Microsoft
Security Forum 2020

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

B-1

Symantec 製品ご利用中のお客様に捧げる Microsoft セキュリティへの移行のススメ

クラウド & ソリューション事業本部 モダンワークプレイス統括本部
日本マイクロソフト株式会社
和田 健太

Microsoft

移行・切替の準備、できていますか？

エンタープライズセキュリティ事業の売却により さまざまなところで **波紋** が広がっています

ZDNet Japan　海外発　デジタル変革　CIO　ITインフラ　セキュリティ

ZDNet Japan › セキュリティ

企業買収

Broadcom、シマンテックのエンタープライズ向けセキュリティ事業を買収へ--約1兆円

Natalie Gagliordi（ZDNet.com）翻訳校正：編集部　2019-08-09 10:28

シェア 412　ツイート　B! 4　noteで書く　Pocket　10

PR　講演レポート：データ活用の未来像は・・・AWSセミナー
PR　IT探偵しおんが解決！マルウェア感染！？万が一はエキスパートに
PR　導入事例、製品情報、調査・レポートなど、ホワイトペーパー多数掲載

Broadcomは米国時間8月8日、Symantecのエンタープライズ向けセキュリティ事業を107億ドル（約1兆1300億円）で買収する契約を締結したと発表した。今回の買収によってSymantecは実質的に分社化され、同社のエンタープライズ向けセキュリティポートフォリオと、「Symantec」というブランド名はBroadcomのものとなる。Symantecは、「LifeLock」というID保護のブランドや、ウイルス対策ソフトウェア「Norton」などのコンシューマー向けポートフォリオを維持するという。

ZDNet Japan　海外発　デジタル変革　CIO　ITインフラ　セキュリティ

ZDNet Japan › セキュリティ

シマンテックのサイバーセキュリティサービス事業、アクセンチュアがBroadcomから買収へ

Asha Barbaschow（ZDNet.com.au）翻訳校正：編集部　2020-01-08 11:47

シェア 1,093　ツイート　B! 6　noteで書く　Pocket　23

PR　講演レポート：データ活用の未来像は・・・AWSセミナー
PR　セキュリティ対策に100%はない！いざというときにどうする？！
PR　導入事例、製品情報、調査・レポートなど、ホワイトペーパー多数掲載

Accentureは、Symantecの「Cyber Security Services」（サイバーセキュリティサービス）事業をBroadcom, Incから買収する意向であることを発表した。

Broadcomは2019年8月、Symantecのエンタープライズ向けセキュリティ事業を107億ドル（約1兆1300億円）で買収すると発表した。AccentureによるCyber Security Services部門の買収金額は明らかにされていない。

この買収により、AccentureはSymantecのCyber Security Servicesのポートフォリオを引き継ぐことになる。セキュリティオペレーションセンターのネットワークを介したグローバルな脅威

あるお客様の声

“営業担当者がいなくなり、相談できずに困っている。”

“次回のライセンス更新時は、3 倍以上の値上げとなると言われていて、IT 予算計画が立てられない状況になっている。”

“今後の製品やサービスのロードマップが不明確で不安。”

etc...

ソリューションマッピング

安心してください - それぞれ 最適な移行先をご用意しています

主なソリューション		Symantec	Microsoft 365
PC/モバイルの保護	アンチウイルス	Symantec Endpoint Protection (SEP)	Microsoft Defender ウイルス対策 Microsoft Defender ATP
	EDR	Symantec ATP	
メールの保護	マルウェア・ スパム対策 未知への対応 サンドボックス	Symantec Email Security.cloud Email Threat Detection and Response	Exchange Online Protection Office 365 ATP
データの保護 情報漏洩対策	データ損失防止	Symantec Data Loss Prevention (DLP)	Microsoft 365 DLP (Cloud, Endpoint, Communication)
	CASB	Symantec CloudSOC CASB Gateway	Microsoft Cloud App Security
	Web フィルタ	Symantec Web Security Service Symantec ProxySG	Microsoft Defender ATP + CYREN (Web コンテンツフィルタリング)
⋮	⋮	⋮	⋮

本セッションの内容

お問合せの多い以下の 2 つを例にあげて移行例をご説明

エンドポイントの保護

Symantec
Endpoint Protection (SEP)

Microsoft Defender
ウイルス対策 &
Advanced Threat Protection (ATP)

メール・コンテンツの保護

Symantec
Email Security.cloud

Exchange Online Protection &
Office 365 **Advanced Threat Protection (ATP)**

Microsoft
Security Forum 2020

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

エンドポイントの保護

Microsoft

どのようにマルウェア対策製品を選択するか？

過去

マルウェア検知率だけが
製品の高評価につながった時代

Windows 10: December 2019

Producer		Certified	Protection	Performance	Usability
avast	Business Antivirus Pro Plus 19.7		6	5.5	5.5
Bitdefender	Endpoint Security 6.6		6	5.5	5.5
Bitdefender	Endpoint Security (Ultra) 6.6		6	4.5	5.5
eset	Endpoint Security 7.1		5	6	6
	AntiVirus Business 14.2		5.5	5	6
kaspersky	Endpoint Security 11.1 & 11.2		6	6	6
kaspersky	Small Office Security 7		6	6	6
McAfee	Endpoint Security 10.6		5	6	6
McAfee	Small Business Security 18.1 & 18.2		5	6	6
Microsoft	Windows Defender Antivirus 4.18		6	5.5	5.5
SECRITE	Endpoint Security 18.00		6	5.5	5.5
SOPHOS	Endpoint Security and Control 10.8		6	5.5	5.5
Symantec	Endpoint Protection 14.2		6	6	6
Symantec	Endpoint Protection Cloud 22.19		6	6	6
TREND MICRO	Apex One 14.0		6	5.5	5.5

AV-TEST : The best Windows antivirus software for business users
https://www.av-test.org/en/antivirus/business-windows-client/

現在/未来

製品ベンダーそのものの評価や
事業継続性が重要な時代

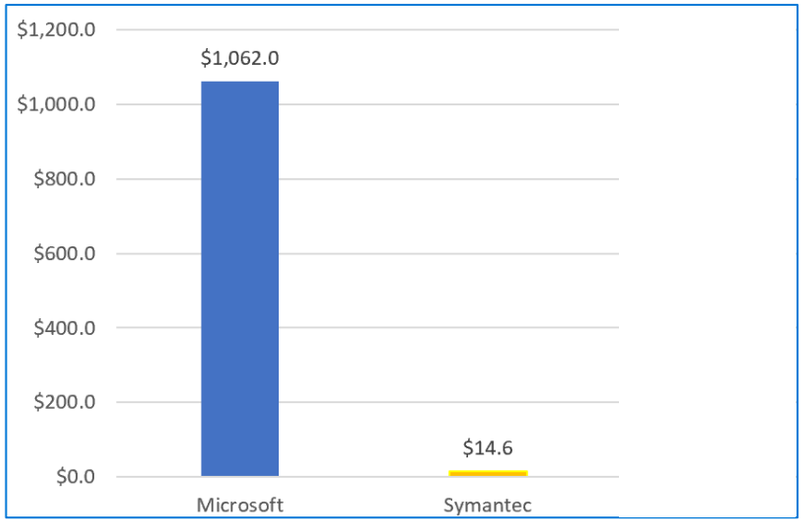
- 事業規模
  企業価値(株価)
- 企業ヴィジョン
  製品ロードマップ・思想
- 第三者機関による
  ベンダー評価

マイクロソフトの企業規模

買収・撤退等による影響を避けるため企業規模は重要

$ 1 兆

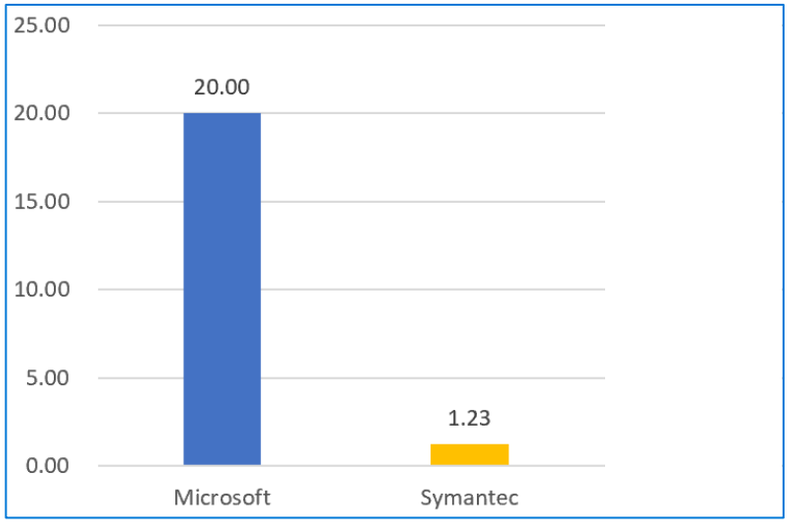
時価総額(2019年10月)



企業規模 ($B)

10 億台 + 10 億人

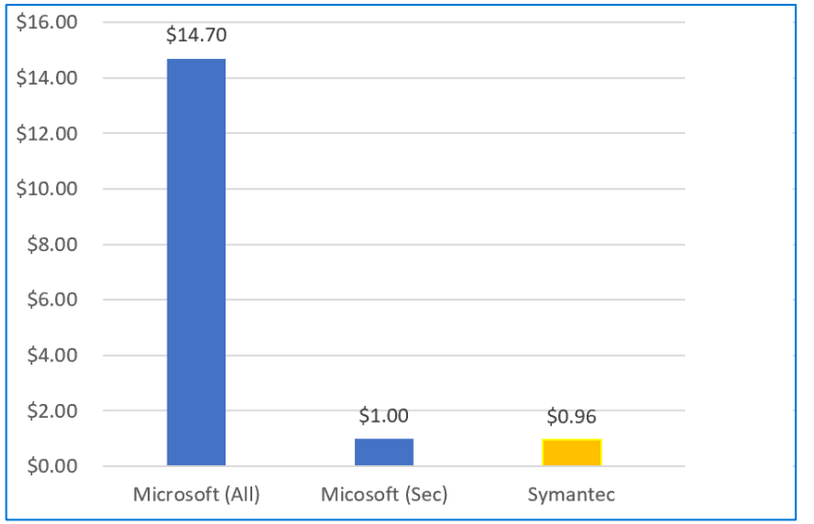
個人 & 企業での Windows
およびクラウド ユーザー



情報ソースの規模 (億)

$ 147 億

年間の研究開発費
うちセキュリティ $ 10 億



投資規模 ($B)

ガートナー Magic Quadrant で 5 つのリーダーポジションを獲得

エンドポイント保護 (EPP/EDR)

Endpoint Protection Platforms

Microsoft Defender Anti Virus
Microsoft Defender Advanced Threat Protection

クラウド監視(CASB)

Cloud Access Security Broker (CASB) solutions

Microsoft Cloud App Security

アクセス制御 (IDaaS/idP)

Access Management

Azure Active Directory

データアーカイブ

Enterprise Information Archiving

Office 365 Archiving
(emails, instant messages, SMS, and social media content)

デバイス管理 (MDM/MAM)

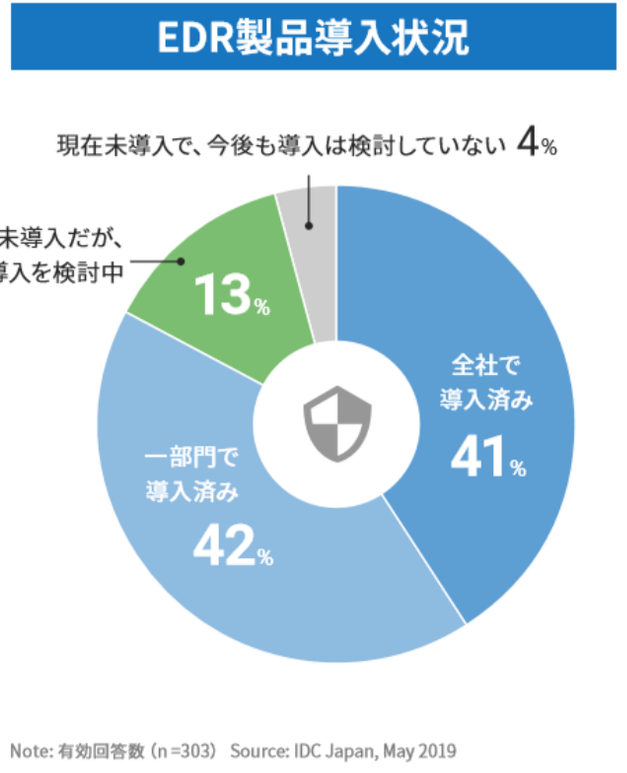
Unified Endpoint Management (UEM) tools

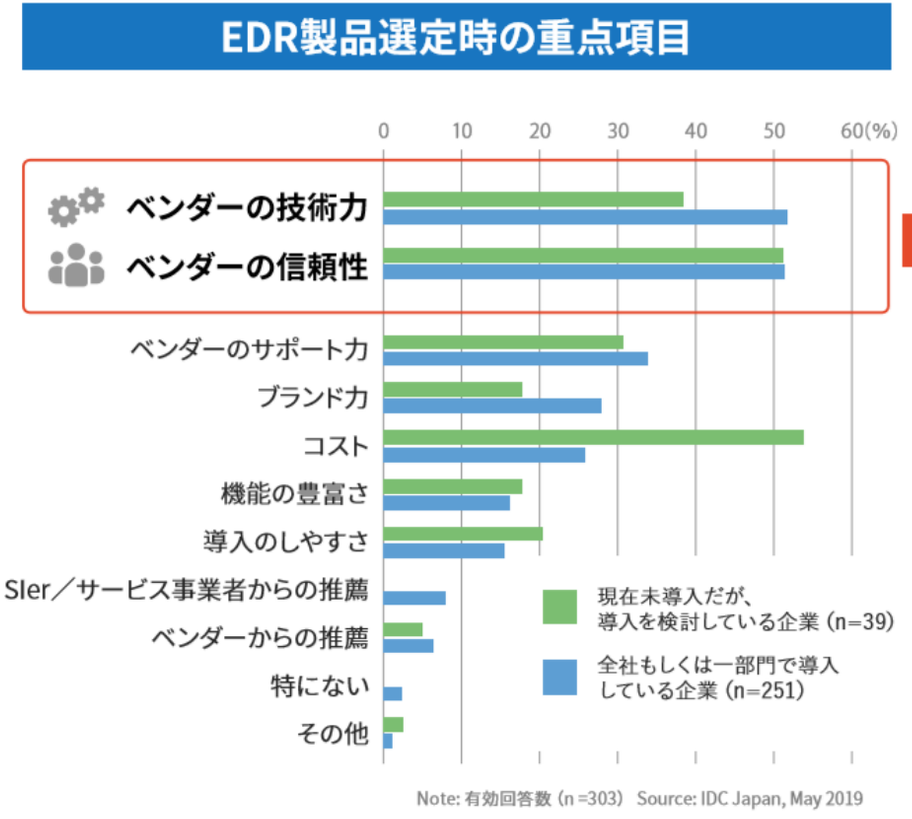
Microsoft Intune

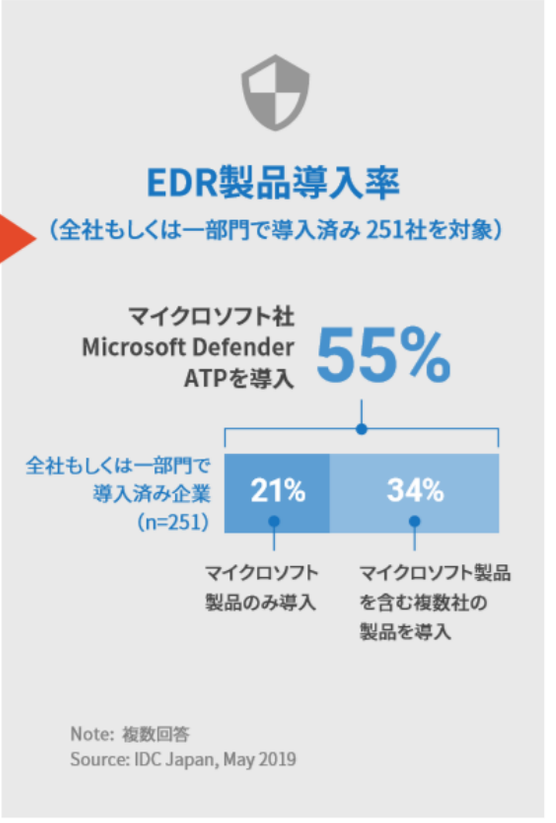
Microsoft Security—a Leader in 5 Gartner Magic Quadrants
https://www.microsoft.com/security/blog/2019/12/03/microsoft-security-leader-5-gartner-magic-quadrants/

国内エンドポイントセキュリティのトレンド

未導入済み企業はコストを重視しているのに対し、導入企業は、ベンダーの信頼性とコストを重視
ウイルス対策製品は、導入済み企業の 57.3% が Microsoft Defender ウイルス対策を導入
EDR 製品は、導入済みの企業の 55% が Microsoft Defender ATP を導入

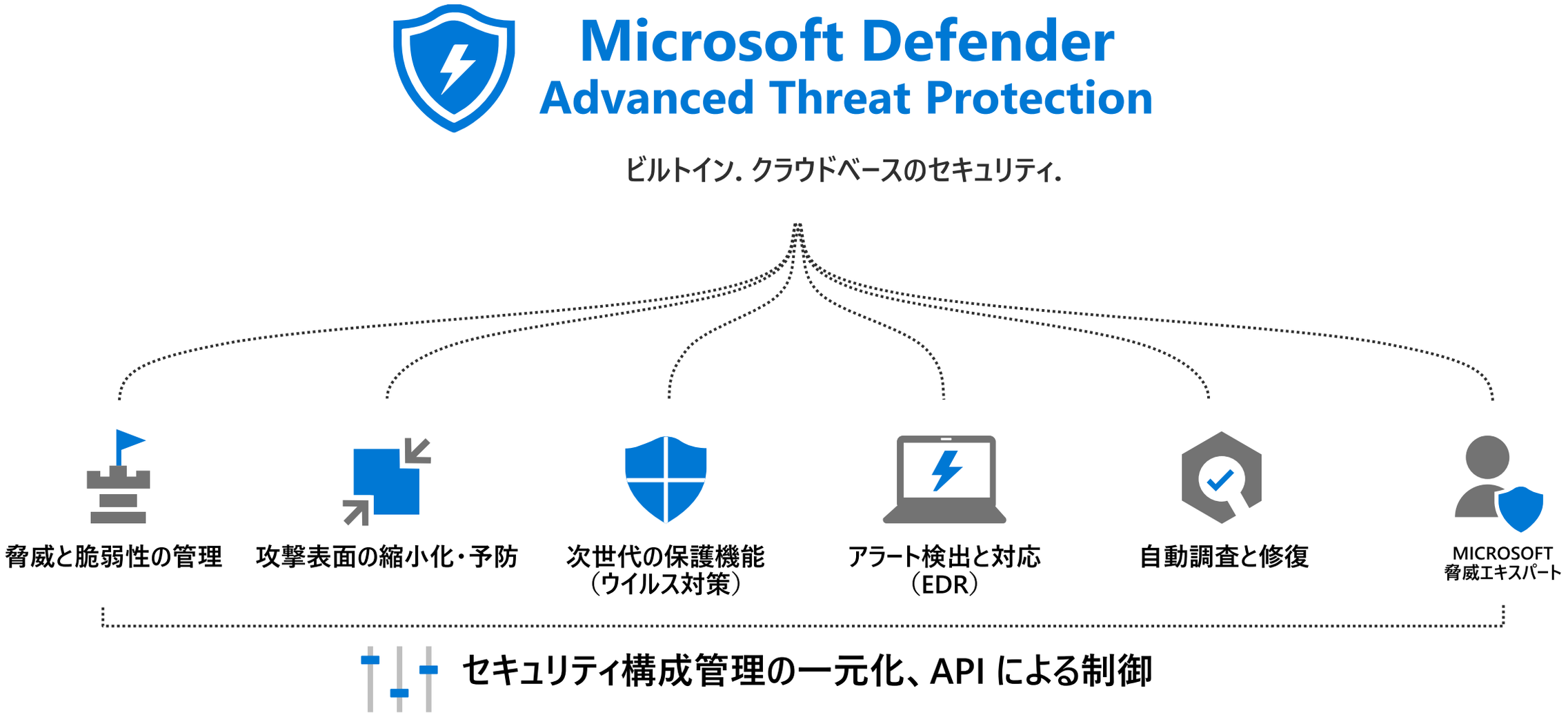






出典：IDC InfoBrief, sponsored by Microsoft,「高度化するサイバー攻撃へのエンドポイントソリューション」(2019年5月)
（IDC JapanがWindows PCを導入している国内従業員規模500人以上の企業と教育関連303社の調査結果）

Microsoft Defender ATP とは

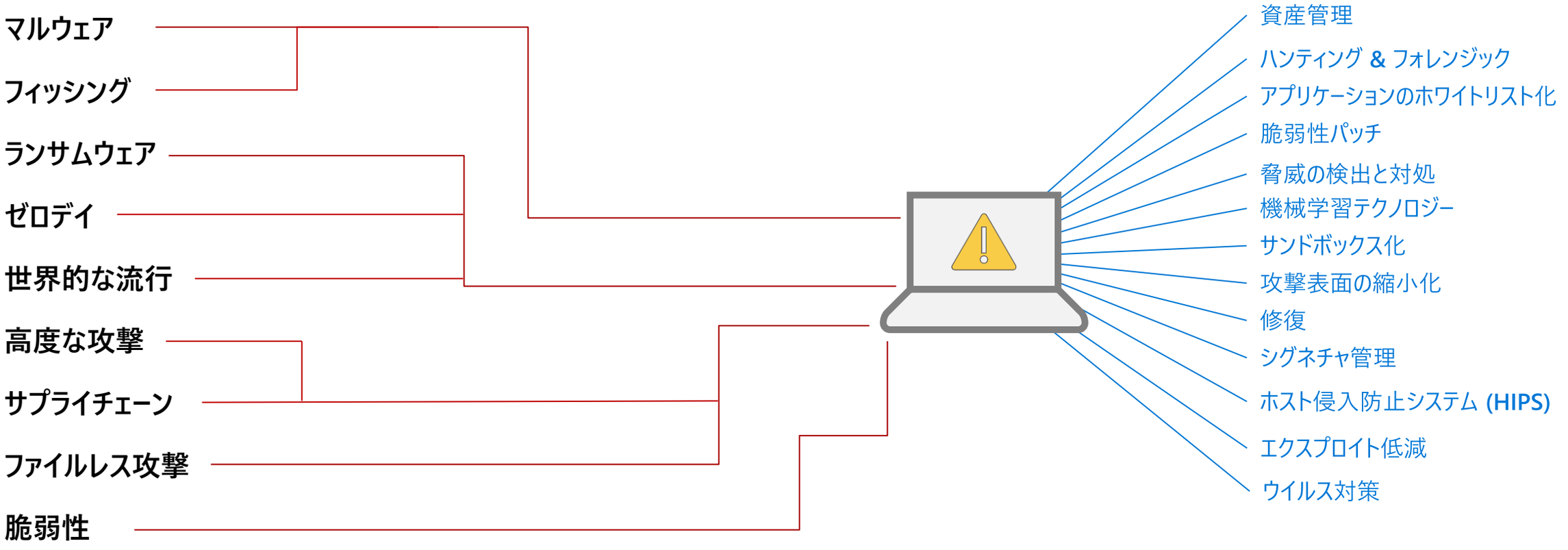


エンドポイントの保護は大変！

パフーマンス
生産性の低下

セキュリティチーム
時間、テクニカルスキル

コスト
複数のソリューション、オンプレミスのインフラ



エンドポイントの保護は大変！だった

マルウェア

フィッシング

ランサムウェア

ゼロデイ

世界的な流行

高度な攻撃

サプライチェーン

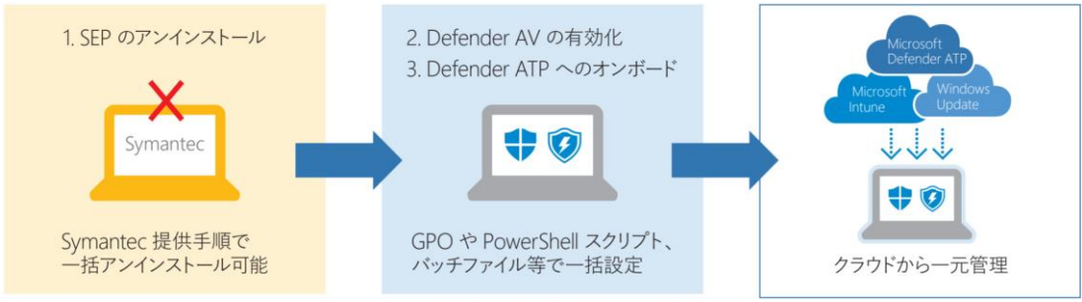
ファイルレス攻撃

脆弱性

Microsoft Defender ウイルス対策
+
Microsoft Defender ATP

Built-in. Cloud-powered.

Symantec Endpoint Protection から Microsoft Defender への切替え

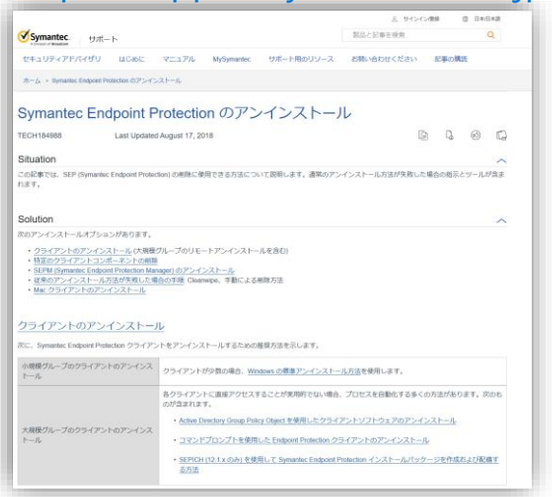


STEP 1

SEP の一括アンインストール

Symantec 提供の方法（バッチファイルなど）で
一括で SEP をアンインストール

Symantec Endpoint Protection のアンインストール
https://support.symantec.com/jp/ja/article.tech184988.html



STEP 2

Microsoft Defender ウイルス対策の有効化

グループポリシーやバッチファイル等を使用して
一括でウイルス対策を有効化

Windows Defender をオンにする
https://docs.microsoft.com/ja-jp/intune-user-help/turn-on-defender-windows#turn-on-windows-defender

STEP 3

クラウドの準備 Microsoft Defender ATP の有効化

グループポリシーやバッチファイル等を使用して
一括で Defender ATP へオンボード

Windows 10 マシンのオンボードツールとその他の方法
https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-atp/configure-endpoints

Windows 10 以外のデバイスの Microsoft Defender ATP へのオンボード

Windows Server のオンボーディング

https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-atp/configure-server-endpoints

サポートしている OS

- Windows Server 2008 R2 SP1
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Version 1803
- Windows Server 2019

旧 Windows のオンボーディング

https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-atp/onboard-downlevel

サポートしている OS

- Windows 7 SP1 Enterprise
- Windows 7 SP1 Pro
- Windows 8.1 Pro
- Windows 8.1 Enterprise

Windows 以外のオンボーディング

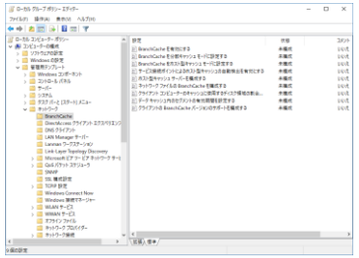
https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-atp/configure-endpoints-non-windows

サポートしているプラットフォーム

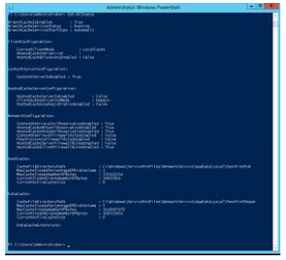
- macOS - 10.15 (Catalina), 10.14 (Mojave),10.13 (High Sierra)
- Linux Server (プレビュー)
  Red Hat Enterprise Linux 7 以降, CentOS 7 以上, Ubuntu 16.04 LTS 以上の LTS, Debian 9 以降, SUSE Linux Enterprise Server 12 以上, Oracle Enterprise Linux 7
- iOS, Android (プレビュー)

設定・管理・運用

① ポリシー設定



グループ ポリシー



PowerShell

Intune, SCCM

② 定義ファイル更新

クラウド

Windows Update

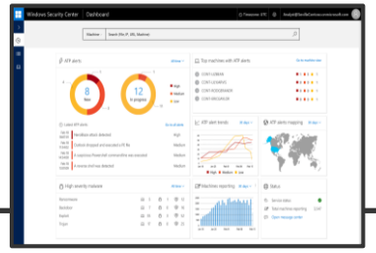
オンプレ

SCCM

③ レポート・通知
(必要な場合)

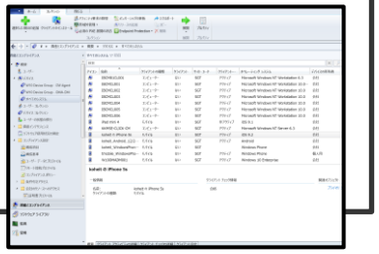
クラウド

Windows Defender ATP



オンプレ

SCCM



管理構成例

クラウド

ハイブリッド

オンプレミス

	構成例 1	構成例 2	構成例 3
設定配布	Microsoft Endpoint Manager (Intune)	GPO/PowerShell	SCCM
定義更新	Windows Update	WSUS	SCCM
レポート	Microsoft Defender ATP	Microsoft Defender ATP	SCCM
リモート スキャン	Microsoft Defender ATP Microsoft Endpoint Manager	Microsoft Defender ATP Microsoft Endpoint Manager	SCCM
EDR	Microsoft Defender ATP	Microsoft Defender ATP	Microsoft Defender ATP
メリット	クラウドからまとめて管理	既存インフラを極力活用	SCCM に管理を集約 詳細なレポート

構成・管理の比較

	Symantec Endpoint Protection	Microsoft Defender AV/ATP
クライアント管理	Symantec Endpoint Protection Manager (SEPM)	• Microsoft Defender ATP • SCCM
クライアントソフトウェアのインストール	SEPM からプッシュインストール	不要（ビルトイン）
スキャン設定に関わるポリシー配布	SEPM からポリシー展開	• Microsoft Endpoint Manager (MEM) • SCCM
定義ファイルの更新	• Live Update • SEPM から展開	• Windows Update • SCCM から展開
クライアント/サーバー間通信	既定では http オプション設定で https 通信が可能	クライアント管理方法により異なるが https による通信が簡単に選択可能
ヒューリスティックスキャン設定	既定で実装	既定で実装
改ざん防止	既定で実装	Windows 10 1903 から既定で実装
ファイアウォール設定	SEPM から展開	• GPO, MEM から展開 • SCCM から展開
ホスト側 IPS/IDS 機能	SEPM から展開 シグネチャを定期的に Live Update からダウンロード	Microsoft Defender ATP で実装

Traditional Workplace

発想の転換

Modern Workplace

これまでのウイルス対策
レガシー管理

Microsoft Defender ATP
モダン管理

定義ファイルの更新管理 (定義ファイル)	vs	潜在的なリスクの管理 (ウイルス対策の状態、OS やアプリの脆弱性、セキュリティ設定・構成)
ファイル単位でのチェック		行動や動作、AI / 機械学習による検知 (ふるまい検知、未知の脅威への対応)
社内ネットワーク・異常検知時のみ		場所を選ばず常時監視・脅威の可視化
オペレーションと時間を要する対応		即時対処、自動調査・対応
サーバー保守運用とアップデート管理		クラウド側で自動対応

Microsoft
Security Forum 2020

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

メール・コンテンツの保護

Microsoft

世界における脅威の状況

91%

サイバー攻撃の
始まりはメールから

60%

2019 年における
フィッシング攻撃の増加

$260億

2016年7月 以降の
ビジネスメール詐欺による
損失

300%

ID・パスワードを狙った
攻撃の増加

20% が 5 分以内に

フィッシング URL
をクリック

68%

侵害の発見に
1ヵ月 以上要する

業界をリードする
“保護 Protect, 検出 Detect, 対処 Response”

4.7兆
2019年における
メッセージスキャン数

120億
Office 365 ATP によってブロックされた悪意のあるメール

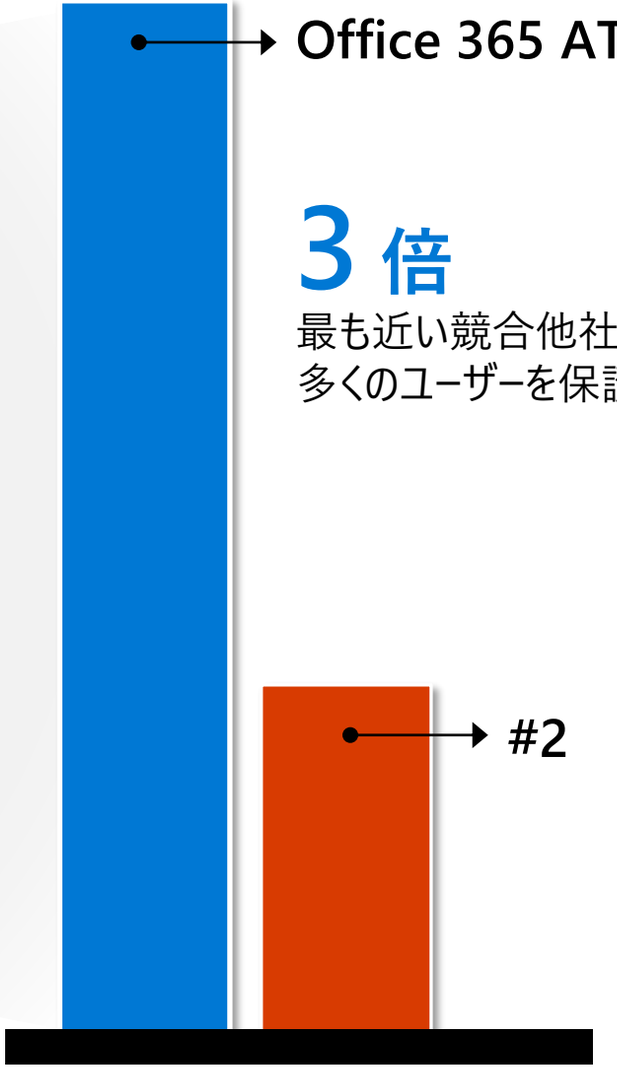
4x↑
2019年6月以降
トリガーされた自動調査

200億
Office 365 ATP による
デトネーション

10億
ブロックされたゼロデイ
メール攻撃

10x↑
2019年7月以降の
自動調査による修復

Office 365 ATP: 利用ユーザーの爆発的な増加



3 倍

最も近い競合他社よりも
多くのユーザーを保護

国内エンドポイントセキュリティのトレンド

Windows PC を導入している国内従業員規模500人以上の企業と教育関連 303社の調査結果による導入率

ウイルス対策製品

Windows Defender
ウイルス対策

導入率

57.3%

EDR 製品

Microsoft Defender
Advanced Threat Protection (ATP)

導入率

55%

標的型メール攻撃対策製品

Office 365
Advanced Threat Protection (ATP)

導入率

51%

出典：IDC InfoBrief, sponsored by Microsoft,「高度化するサイバー攻撃へのエンドポイントソリューション」(2019年5月)
（IDC JapanがWindows PCを導入している国内従業員規模500人以上の企業と教育関連303社の調査結果）

Office 365 ATP フィルタリングスタック

エッジ保護機能


ネットワークスロットリング

IP レピュテーション/スロットリング


ドメインレピュテーション

ディレクトリベースの
エッジフィルタリング


バックスキャッターの検出

送信者インテリジェンス機能

DMARC
DKIM, SPF


組織内スプー
フィングインテ
リジェンス


ドメイン間のス
プーフィングインテ
リジェンス


バルク
フィルタリング


メールボックス
インテリジェンス


ユーザー偽装

micr0soft.com
ドメイン偽装

コンテンツフィルタリング機能


トランスポート
カスタムルール


アンチウイルス
エンジン


拡張子・形式ブロック


添付ファイル
レピュテーションブロック


ヒューリスティック
クラスタリング


機械学習モデル


URL
レピュテーション
ブロック


コンテンツ
ヒューリスティック


安全な
添付ファイル保護


リンクされたコンテンツ
デトネーション


URL デトネーション

メール配信後の保護機能

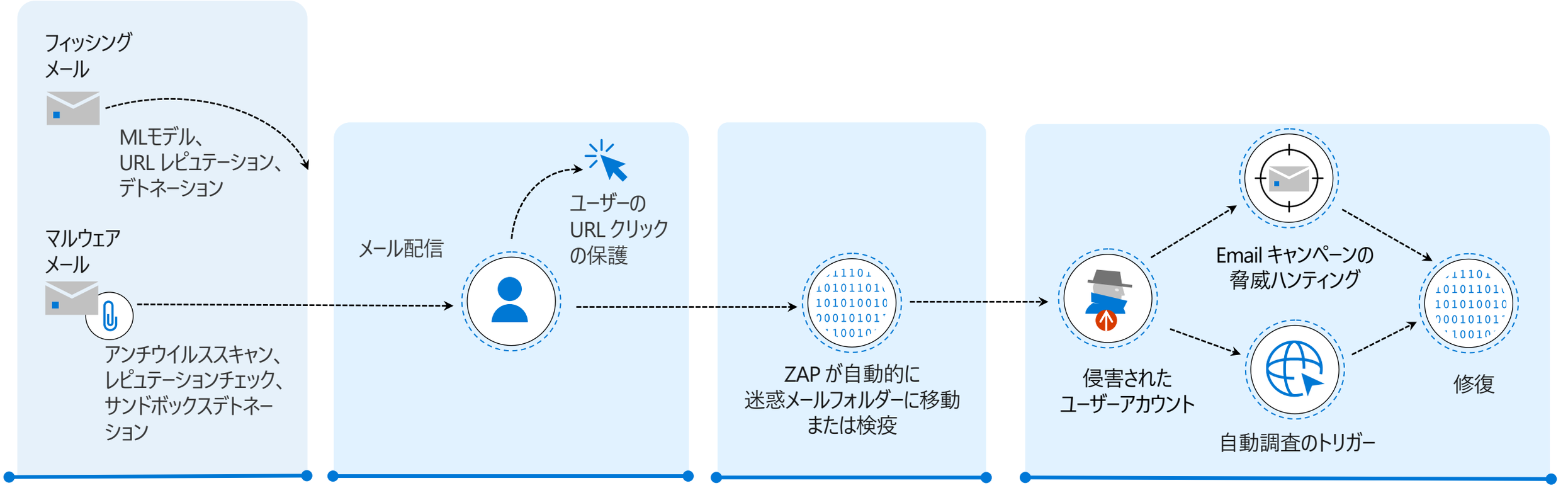

リンクされたコンテンツ
デトネーション


安全なリンク保護


ゼロアワー自動消去


Office クライアントの
安全なリンク保護

サイバーキルチェーン全体に渡る保護機能の提供

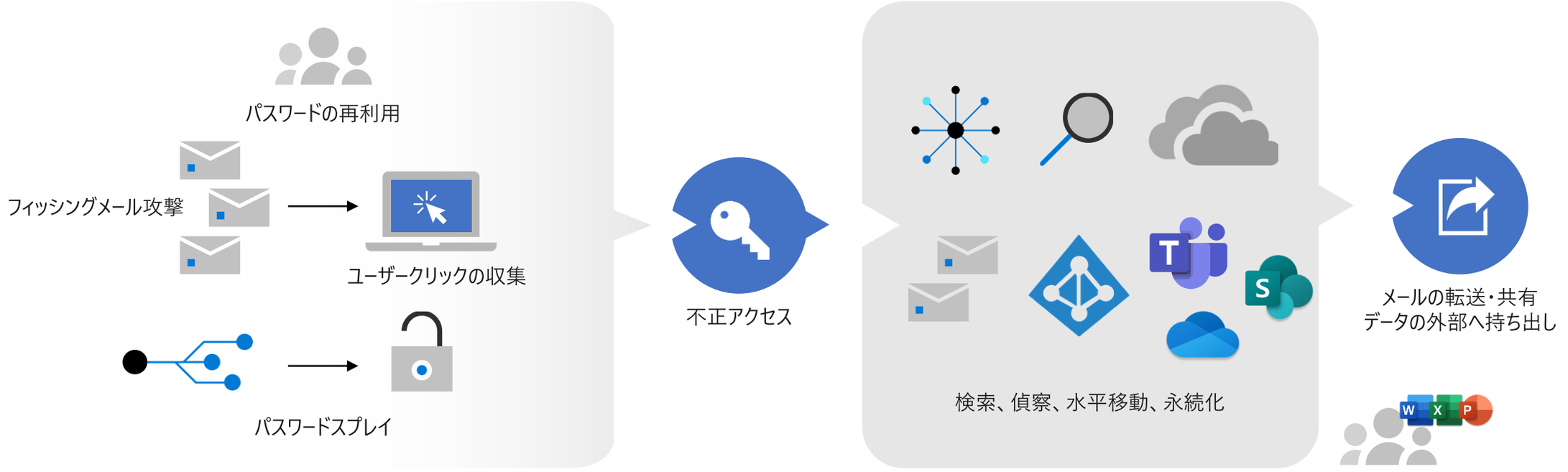


保護 | 検出 | 調査 | 修復

Microsoft 365 全体の保護

組織における脆弱性の検出と訓練

メールだけではなく, Teams チャット, SharePoint/OneDrive クラウドストレージ, および Office クライアント単体の保護



識別 | 保護 | 検出 | 調査 | 修復

Symantec Email Security.cloud から Exchange Online Protection + Office 365 ATP への切替え

STEP 1

クラウド環境の準備

EOP, ATP をホストするためのテナント、ライセンスを準備
Office 365 を利用されている場合は既存テナントをそのまま使用
(必要に応じて) ディレクトリ同期等を設定

EOP サービスを設定する
https://docs.microsoft.com/ja-jp/microsoft-365/security/office-365-security/set-up-your-eop-service

他社サードパーティから EOP に切り替える
https://docs.microsoft.com/ja-jp/microsoft-365/security/office-365-security/switch-to-eop-from-google-postini-the-barracuda-spam-and-virus-firewall-or-cisco

STEP 2

フィルタリングポリシーの設定

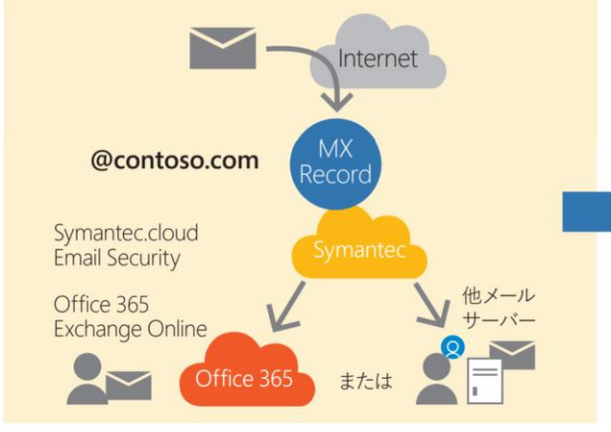
マルウェア対策、スパム対策、高度なフィッシング対策、URL保護等、各種ポリシーを設定
(必要に応じて) ルーティング用コネクタ等を追加

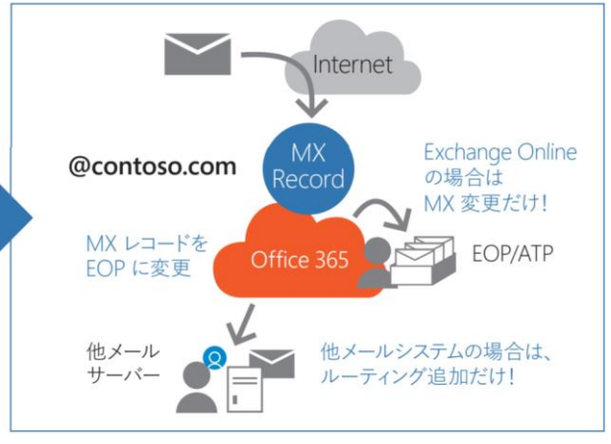
EOP および Office 365 ATP セキュリティに関する推奨設定
https://docs.microsoft.com/ja-jp/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365-atp

STEP 3

MX レコードの切替え

MX レコードを Microsoft データセンターへ切替え





Office 365 - Exchange Online 以外の他社メールシステムをお使いの場合

一部の機能は利用不可

エッジ保護機能

- ネットワークスロットリング
- IP レピュテーション/スロットリング
- ドメインレピュテーション
- ディレクトリベースのエッジフィルタリング
- バックスキャッターの検出

送信者インテリジェンス機能

- DMARC
  DKIM, SPF
- 組織内スプーフィングインテリジェンス
- ドメイン間のスプーフィングインテリジェンス
- バルクフィルタリング
- メールボックスインテリジェンス
- ユーザー偽装
- ドメイン偽装

コンテンツフィルタリング機能

- トランスポートカスタムルール
- アンチウイルスエンジン
- 拡張子・形式ブロック
- 添付ファイルレピュテーションブロック
- ヒューリスティッククラスタリング
- 機械学習モデル
- URLレピュテーションブロック
- コンテンツヒューリスティック
- 安全な添付ファイル保護
- リンクされたコンテンツデトネーション
- URL デトネーション

メール配信後の保護機能

- リンクされたコンテンツデトネーション
- 安全なリンク保護
- ゼロアワー自動消去
- Office クライアントの安全なリンク保護

自動調査と対処 Automated Investigation and Response (AIR)

アップデート

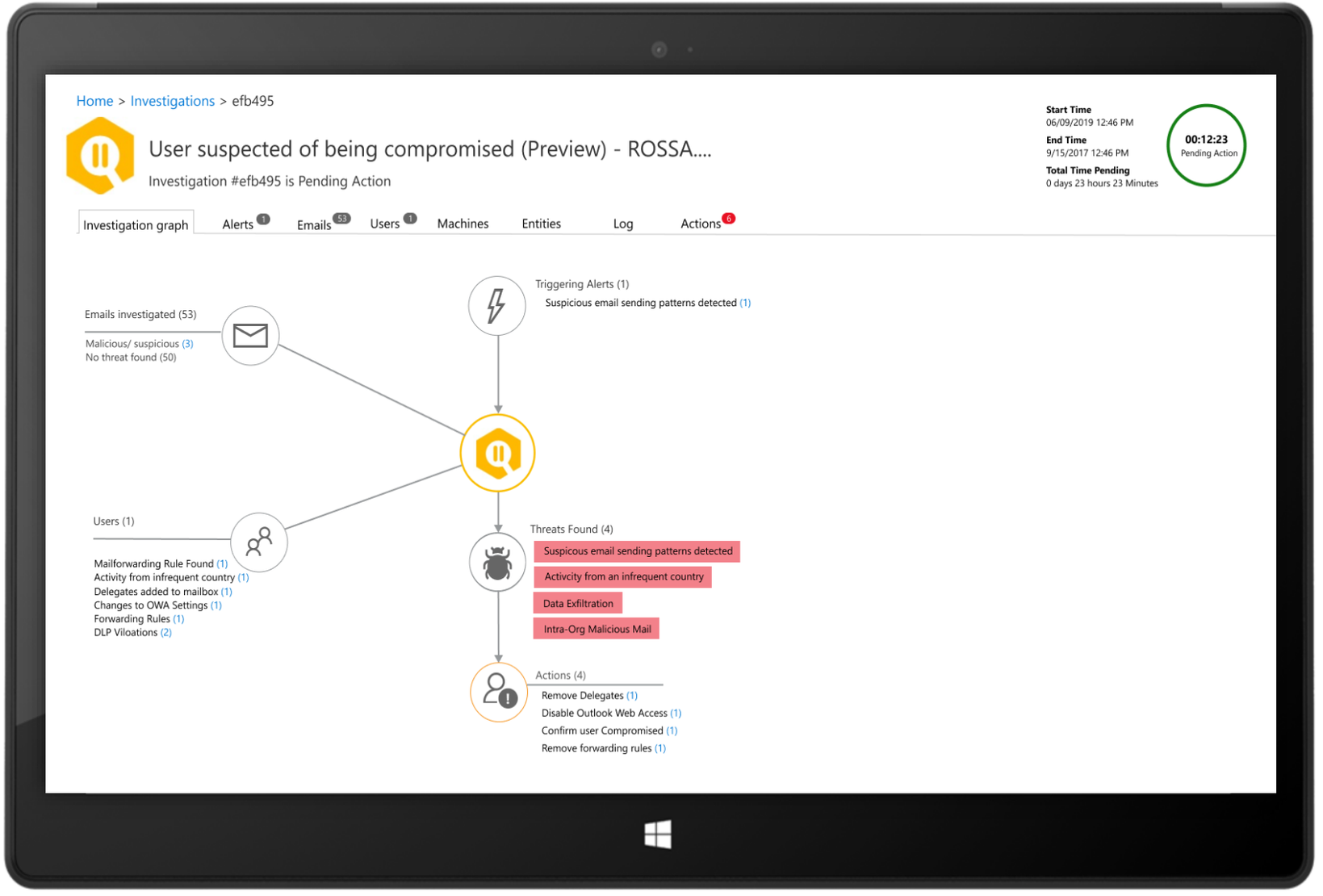
2 種類の対処 — 自動調査、または手動でトリガーされた調査

自動調査 – アラート発生時にトリガー:

- ユーザーから報告されたフィッシングメール
- 判定変更された悪意のあるURLリンクをユーザーがクリック
- メール配信後にマルウェアを検出
  - ゼロアワー自動消去 (ZAP) -
- メール配信後にフィッシングメールを検出 (フィッシング ZAP)
- [プレビュー] 侵害されたユーザーの検出 (不審なメール送信、メール送信制限)

手動でトリガーされた調査

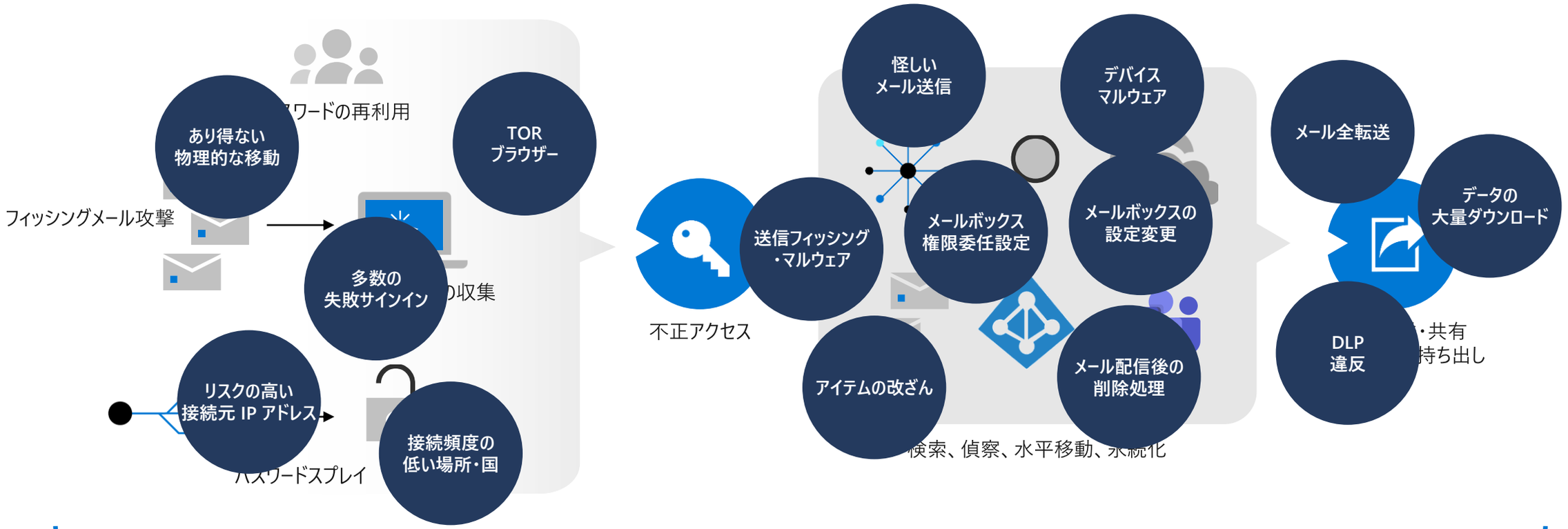
セキュリティワークフローの統合



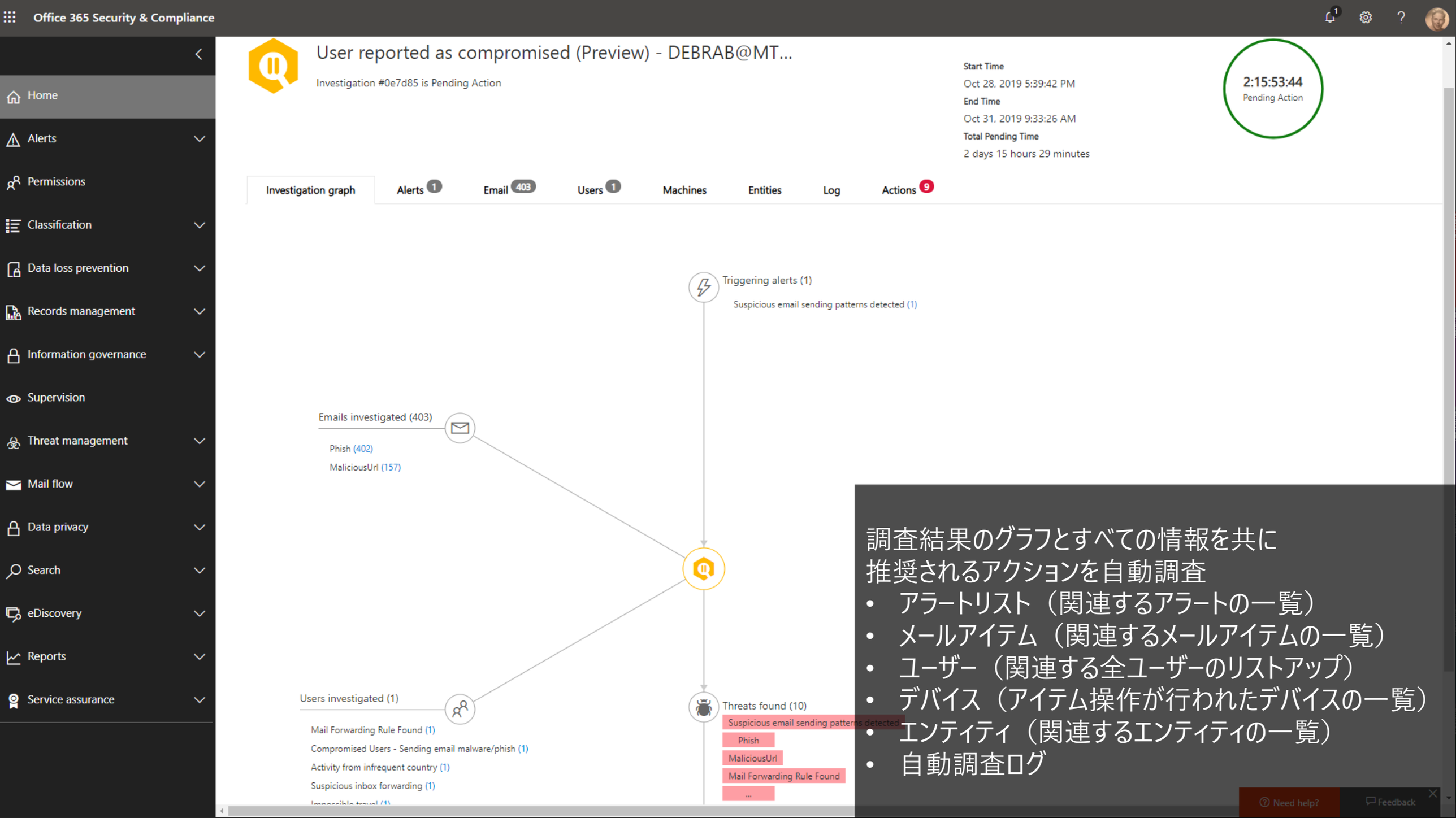
Learn more:
[Office 365 での自動調査および対応 (AIR)]

シグナルをノイズにしないために

複数ソリューションによる単なるアラート発砲では、関連性や根本原因にたどり着けない
何が起こっているのか、全体像を即座に把握することが難しい



すべてのアラートとメールシグナルを、自動的に集約して
どのユーザーアカウントが、どのように侵害されたのかを自動的に調査


Office 365 Security & Compliance
Home
Alerts
Permissions
Classification
Data loss prevention
Records management
Information governance
Supervision
Threat management
Mail flow
Data privacy
Search
eDiscovery
Reports
Service assurance
User reported as compromised (Preview) - DEBRAB@MT...
Investigation #0e7d85 is Pending Action
Start Time
Oct 28, 2019 5:39:42 PM
End Time
Oct 31, 2019 9:33:26 AM
Total Pending Time
2 days 15 hours 29 minutes
2:15:53:44
Pending Action
Investigation graph
Alerts 1
Email 403
Users 1
Machines
Entities
Log
Actions 9
Triggering alerts (1)
Suspicious email sending patterns detected (1)
Emails investigated (403)
Phish (402)
MaliciousUrl (157)
Users investigated (1)
Mail Forwarding Rule Found (1)
Compromised Users - Sending email malware/phish (1)
Activity from infrequent country (1)
Suspicious inbox forwarding (1)
Threats found (10)
Suspicious email sending patterns detected
Phish
MaliciousUrl
Mail Forwarding Rule Found
...
調査結果のグラフとすべての情報を共に
推奨されるアクションを自動調査
• アラートリスト（関連するアラートの一覧）
• メールアイテム（関連するメールアイテムの一覧）
• ユーザー（関連する全ユーザーのリストアップ）
• デバイス（アイテム操作が行われたデバイスの一覧）
• エンティティ（関連するエンティティの一覧）
• 自動調査ログ
Need help?
Feedback

User reported as compromised (Preview) - DEBRAB@MT...

Investigation #0e7d85 is Pending Action

Start Time
28 Oct 2019 5:39:42 PM
End Time
4 Nov 2019 8:35:49 AM
Total Pending Time
6 days 15 hours 33 minutes

6:15:56:07
Pending Action

Investigation graph | Alerts 1 | Email 403 | Users 1 | Machines | Entities | Log | Actions 9

Emails containing	Threats	Volume ano...	Total	Malware	Phish	Delivered	Junked	Replaced	Blocked
Cluster ID:("2397206697") and Sender domain:("MTPDemos.OnMicrosoft.com...	Phish	No	100	0	100	100	-	-	-
Subject:("Voice Message") and SenderIp:("2001:4898:80e8:9:fc95:5812:f5f0:5c9...	Phish	No	48	0	48	48	-	-	-
Subject:("Voice Message") and Sender domain:("MTPDemos.OnMicrosoft.com...	Phish	No	49	0	48	49	-	-	-
Cluster ID:("2397206697") and SenderIp:("2001:4898:80e8:9:fc95:5812:f5f0:5c9...	Phish	No	48	0	48	48	-	-	-
CanonicalizedUrl:("https://spamblock.contoso.com/user@domain.com")	MaliciousUrl, ...	Yes	157	0	157	157	-	-	-

5 item(s) loaded.

Entity type	Entity value	Description	Threats	Status	Execution start time
Emails	Email received by user ross.adams@...	Individual emails relevant to the inve...	Phish	Pending action	28/10/2019 5:39 PM

インシデントに関連する組織内の全メールアイテムが
一覧で表示され、影響範囲をすぐに把握

User reported as compromised (Preview) - DEBRAB@MT...

Investigation #0e7d85 is Pending Action

Investigation graph | Alerts 1 | Email 403 | Users 1 | Machines | Entities | Log

Action	Entity type	Entity value	Description	Threats	Status
Previous URL click in...	Users	DEBRAB@MTPDEM...	Investigate any recen...	Mail Forwarding Rul...	Completed
Force password reset	Users	DEBRAB@MTPDEM...	Force the compromis...	Mail Forwarding Rul...	Pending ap
Outbound mail ano...	Users	DEBRAB@MTPDEM...	Detect anomalies ba...	Mail Forwarding Rul...	Completed
URL reputation inves...	Emails	Email received by us...	On-demand check o...	Phish	Terminated
Mail delegation inve...	Users	DEBRAB@MTPDEM...	Investigate mail dele...	Mail Forwarding Rul...	Completed
Mail forwarding rule...	Users	DEBRAB@MTPDEM...	Investigate any mail f...	Mail Forwarding Rul...	Completed
Outbound malware ...	Users	DEBRAB@MTPDEM...	Detect intra-org and ...	Mail Forwarding Rul...	Compl
Mail cluster identific...	Emails	Email received by us...	Email cluster analysis...	Phish	Completed
DLP violations invest...	Users	DEBRAB@MTPDEM...	Investigate any violat...	Mail Forwarding Rul...	Completed

Debra Berger
DebraB@MTPDemos.OnMicrosoft.com

+ New alert policy

Summary | Recent activity | Recent alerts | Email list | Evidence

Source	Description	Threats found	Details
AuditLog	AuditLog	Mail Forwarding Rule F...	View raw data
EopMailProtection	EopMailProtection	Compromised Users - S...	View raw data
Microsoft Cloud App Se...	Microsoft Cloud App Se...	Activity from infrequent...	View raw data
Microsoft Cloud App Se...	Microsoft Cloud App Se...	Activity from anonymo...	View raw data
Microsoft Cloud App Se...	Microsoft Cloud App Se...	Impossible travel	View raw data
Microsoft Cloud App Se...	Microsoft Cloud App Se...	Suspicious inbox forwar...	View raw data

6 item(s) loaded.


```
{
  "Urn": "8B0EC4CB4C9ED28B4F16A7C22DBB2CE505EF8E21727AAED506596967B8F81197",
  "ContainerUrn": "urn:UserCompromisedInvestiga:0915f66d631adf7f051906ce8a0e7d85",
  "ParentUrn": "urn:McasAlertModel:2ec31df444a8752184c5fccf91906971",
  "Source": "Microsoft Cloud App Security",
  "Threats": [
    "Impossible travel"
  ],
  "ReportedDateTime": "2019-10-29T01:19:05",
  "AdditionalMetadata": {
    "McasAlertData": "User:debrab@mtpdemos.onmicrosoft.com;AlertType:MCAS_ALERT_ANUBIS_DETEC
```


監査ログ、メールフロー、Azure AD、Cloud App Security などで特定された、関連するユーザーアクティビティをワンクリックで表示

Home > Investigation > 0e7d85

User reported as compromised (Preview) - DEBRAB@MT...

Investigation #0e7d85 is Pending Action

Start Time
28 Oct 2019 5:39:42 PM
End Time
4 Nov 2019 8:35:49 AM
Total Pending Time
6 days 15 hours 33 minutes

6:15:56:07
Pending Action

Investigation graph | Alerts 1 | Email 403 | Users 1 | Machines | Entities | Log | Actions 9

✓ Approve | ✗ Reject | Filter | Export | Column options

Action	Entity type	Entity value	Description	Threats	Total	Status	Execution start ti...	Approved by	Decision
Force password reset	Users	DEBRAB@MTPDEM...	Force the compromi...	Mail Forwarding Rul...	1	Pending approval	28/10/2019 5:39 PM		
Soft delete emails	Emails	Email received by us...	For malicious emails...	Phish	1	Pending approval	28/10/2019 5:39 PM		
Soft delete emails	Email clusters	Cluster ID:("2397206...	For malicious emails...	Phish	100	Pending approval	28/10/2019 6:08 PM		
Soft delete emails	Email clusters	Subject:("Voice Mes...	For malicious emails...	Phish	48	Pending approval	28/10/2019 6:08 PM		
Soft delete emails	Email clusters	Cluster ID:("2397206...	For malicious emails...	Phish	48	Pending approval	28/10/2019 6:08 PM		
Soft delete emails	Email clusters	Subject:("Voice Mes...	For malicious emails...	Phish	49	Pending approval	28/10/2019 6:08 PM		
Block URL(time-of-c...	URLs	https://spamblock.c...	Protect against ema...	Phish, Volume Ano...	1	Pending approval	28/10/2019 6:08 PM		
Turn off external ma...	Users	DEBRAB@MTPDEM...	Mail forwarding is a...	Mail Forwarding Rul...	1	Pending approval	28/10/2019 6:08 PM		

自動調査の結果、提示されたアクションを選択して
承認するだけでインシデント対応が完了

Microsoft
Security Forum 2020

Microsoft DIGITAL TRUST SECURITY

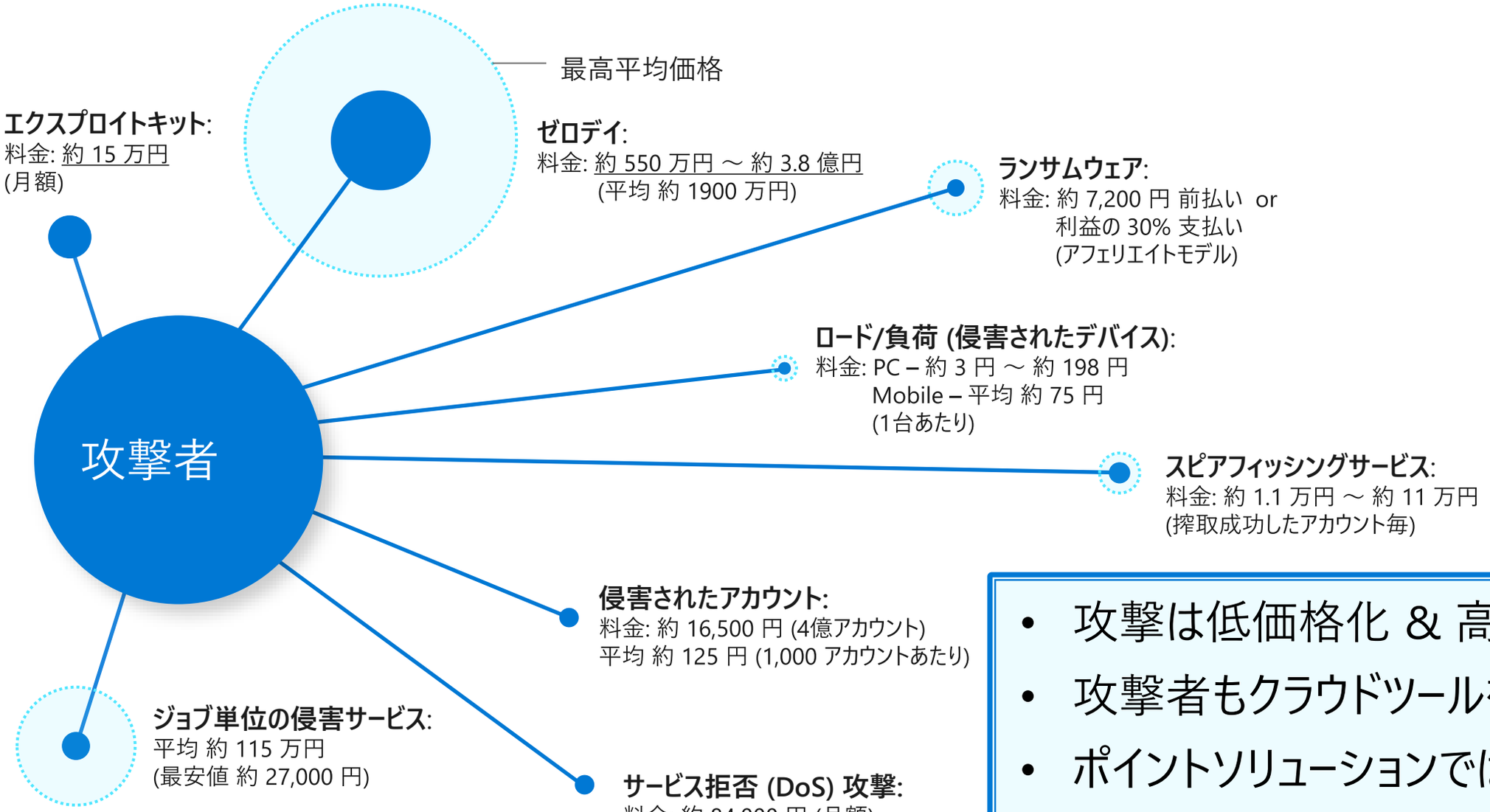
#digitaltrust

これからの時代に必要なセキュリティ

Microsoft

攻撃サービスの低価格化

Updated Winter 2020



- 攻撃は低価格化 & 高度化の一途
- 攻撃者もクラウドツールをフル活用
- ポイントソリューションでは防げない時代

ゼロトラスト

セキュリティ戦略 – すべてのアクセスは、
信頼されていないネットワークから発信されたものとして扱う

アクセス制御のアーキテクチャ

動的ポリシーを使用:

1. 信頼性を十分に検証する
2. 怪しい行動に動的に対処する
   - 信頼を高める
   - アクセスを制限
   - アクセスのブロック

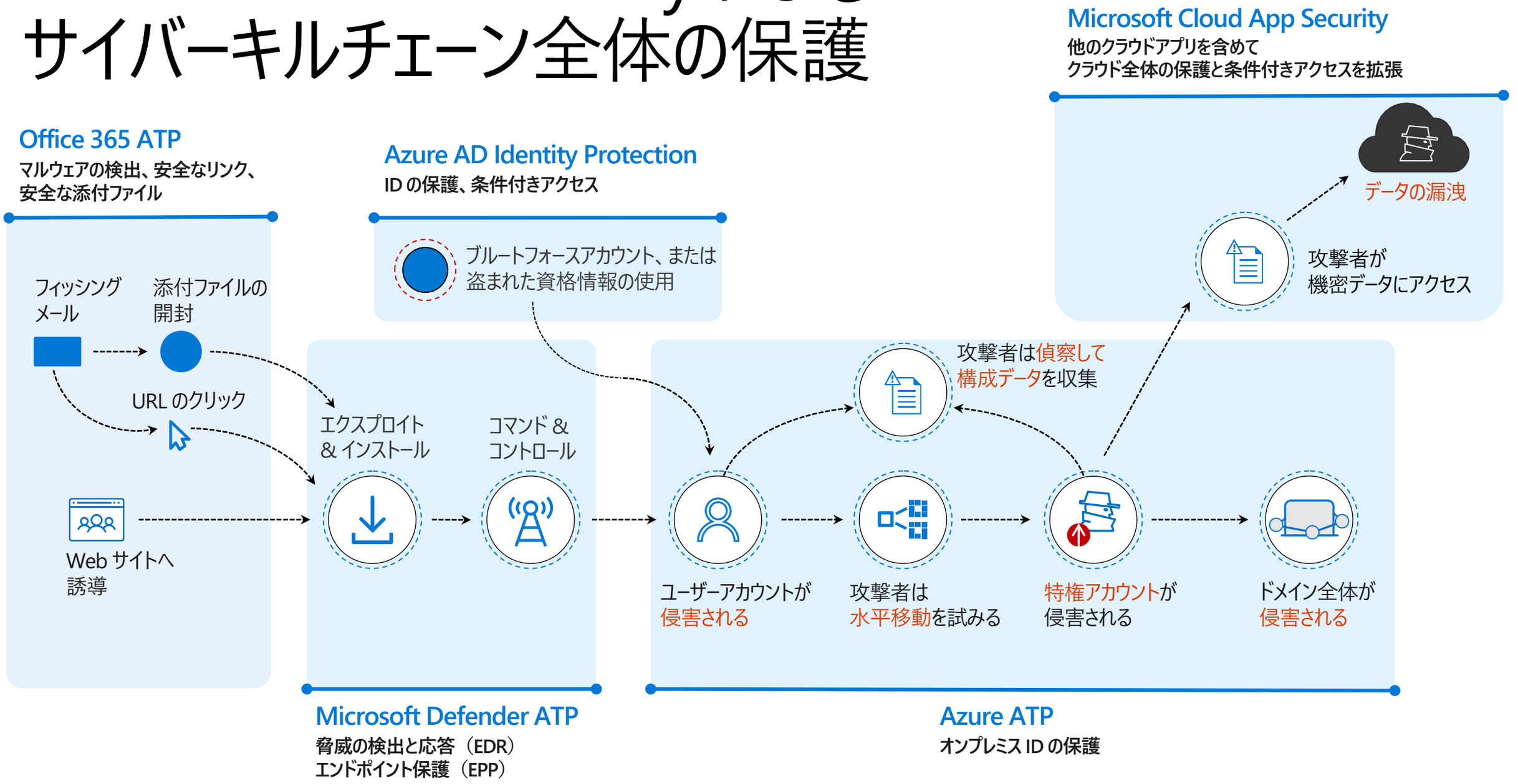
モビリティ & 選択の自由

生産性を向上させる:

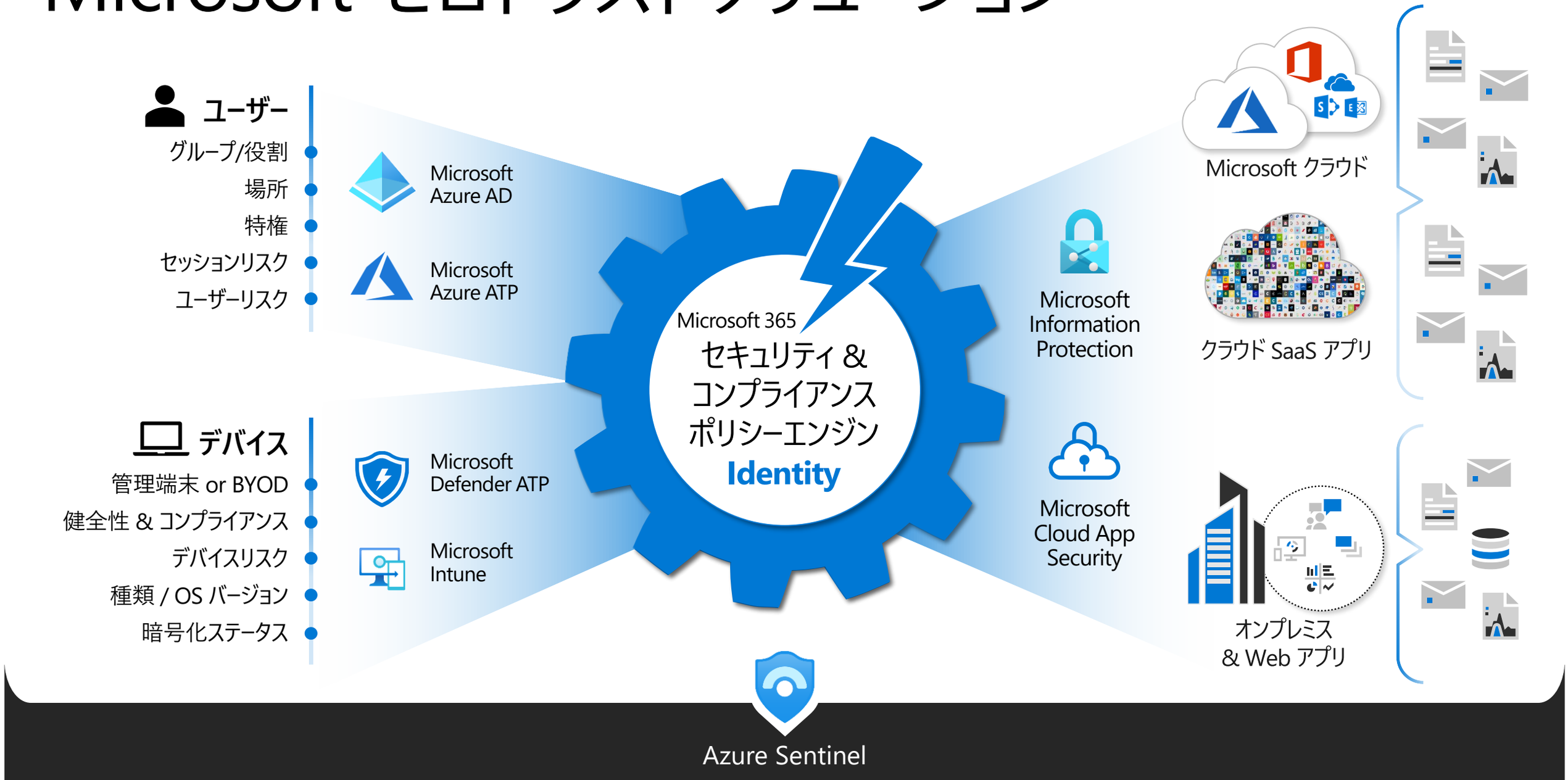
1. どこからでも働ける:
   - どこでも利用可能なアプリケーションとデータ
   - どこでもセキュリティ保護が機能する
2. ユーザーが任意のデバイスを選択できる

セキュリティ と 生産性 の両方を向上

Microsoft 365 Security による サイバーキルチェーン全体の保護



Microsoft ゼロトラストソリューション



期間限定キャンペーン

Symantec 製品を現在ご利用のお客様が

Microsoft 365 E5 Security,

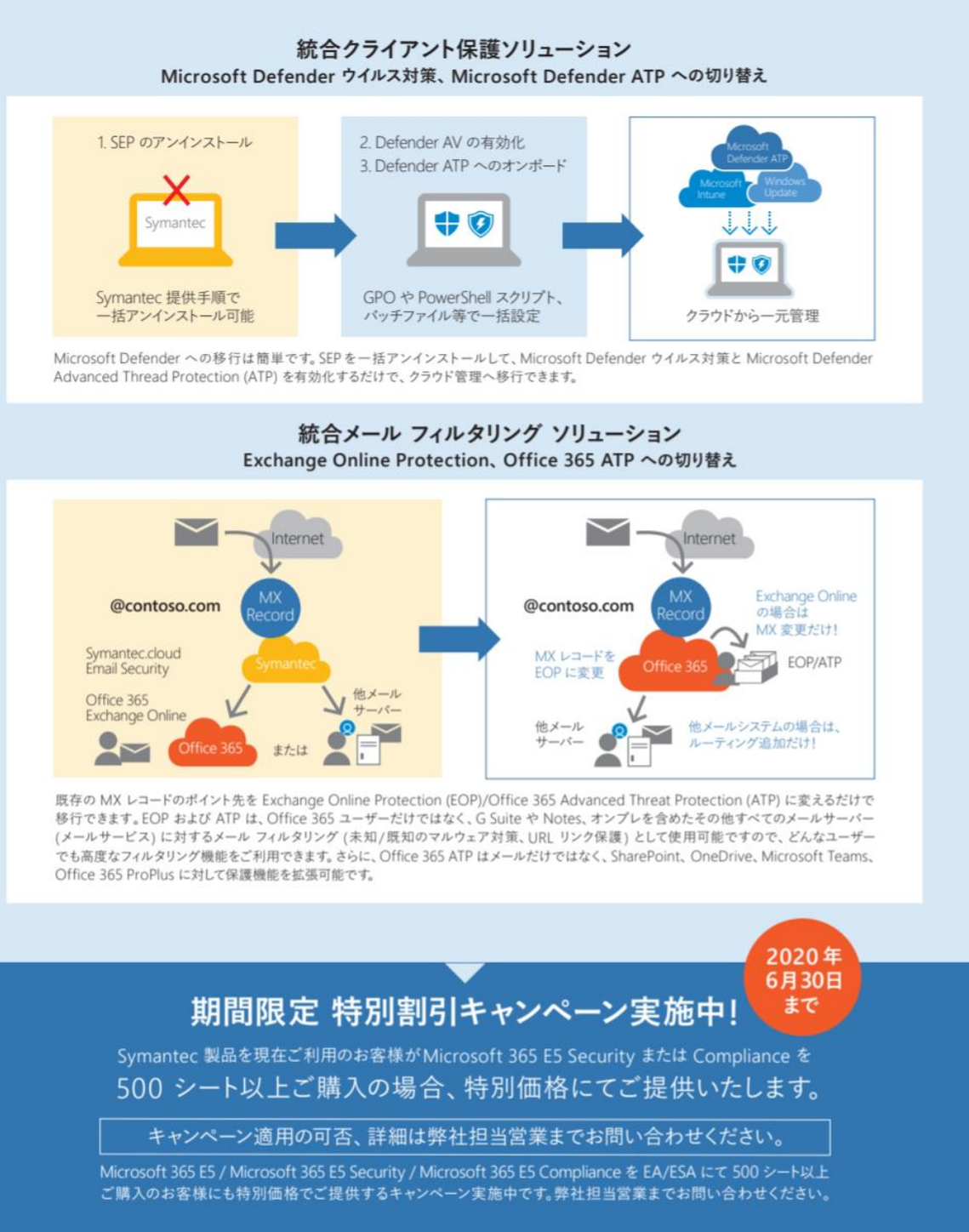
または **Microsoft 365 E5 Compliance** を

500 シート以上 ご購入の場合、

特別価格にてご提供可能！

2020年
6月30日
まで

キャンペーン適用の可否、詳細は
弊社営業担当までお問合せ下さい



Microsoft

Microsoft
DIGITAL TRUST
SECURITY

#digitaltrust