HPのセキュリティへの取り組みとソリューション

株式会社 日本HP
専務執行役員
パーソナルシステムズ 事業統括
九嶋 俊一

2019年 IT管理者は

脅威の前例の無い拡がりに直面する

60万デバイスのファームウェアが
ボットネットMiraiに感染

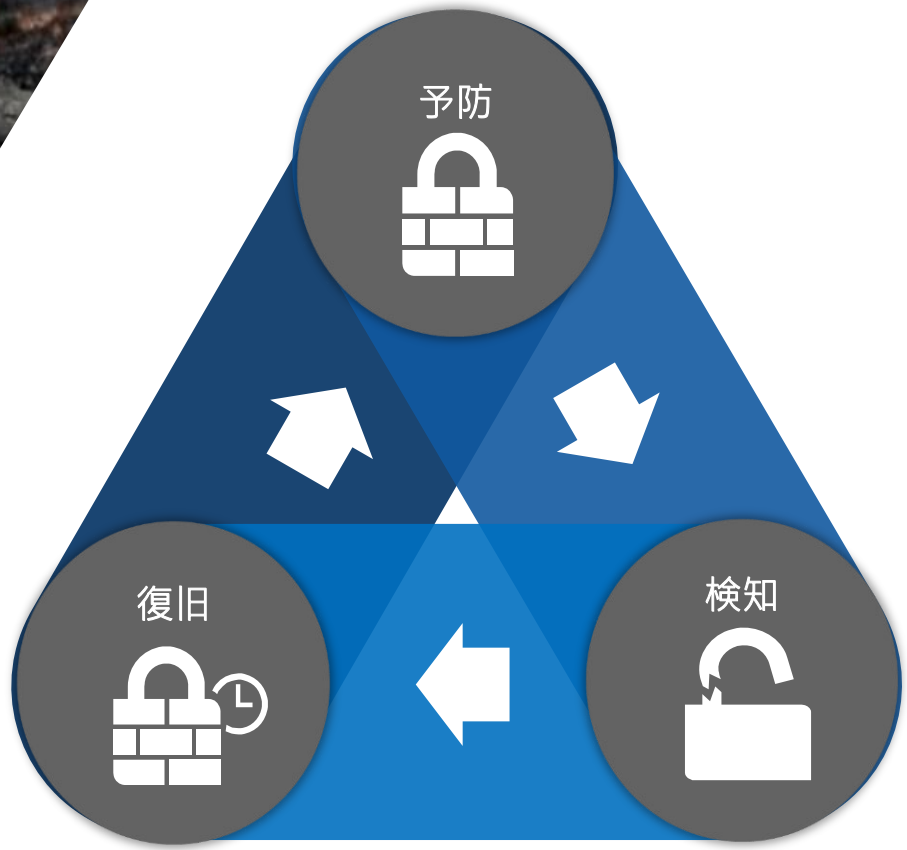
ファームウェア
攻撃の増加

2018年、2億回以上の
ランサムウェア攻撃が観測

破壊的
攻撃の勃興

毎日35万以上の新しい
マルウェア 亜種

急速なマルウェアの
進化



レジリエンス:

予防 + 検知 + 復旧

プロアクティブ管理

セキュリティポリシーの強制、悪意のある行動に対するアクティブな監視と対応

レジリエンス ハードウェア

攻撃の際に自己監視、自己回復できるハードウェア

階層的 防御

プロアクティブに脅威を防止
- OSの上、中、下

進化する“世界で最も安全で管理性に優れたビジネスPC”

レジリエンス ハードウェア

攻撃の際に自己監視、自己回復できるハードウェア

- HP Sure Start
- HP Sure Run
- HP Sure Recover

どれぐらいの時間がPC 1000台のリカバリーにかかるか？

HP エンドポイント セキュリティコントローラー

ユニークなハードウェアがレジリエントな
デバイスを可能にする

- ✓ 物理的に隔離
- ✓ 暗号化により安全

第三者機関の認証
認定された独立検証機関による
(ANSSIによる監督)

HP Sure Start

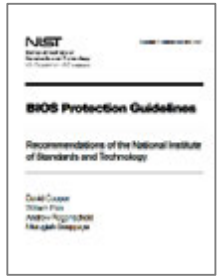
HP Sure Run

HP Sure Recover

HP 独自の優位点:

N.I.S.T.

標準



2011:
BIOS 保護
NIST SP 800-147

2019:
ファームウェア レジリエンス
NIST SP 800-193

HP SURE START GEN5 は
NIST SP 800-193に
準拠
対象は全ての主要組み込み
プラットフォーム
ファームウェア

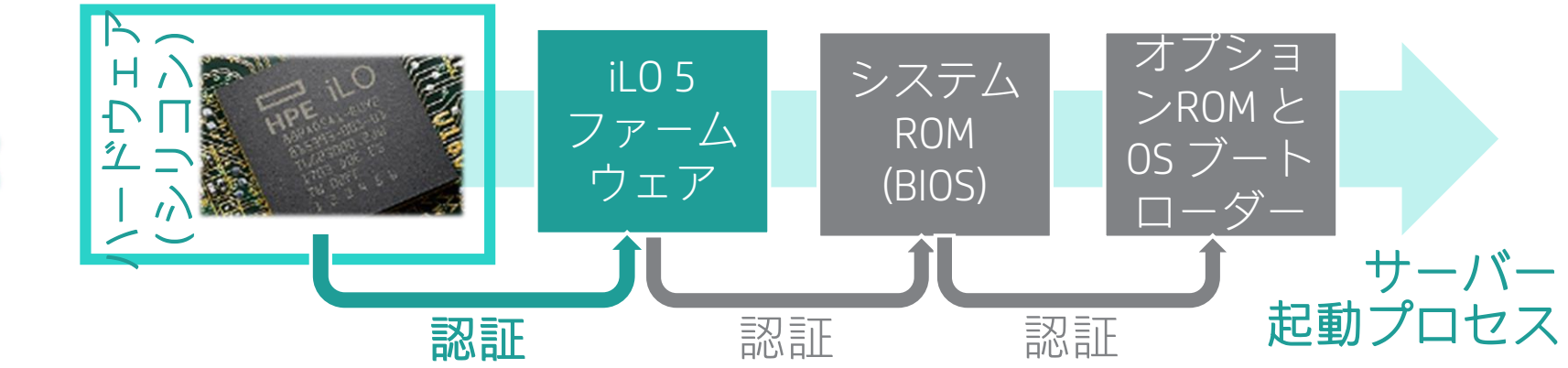
詳しくは:
詳細はHP Sure Start
ホワイトペーパー
(Gen5は近日公開!)

**See HP Sure Start whitepaper for details.*

サーバーにおける自己回復機能

世界標準の安心を提供　「HPE Gen10サーバープラットフォーム」

- Silicon Root of Trust （シリコンレベルの信頼性）
  - HPE自社開発管理チップのiLO 5 内に、ファームウェアの正常性確認ロジックを組み込み
  - iLO 5 がその後に続くファームウェアの改ざんがないことを認証して安全にサーバーを起動
  - 稼働中もオンラインのまま定期チェック、万一の改ざん時は自動検知・自動復旧



Hewlett Packard Enterprise

どれぐらいの時間がPC 1000台のリカバリーにかかるか？

攻撃:	HP以外	HPの場合
ファームウェア攻撃 例　LoJax	**週、月**- ファームウェアの手動フラッシュかマザーボード交換	Sure StartがBIOSを保護し、ITの関与無しに**数分**で復旧することができる
防御ターゲットマルウェア 例　H1N1	**不明** – 防御機構が止められてもIT部門は機器が感染していることを知ることができない	Sure Runが防御機構を再起動し、攻撃が続く場合には**すぐに**ネットワークを隔離し、犠牲無しで攻撃の拡散を防ぐ
ワイパーやランサムウェア 例　Satana	**週**　機器は手動で再イメージする必要	Sure Recover - ITの関与なしに**数分あるいは数時間**

レジリエンス ハードウェア

攻撃の際に自己監視、自己回復できるハードウェア

HP Sure Start
HP Sure Run
HP Sure Recover

階層的 防御

プロアクティブに脅威を防止 - OSの上、中、下

- HP Sure Click
- HP Sure Sense
- HP Multi-Factor Authenticate

どのようにして見たことの無いマルウェアから守るか？

HP SURE SENSE

ディープラーニングAI
を利用し
まだ見たこともない
マルウェアから
リアルタイムで保護する

約

350,000

毎日機械で生成される
新しいマルウェア
の数

攻撃者は

人工知能

をより洗練された攻撃
のために利用する

ゼロデイ攻撃は

4倍

組織を侵害する可能性
が高い

これまでの防御は

ゼロデイ攻撃を防げない

これまでのアンチウイルス:
シグネチャベース

アンチウイルスは既知のマルウェアリストに対してチェックを行う

既知の攻撃のみ

時間がかかる

頻繁なアップデート

AI:
マシンラーニング

AI がマルウェアの共通の特徴を理解するために学習する

幾つかの新しい攻撃

特徴抽出

頻繁なアップデート

AI:
ディープラーニング

AI がマルウェアを直感的に理解するために生データで学習する

既知と**未知**の攻撃

ミリ秒で動作

最小限のアップデート

エンドポイントの防御を再発明

ディープラーニングの利用

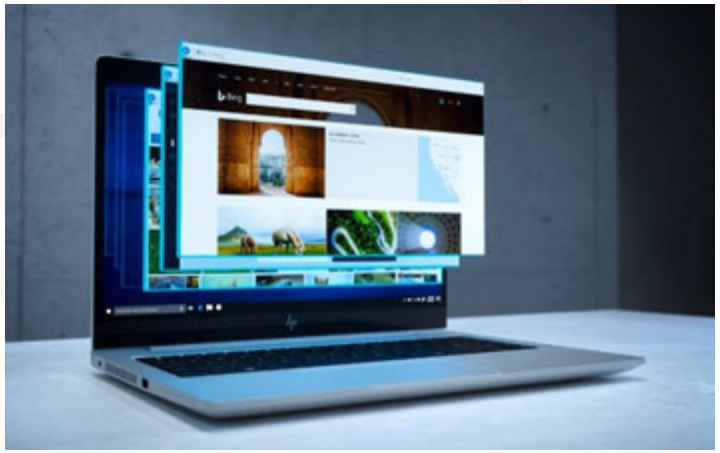
>99%
効果的

<20ミリ秒
平均検知時間

1%
CPU 負荷

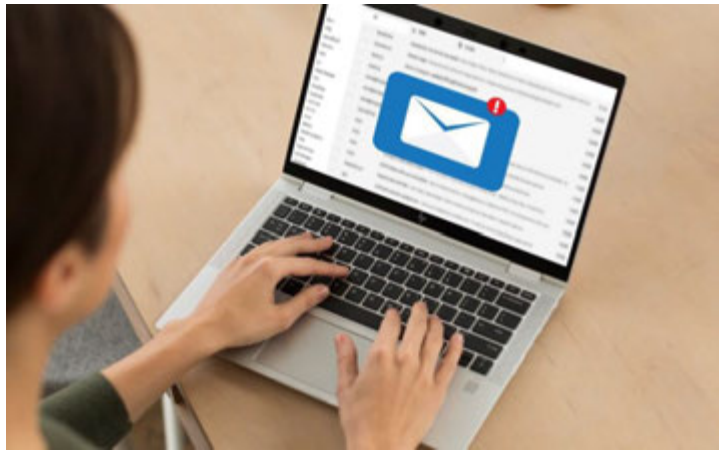
HP SURE CLICK: 信頼できるクリック

HP Sure Click[4]で添付ファイルを開きオンラインで仕事をする



悪意のあるWEBサイトから守る

✓各タブを安全な仮想コンテナで隔離する
✓単純にタブをクローズするとマルウェアも消える
✓IEとChromeと統合され簡単な利用方法



悪い添付ファイルから守る

✓感染したファイルは一般的攻撃経路
✓リードオンリーモードで閲覧しWord、Office、PDFファイルを保護する

HP Sure Clickは「インテル® バーチャライゼーション・テクノロジー（インテル® VT）」を活用。

「インテル® VT」は、仮想化をハードウェアで支援する機能。仮想化とは、1台のパソコンにて複数の仮想マシンを同時に動作させる技術だ。通常は1台のパソコンにて動作するOSは1つだが、仮想マシンを利用すれば、例えばWindows 10と過去のWindowsの同時動作が可能となっている。

階層的防御

エンドポイントのレジリエンスを実現

全ての会社が必要とするもの:

HP が提供するもの:

4 AI による脅威への対処
未知の攻撃に対する保護
例：機械生成マルウェア

→ HP SURE SENSE

3 隔離ソリューション
リスクの高い攻撃方法に対する保護
例：悪意のあるWeb

→ HP SURE CLICK

2 伝統的 AV
既知の攻撃に対する保護
例：LoveLetter（マルウェア）

→ WINDOWS DEFENDER

1 レジリエンスH/W
最悪シナリオからの復旧
例：ワイパー攻撃

→ HP SURE RUN
HP SURE RECOVER
HP SURE START

プロアクティブ管理

セキュリティポリシーの強制、悪意のある行動に対するアクティブな監視と対応

レジリエンスハードウェア

攻撃の際に自己監視、自己回復できるハードウェア

HP Sure Start1
HP Sure Run2
HP Sure Recover3

階層的防御

プロアクティブに脅威を防止 - OSの上、中、下

- HP Sure Click[4]
- HP Sure Sense[8]
- HP Multi-Factor Authenticate[11]

どのようにして攻撃を受けている事を知るのか？

HP プロアクティブセキュリティ

Sherban Naum
Bromium
Senior Vice President
Corporate Strategy and Technology

エンドポイントは組織の最大のセキュリティリスク

92%

Eメールの添付ファイルに起因する感染[1]

57%

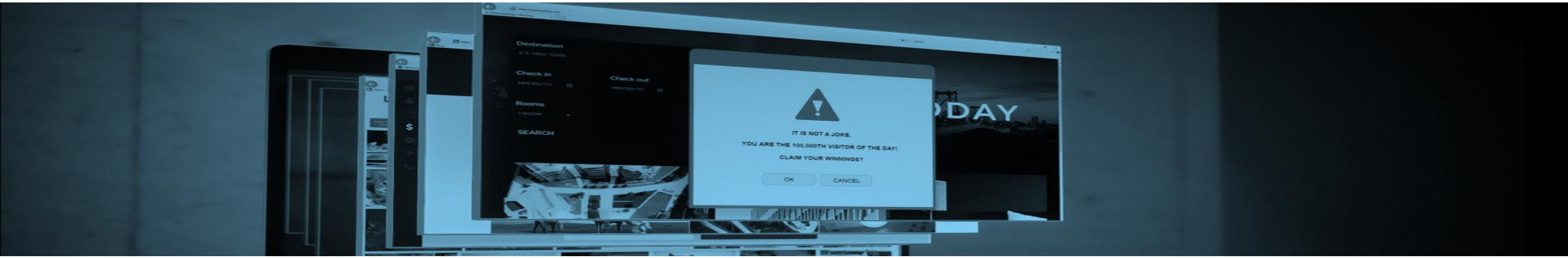
アンチウィルスが見逃した事で成功したエンドポイント攻撃[2]

セキュリティポリシーとアンチウィルスだけでは不十分

HP プロアクティブセキュリティが最終防衛線！

Source: [1] 2018 Data Breach Investigations report 11th Edition, Verizon, 2018; [2] Ponemon Institute 2018 State of Endpoint Security Risk sponsored by Barkly, October 2018

なぜEDRやEPPでは十分でないのか？



“ペイシェント・ゼロ”

脅威はエンドポイントセキュリティ製品を回避するように設計される

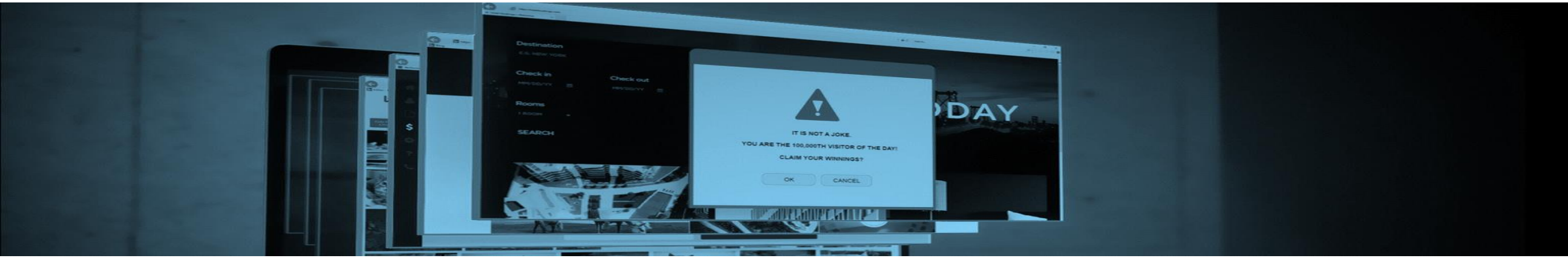
脅威分析が無い

攻撃を阻止することに集中すると、攻撃操作とIOCに対する洞察がほとんど得られない

高コストのフォレンジック分析

攻撃操作の発見と分析は長期に渡る

なぜEPPやEDRに加えて隔離が必要なのか？



人的エラー
54%

中小企業におけるデータ侵害の原因が従業員の過失によるものであった割合[1]

ゼロデイ攻撃
4x

組織を危険にさらす可能性が高まる倍率[2]

可視化の欠如
96%

数か月後になるまで発覚しなかった侵害の割合[3]

Source: 1. The 2017 State of Cybercrime in Small and Medium-Sized Business Sponsored by Keeper Security Independently conducted by Ponemon Institute LLC Publication Date: September 2017; 2.Ponemon Institute 2018 State of Endpoint Security Risk sponsored by Barkly , October 2018; 3. 2018 Data Breach Investigations report 11th Edition, Verizon, 2018

HP Sure Click Advancedはエンドポイントをランタイム保護

悪意のあるリンクや添付ファイルによる人的エラーに対して保護

最も多い経路からのゼロデイ攻撃を分離環境に封じ込め

セキュリティの現状を可視化

- 保護されたデバイスの分析

ITインフラストラクチャ全体をランタイム保護

詳細なフォレンジックとキルチェーン分析で脅威インテリジェンスを強化

検出に失敗した場合も保護

- 一番の攻撃経路の保護: 最も多い侵入ポイントからの信頼されないコンテンツは隔離されます
  - Outlook Eメール
  - 信頼されないWebサイト
  - WebからのダウンロードやUSBメモリからのコンテンツ
- プロアクティブな隔離により保護範囲を拡大します
  - 信頼されない未知のコンテンツ用のデジタル“グローブ”
  - 未知の信頼されないコンテンツは、ハードウェアレベルで保護された、使い捨ての“マイクロ”仮想マシンに閉じ込められます。
- 隔離されている間、不審な行動について行動が継続的に監視されます
  - 悪意のある場合は、詳しい分析のために詳細な診断データが収集されます。
  - 無害であったもそうでなくても、コンテンツは常に隔離されたままになります。

HPプロアクティブセキュリティ

Windows 10 PCのファイルとブラウジング向けの世界で最も進んだ隔離セキュリティサービス

保護とセキュリティインテリジェンスを拡張し、
エンドポイントを最大のリスクから最善の防御
に変換

脅威からのリアルタイム保護

ゼロデイ、Eメール、ブラウザ、ファイル攻撃からの
隔離技術による高度なマルウェア保護

セキュリティインテリジェンスの強化

HP TechPulseによるセキュリティ分析とレポート

プロアクティブセキュリティ管理

サイバーセキュリティのエキスパートによる
HPマネージドサービス

マルチベンダーのWindows 10 PCで利用可能

隔離保護は脅威に対処するための主要ユースケースを対象

エンドポイントの攻撃対象領域を減らす

Eメール添付	共有リンク	ファイルダウンロード
悪意のあるEメールに対する保護	**悪意のあるリンクに対する保護**	**悪意のあるダウンロードに対する保護**
ランサムウェア マクロを悪用したトロイの木馬 ファイルレスマルウェア 悪意のあるリンク	Eメール内の悪意のあるリンク ブラウザーエクスプロイト 偽のFlash/Javaアップデート 悪意のある広告 Skype内のリンク	意図的なダウンロード 実行可能ファイルの 偽造アップデート ドキュメントへのリンク 不正なDNS/URLリダイレクト 偽のドライバとユーティリティ

HP Sure Click Advancedの機能

封じ込め: リアルタイム攻撃隔離

- マルウェアの実行を完全に隔離
- ハードウェア、カーネル、OS、アプリケーション、ゼロデイ、国家、多形
- 侵害、修復、摘出、立ち退きが無い
- 多層防御を回避するすべての攻撃を隔離
- リアルタイムでの攻撃の識別、サイバーOPSへの通知、リルタイムでの対応を可能にする
- ほとんどのWindowsアプリケーション

リアルタイム 脅威テレメトリー

- 仮想マシンが破壊された場合、フルキルチェーン、バイナリ、および完全な攻撃テレメトリーをサイバーチームと共有
- 自己削除、ネットワーク、アンチフォレンジック、カーネルなど、全ての攻撃の指標が収集される
- エグゼクティブビュー、アナリストビュー、およびレスポンスビューによる完全な攻撃の視覚化

脅威インテリジェンスの共有

- Tanium、Splunk、ArcSight、などの既存のプラットフォームへの脅威の共有
- STIX/TAXI
- MITRE ATT&CK
- SYSLOG, CIF
- 実行後のハニーポットサービス/ Cyber-Opsと共有可能なバイナリ
- 完全または匿名編集済み
- 階層的配布機能
- イベントごとに複数の宛先

Bromium強化アクセス/ゼロトラストモデル (AX)

- 感染した状態での運用上の整合性
- 保護されたアプリケーション
- 完全性と機密性
- 安全なモビリティ
- クラウド、VDI、アプリケーション仮想化へのセキュアリモートアクセス
- 特権リモートアクセス
- 結合アクセス
- 感染したデバイスからの信頼できるアクセス
- キーロギング/スクリーンキャプチャ/データ漏洩を停止
- NISTゼロトラストアーキテクチャ

HP Sure Click Advancedによる封じ込め：より高度な保護

最初に隔離し保護する:
すべてのマルウェアは
隔離してから実行する。

隔離された攻撃は他の
すべてのソリューショ
ンを回避し、企業のイ
ンフラストラクチャを
危険にさらしていた。

実行前に悪意があるか
どうかを判断するため
の検出や動作モデリン
グを行わない。

仮想環境で攻撃が発生
し、企業リソースにア
クセスでない。

隔離されたマルウェア
は完全な実行を許可さ
れすべての攻撃のテレ
メトリーが公開されま
す。

攻撃後に不完全な情報
を再構成する必要はあ
りません。

インターネットとイン
トラネットは互いに分
離されています。企業
への攻撃からマイクロ
セグメントへの攻撃に
なります。

攻撃のテレメトリはリ
アルタイムで記録され、
キルチェーン全体、バ
イナリ、詳細が報告さ
れます。

完全な脅威テレメト
リーを正確さと完全な
キルチェーンと共に
SOCにリアルタイムで
共有および提供します。

リアルタイムに利用可
能で共有可能な、完全
でタイムリーなリアル
タイム対応脅威検出イ
ンテリジェンスを提供
するソリューションは
他にはありません。

高度な分離テクノロジーが脅威分析を採取します

各マイクロVMごとに個別のアプリケーションのハードウェアによる仮想化を利用します。

マイクロVMはEメール添付、リンク、ダウンロードなどの信頼されないソースからのアプリケーションを実行します。

マイクロVMは監視され、マルウェアが実行すると脅威分析[3]がHP TechPulseに採取されます。

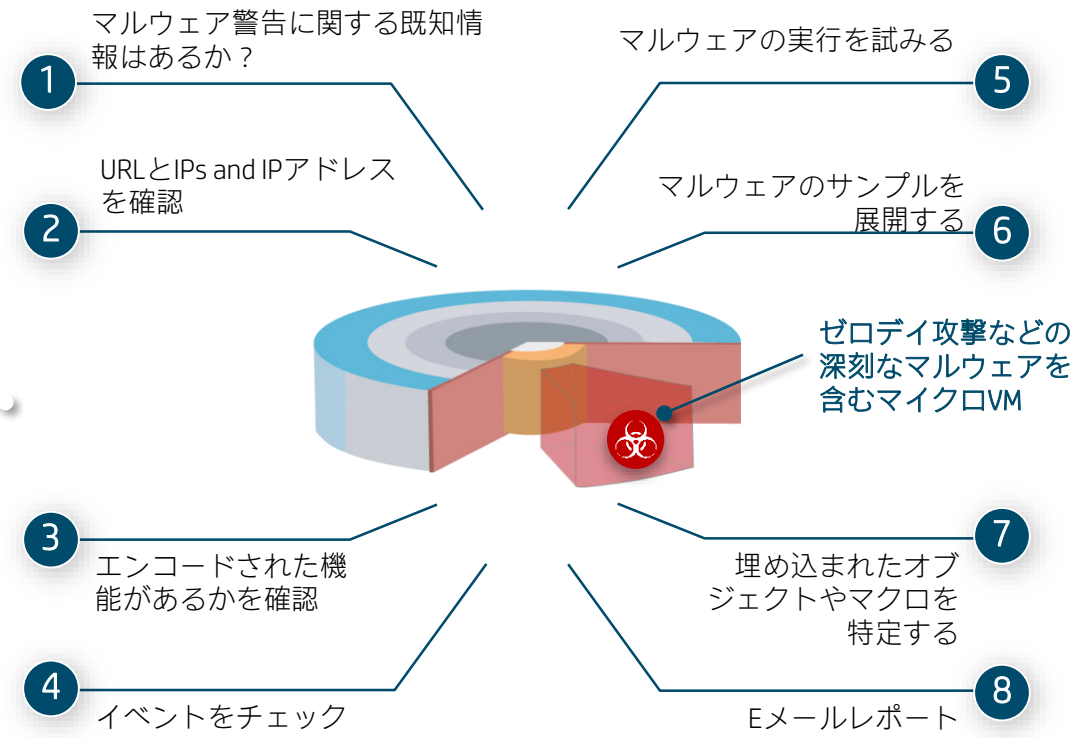
HPのキルチェーン解析による脅威インテリジェンスの価値

HPの脅威解析
キルチェーンの理解

攻撃キルチェーン

偵察	ターゲットを選択して脆弱性を調査する。
武器化	マルウェアを作成する
展開	マルウェアを送信する（Eメール添付等）
侵入	マルウェアがターゲットのネットワークに侵入する
インストール	マルウェアは侵入者のアクセスを可能にする
指令と制御	侵入者は持続的に制御可能となる
行動と目的	身代金のためのデータ盗難、破壊、暗号化

HPによる解析と評価



状況認識: HPの4半期ごとの脅威ビジネスレポート

検知できない隔離された攻撃のクイックビュー:

発生時に他のセキュリティ製品に知られていなかった攻撃

マルウェアファミリーごとのドリルダウン

隔離された攻撃のマルウェア名

7. Win32.Trojan.Wanna	8	20. Script-BAT.Trojan.CVE-2017-11882	1
8. Win32.Trojan.Generickd	8	21. Win32.Ransomware.Wannacrypt	1
9. Document-Word.Trojan.CVE-2017-11882	4	22. Win32.Trojan.Cqc	1
10. Document-Excel.Trojan.CVE-2003-0347	3	23. Document-Word.Downloader.Sload	1
11. Document-Word.Trojan.CVE-2017-1182	3	24. Document-Excel.Downloader.Powload	1
12. Win32.Trojan.Emotet	3	25. Document-Word.Trojan.Autoruns	1
13. Win32.Trojan.Phishing	2	26. Win32.Trojan.Loi	1

MITRE | ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control

0. T1106: Execution through API	12
1. T1059: Command-Line Interface	5
2. T1129: Execution through Module Load	4
3. T1107: File Deletion	4
4. T1086: PowerShell	4
5. T1060: Registry Run Keys / Startup Folder	4
6. T1112: Modify Registry	1

We saw 7 different Mitre Att&ck techniques this period. The most prevalent was T1106 (Execution through API) with 12 occurrences.

The heat map above groups the 11 stages of the enterprise kill chain into columns. Since the kill chain moves from left to right, the further to the right a spot appears, the deeper into its kill chain the malware ran.

MITRE ATT&CK フレームワークによる隔離した攻撃の可視化

隔離した攻撃のMITRE ATT&CK カテゴリ

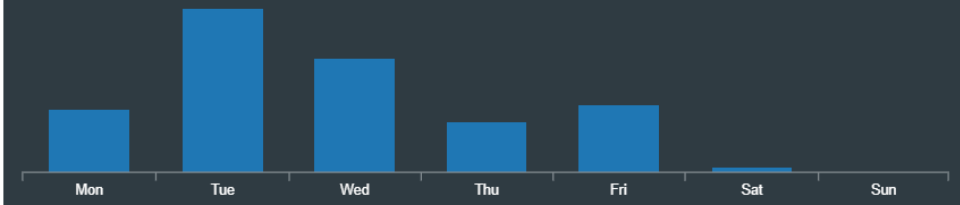
5. T1060: Registry Run Keys / Startup Folder 4

6. T1112: Modify Registry 1

Broken down by time

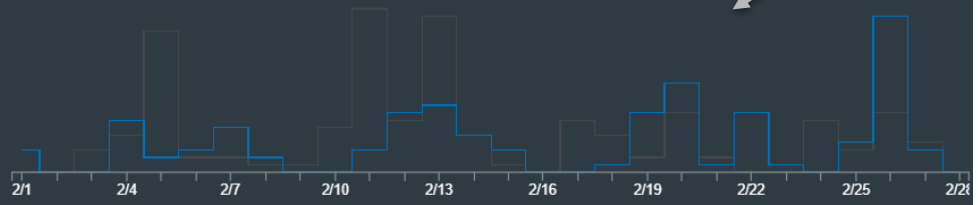
By day

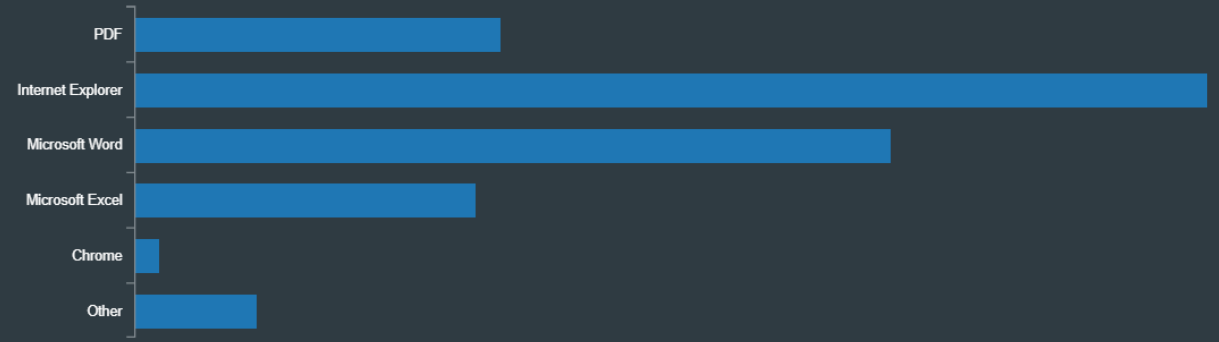
Breaking down the threat activity into days can be useful to see when your organisation is most at risk. Either because actors are more active, or more likely because your users are.



Over this period

This period saw 110 threats, and the figure below charts the frequency at which they are received. The darker line denotes the activity over the previous period compared to this one.





By application

Bromium secures various applications. This breakdown charts those applications which receive the most threats.

GDPR regulations require Bromium to redact and / or delete executable files and associated metadata from our storage systems within specific time periods, precluding further remote analysis at this time. Bromium is happy to provide you with the UUIDs for any items listed to pursue investigations of identified risky executable files on your own Bromium Controller.

Thank you for sharing your sensitive threat intelligence data with Bromium. We hope that this information proves useful to you. Please let us know how we can make this Threat Summary Report even more valuable to you going forward.

時間/ 期間ごとの隔離した攻撃

アプリケーションごとの隔離した攻撃

隔離されたゼロデイ攻撃と高度なマルウェア攻撃に関するHP DaaSマネージドプロアクティブセキュリティ脅威トリアージレポート

9 May 2019

HP Threat Triage Brief on Emotet Malware

Summary

- Emotet is a modular banking Trojan that can brute force passwords, steal credentials from web browsers and email clients, send spam and be used as a beachhead to download other malware.
- Due to Emotet's capability to deliver obfuscated payloads and extend its capabilities through self-upgradable modules, it has become a commonly-used payload launcher in targeted attacks on organizations.
- Emotet's operators have adopted a "malware-as-a-service" business model, where the Trojan is used to distribute other malware families, such as Trickbot.

Introduction

Emotet is a modular banking Trojan that is capable of stealing credentials from web browsers and email clie
functioning as a dropper f
using the Server Messag
Emotet has developed a
functionalities:

- Use of packers to e
- Use of anti-analysi
- Indirect execution
- Privilege escalatic
  administrator crede
- Obfuscated code a
- Use of multiple per
- Encrypted imports
- Multiple JMP instru
- Self-upgradable m
- Ability to move late
- Ability to make in
  address books and

HP Triage Report for the Government Entity

Summary

- On 2 May 2019, Bromium Secure Platform isolated the running of a malicious Word document containing script-based malware (HTA, VBScript, JavaScript and PowerShell)
- The malware solely relied upon tools built into Windows for code execution, reconnaissance and persistence, epitomising 'Living Off the Land' adversary tactics.
- The Word document opened by the user was not detected by any signature-based scanning engines.

Investigation

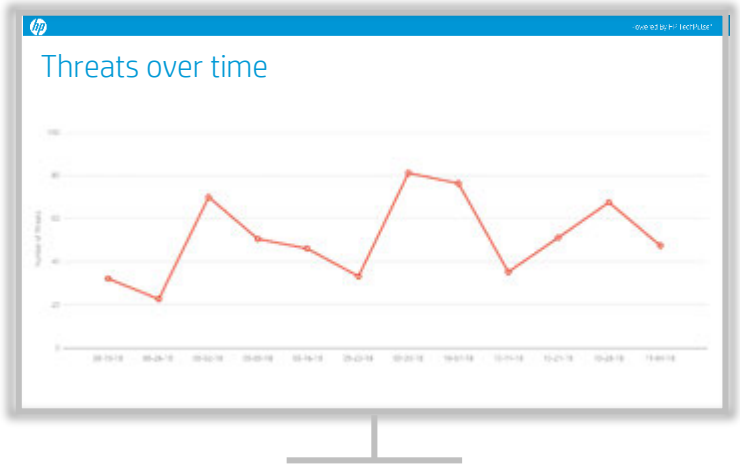
On 2 May 2019, Bromium isolated the running of a malicious Microsoft Word document ('srl-201904.doc') on a *Customer* computer. The sample was shared with Bromium Threat Labs by *The Customer* for analysis.

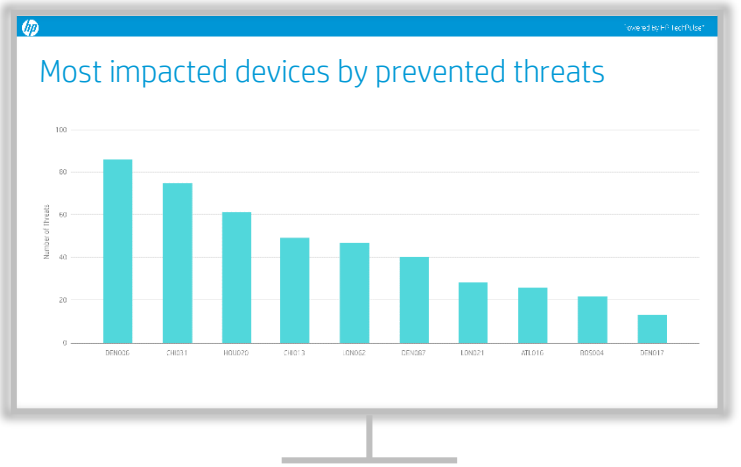
Static analysis of the document found that it is a Composite Document File V2 (CDFV2) file that was encrypted using AES in Cipher Blocking Chaining (CBC) mode with a 256-bit key. The password to decrypt the document is '95Cv62aCDmpbbZBC'. On 1 May 2019 at 20:52, the document was uploaded to VirusTotal. No scanning engines (0/58) detected the file as malicious.[1] The file contains a Visual Basic for Applications (VBA) AutoOpen macro that executes when the document is opened. The document also contains an embedded image (Figure 1) that requests the user to click the 'Enable Editing' button to disable Microsoft Word's read-only mode (Protected View) and 'Enable Content' to cause the macro to run.

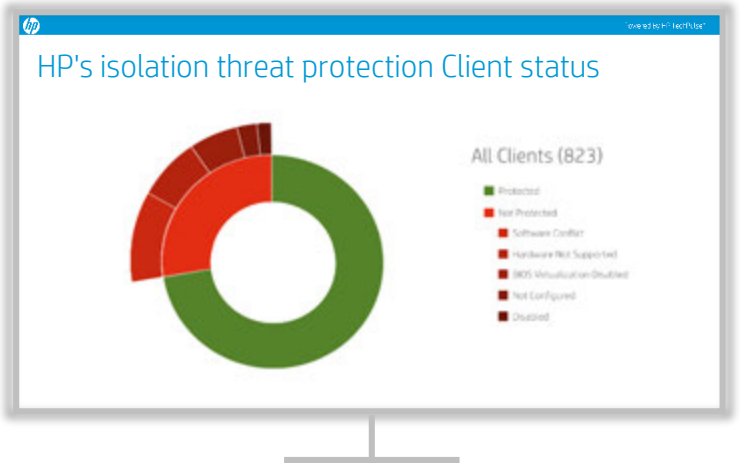
脅威トリアージレポート

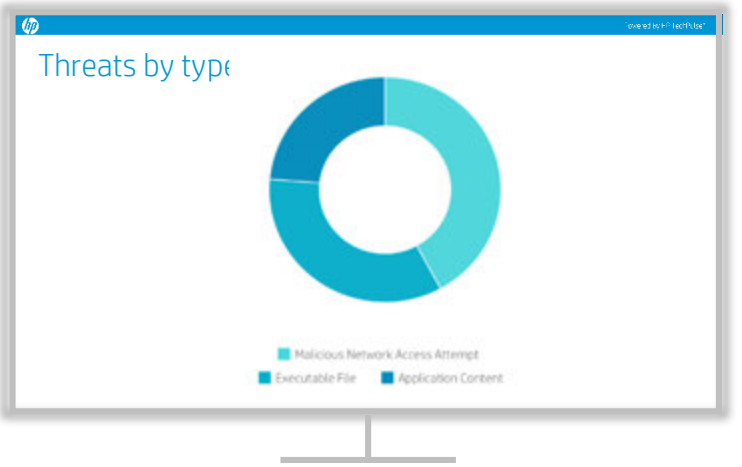
- 隔離されたゼロデイ攻撃または重大な標的型攻撃ごとに作成されたカスタムレポート
- 完全なフォレンジックおよび脅威テレメトリーと攻撃の指標（IOA）を使用したレポート
- 4半期ごとのビジネスレビューマクロレポートに加えて

HP TechPulseの脅威分析によるプロアクティブ管理







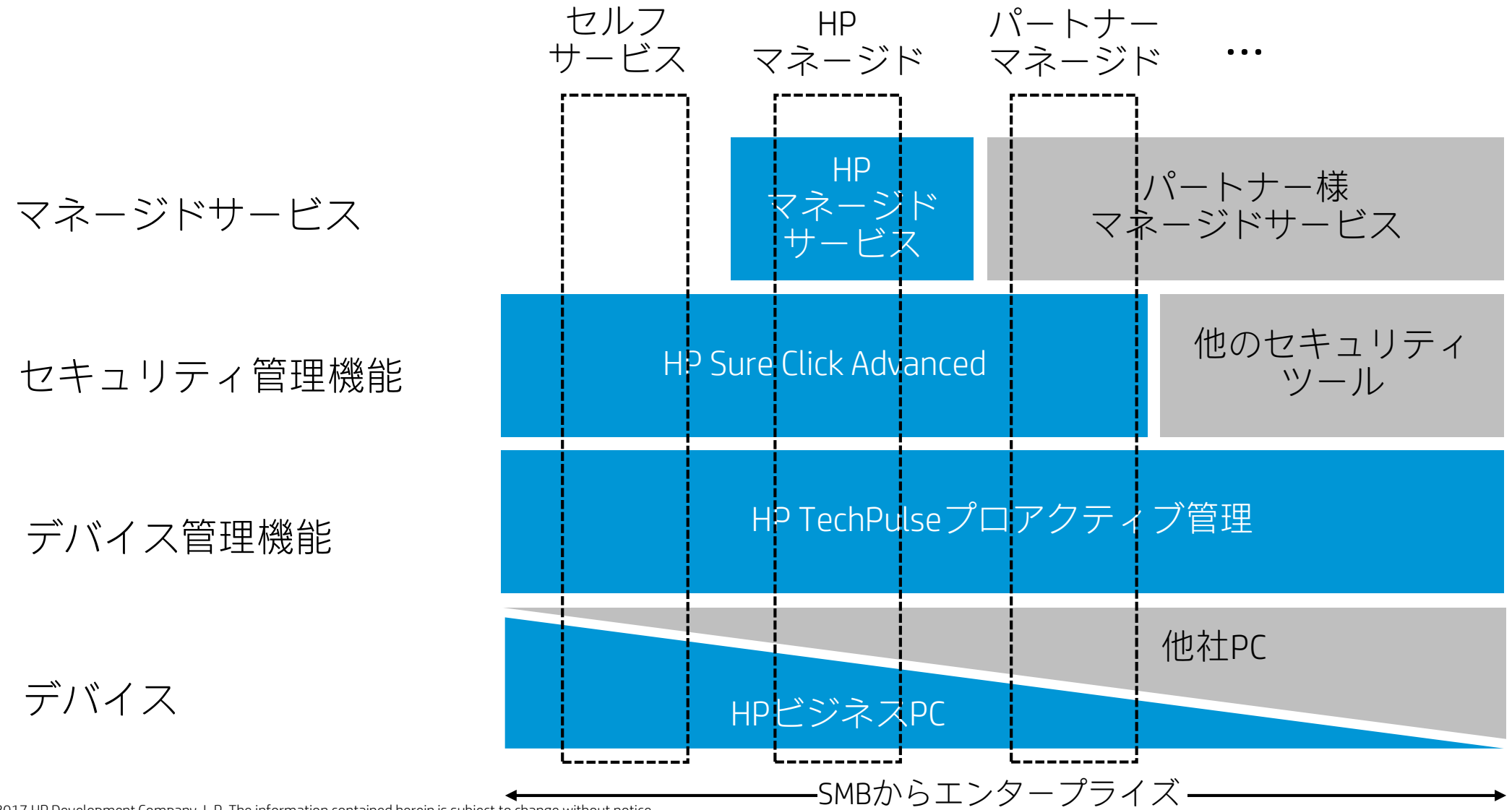


エンドポイントの階層的防御とプロアクティブ管理

全ての会社が必要とするもの

	ハードウェアに組み込み機能	セルフサービス	マネージドサービス
4 AIによる脅威への対処 *未知の攻撃に対する保護* ***例: 機械生成マルウェア***	HP SURE SENSE		
3 隔離ソリューション *ゼロデイ攻撃、カーネル、ルートキット、ファイルレス、エモテット等からの保護を想定* ***例: 悪意のあるドキュメント、ランサムウェア、標的側攻撃***	HP SURE CLICK	HP DAAS PROACTIVE SECURITY STANDARD (HP Sure Click Advance)	HP DAAS PROACTIVE SECURITY ENHANCED (HP Sure Click Advance)
2 伝統的 AV *既知の攻撃に対する保護を想定* ***例: LoveLetter（マルウェア）***	WINDOWS DEFENDER		HP DAAS ENHANCED OR PREMIUM
1 レジリエンスHW *ハードウェアによる保護と復旧* ***例: ワイパー攻撃***	HP SURE RUN HP SURE RECOVER HP SURE START		

柔軟なビジネスモデルで多様なサービスをパートナー様と提供



全ての組織が計画を持つ必要がある
レジリエンス

1

どれぐらいの
時間がPC 1000台
のリカバリーに
かかるか？

HP Sure Recover と
組み込み再イメージング
で**5分以内**

2

どのようにして
見たことの無い
マルウェアから
守るか？

HP Sure Senseの
ディープラーニングAIを
含む**階層的防御**

3

どのようにして攻撃
を受けている事をプ
ロアクティブに知る
のか？

HP プロアクティブ
セキュリティによる
管理性

HP エンドポイントセキュリティスタック2019

新規

アップデート

アップデート無し

	デバイス	アイデンティティ	データ
OSの上	HP MIK Gen3 セキュリティの集中管理	HP Proactive Security (DaaS) エンフォース、監視、分析	HP Sure View Gen3 組み込みプライバシーフィルター HP Sure Click 安全なWebブラウジングとファイルの閲覧
OSの中	HP Sure Recover Gen2 ネットワークベースの自動化イメージ復旧 HP Sure Run Gen2 クリティカルアプリケーションの保護	HP Client Security Manager Gen5 • HP Multi-Factor Authenticate Gen3 ポリシー堅牢化、顔認証を含む多要素認証 • HP SpareKey セルフサービスのパスワードリカバリ	HP Sure Sense ディープラーニングによるマルウェアの保護 HP Secure Erase HDD/SSD上のデータの完全除去
OSの下	HP Sure Start Gen5 インテルMEとBIOSの自己回復 HP BIOSphere Gen5 包括的BIOS管理		Certified Self-Encrypting Drives HW データ暗号化

HP Endpoint Security Controller

Thank you