

セッションに関するご質問

シスコ コンタクトセンター



アンケートフォームにご記入ください。

担当営業やシスココンタクトセンターまでにお問い合わせください。

今後のシスコセキュリティウェビナー

https://www.cisco.com/c/ja_jp/training-events/events-webinars/webinars.html

毎週木曜日開催を予定。当面の予定は以下となります。

2020/6/4	木	14:00-14:30	30分でわかる最新の多要素認証 (Duo Security)
2020/6/4	木	15:00-15:30	30分でわかるマイクロセグメンテーション
2020/6/11	木	14:00-14:30	30分でわかるVPN (AnyConnect)
2020/6/11	木	15:00-15:30	30分でわかるクラウドセキュリティ (Umbrella)
2020/6/18	木	14:00-14:30	30分でわかるメールセキュリティ
2020/6/18	木	15:00-15:30	30分でわかるエンドポイントセキュリティ (AMP)
2020/6/25	木	14:00-14:30	30分でわかる認証基盤 (ISE)
2020/6/25	木	15:00-15:30	30分でわかる可視化と脅威検出 (StealthWatch)



30分でわかるエンドポイントセキュリティ

Cisco AMP for Endpointsで、セキュアなリモートワークを

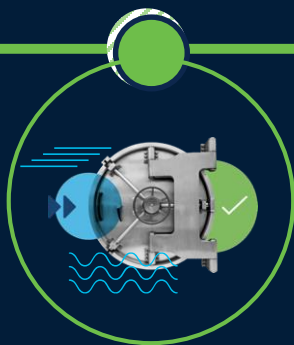
坂川 健太

テクニカルソリューションズアーキテクト

2020年6月18日

Cisco Secure Remote Worker ソリューションの統合

Cisco
Duo



Cisco
AnyConnect



Cisco
Umbrella



Cisco
AMP for Endpoints



会社が承認したアプリケーションへのアクセスを承認する前に、ユーザーのアイデンティティを確認

いつでも、どこでも、どのデバイスからでも、ネットワークへのセキュアなアクセスを実現

ユーザーがどこにいても、インターネット上の脅威からの最初の防衛線を確保

セキュアエンドポイントによる最後の防御ラインの維持

Cisco Secure Remote Worker



Cisco AMP for Endpoints



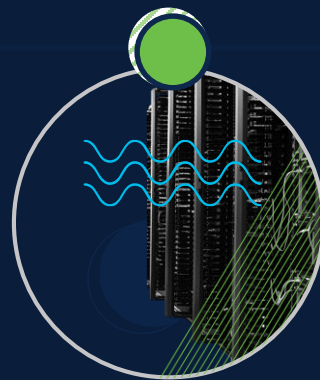
最後の防御ライン、セキュアエンドポイント すべてのコントロールポイントで脅威を完全に防御。



最先端の脅威もブロックする
プロアクティブな保護(EPP)



高度なEDRで継続的に
脅威を検知して対応



Cisco Talosを介したグローバル
な脅威インテリジェンスの活用





脅威をブロック

攻撃者があなたを標的とするより前に



脅威をブロック

パワフルな保護エンジンで
すべての場所のエンドポイントを保護

短期

検知までの時間

長期

メモリ内

Exploit Prevention
(ファイルレスマルウェアからの保護)

System Process Protection

ディスク上

AMP Cloud
(ファイルレピュテーション)

Malicious Activity Protection
(ランサムウェアからの保護)

Antivirus

Custom Detections

侵害後

Device Flow Correlation

Cloud & Endpoint IOC's

Static & Dynamic Analysis

機械学習



脅威をブロック

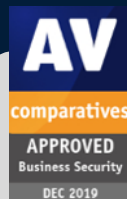


誤検知が少なく、より高いセキュリティ効果を実現

サードパーティによる検証：
AV Comparatives, Miercom,
and NSS Labs

精度、信頼性、安定性が認められ
ています

強力な保護 – 複数のエンジンと
ブロッキングツール



Malware
Protection Test

Protection
Rate

100%

False
Alarms

0

Real World
Protection Test

99.3%

1

False Alarm
Test

- “Very High” FP has as many as 100-150 false positives

	FP rate on non-business software
Acronis, Avast, Bitdefender, Cisco, ESET, Fortinet, G Data, Kaspersky, Sophos	Very low
Cybereason, FireEye, SparkCognition, Microsoft	Low
Elastic, Vipre, VMware	Medium
K7, Panda	High
CrowdStrike	Very high

Factsheet Business Test (March-April 2020), go to: <https://www.av-comparatives.org/tests/business-security-test-march-april-2020-factsheet/>



脅威をブロック

Cisco Talosからの脅威インテリジェンス

多くの脅威をブロック

- 世界最大の非政府系の脅威情報機関
- 毎日2.2兆のアーティファクトを分析
- 昨年、攻撃者が攻撃する前に、350を超える脆弱性*からお客様を保護
- 誰よりも多くのトラフィックを観測

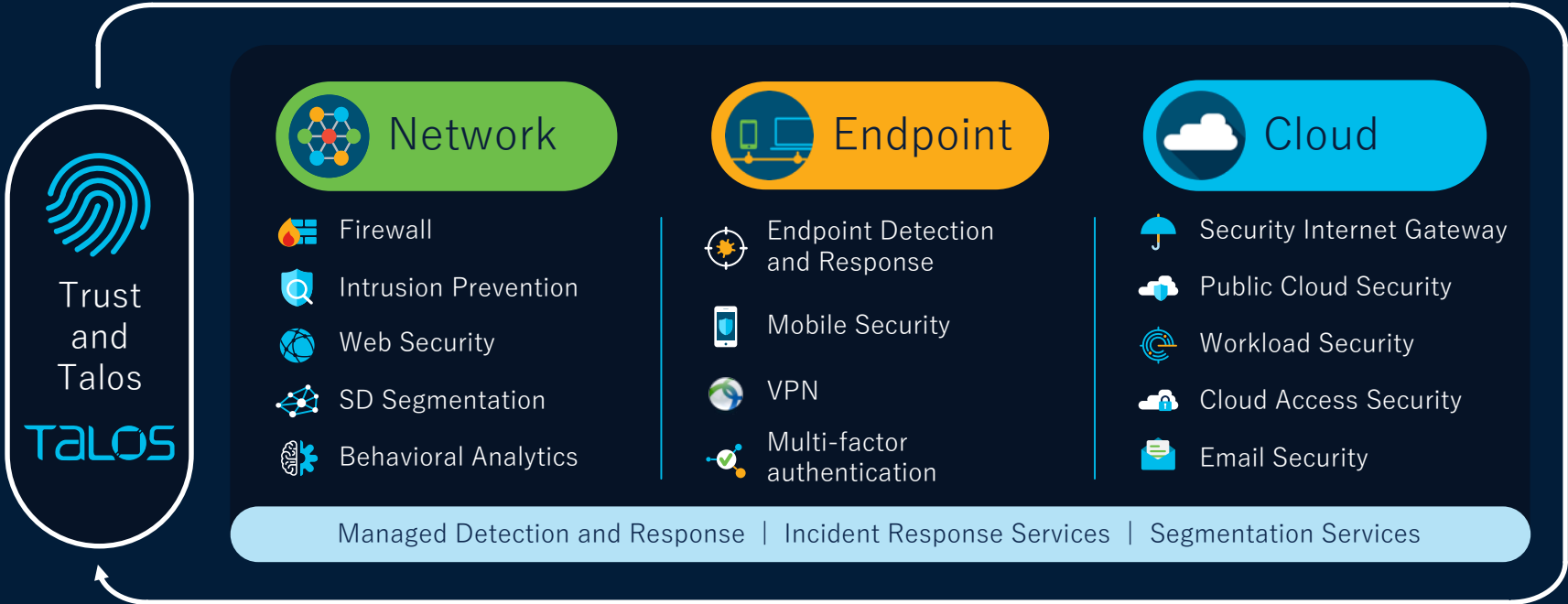


*Cisco Talos, 2018



脅威をブロック

幅広い保護セット

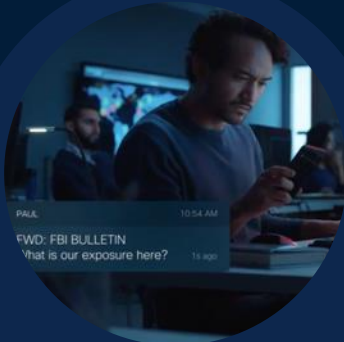




継続的な脅威検出と応答

エンドポイントでの挙動を捕捉

ユースケース



脅威ハンティング

悪意のあるアーティファクトをほぼリアルタイムで検索して、脅威ハントを加速



インシデント調査

迅速に修復するためにインシデントの根本原因をすばやく発見



脆弱性と コンプライアンス

システムの状態（OSバージョン、パッチなど）を確認し、ホストがポリシーに準拠していることを確認



IT オペレーション

ディスク容量、メモリ、およびその他のIT操作の証跡をすばやく追跡

Endpoint Detection and Response

継続的なモニタリング



継続的な脅威検出と応答



EDR

検出

- 継続的なアクティビティモニタリング
- アドバンスドエンドポイントサーチ
- サンドボクシング
- クラウド型侵害の兆候検知
- 脆弱性と低普及のソフトウェアの認識

応答

- カスタムブラック/ホワイトリスト (ファイル・ネットワークラフィック)
- 管理外端末の発見
- エンドポイント隔離
- フォレンジックスナップショット
- 自動化アクション

Device Trajectory



継続的な脅威検出と応答

何が起きたのか？

Malwareはどこから来たのか？

Malwareはどこにいたのか？

何をしたのか？

どうやって止めるのか？

The screenshot displays the Cisco AMP for Endpoints interface. The main section is titled "Device Trajectory 2" and shows a timeline from 21 FEB to 28 FEB. Below the timeline is a list of system files, including:

- System
- nvccontainer.exe [PS]
- netmgr.exe [PS]
- compattelrunner.exe [PE]
- msiexec.exe [PE]
- netmon.exe [PE]
- svchost.exe [PE]
- office2019.exe [PE]
- officebackgroundtaskhandler.exe [PE]
- npntrfupdate.exe [PE]
- officeidmapi.exe [PE]
- far cry 4 v1.4.0-1.0 plus 20 tr..._exe [PE]
- 81b495f95d32a.automalcode [OLE2]
- 81b495f95d32a.automalcode [OLE2]
- 81b495f95d32a.automalcode [OLE2]
- 5f765f401983767.automalcode [OLE2]
- 81b495f95d32a.automalcode [OLE2]
- 5f765f401983767.automalcode [OLE2]
- 5f765f401983767.automalcode [OLE2]
- 5f765f401983767.automalcode [OLE2]
- regstore.exe [PE]
- pingsender.exe [PE]
- fanotify trainer v30 [ver 1.10] [psd] -rar [PE]
- fanotify trainer v30 [ver 1.10] -rar [PE]
- 7h18akoly.zipid.part [ZIP]
- 69647eb4251811984ad48deb28 [ZIP]
- Finfox.exe [PE]
- 69647eb4251811984ad48deb28 [ZIP]
- warpspochk-8.0.exe [ZIP]
- ... [PE]

The "Indicators" section on the right lists several indicators:

- Crossrider.Ioc (Impact: Medium)
- Dummy.Ioc (Execution Persistence: Medium)
- GateDetPhp.Ioc (1.2K Compromises Observed, Command and Control: High)
- JS.Trojan.Generic_48153.Ioc (Command and Control: Critical)
- Linux.Autostar.Persistence.Ioc
- Linux.CurlDownloadExecute.Ioc
- Linux.MultiKill.Ioc
- Mshelper.Ioc
- OSX.Applescript.CredentialTheft.Ioc

A detailed view of the JS.Trojan.Generic_48153.Ioc indicator is shown, including a description: "JS.Trojan.Generic_48153 is malware that contacts a remote server over HTTP. This IOC is based on malware detection rulesets. This IOC fires when a URI pattern similar to this malware has been observed." It also includes a "MITRE ATTACK" section with details on tactics, platforms, data sources, and adversaries.

Cisco Threat Response

詳細な調査を実行

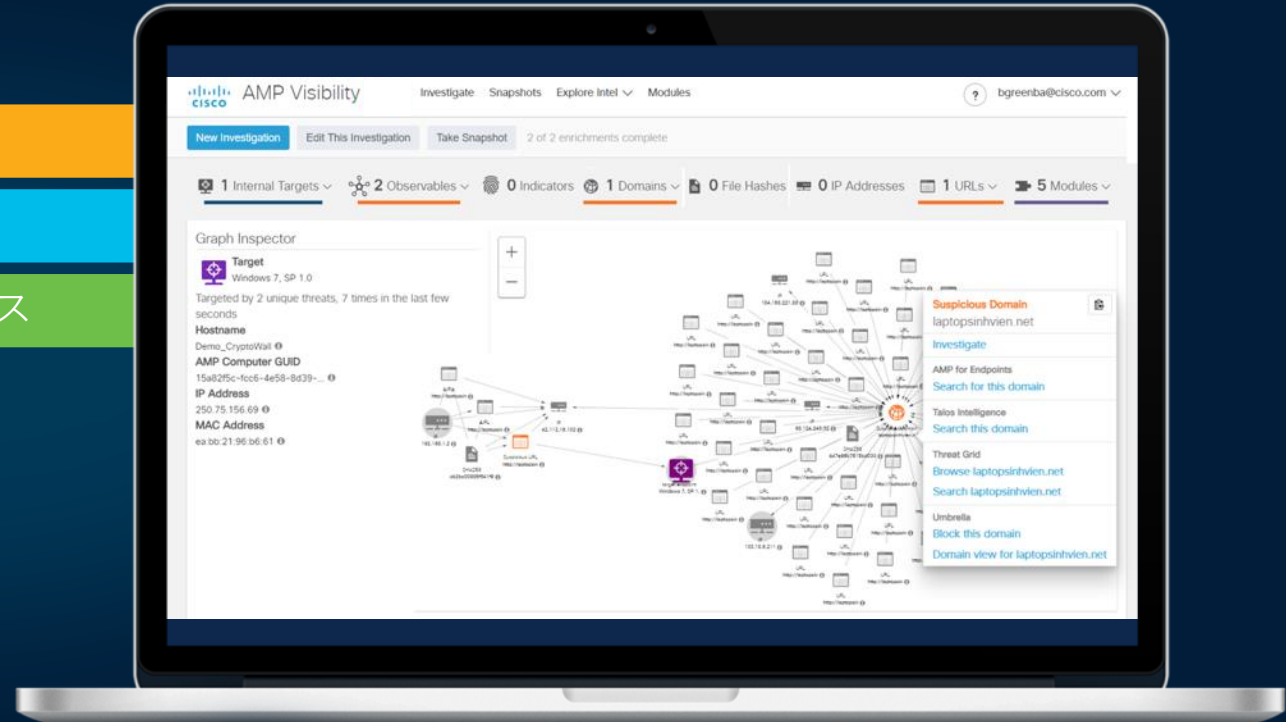


継続的な脅威検出と応答

脅威ハンティング

ワンクリックでの修復

関連的なインテリジェンス



Orbital Advanced Search

IT運用と脅威ハンティングをシンプルに



継続的な脅威検出と応答

- 主な機能:

Advanced search; 事前定義されたカスタマイズ可能なクエリ、フォレンジックスナップショット。

- 主なユースケース:

脅威ハンティング; IT運用の効率化、脆弱性とコンプライアンスのトラッキング

- 効果:

より迅速な調査と迅速な対応、シームレスな調査と修復

The screenshot displays the Orbital Advanced Search interface. On the left, there is a 'Query Catalog' section with a 'Filters' sidebar containing categories like Forensics, Threat Hunting, Malware, Posture Assessment, Live Acquisition Of Volatile Data, and ATT&CK™ Tactics. The main area shows a table with columns for CREATED, UPDATED, ID, OS, CATEGORY, and ATT&CK™ TACTIC. A search modal is open, showing a search bar with 'powershell' and a list of results including Posture Assessment, Threat Hunting, Live Acquisition Of Volatile Data, Forensics, and Malware. On the right side of the interface, there are several red buttons labeled with actions like Execution, Defense Evasion, Persistence, Discovery, Collection, and Credential Access.

CREATED	UPDATED	ID	OS	CATEGORY	ATT&CK™ TACTIC
2019-03-11	2019-08-15	powershell_useragent_masquerade_attempt	Windows	Threat Hunting	Defense Evasion
2019-07-31	2019-10-16	powershell_event_auditing_state	Windows	Posture Assessment	

自動化アクション

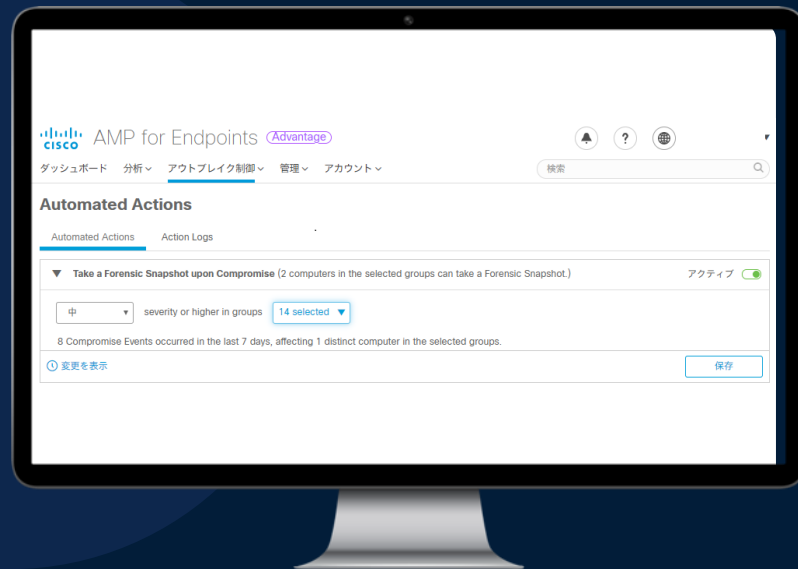
イベント発生をトリガーに自動でアクションを実行



継続的な脅威検出と応答

- 事前に選択したSeverity(Critical/高/中/低)のイベントが発生した際、次のアクションを自動で実行

- フォレンジックスナップショット取得
- エンドポイント隔離
- 任意のグループへの移動
- Threat Gridへのファイルアップロード





連携して動作するセキュリティ
業務効率を最大化するために



連携して動作する
セキュリティ

AMP for Endpointsから 幅広いサードパーティとの統合

alibaba
cisco



Threat Visualization/
Response



Malware Analysis



Email



Network

SOAR:レスポンス - 検疫



Managed SOC

SIEM:イベントストリームの可視化



panaseer

Unified View of
Assets and Controls



chrome

Unsupported Python
Integrations

Open
Ecosystem

DevNet: <https://developer.cisco.com/amp-for-endpoints/>
GitHub: <https://github.com/CiscoSecurity>



連携して動作する
セキュリティ

感染したデバイスからアプリケーションを保護

“エンドポイントでのゼロトラスト”アプローチ

Duo + AMP for Endpoints は、侵害されたエンドポイントから、
Duoで保護されたアプリケーションへのアクセスをブロック



ユーザーは自分の
デバイスを使って
アプリケーション
にアクセス

AMP for Endpoints が
デバイス上で実行されて
いるマルウェアを検出

感染したデバイスに
ついてMFAに通知

MFAは、そのデバイスが
アプリケーションにアク
セスするのをブロック

Demo：管理コンソールの紹介

まとめ：AMP for Endpoints

脅威をブロック



- ・強力な複数の保護エンジンでメモリ上、ディスク上、侵害後の全てを保護
- ・誤検知が非常に少なく、より高いセキュリティ効果を実現
- ・Cisco Talosからの提供される脅威インテリジェンス

継続的な脅威検出と応答



- ・継続的なモニタリングにより端末内のアクティビティを過去に遡り把握
- ・Orbital Advanced Searchにより脅威ハンティング、IT運用をシンプルに
- ・イベント発生をトリガーに自動でアクションを実行

連携して動作するセキュリティ



- ・幅広いサードパーティとの統合
- ・Duo + AMP4E の連携により、感染した端末からアプリケーションを保護

