中小企業だってEDR導入したい！どうするデジタルテクノロジー!?
～わたしたちのSentinelOne導入までのあれやこれ、お見せします～

デジタルテクノロジー株式会社

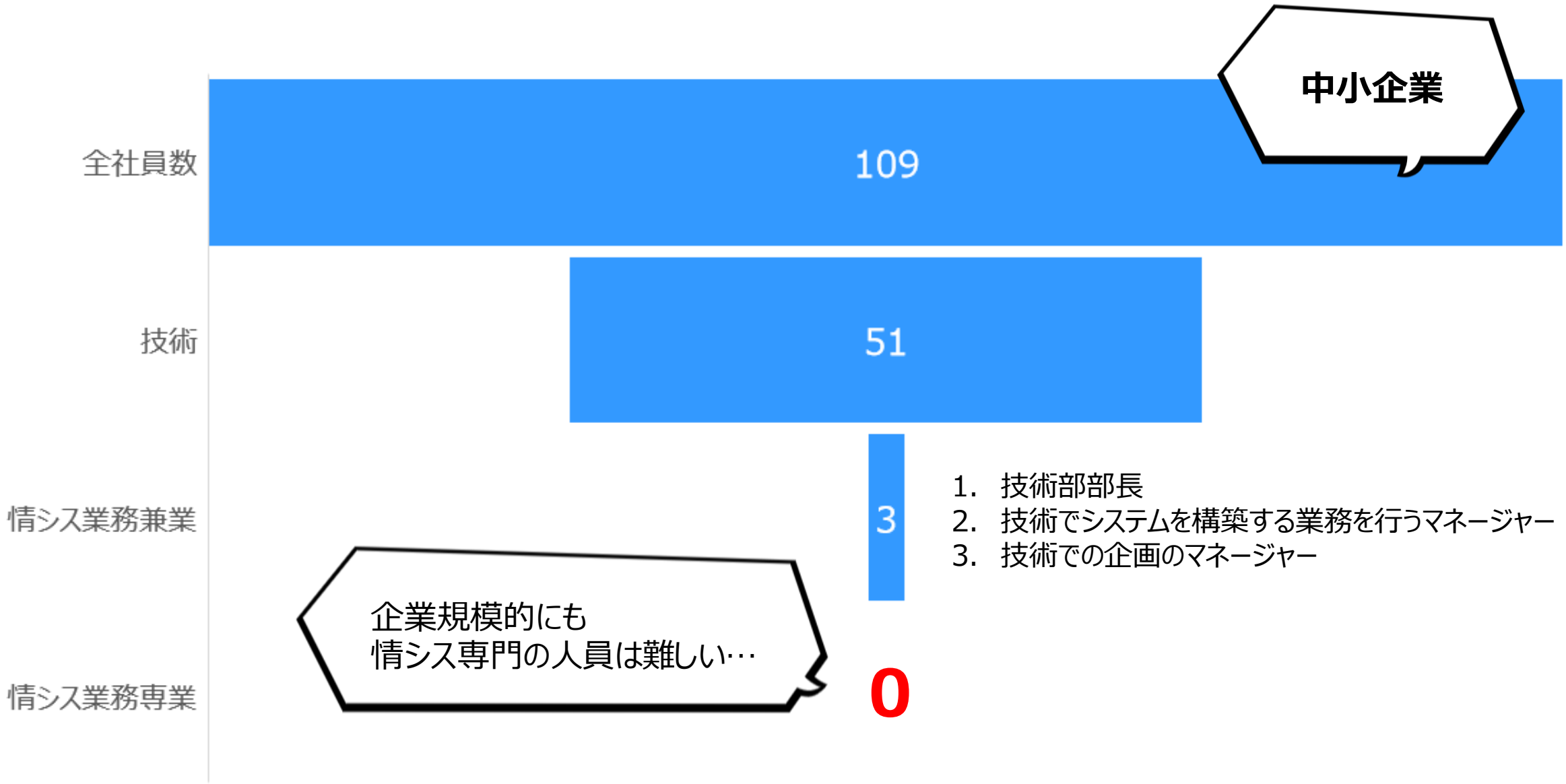
ITインテグレーション部 企画課 マネージャー
牧谷嘉明

2023/08/08

もくじ

当社の状況

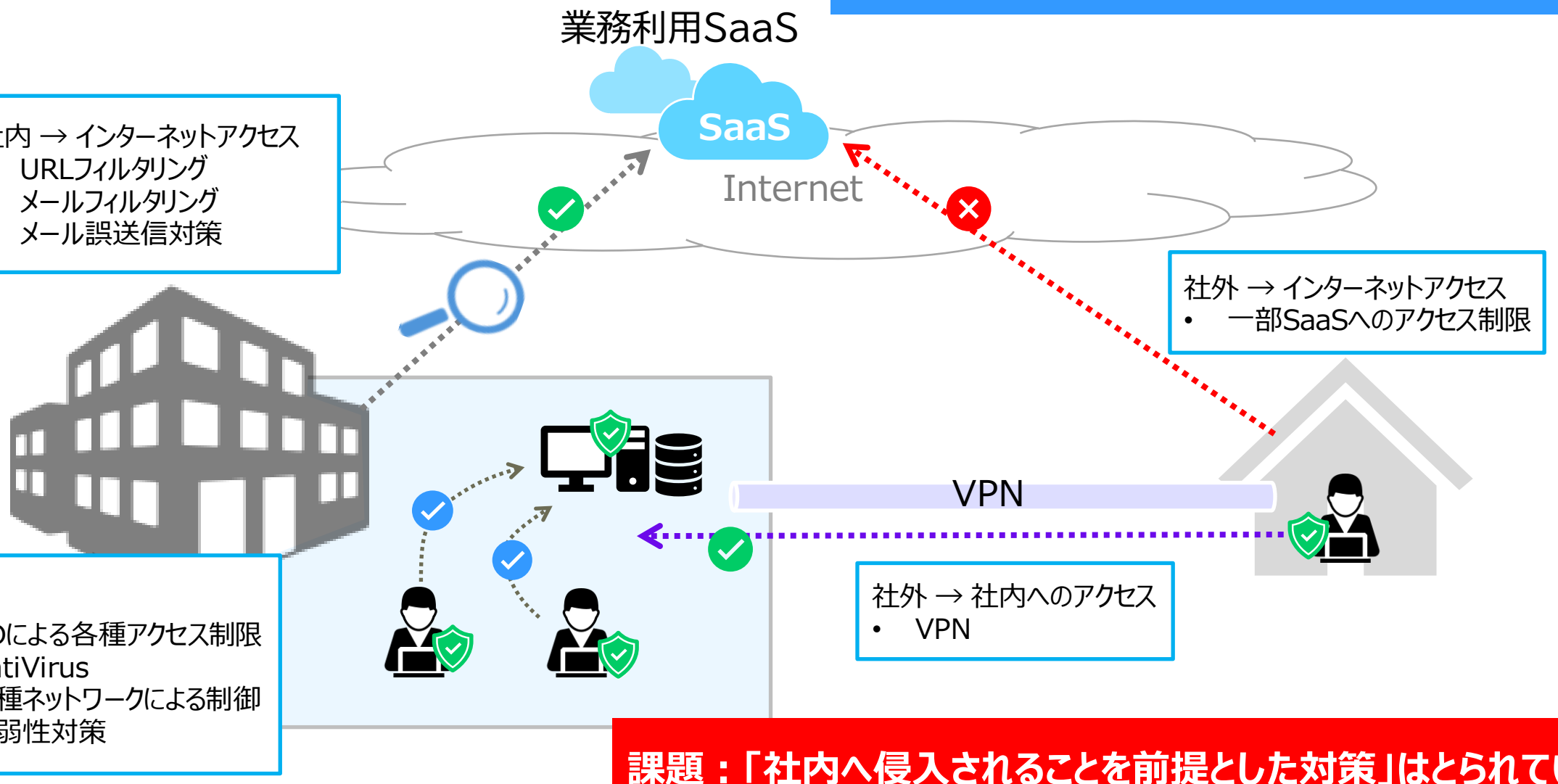
デジタルテクノロジーは中小規模の会社です



1. 技術部部長
2. 技術でシステムを構築する業務を行うマネージャー
3. 技術での企画のマネージャー

セキュリティ環境～現状と課題～

現状：今までの考え方で必要な対策はとられている



課題：「社内へ侵入されることを前提とした対策」はとられていない

EDRの選定

中小企業でも買えるEDR

中小企業ユーザーのニーズ

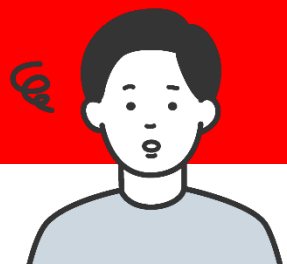
ライセンスを1本から自社の必要な本数に合わせて購入可能

ライセンス費用がAnti-Virusに比べ高くなりすぎない

運用に費用、稼働がかからない

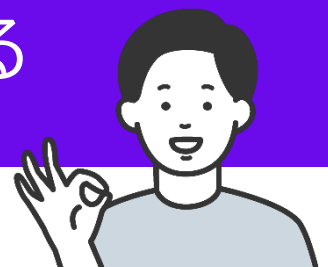
中小企業でも買えるEDR

中小企業ユーザーのニーズ	今までのEDR
ライセンスを1本から自社の必要な本数に合わせて購入可能	ライセンスを100本から提供
ライセンス費用がAnti-Virusに比べ高くなりすぎない	ライセンスがAnti-Virusに比べ7~10倍程度
運用に費用、稼働がかからない	基本SOC利用が前提



中小企業でも買えるEDR

中小企業ユーザーのニーズ	SentinelOne
ライセンスを1本から自社の必要な本数に合わせて購入可能	ライセンスを1本から提供 ※弊社商流で可能。別代理店では最小ライセンス数が異なる場合あり。
ライセンス費用がAnti-Virusに比べ高くなりすぎない	ライセンスがAnti-Virusに比べ3~5倍程度
運用に費用、稼働がかからない	SOCがなくても運用できる



中小企業でも買えるEDR

我々のような中小企業でも導入可能なEDRとして
SentinelOneを選定

中小企業ユーザーのニーズ

- ライセンスを1本から自社の必要な本数に合わせて購入可能
- ライセンス費用がAnti-Virusに比べ高くなりすぎない
- 運用に費用、稼働がかからない

ニーズにマッチ

＝

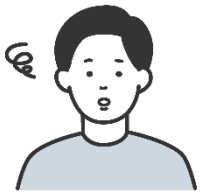
≠

SentinelOne

- ライセンスを1本から提供
  ※弊社商流で可能。別代理店では最小ライセンス数が異なる場合あり。
- ライセンスがAnti-Virusに比べ3~5倍程度
- SOCがなくても運用できる

他社EDR

- ライセンスを100本から提供
- ライセンスがAnti-Virusに比べ7~10倍程度
- 基本SOC利用が前提



SentinelOneの評価

EDR専業ベンダーとしてはCrowdStrikeに次いで2番手の評価

SentinelOneで評価した側面

インシデントへの自動復旧機能を有する
唯一の製品

×

第三者機関(MITRE)による評価で
検知・保護性能が非常に高い

第三者機関評価

高

SentinelOne

cybereason

CROWDSTRIKE

Microsoft

手動

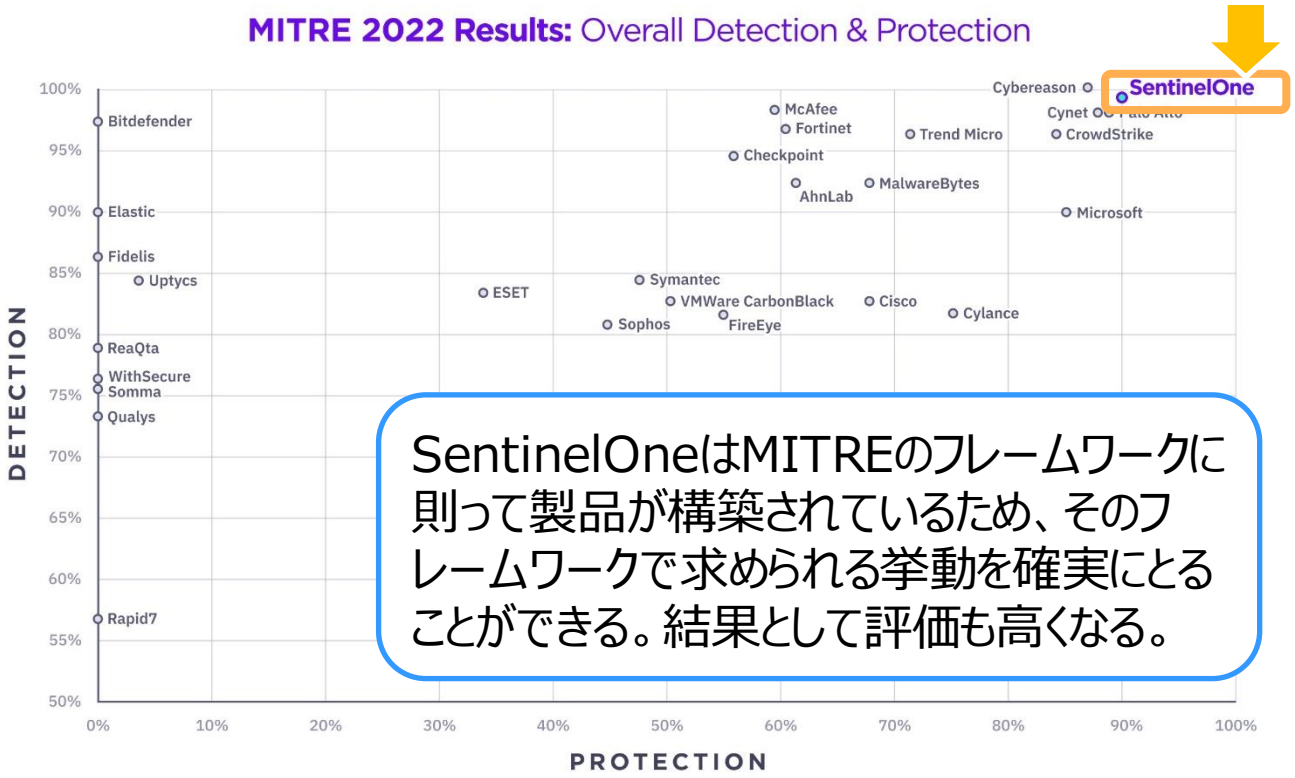
自動

インシデント自動対応

vmware Carbon Black

eset

低



SentinelOneはMITREのフレームワークに則って製品が構築されているため、そのフレームワークで求められる挙動を確実にとることができる。結果として評価も高くなる。

SentinelOneで評価した側面

インシデントへの自動復旧機能を有する
唯一の製品

×

第三者機関(MITRE)による評価で
検知・保護性能が非常に高い

SOC不要での運用が可能と判断

導入に向けて

導入に向けての整理

一か月程度の期間を設けて導入前に下記を実施

- 導入対象の選定
  - ① クライアントは
  - ② サーバーは

- ボリュームシャドウコピーの設定
  挙動に影響があると想定されるため、現状VDIではできないように設定をしてある
  - ①VSSが動くかを確認
  - ②挙動に影響がないかを確認
  - ③ロールバックをしない場合の運用設計

- 管理コンソールの設定
  - ①メール通知の設定
  - ②グループ作成
  - ③その他設定の確認

- 現在のリソース使用状況の確認
  可能であれば実施

- メール通知システム
  - ①通知内容の精査
  - ②構築
  - ③検証
  - ④通知を受けた際の運用設計

- 配布方法の検討
  exeもしくはmsiの配布方法の検討
  VDIでの配布方法はまた別になるはずなので要確認

- 社内での運用設計
  検知された際の運用設計
  - 実オペレーション者
  - 連絡先
  - 検知時の行動

- 各フェーズにおける導入対象者の選定
  導入対象者の選定

PCの要件1

管理コンソールアクセス用ブラウザ
- Chrome
- Safari
- Firefox
- Edge Chromium

CPU
以下のマイクロアーキテクチャには対応していません。
ppc64, x86_32, ARM, RISC, MIPS

Windows OS

Windows Server Core	2012, 2016, 2019
Windows Server	2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1
Windows Storage Server	2016, 2012 R2, 2012
Windows 7 SP1, 8, 8.1, 10, 11	32/64 Bit

Edition: Home, Pro, Pro for Workstations, Enterprise, Education, Pro Education, Enterprise LTSC, Embedded

最小ハードウエア要件
CPU: 1GHz / 1 core
RAM: 3GB
Disk: 2GB（エージェントが消費する領域）
リソース消費の目安：RAM 300 MB、CPU 2 %、通信量 1日に4 - 8 MB（Complete の場合 +11 MB）

レガシー Windows OS
Windows XP SP3 or later (KB968730) 32/64-bit NTFS/FAT32
Windows Server 2003 SP2 or later, or R2 SP2 or later, (KB968730) 32/64-bit
Windows 2008 (Pre-R2)
Windows Embedded POSReady 2009

機能制限あり
Reputation Scan（ハッシュ値パターンマッチング）とプロセスの停止のみ提供。

AWS Tokyo リージョン利用時のネットワーク要件

ブラウザのアクセス先
- https://apne1-1002.sentinelone.net:443
- https://www.google-analytics.com:443
- https://cdn.pendo.io:443
- https://data.pendo.io:443
- https://sentry.io:443

エージェントのアクセス先
- https://apne1-1002.sentinelone.net:443

Singularity Complete 利用時にエージェントがアクセス
- https://dv-ap-prod.sentinelone.net:443
- https://ioc-gw-prod-ap-1a.sentinelone.net:443
- https://ioc-gw-prod-ap-1c.sentinelone.net:443

RSO 機能利用時にエージェントがアクセス
- https://file-services-ap-northeast-1-prod.sentinelone.net:443
- https://ap-northeast-1-prod-remote-scripts.s3.ap-northeast-1.amazonaws.com:443
- https://ap-northeast-1-prod-remote-scripts-uploads.s3.ap-northeast-1.amazonaws.com:443

macOS
12.[0-2], 11.6, 11.5.[0,1,2], 11.4, 11.3.[0,1], 11.[0,1,2], 10.15.[1,2,3,4,5,6,7]. 10.14

最小ハードウエア要件
CPU: Intel / M1, 1GHz / 2 core
RAM: 1GB
Disk: 2GB（エージェントが消費する領域）
リソース消費の目安：RAM 300 MB、CPU 2 %、通信量 1日に2 - 4 MB（Complete の場合 +25 MB）

PCの要件2

Linux OS

CentOS		6.4, 7.[0-9], 8.[0-4]
Red Hat Enterprise Linux(RHEL)	6.4, 7.[0-9], 8.[0-5]	
Ubuntu		14.04, 16.04, 18.04, 18.04.5, 19.04, 19.10, 20.04, 20.04.1
Oracle		6.[9-10], 7.[0-9], 8.[0-5]
Amazon		2017.03, 2018.03, AMI 2
SUSE Linux Enterprise Server	12.x, 15.x	
Fedora		25, 26, 27, 28, 29, 30, 31, 32, 33
Debian		8, 9, 10, 11
Virtuozzo		7
Scientific Linux		6, 7
Alma Linux		8.4, 8.5
Rocky Linux		8.4, 8.5

最小ハードウエア要件
CPU: 2GHz / 2 core
RAM: 4GB
Disk: 2GB （エージェントが消費する領域）
リソース消費の目安：RAM 450 MB、CPU 1 - 5 %、通信量 1日に13 -17 MB（Complete の場合 +52 MB）

サポート
64-bit カーネル＆ライブラリ
SELinux
K8s

非サポート
32-bit カーネル＆ライブラリ
FreeBSD, AIX, Solaris
CPU: SSE4a
2.6 より前の Kernel バージョンには対応していません
3.8 より前の Kernel バージョンでは書き込み時のファイル検査をしません
3.10 より前の Kernel バージョンではコンテナに対応していません
3.11 より前の Kernel バージョンではコンテナ上で書き込み時のファイル検査をしません
Kernel Lockdown 機能の Confidentiality モード

K8s
コンテナエンジン: Docker, ContainerD, CRI-O
サポートプラットフォーム: Kubernetes version 1.13 以上, OpenShift 4.4, 4.5, 4.6, 4.7
サポート CSP 環境: GKE, EKS, AKS

最小環境要件
エージェント

Limits:	requests:
memory: 1.2Gi	memory: 100Mi
cpu: 900m	cpu: 100m

ヘルパー

Limits:	requests:
memory: 1.8Gi	memory: 100Mi
cpu: 900m	cpu: 100m

必要ソフトウエア: kubectl / oc, helm3, docker

仮想・VDI環境
- Citrix XenApp
- Citrix XenDesktop
- Oracle VirtualBox
- VMware vSphere
- VMware Workstation
- VMware Fusion
- VMware Horizon
- Microsoft Hyper-V (要VHDファイル)

クラウドサービスVM
- AWS EC2
- AWS EKS Anywhere
- Azure VM
- Google Compute Engine

EDRのそれぞれの対象での動き

EDR導入サーバ及び端末は、下記3グループのいずれかに所属。グループ毎に挙動は変える。
検知後、NWから切り離す等の対応は、自動的に実施され、ユーザでの操作は不要。

サーバ

- VSS、Rollbackの設定は対象によって検討
- 悪意のあるもの:protect
  疑わしいもの　:detect

VDI

- VSS、Rollbackは設定しないがNWから切り離す
- 悪意のあるもの:protect
  疑わしいもの　:detect

Default (デスクトップ、ノート)

- VSS、Rollbackの設定
- 悪意のあるもの:protect
  疑わしいもの　:detect

社内運用フロー

社内

情シスA
- 運用設計
- 技術的問合せ・サポート
- 導入検討
- 設定

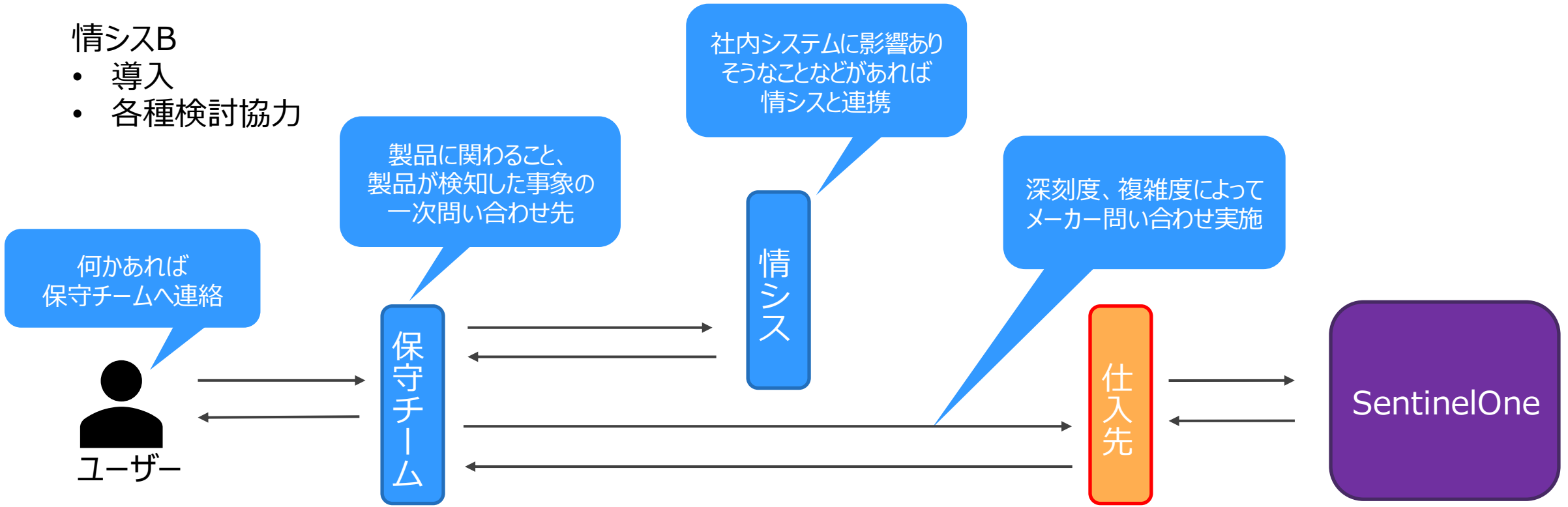
情シスB
- 導入
- 各種検討協力

保守チーム
- 検知時の各種対応

社外

仕入先
- 製品サポート

SentinelOne
- 製品サポート



導入の流れ（当初想定）

現在ココまで進んでいます

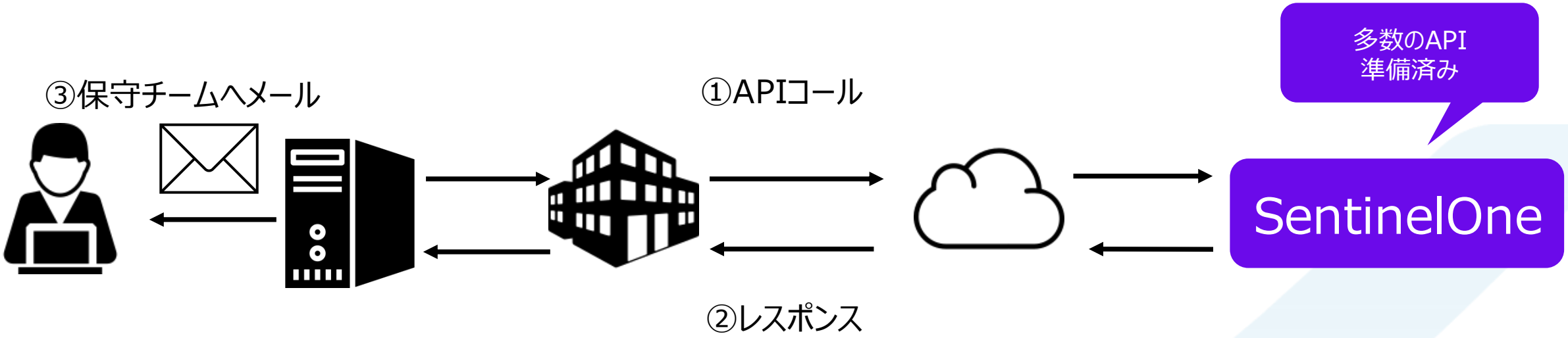
購入後2週間	購入後4週間	購入後6週間	購入後8週間
Step1	Step2	Step3	Step4
◘ 誤検知の洗い出し 固有のアプリケーションを利用する機会のある、部課の特定環境にインストール。 業務を一通り実施し、利用するアプリ、exe、マクロなどを実行。 誤検知の場合は除外登録を実施。 ◘ 使用リソースの確認 PCの挙動が異常に遅くなるなどが出てないかを確認。	◘ 誤検知の洗い出し 継続して実施 ◘ 使用リソースの確認 継続して実施	◘ 誤検知の洗い出し 継続して実施 ◘ 使用リソースの確認 継続して実施	◘ 設定の変更 ◘ ロールバック設定の導入
	メール通知システムの試験		
社内導入数は10台程度	社内導入数は40台程度	社内導入数は全台	

メール通知システム概要

当社でのメール通知システムの仕組み

社内

社外



① Threats情報（脅威を検知した履歴）の情報をリクエスト
② 情報を取得
③ 取得した情報を保守チームへメール通知

やってみて分かったつまずきポイント

- VDI環境への導入
- GPO(Group Policy Object)による展開
- IaC(Infrastructure as Code)による展開

お客様が導入されるときも、
考慮必要なポイント。

自社導入経験でのノウハウを
フィードバックしてご案内可能。

SentinelOne 自社運用の感触

誤検知が少なく
ほぼ運用らしい運用をしなくていい

最初のインストール以外再起動も不要だし、
管理コンソールで一通りの操作が出来るから
使い勝手がいい

弊社情シス担当者の『生の声』です

デジタルテクノロジーの提供サポート

お客様が導入された場合の運用フロー

社内

情シス担当者

- SentinelOneの内製運用
- 検知時の各種対応
- 自社ユーザからの問い合わせ対応
- 窓口への問い合わせ

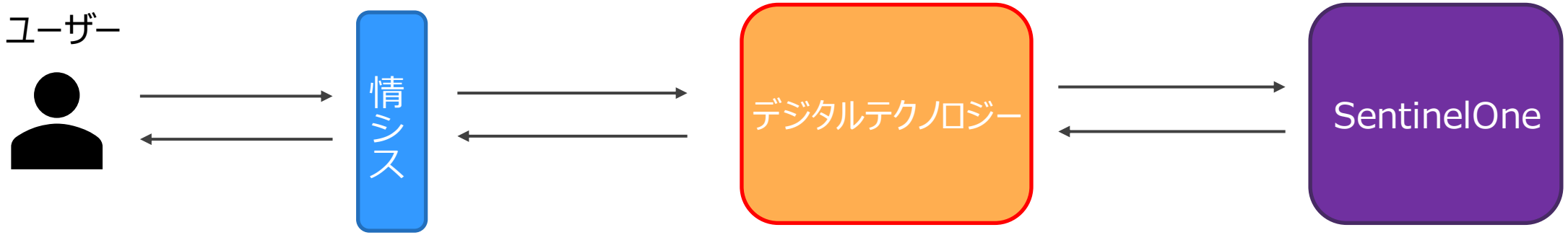
社外

デジタルテクノロジー

- お問い合わせ窓口
- 製品サポートプラン
  (2種類から選択)

SentinelOne

- 製品サポート



SentinelOneサポートプラン

サービス項目	SentinelOne サポート	SentinelOne アクティブサポート
プランの概要	EDRの内製運用を円滑に支援する メール通知を基本とするプラン	重要なインシデント検知時に能動的な脅威情報の確認・判定を追加するプラン
サポート窓口 対応時間帯	平日　9時～17時	平日　9時～17時
コミュニケーション方式	Email/Web	Email/Web
使い方や一般的な問い合わせ	○	○
ホワイトリスト登録支援	○	○
インシデントのエスカレーション ※お客様よりエスカレーションされたインシデントに対処します	○ ※回数上限あり	○
アクティブインシデント対応 ※発生したインシデントの確認や誤検知判断などを能動的に実施します	×	○
エージェントのバージョンアップ代行	別紙 ご参考価格参照	別紙 ご参考価格参照
チューニング代行	別途見積	別途見積
重大事故発生時のフォレンジック調査	別途見積	別途見積

※本サポートサービスにはフォレンジック調査は含みません。
　SentinelOneが脅威を検知した場合、実際そのような侵害があったかの調査はお客様のご判断により実施いただくものとします。

インシデントのエスカレーション回数の上限（SentinelOneサポート）

ライセンス数	月間エスカレーション数
1-50	3
51-100	5
101-500	10
501-1000	20
1001以上	別途見積

※検知されたインシデントに関する問い合わせが月間エスカレーション数にカウントされます
※エスカレーション数は翌月及び次年度へ繰り越しすることはできません
※DeepVisibility（脅威ハンティング機能）による詳細なクエリ調査は対象外です
※上限を超えるエスカレーションが必要な場合、別途お見積りとなります
※本サービスはお客様の運用判断を支援するものであり、インシデントの最終判定はお客様にてお願いします

“エージェントのバージョンアップ代行” ご参考価格

SentinelOneエージェントのバージョンアップ作業は『4回/年』発生。

【実施方法について】
・バージョンアップ作業は1グループ＝最大20台までで行うものとします。
・作業を実施する時間帯、間隔はお客様と打合せの上、決定するものとします。
・1グループの同時実行台数が多くなるとインターネット接続回線を圧迫し業務に影響が出ることが想定されるため、
上限を設けています。

グループ数	提供価格（税抜）
2	1,500円/台　（年額）
3	2,000円/台　（年額）
4	2,500円/台　（年額）
5	3,000円/台　（年額）

提供価格有効期限：2024年3月31日
SentinelOneサポート、SentinelOneアクティブサポート共通

グループ数によって作業期間が延びるため、1台当たりの作業単価が異なります。

6グループ以上の場合は別途お見積りとなります。

まとめ

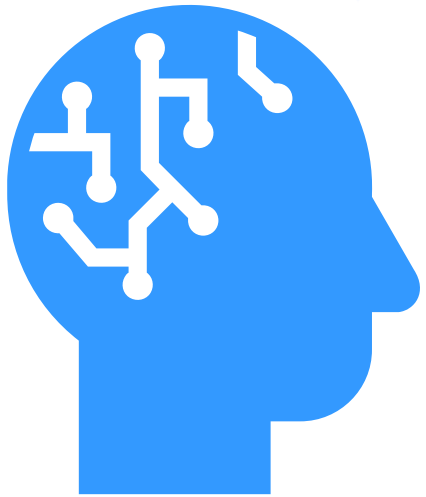
1. 中小企業でも、EDRの導入は必要になってきます。

2. SentinelOneは
中小企業のニーズにマッチしたEDRです。

3. デジタルテクノロジーは
自社導入のノウハウでお客様をご支援します。

自動修復・自律型AIが

一人情シスの強い味方！



SentinelOne®

ご検討の際は、是非デジタルテクノロジーへご連絡ください！

お問い合わせ

デジタルテクノロジー株式会社

Mail　sales@dtc.co.jp

URL　https://www.dtc.co.jp/sentinelone

東京セールスオフィス　〒104-0032 東京都中央区八丁堀2-23-1 エンパイヤビル
TEL:03-6914-5499

大阪支店　〒532-0004 大阪市淀川区西宮原2-7-53 Marutaビル
TEL:06-6393-1301

SentinelOne 製品ページはこちら

↓↓↓

SentinelOne 紹介動画はこちら

↓↓↓