンデミック
  - 2020年→2021年でサイバー攻撃は50%増加
  - 特に、ランサムウェア攻撃、フィッシング攻撃は倍増
- セキュリティ侵害の70%はエンドポイントから発生 by IDC



# ランサムウェアの進化

## 攻撃の高度化と、コストの増加




**三重恐喝**

*“我々は、あなたの取引先から機密情報を入手した”*

**二重恐喝**

*“支払いに応じないなら、機密情報を公開する“*

*WannaCry, NotPetya*

**クラシック**

*“暗号化された情報を復元したかったら、身代金を支払え”*

# Emotet復活

**2021年11月から、Emotet が国内で再流行！**
**爆発的な広がりを見せています**

1～3月のEmotet相談件数は計656件　前四半期から約54.7倍と“爆増”　IPAが報告

2022年04月19日 15時45分 公開　[松浦立樹，ITmedia]

印刷　82　Share　B!　4　0

PR 今日からはじめるGitHub。導入や初歩的な使い方を解説

PR クラウド管理は“静”から“動”へ　ITR甲元氏とSIerが対談

情報処理推進機構（IPA）は4月19日、マルウェア「Emotet」に関する相談が1月から3月までに656件あったと明かした。10月から12月までの前四半期の相談件数は12件であり、そこから約54.7倍増加したという。

「Emotet」ウイルス相談件数の推移

| | 2021/1～3 | 2021/4～6 | 2021/7～9 | 2021/10～12 | 2022/1～3 |
|---|---|---|---|---|---|
| 相談件数 | 12 | 0 | 0 | 12 | 656 |

Emotet相談件数の推移

https://xtech.nikkei.com/atcl/nxt/column/18/00001/06309/

- ✓ 2021年1月に封じ込めが成功したとされていたEmotet
- ✓ Microsoft Officeの更新を装うEmotetのスパムメッセージが生成されていることを確認
- ✓ 2022年1月から3月にかけて、日本国内での被害が拡大

# セキュリティインシデント例

- ✓ 子会社や取引先から攻撃がはじまる「サプライチェーン攻撃」が多く見られた
  - ➢ 大企業はセキュリティ強度が高く攻撃が成功しづらいため、セキュリティ対策が十分でない関連会社、取引先、海外拠点が狙われやすい傾向がある

中堅中小企業にとってもサイバー攻撃は他人事ではありません！

ビジネスの信頼を保つためにも、セキュリティ対策が必要です！

| 令和3年度に判明した主なランサムウエアの被害 | | | |
|---|---|---|---|
| | 4月 | 鹿島 | 海外子会社で約130万件のデータが流出 |
| | | HOYA | 米子会社で盗まれた情報がダークウェブ上で公開 |
| | 6 | 富士フイルム | 情報漏洩（ろうえい）はないが、ネットワークの遮断で、一部業務に影響 |
| | 7 | ニップン | 基幹システムが暗号化され、四半期報告書の提出期限を延期 |
| | 8 | オリエンタルコンサルタンツ | 公共事業の情報などが流出した可能性があり、約7億5000万円の特別損失を計上 |
| | 9 | JVCケンウッド | 欧州拠点で個人情報が流出 |
| | 10 | 半田病院（徳島県つるぎ町） | 電子カルテが閲覧できず、約2カ月間、全面診療停止に |
| | 令和4年2月 | 小島プレス工業（愛知県豊田市） | トヨタの国内工場が一時稼働停止に |
| | | ブリヂストン | 米工場が一時稼働停止に |
| | 3月 | デンソー | 発注書や図面など15万7000件以上の情報が流出 |
| | | 森永製菓 | 164万人以上の個人情報流出の可能性 |
| | | 日本アンテナ | 社内のほとんどのパソコンが使用できない状態に |

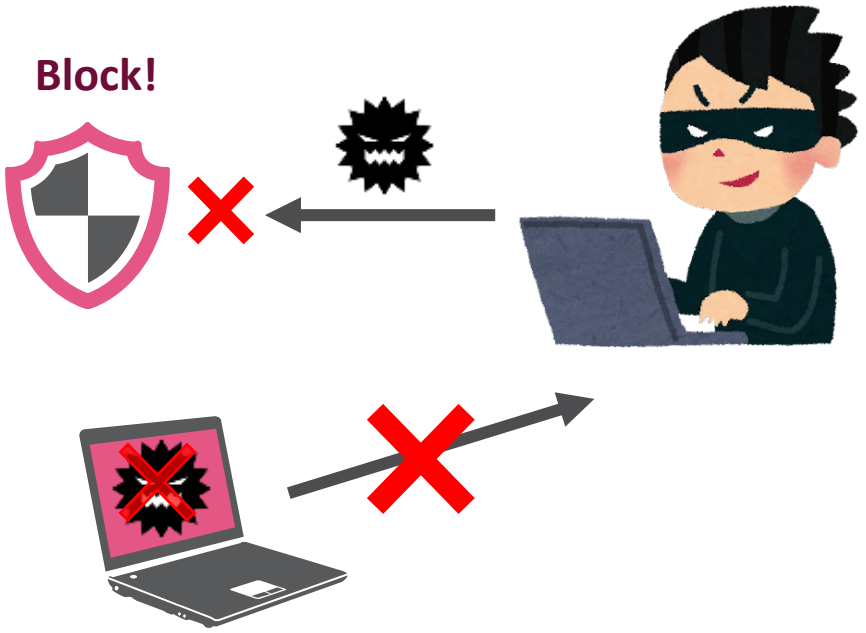
https://www.itmedia.co.jp/news/articles/2204/07/news053.html

# どんな対策が必要なのか？

**01** **検知＆防止**
まずはウイルスに感染しないように対策をする！

**02** **封じ込め**
万が一感染した場合、ウイルスを封じ込め被害を抑える

**03** **可視化と分析**
ウイルスを駆除したあと、なにがあったのかを把握し、再発防止の材料にする



# HARMONY ENDPOINT について

YOU DESERVE THE BEST SECURITY

Harmony
Endpoint

# セキュリティ運用の成功に向けた3つの防御戦略

# エンドポイントに必要なすべての保護を提供

攻撃対象の削減
Base

攻撃からの防御
EPP & NGAV

攻撃の検知と対応
EDR

検知＆防止

- ファイヤーウォール
- URL フィルタリング
- リモートアクセス VPN
- コンプライアンス
- アンチ・マルウェア
- サンドボックス
- ファイル無害化
- ゼロ・フィッシング

封じ込め

- アンチ・ランサムウェア
- アンチ・ボット
- アンチ・エクスプロイト

可視化と分析

- フォレンジックレポート

# Harmony Endpoint がご提供する先進の防御技術

### サンドボックス
OSレベルとCPUレベルの
統合型サンドボックスで
攻撃を遮断

### ファイル無害化
ファイルの無害化による
安全性と生産性の両立

### ゼロフィッシング
フィッシングサイトから
ユーザの認証情報を保護

### アンチ・ランサムウェア
ランサムウェアの攻撃を停止し、
ファイルを自動復旧

### アンチ・ボット
攻撃者との通信を遮断し、
攻撃の拡大を阻止

### フォレンジックレポート
独自の解析技術による
正確性の高い攻撃解析

Harmony
Endpoint

# セキュリティ運用の成功に向けた3つの防御戦略

Harmony
Endpoint

# セキュリティ運用の成功に向けた3つの防御戦略

**検知と防止**

サンドボックス

ファイル無害化

ゼロ・フィッシング

**封じ込め**

感染した脅威による
影響を最小限に抑制

**可視化と分析**

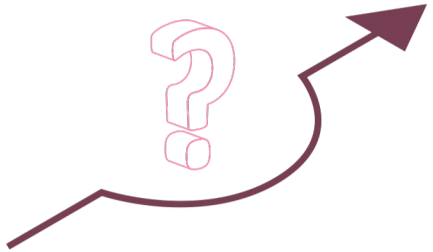
適切な事後対応の
ための事象把握

# 検知＆防止：サンドボックス（Threat Emulation）

## サンドボックスの必要性

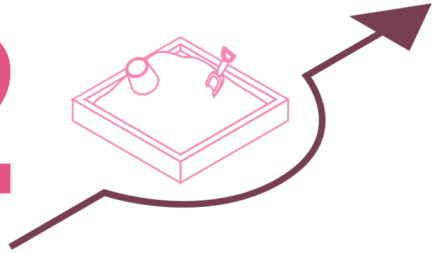
**次世代型サンドボックスにより、未知の脅威や高度な脅威へも対応**

1



**攻撃者は、未知の脅威を使いシグネチャー
ベースのセキュリティ機能をバイパスします**

2



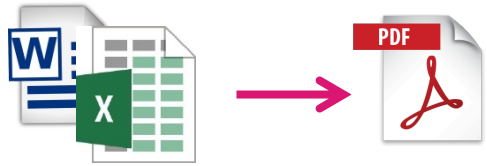
**攻撃者は、回避技術を使って、第一世代の
サンドボックスをバイパスします**

# 検知＆防止：ファイル無害化（Threat Extraction）

**無害化された安全なファイルをユーザに届け、セキュリティと生産性を両立**

- ✓ Webダウンロードするファイルが対象
- ✓ 2つのモードを選択可能
  - PDF変換 (100%無害化)
  - マクロや埋め込みオブジェクトを削除
- ✓ 内容を維持し、ユーザに迅速にファイルを提供

**Option1 – PDF変換**




**Option2 – 悪用可能なコンテンツ除去**

# サンドボックス ＆ ファイルの無害化の動作イメージ

## ユーザの生産性に影響を与えることなく、悪意のあるダウンロードをブロック


**1** **WEB ダウンロード**を Harmony Endpoint が検出

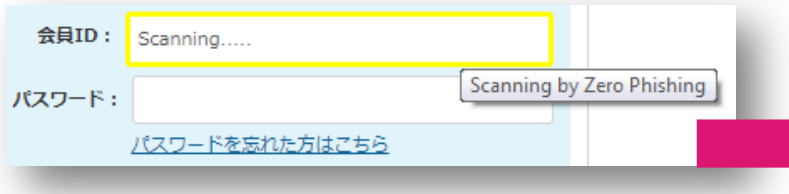
**2** アクティブなコンテンツを取り除いたファイルをユーザへ提供（**ファイル無害化**）

**3** バックグラウンドでオリジナルファイルを**サンドボックス**で検査し安全性を確保

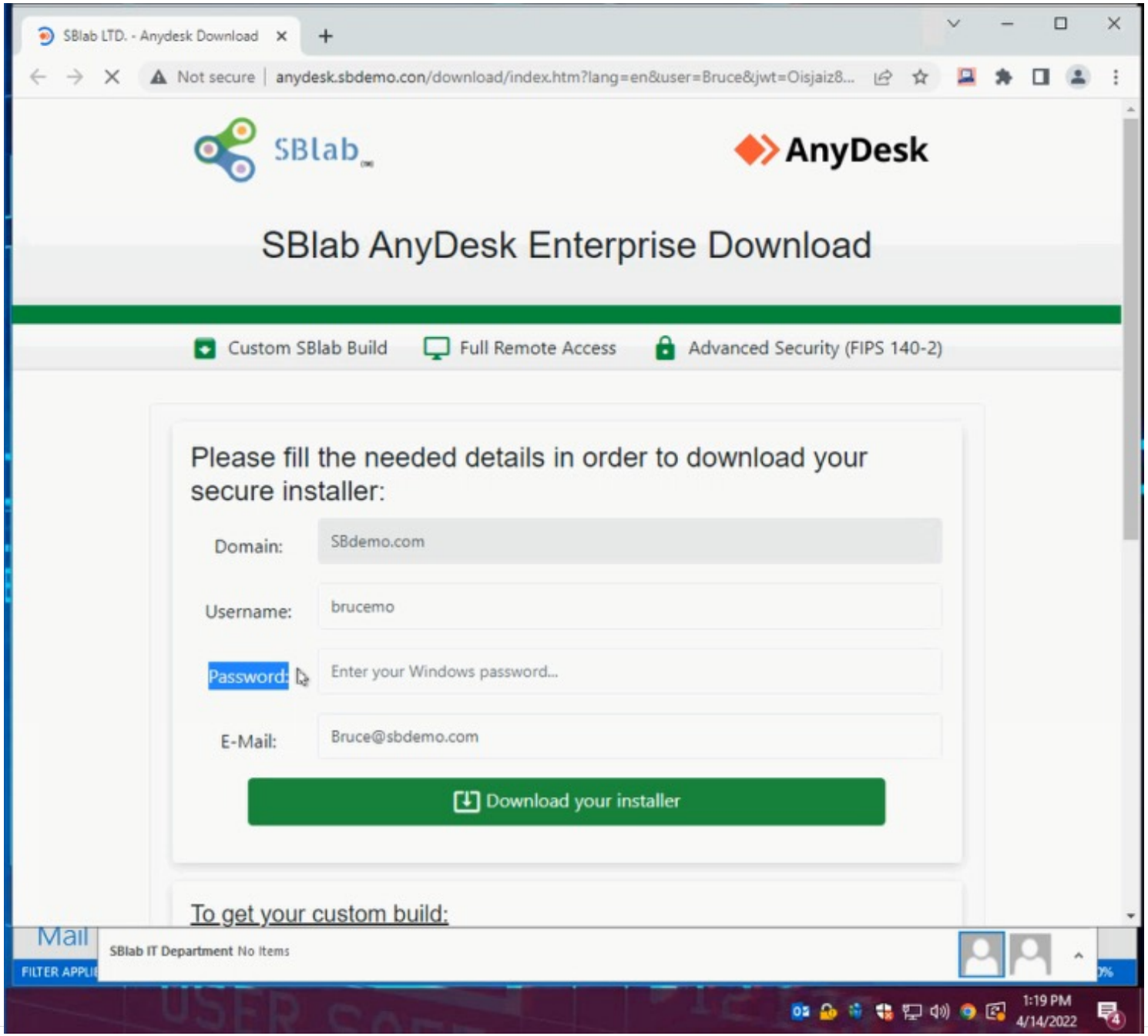
# 検知＆防止：ゼロ・フィッシング

## リアルタイムにフィッシングサイトを検出し、認証情報の漏洩を防止

- ✓ ゼロデイのフィッシングサイトをブロック
- ✓ Webサイト上の不審な要素を検査
- ✓ 検査終了までID/Passwordの入力を無効化




- ✓ IPレピュテーション
- ✓ ドメインレピュテーション
- ✗ URLの類似性
- ✓ よく似た文字列
- ✗ タイトルの類似性
- ✗ 画像のみのページ
- ✗ 視覚的な類似性
- ✗ 複数の最上位ドメイン
- ✗ 文章の類似性
- ✗ よく似たファビコン



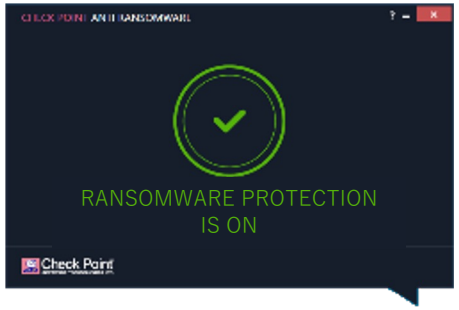
Harmony
Endpoint

# セキュリティ運用の成功に向けた3つの防御戦略

# 封じ込め：アンチ・ランサムウェア

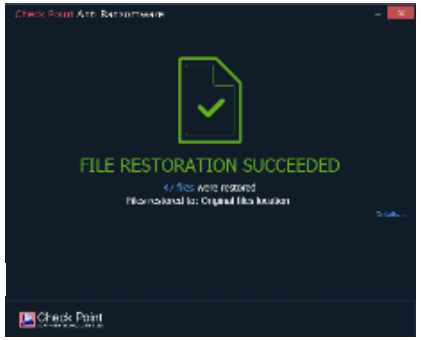
## ランサムウェアの攻撃を阻止して、暗号化されたファイルを自動復旧

### 進行中




### 検出時






**振る舞い分析**

ランサムウェア独自の振る舞いを常時モニタ

**分析**

攻撃の詳細を分析するため、フォレンジック分析実施

**隔離**

攻撃のあらゆる要素を停止および隔離

**データのバックアップ**

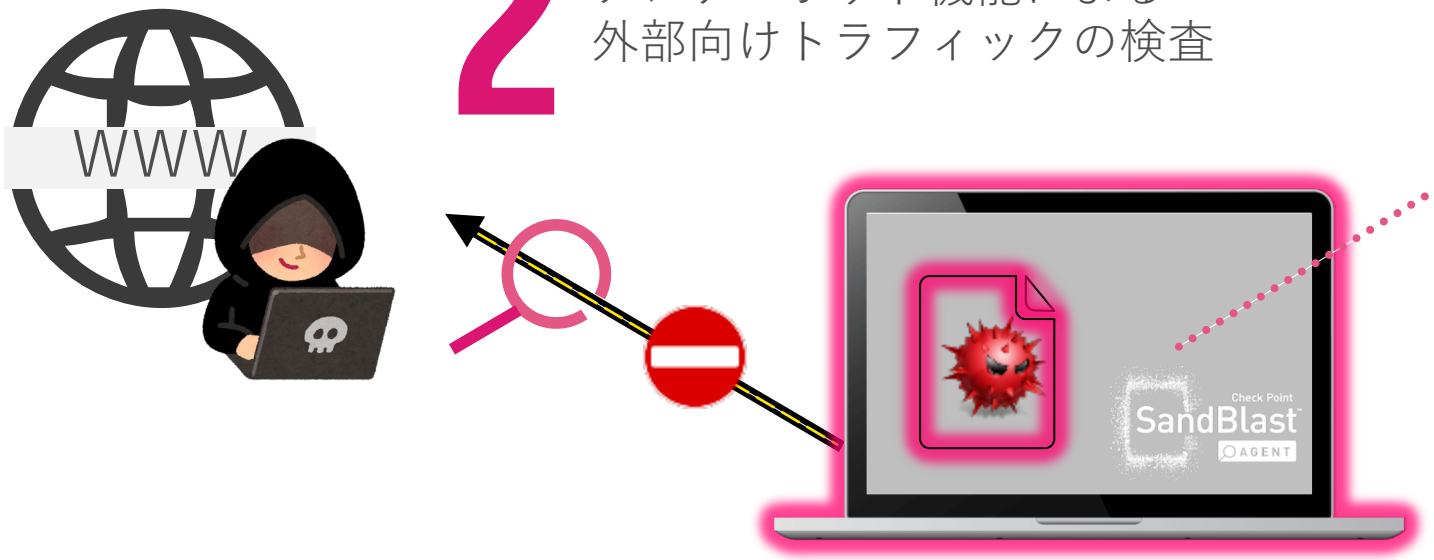
ファイルのバックアップを継続的に作成

**リストア**

暗号化されたファイルを自動復旧

# 封じ込め：アンチボット

## ボットに感染したパソコンと攻撃者との通信を遮断し、情報漏洩を防ぎます




**1** 「Threat intelligence」が脅威情報を継続的にエンドポイントへ配布

THREATCLOUD

- 疑わしい URL
- 疑わしいIPアドレス
- ボットの振る舞い
- ボットの通信パターン

**2** アンチ・ボット機能による外部向けトラフィックの検査

**3** C&Cサーバへのトラフィックおよびデータの流出をブロック

**4** 疑わしいプロセスを隔離

Harmony
Endpoint

# セキュリティ運用の成功に向けた3つの防御戦略

# 可視化と分析：フォレンジックレポート

## 自動的に攻撃の詳細を分析し、全体像の把握、事後対応に役立つ情報を提供します

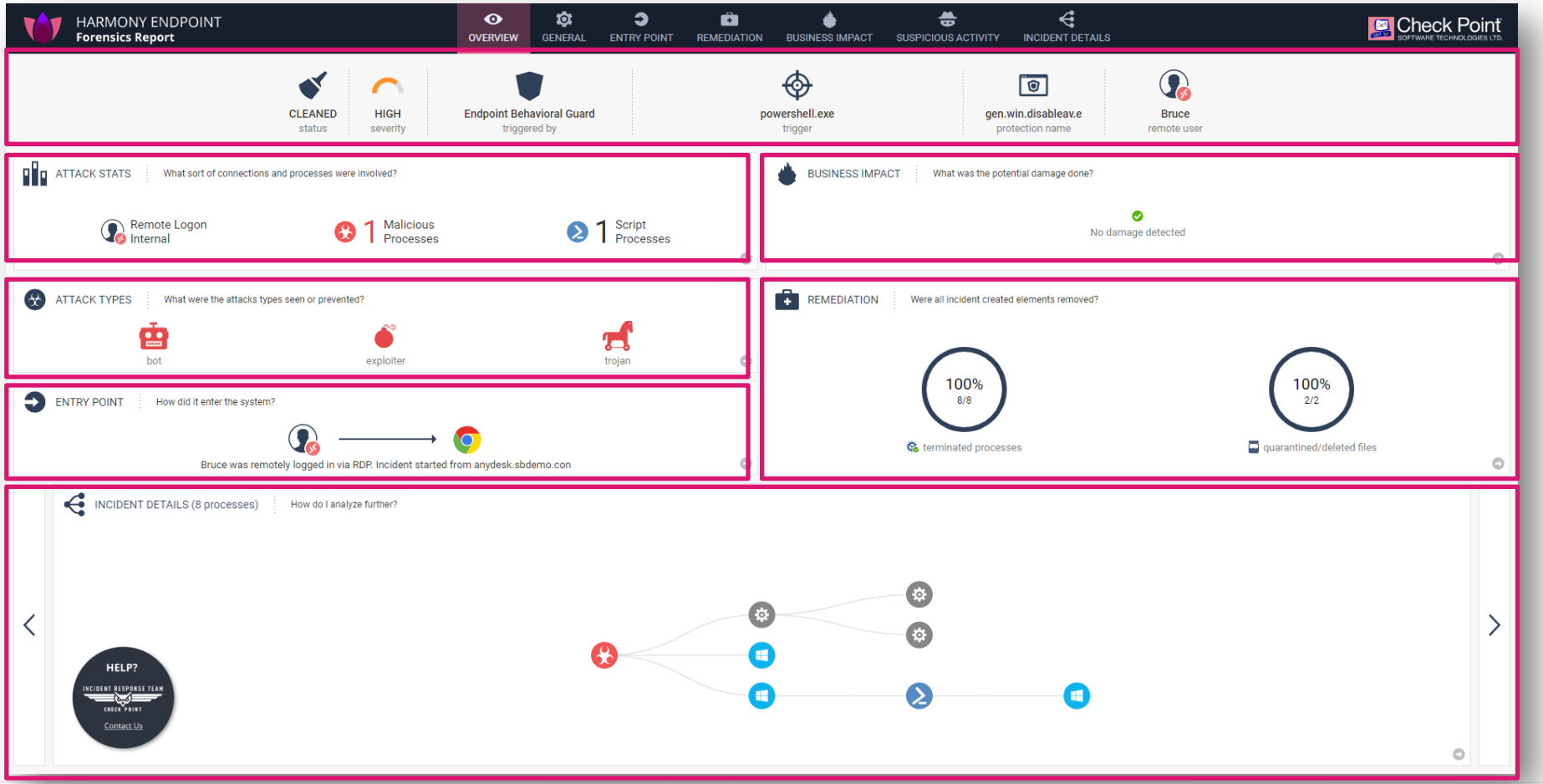
攻撃概要

攻撃統計

攻撃タイプ

侵入経路

プロセスツリー




被害状況

修復状況

# Harmony Endpoint

## EPPとEDRの両方の機能を兼ね備えた統合セキュリティ

### Access Control
Host Firewall
Compliance
Web-browsing protection

### Threat Intelligence

### Sandbox & CDR
Threat Emulation
Threat Extraction

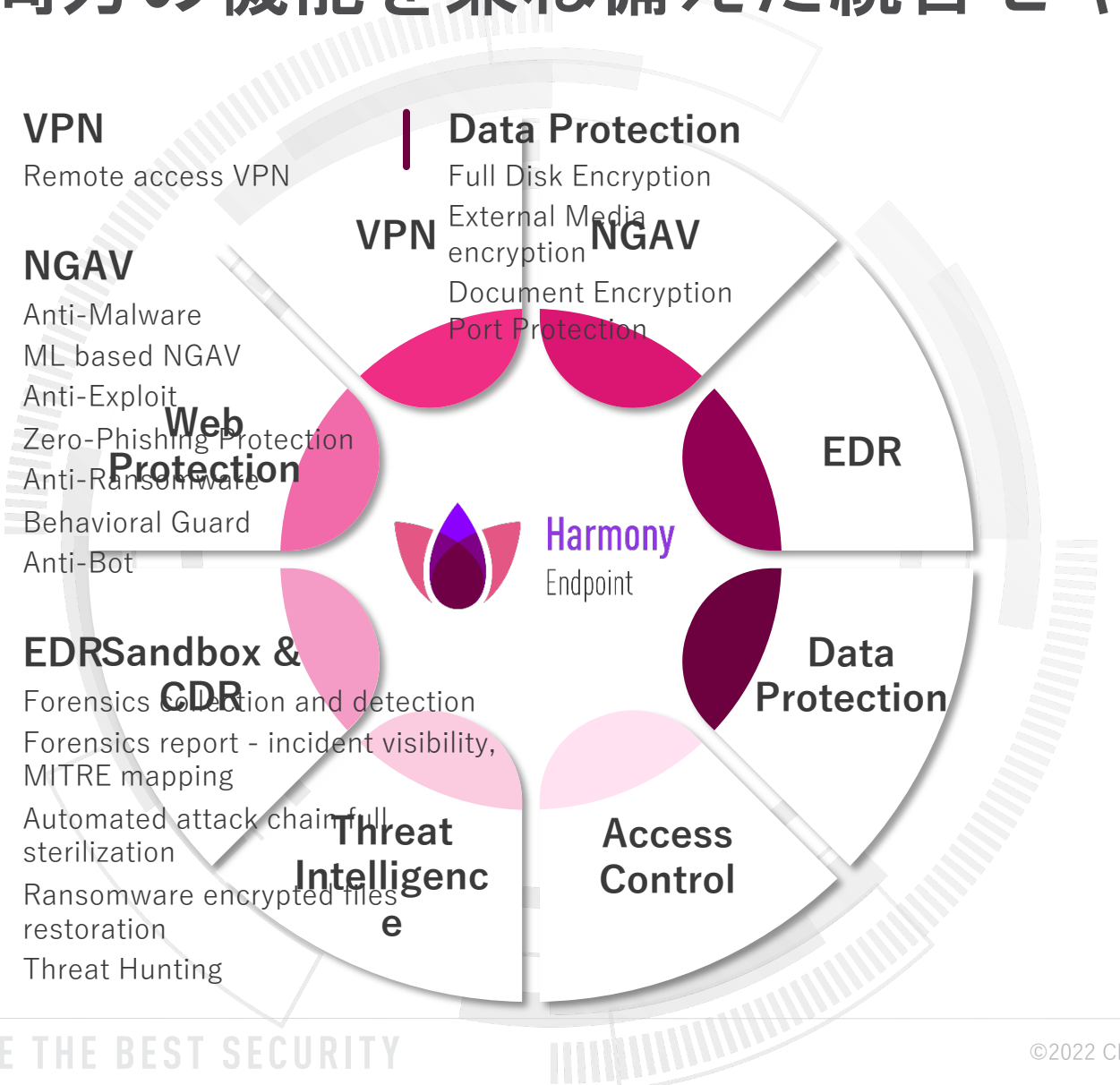
### Web Protection
Zero-day Phishing site protection
Corporate Password Reuse Protection
URL Filtering
Malicious site protection

### VPN
Remote access VPN

### NGAV
Anti-Malware
ML based NGAV
Anti-Exploit
Zero-Phishing Protection
Anti-Ransomware
Behavioral Guard
Anti-Bot

### EDR
Sandbox & CDR
Forensics collection and detection
Forensics report - incident visibility, MITRE mapping
Automated attack chain full sterilization
Ransomware encrypted files restoration
Threat Hunting

### Data Protection
Full Disk Encryption
External Media encryption
Document Encryption
Port Protection



# よくある質問

YOU DESERVE THE BEST SECURITY

「Harmony Endpoint」の性能は、
他社製品と比べてどうですか？

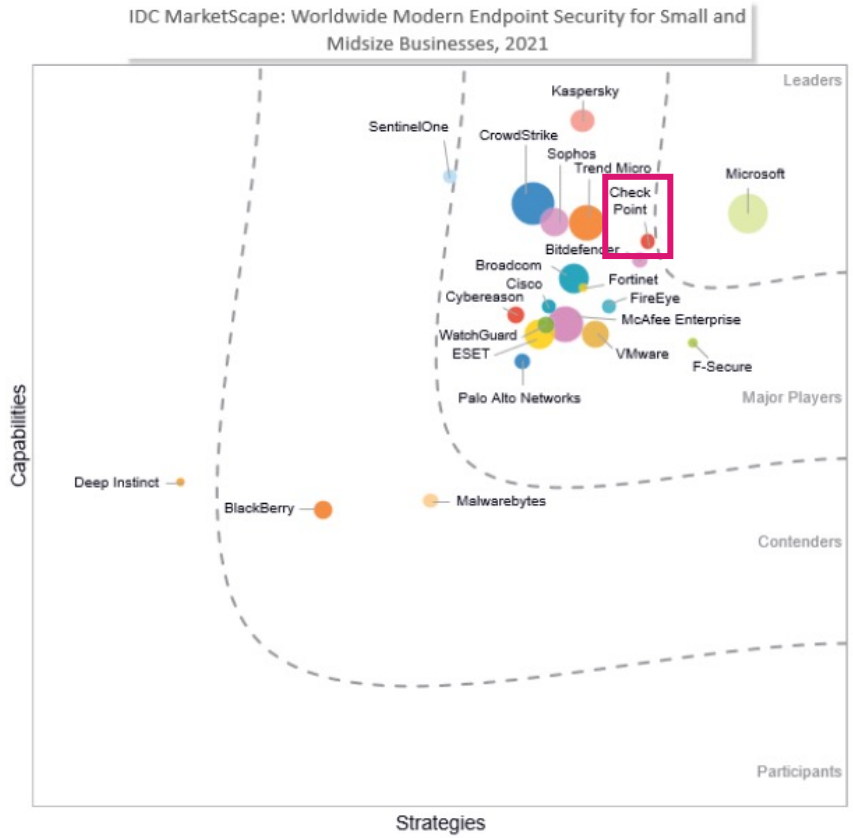
YOU DESERVE THE BEST SECURITY

# Harmony Endpointの第三者評価

MITRE ENGENUITY™

AV comparatives Certified EPR 2021 Strategic Leader

## 第三者評価機関からも高い評価を受けている製品です！安心してご利用ください！




Source: IDC, 2021

- IDCの調査において、メジャープレイヤーの評価
- ファイル無害化や次世代サンドボックス、アンチランサムウェア等他社との差別化が可能な機能が評価された
- 実際のサイバー攻撃の戦術やテクニックをシミュレートするMITRE ATT&CK evaluationにおいても攻撃ステップを100%検知、最高水準を記録

「Harmony Endpoint」の導入事例を教えてください

YOU DESERVE THE BEST SECURITY

# Harmony Endpoint の導入事例

世界中でお客様のエンドポイントを保護しています

**政府、自治体、電力、通信、金融、保険、医療、製造、流通、観光、大学など**


https://www.checkpoint.com/customer-stories/

他社製品でもランサムウェアからの
ファイル復旧を謳っているけれど、
チェックポイントは何が違うの？

YOU DESERVE THE BEST SECURITY

# アンチ・ランサムウェアの特徴

**Harmony Endpoint のアンチ・ランサムウェアによるバックアップは、ランサムウェアによって破壊されません！**

## It’s all fun and games until ransomware deletes the shadow copies

Adversaries reliably use the Vssadmin Windows process to delete backup files during ransomware infections.

https://redcanary.com/blog/its-all-fun-and-games-until-ransomware-deletes-the-shadow-copies/

- 高度化なランサムウェア攻撃では、Windowsのシャドーコピーによるバックアップは削除されてしまいます

| | バックアップ方法 |
|---|---|
| MS社 | Windows Shadow Copy |
| CS社 | Windows Shadow Copy |
| CB社 | バックアップなし＝復旧機能なし |
| CP | 独自機能 |

他社製品を利用していて、機能面で不安があります。

更新時期がまだ先なのですが、手軽にエンドポイントのセキュリティを強化する方法はありますか？

YOU DESERVE THE BEST SECURITY

# Harmony Browse によるセキュリティ強化

## Harmony Browse で SSL を可視化し、Web セキュリティを強化できます
## サンドボックス、ファイル無害化、ゼロ・フィッシング、URL フィルタリングなど

| 機能リスト ＼ Harmony パッケージ | Harmony Advanced | Harmony Complete | Harmony Browse |
|---|---|---|---|
| 攻撃対象領域の削減:<br>エンドポイント ファイアウォール、アプリケーション制御、コンプライアンス、ポート防御、VPN | + | + | |
| 攻撃防御:<br>アンチウイルス、静的分析、ファイルレピュテーション、次世代アンチウイルス、アンチマルウェア | + | + | |
| 継続的な防御:<br>アンチ ランサムウェア、振る舞い防御、アンチボット、アンチエクスプロイト | + | + | |
| 攻撃調査と対応:<br>フォレンジック収集、インシデント可視化、MITREマッピング、脅威ハンティング、自動化された攻撃チェーンの完全無害化、暗号化ファイルの復元 | + | + | |
| Threat Intelligence:<br>ThreatCloud™による自動 IoCとIoAクラウド共有 | + | + | |
| **安全なインターネットブラウジング:**<br>**ゼロ・フィッシング、企業パスワードの再利用防止、URL フィルタリング、SSL 可視化、悪質なサイト防御** | + | + | + |
| **Web ダウンロード保護:**<br>**サンドボックス, ファイル無害化** | + | + | + |
| データ保護:<br>ホスト暗号化、メディア暗号化 | | + | |

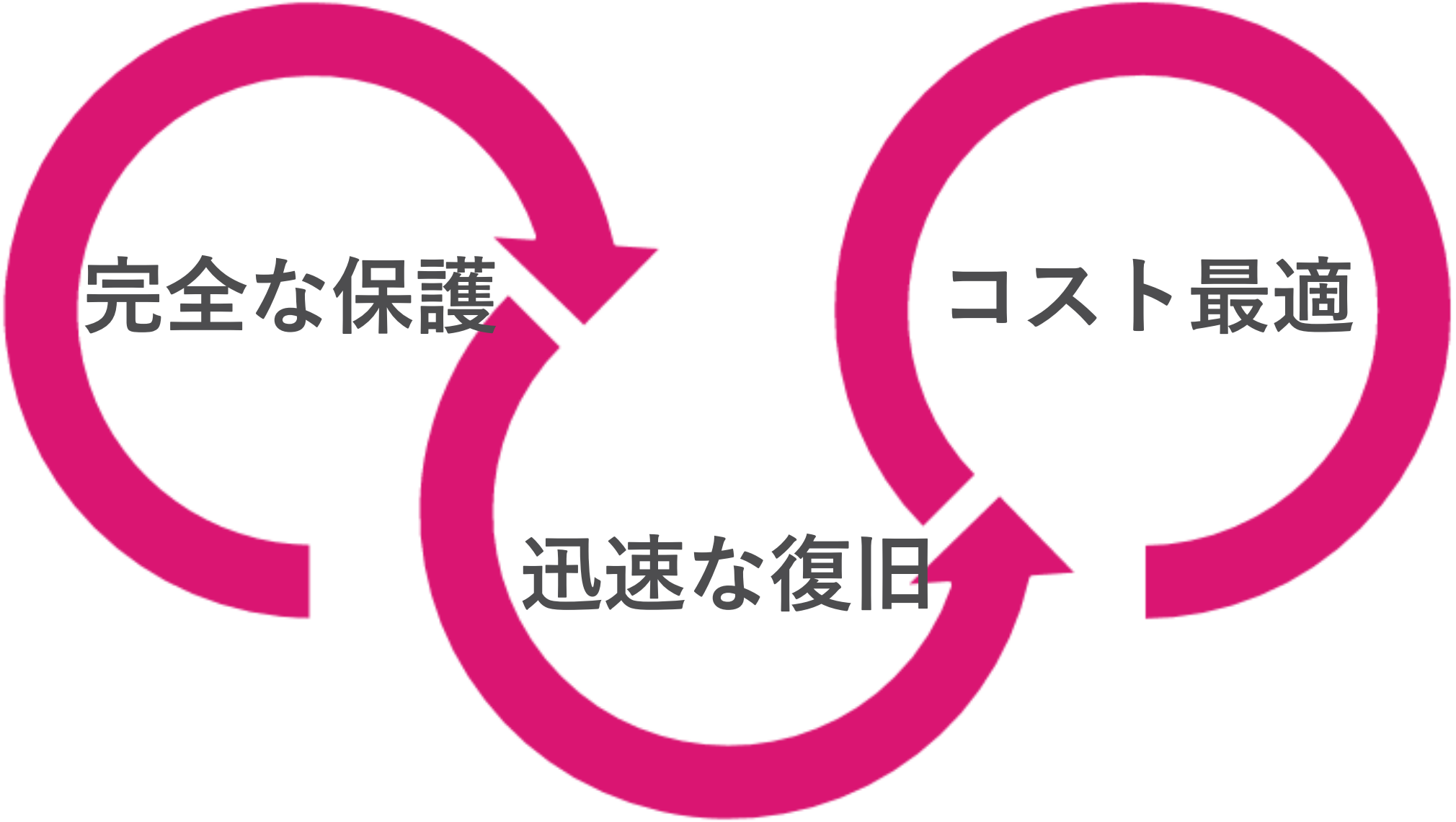
# よくある質問（その他）

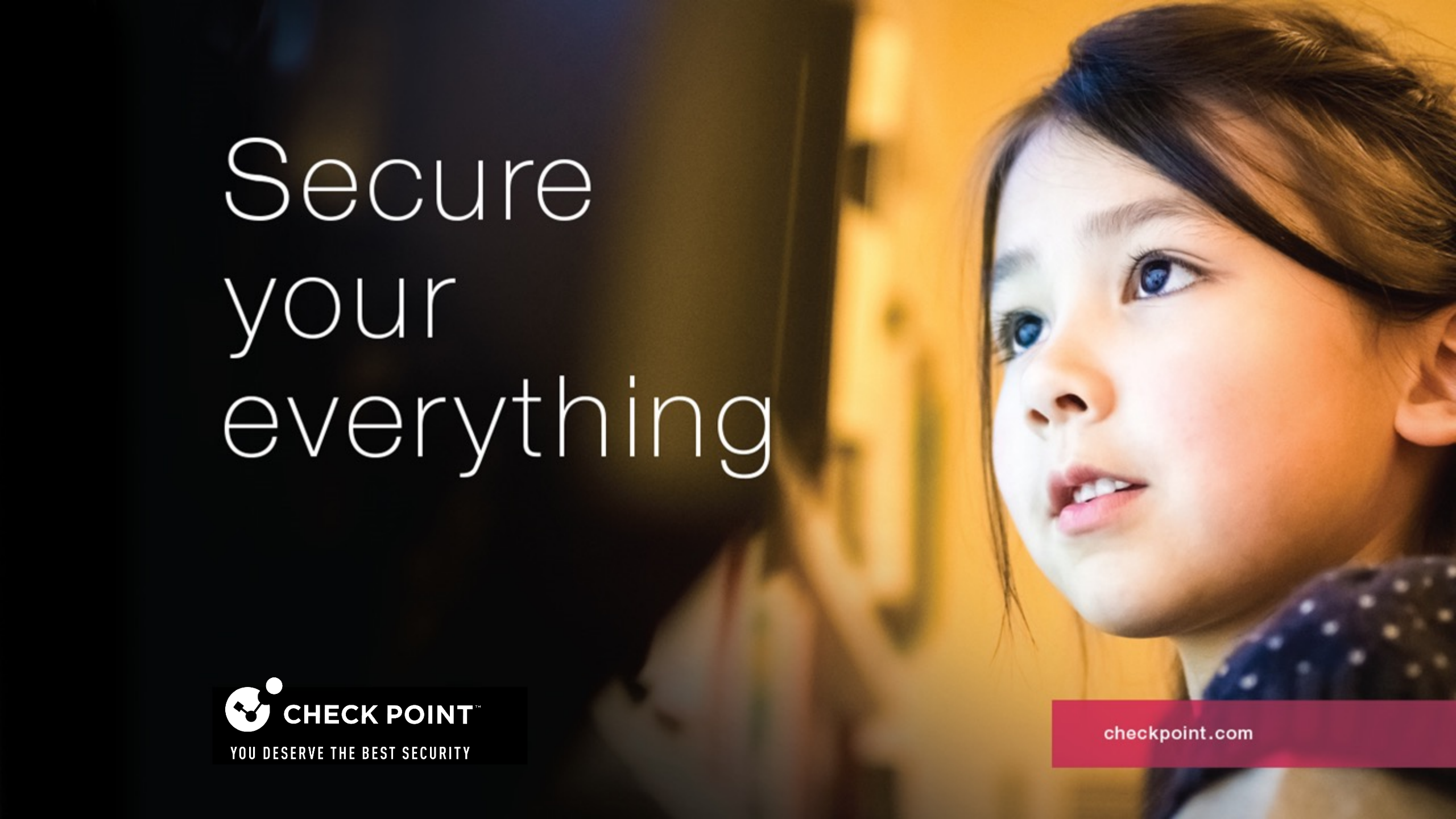
- **Windows Home Editionには対応していますか？**
  - Windows パソコンは、Pro、Enterprise 、Server にのみ対応しています。
  - 対応 OS は、以下の Web ページをご覧ください。
    - https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk178408
- **ライセンスの購入単位を教えてください**
  - デバイスライセンスで、1 ライセンスから購入可能です。
- **最低利用期間を教えてください**
  - 最低利用期間は1年間です。1年以上のご購入の場合は、13ヶ月、15ヶ月等、月単位での契約も可能です。
- **ランランサムウェアの自動復旧機能は、どのファイルが復旧できますか？**
  - 管理画面でバックアップ対象として指定したファイル拡張子、ファイルサイズ上限（初期値：25MB）に合致するファイルが対象です。バックアップシステムと併用していただくことを推奨します。
  - %SystemRoot%、%USERPROFILE%¥AppData、%ProgramData%、%ProgramFiles(x86)%、%ProgramFiles%はど、一部のフォルダはバックアップ対象外です。

# サマリー

YOU DESERVE THE BEST SECURITY

# Harmony Endpoint の特徴




Secure
your
everything
CHECK POINT™
YOU DESERVE THE BEST SECURITY
checkpoint.com

CHECK POINT™

# ありがとうございました

YOU DESERVE THE BEST SECURITY