【30分で分かるセキュリティ シリーズ】

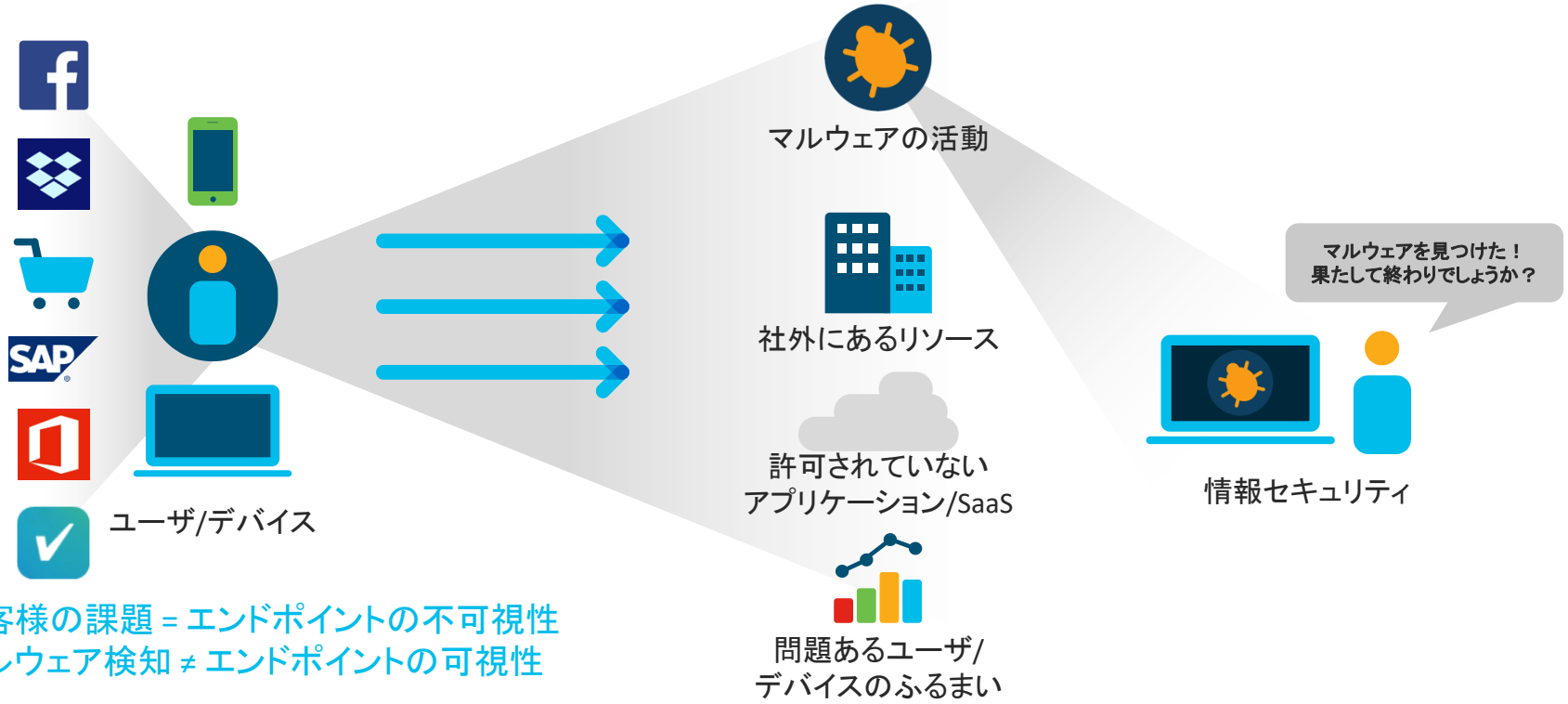
リモートワークを徹底的に可視化する、新しいエンドポイントセキュリティご紹介

Cisco Endpoint Security Analytics Built on Splunk (CESA)

シスコシステムズ合同会社
セキュリティ事業　福留 康修
2020.11.5

内容

課題:
リモートワーク環境のエンドポイントで起きている悪いことを見ることができない



お客様の課題 = エンドポイントの不可視性
マルウェア検知 ≠ エンドポイントの可視性

CESA はエンドポイントにおける可視性のギャップに対応

CESA: エンドポイント可視性のギャップに対応

詳細なユーザー/エンドポイントの動作をそのネットワークアクティビティに関連付け

ネットワーク セキュリティ アナリティクス

e.g. Stealthwatch, Darktrace, etc.

ネットワークに入ってきたトラフィックの可視化

ネットワーク上のふるまいを分析

EDR & EPP

e.g. AMP, CrowdStrike, Symantec, etc.

エンドポイント内で動作

マルウェア検出、ファイル分析、ファイルの取り消し、アプリ/プロセスの終了

Cisco Endpoint Security Analytics Built on Splunk
従来のソリューションでカバーされない点に着目

マルウェアを見つけた！ 果たして終わりでしょうか？
(いいえ)

情報セキュリティ

CESAは、動作を分析して、「悪質なユーザーやエンドポイントの問題」を検出

プロセスが不自然なトラフィックを生成

トラフィックを生成するプロセス
エンドポイントのネットワークインターフェース
トラフィックの方向、ボリューム、宛先、プロトコル、ポート

エンドポイント セキュリティが無効に

実行プロセスが不在
エンドポイントから送信されるセキュリティテレメトリの不在

ユーザが不自然なドメインへアクセス

過去にアクセスが無いドメイン
未知ドメインへのユーザーのバースト
ドメインとの間の異常トラフィック
ドメインのレピュテーションとの関連付け

許可されていないアプリ / SaaS

実行されているプロセス
実行されている不明なプロセス
データの行き先
アクセスしたドメイン

エンドポイントでのアカウント生成

エンドポイント上のユーザーアカウント
アカウントの作成・削除
アカウントに関連したトラフィック

ゼロデイ脅威

新規/未知ドメインへのアクセス
ポート上の奇妙なプロトコル
不明なプロセスとハッシュの実行
ルート権限で実行されている奇妙なプロセス
移動中のデータ量

ゼロトラストにもとづくユーザの可視化

オフネット監視
ユーザー/デバイスとトラフィックの属性
アクセスしたSaaSドメイン
プロセス、プロトコル、ポートの異常な動作を監視

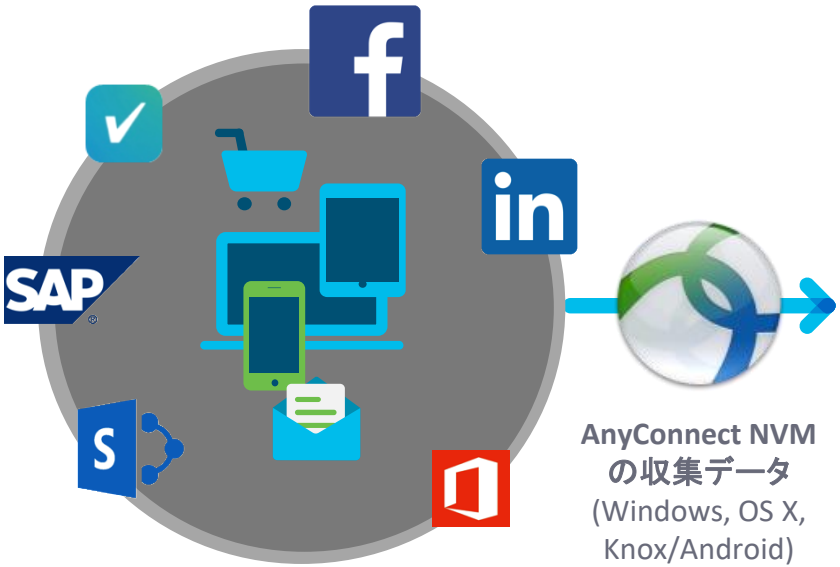
ユーザによるデータの溜め込み

移動中のデータ量
データの送信元/送信先
誰がやっているのか – ノーマル？
関与するエンドポイント

ユーザ/デバイス/通信/App 関連付け

ユーザー＆アカウントは？
関与するエンドポイント
エンドポイントのネットワークインターフェース
通信の方向、ボリューム、送信元/受信元等
実行中のプロセス

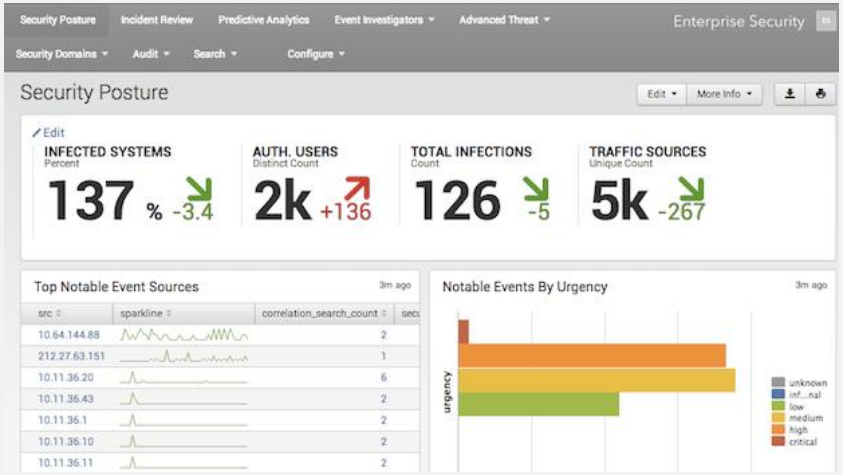
Cisco Endpoint Security Analytics (CESA) Built on Splunk とは



AnyConnect NVM の収集データ
(Windows, OS X, Knox/Android)

新製品

CESA – NVM 用にカスタマイズされた Splunk Analytics と価格設定



Splunk でデータを取り込み、分析しエンドポイントのインサイトを提供

AnyConnect Network Visibility Module (NVM)

マルウェアを超えてエンドポイントを見る…マルウェアも見る

- ユーザー、エンドポイント、アプリケーション、権限をまたがって広範な行動の可視化と分析
- オンプレミス、オフプレミス時にエンドポイントから IPFIX(NetFlow) の収集、キャッシュ、エクスポート
- エンドポイント上の既存のAnyConnect VPNクライアントを活用
- プライバシー要件を満たすために選択した変数を除外

NVM – エンドポイントの可視性がご提供するのは…

Netflow/IPFIX

- Source IP
- Destination IP
- Source Port
- Destination Port
- Bytes Sent
- Bytes Received

NVM (IPFIX フォーマット)

- Source IP
- Destination IP
- Source Port
- Destination Port
- Bytes Sent
- Bytes Received
- **OS Version**
- **OS Edition**
- **UDID**
- **Host Name**
- **Logged In User**
- **Process Name**
- **Process Hash**
- **Process Account**
- **Parent Process Name**
- **Parent Process Hash**
- **Parent Process Account**
- **DNS/Destination Hostname**
- **Module Hash List**
- **System Manufacturer**
- **System Type**
- **MAC Address**
- **Interface Name / Type / UID**

深いエンドポイントの可視性

ユーザー
トラフィック統計
プロセス
アプリケーション
利用する SaaS アカウント
通信先
端末の詳細情報

CESA 検出と可視化のユースケース

認可されていないアプリと SaaS	• アクセスを行った SaaS ドメイン – コネクションと SaaS 利用行動 • アプリケーションとプロセスの可視化 – デバイス上で実行されているアプリ/プロセスを検索
セキュリティの回避と関連付け	• エンドポイントのセキュリティアプリケーション – 無効かインストールされていないかを検出 • CESA – 無効かインストールされていないかを検出 • ネットワークアクセスにユーザを関連付け – ユーザーアクティビティを NIC レベルまで紐付け
ゼロデイ マルウェアと脅威ハンティング	• アプリやプロセスの異常なふるまい – root または非標準ポートでの実行 • C&C 検知 – 新規、通常ではない、または悪性のドメインに対するバースト通信 • 脅威検知 – アプリケーションプロセスとホスト・ドメインの関連付け
ゼロトラスト モニタリング	• オフネットデバイスの監視 – ユーザ、デバイス、トラフィック、アプリ、データの挙動 • SaaS の利用行動 – SaaS サービスの利用状況を追跡 • 信頼されていないコネクション – 信頼されていないネットワークに接続している人の追跡
データ ロス検出 (DLP)	• データのため込み活動 – ダウンロード＆アップロードのふるまい • 持ち出し – 外部ドメイン＆ネットワーク共有へのアップロード
資産インベントリ	• デバイス タイプと OS インベントリ – タイプ別に識別してレポート • データプライバシーの遵守 – デバイスからの個人データの削除を確認

CESA で検出した脅威とコンプライアンス上の問題へのアクション

検出された脅威とコンプライアンス上の問題

- データロス検出 (DLP)
- 認可されていないアプリと SaaS
- セキュリティの回避と関連付け
- ゼロデイ マルウェアと脅威ハンティング
- ゼロトラスト モニタリング
- 資産インベントリ

改善・対応策

Cisco ISE

CESA/Splunk コンソールより 即時脅威を封じ込め (RTC)

ユーザー/デバイスの調査と隔離

Cisco Umbrella

CESA/Splunk コンソールでのエンフォースメント

悪意のある宛先をブロック

Cisco AMP

AMP Console での端末エンフォースメント

エンドポイントファイルの破棄、プロセスの終了

導入事例：Cisco CSIRT における CESA 展開

ニーズ:

- 他のセキュリティソリューションにはないエンドポイントのフットプリントとふるまいの洞察
- エンドポイントデバイス上における未知の脅威や内部犯行を検出する能力
- エンドポイントのインシデント調査時間と複雑さを軽減
- 社内外のネットワークを継続的に監視
- 既存のツールを可能な限り活用
- 75,000人の従業員と100,000以上のエンドポイントに対応するスケーラビリティ

CESA での結果:

- インシデント調査の時間を数日から数時間に短縮
- エンドポイントの可視性のギャップを解消 - CESAのユースケースの80%は他の技術では未対応
- エンドポイントエージェントの追加導入が不要
- 既存の Splunk を活用
- プライバシーの要件を満たすための位置情報にもとづく収集ルール
- Stealthwatch によるネットワークの可視性と AMP for Endpoints によるエンドポイント制御との連携

ケーススタディの詳細は以下をご覧ください：cisco.com/go/cesa

ライセンス

ライセンスモデル	Top-level SKU : CESA-SPLUNK-SUB
ライセンスタイプ	サブスクリプション
ライセンス ユニット	バンドに応じたシート
最小ユニット	2500 *1
期間	12, 36 ヶ月

SKU	説明
CESA-SPLUNK-LIC	NVM テレメトリ用の Splunk オンプレミス容量ライセンスを含む。Splunk の容量を含めた CESA の初回注文と、それ以降の 2500 以上のエンドポイントを追加するオーダーにて選択可。
CESA-SPLUNK-UPG	既存の CESA-SPLUNK-LIC オンプレミス環境に2500未満のエンドポイントを追加する際に選択可。
CESA-BYOC-LIC	NVM テレメトリ用の Splunk オンプレミス容量ライセンスを含まず、NVM App for CESA 、NVM Add-On for CESA 、およびCisco TACサポートのCiscoコンポーネントのみを対象としたライセンス。

既存 Splunk のお客様向け

*1 既存の CESA 環境に対して追加する場合に限り、CESA-SPLUNK-UPG を指定することで、2,500 未満での購入が可能

参考 Quote

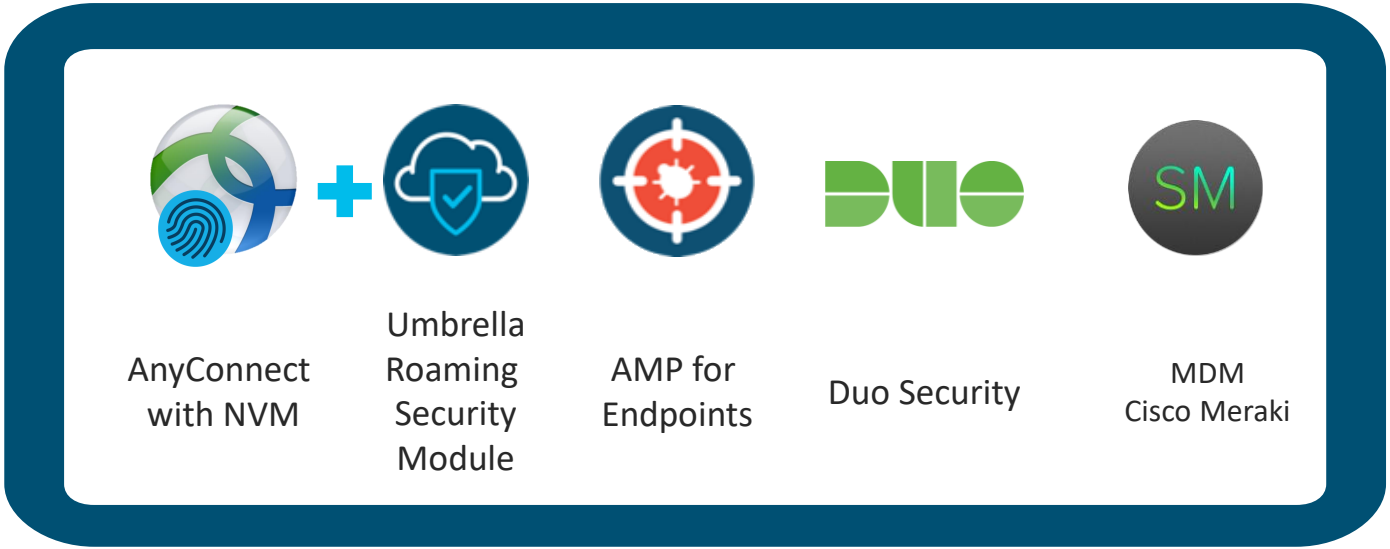
- 3,000 台、1年、自動更新 ON

Line Number	Item Name	Description	Service Duration (Months)	Included Item	Quantity	Pricing Term	ListPrice
1.0	**CESA-SPLUNK-SUB**	Cisco Endpoint Security Analytics - Splunk Subscription	N/A	No	1		0.00
1.1	SVS-SPLUNK-SUP-B	Basic Support for AnyConnect with Splunk	N/A	No	1	1	0.00
1.2	CESA-SPLUNK-LIC	Cisco Endpoint Security Analytics - Splunk Subscription	N/A	No	3000	12	
2.0	**L-AC-APX-LIC=**	Cisco AnyConnect Apex Term License, Total Authorized Users	N/A	No	3000		0.00
2.0.1	L-AC-APX-1Y-S6	Cisco AnyConnect Apex License, 1YR, 2500-4999 Users	12	No	3000		

- 10,000 ユーザ、3年、自動更新 OFF

Line Number	Item Name	Description	Service Duration (Months)	Included Item	Quantity	Pricing Term	ListPrice
1.0	**CESA-SPLUNK-SUB**	Cisco Endpoint Security Analytics - Splunk Subscription	N/A	No	1		0.00
1.1	SVS-SPLUNK-SUP-B	Basic Support for AnyConnect with Splunk	N/A	No	1	1	0.00
1.2	CESA-SPLUNK-LIC	Cisco Endpoint Security Analytics - Splunk Subscription	N/A	No	10,000	12	
2.0	**L-AC-APX-LIC=**	Cisco AnyConnect Apex Term License, Total Authorized Users	N/A	No	10,000		0.00
2.0.1	L-AC-APX-3Y-S8	Cisco AnyConnect Apex License, 3YR,10K-24999 Users	36	No	10,000		

ご参考
ゼロトラストから SASE まであらゆるシーンに対応する　端末セキュリティ



まとめ

- マルウェア以外にも、エンドポイントで起こる悪いことは多い
- CESA は従来ソリューションにはない「その他悪質なもの」をキャッチ
- CESAは単体でエンドポイントの可視性を一括して提供
- 既に AnyConnect エンドポイントがあれば更に有効活用
- 既存導入済み Splunk を活用することも、新たに導入することも可能
- Cisco CSIRT チームは2017年より10万エンドポイントで利用


CISCO