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 ゼネラルマネージャー
松崎 剛史

2023/11/22

もくじ

デジタルテクノロジーについて

デジタルテクノロジーは中小規模の会社です

デジタルテクノロジーの組織体制

中小企業

全社 109名

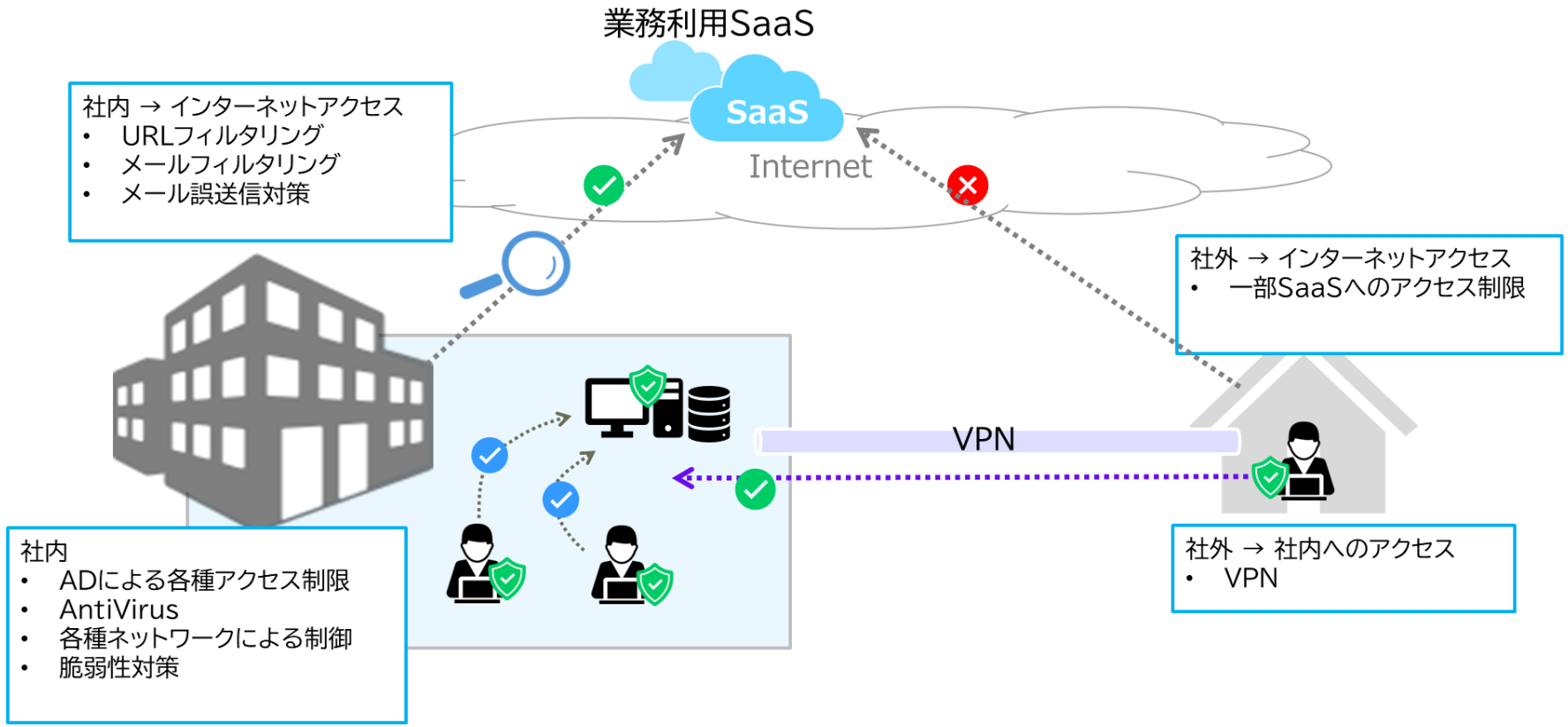
- 営業部門 49名
- 技術(SE)部門 51名
  - 情シス業務 **3名(兼任分業)**
- 管理部門 9名

情シス専任担当 **0名**

企業規模的にも
情シス専門の人員の配置は難しい…

セキュリティ環境～現状(当時)と課題～

当時：今までの考え方で必要な対策はとれている



課題：「内部へ侵入されることを前提とした対策」は脆弱なままだった

EDRの選定

中小企業が求めるEDR

当社＝中小企業のEDRに対するニーズ

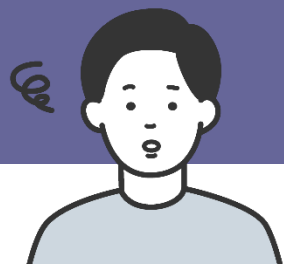
① ライセンス1本から、必要な数に合わせて購入可能

② ライセンス費用がAnti-Virusに比べ高くなりすぎない

③ 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1本から、必要な数に合わせて購入可能	ライセンスは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	ライセンス費用が、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

- ライセンス1本から、必要な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

SentinelOne

ライセンスを1本から提供
※弊社商流の場合。他社では最小ライセンス数が異なる場合あり。

ライセンス費用は、Anti-Virusに比べ、3～5倍 程度

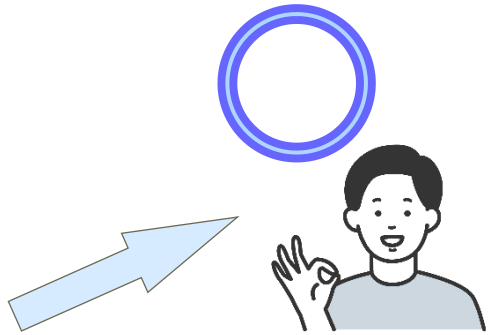
SOCがなくても運用できる

中小企業でも買えるEDR

当社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



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。
- ライセンス費用は、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
- ライセンス費用が、Anti-Virusに比べ7～10倍程度
- 基本SOC利用が前提

SentinelOneの評価

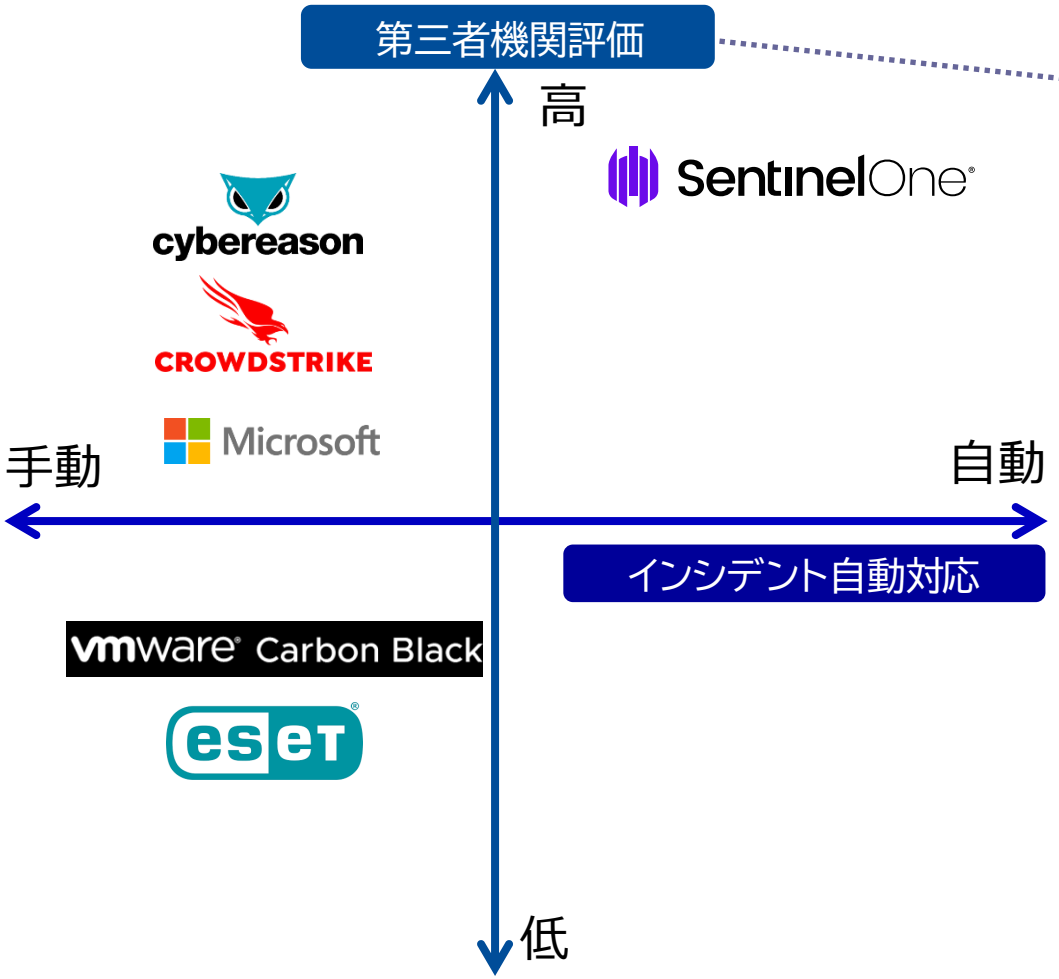
EDR専業ベンダーとしてはCrowdStrikeに次いで2番手の評価

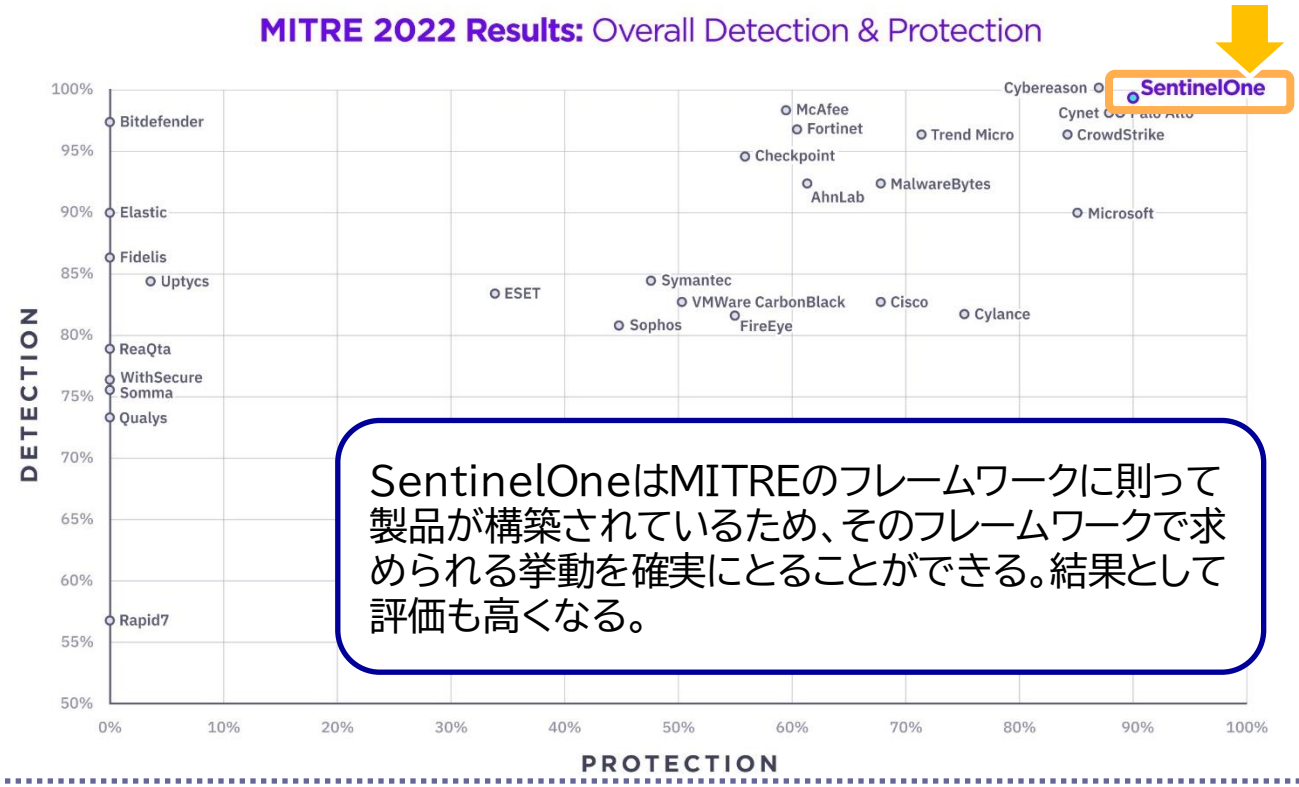
SentinelOneで評価した側面（導入当時の検討）

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





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

SentinelOne®

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

1. 導入対象の選定
   ① クライアントは
   ② サーバーは

2. ボリュームシャドウコピーの設定(Windows)
   挙動に影響があると想定されるため、VDIではVSSを無効にしていた
   ① VDIでVSSが動作するかを確認
   ② 通常利用に影響がないかを確認
   ③ VSSが利用できない場合、ロールバックをしない場合の運用設計

3. 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

4. PCの現在のリソース使用状況の確認
   可能であれば実施

5. 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

6. 配布方法の検討
   .exe もしくは .msi での配布方法の検討
   VDIでの配布方法はまた別になる想定として要確認

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

8. 導入段階各フェーズにおける導入対象者の選定
   障害・業務影響等を考慮して導入対象者の選定

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: 導入対象ごとの考え方

導入対象によりポリシーを区分

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

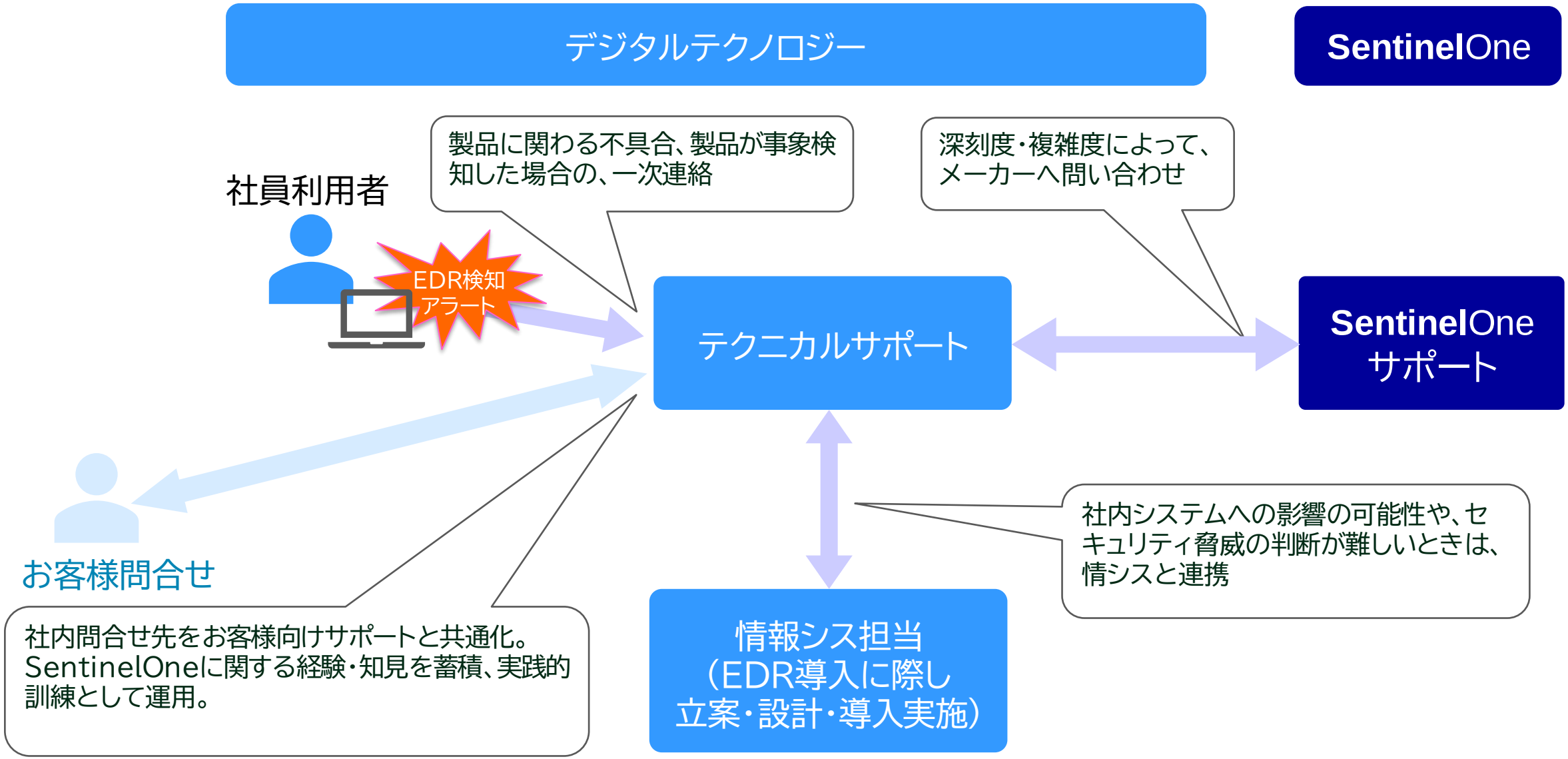
VDI

- 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

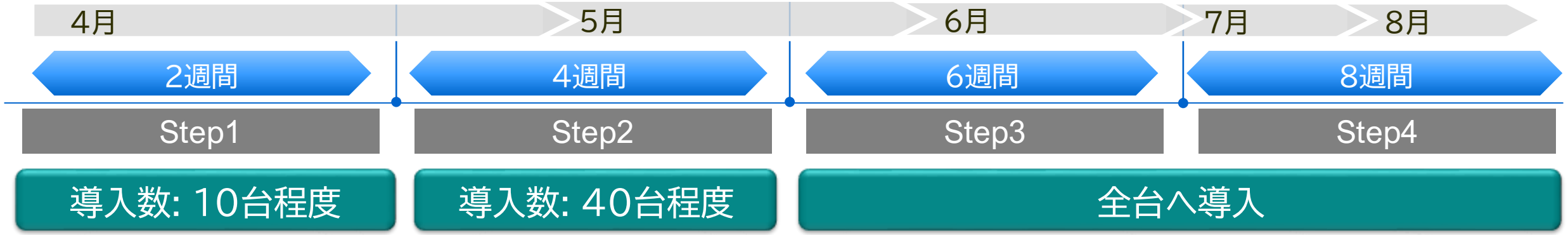
Default（デスクトップ、ノート）

- 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


デジタルテクノロジー
SentinelOne
製品に関わる不具合、製品が事象検知した場合の、一次連絡
深刻度・複雑度によって、メーカーへ問い合わせ
社員利用者
EDR検知
アラート
テクニカルサポート
SentinelOne
サポート
お客様問合せ
社内システムへの影響の可能性や、セキュリティ脅威の判断が難しいときは、情シスと連携
社内問合せ先をお客様向けサポートと共通化。
SentinelOneに関する経験・知見を蓄積、実践的訓練として運用。
情報シス担当
（EDR導入に際し
立案・設計・導入実施）

導入の流れ（当初想定）



① 誤検知の洗い出し
・固有アプリケーションを利用する部署の、限定した環境に導入。
・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。

② PC使用リソースの確認
PCの挙動が異常に遅くなるなどの状況がないか確認。

① 誤検知の洗い出し
→（継続して実施）

② 使用リソースの確認
→（継続して実施）

① 誤検知の洗い出し
→（継続して実施）

② 使用リソースの確認
→（継続して実施）

本番運用移行

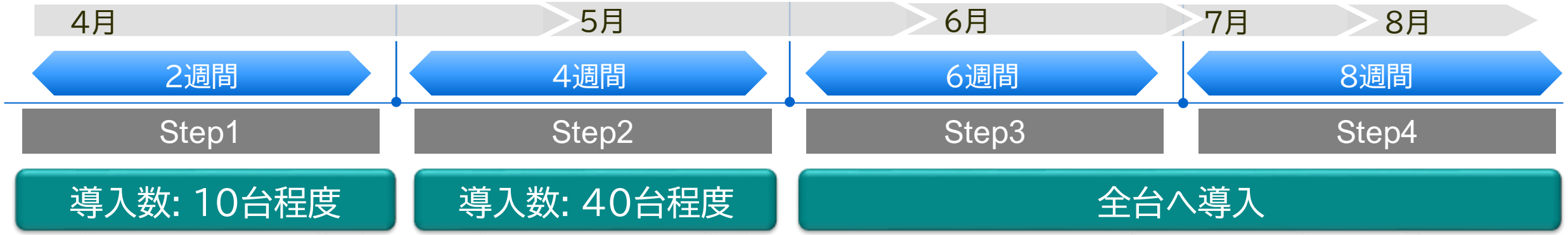
○ 検知設定の変更
○ ロールバック設定の導入

社内への導入通知・調整

運用/通知システムの構築・試験

運用フロー定義、テスト

導入の流れ（実際）



① 誤検知の洗い出し
・固有アプリケーションを利用する部署の、限定した環境に導入。
・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。

② PC使用リソースの確認
PCの挙動が異常に遅くなるなどの状況がないか確認。

① 誤検知の洗い出し
→ EXCELのマクロ、一部のフリーソフトなど

② 使用リソースの確認
→（継続して実施）

① 誤検知の洗い出し
→（継続して実施）

② 使用リソースの確認
→（継続して実施）

本番運用移行

○ 検知設定の変更
○ ロールバック設定の導入
（VDIは非ロールバック）

VDI基盤・VDIデスクトップ更新
VDI再構築（予定外）
VDI-VSS検証

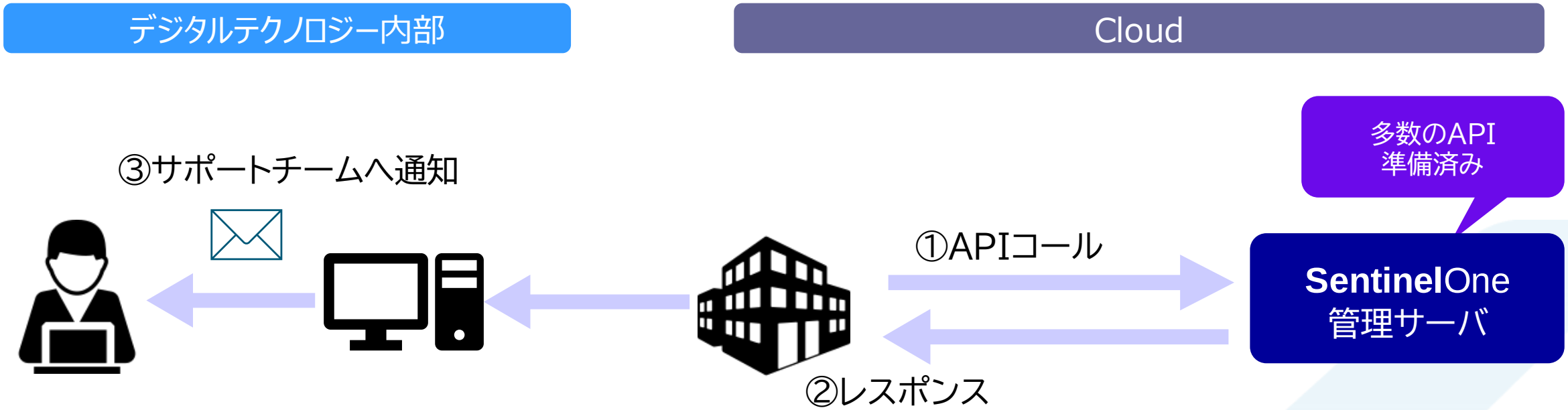
社内への導入通知・調整

運用/通知システムの構築・試験

運用フロー定義、テスト

メール通知システム

当社でのメール通知システムの仕組み



① Threats情報(脅威を検知した履歴)の情報を、管理サーバーへ問合せ(API)
② 情報を取得、脅威検知の有無を確認
③ 検知があった場合、情報をサポートチームへ通知。確認対応を開始。

やってみて分かったつまずきポイント

① VDI環境への導入
※ VSS(ロールバック)の検証、配布方式の違い

② GPO(Group Policy Object)による展開
※ エージェント配布に伴う既存ソフトの削除

③ 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活用し、
自信を持ってご提案できます

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

お客様

デジタルテクノロジー

SentinelOne

利用者

脅威検知
アラート

情シス
ご担当者

- SentinelOneの社内運用
- 脅威検知時の対応
- 利用者からの問い合わせ対応
- サポートへの問い合わせ

デジタルテクノロジー
テクニカルサポート

- お問い合わせ窓口
- 製品サポートプラン

SentinelOneサポート
SentinelOneアクティブサポート

SentinelOne
サポート

- 製品サポート
- アップデート

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で実施ください。
※ インシデントエスカレーションは、お客様の運用上の判断を支援を目的として情報を提供するものです。インシデントの最終判定はお客様にてお願いします。

インシデント エスカレーション件数上限（SentinelOneサポートのみ）

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。
※ インシデントエスカレーションは、お客様の運用上の判断を支援を目的として情報を提供するものです。インシデントの最終判定はお客様にてお願いします。(SentinelOneサポート/アクティブサポート共通)

“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(GAリリース)は『4回/年』

【実施方法について】
- バージョンアップ対応は対象とします。
- 作業は1グループ＝最大20台までで行うものとします。
  ※ 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。
- 作業を実施する時間帯、間隔はお客様と打合せの上、決定します。(自動的・暗黙的には実施されません)

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。

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

お客様導入事例:（運輸系事業者様）

従来のアンチウィルスソフトでのセキュリティに限界を感じ、EDR導入を検討。

ベンダーにEDRの提案を依頼するも、最低購入ライセンス数に達しない、予算に合わないとの理由で、見積もり入手から困難だった。そんな中、**1台から購入可能、他のEDR製品に比べ、現実的な価格感**のSentinelOneの提案を受け採用。

AIによる自動運用で、**インシデント発生時の初期対応はSentinelOneに任せ、人の対応より圧倒的に早い対処でリスクを軽減。**情シスの運用負荷を下げながら、よりセキュリティの高い環境を実現できた。

企業概要

地域　　：関西
事業　　：旅客運送事業
利用ライセンス数：PC 65台、サーバ3台

導入理由

- 100台未満の環境でも購入可能なEDR
- 従来のアンチウィルスソフトに限界を感じていた
- 自社運用でも情シス負担が少ないEDR

検討競合製品

- ESET（※EPPライセンス）
- CrowdStrike（※NGAVライセンス）

まとめ

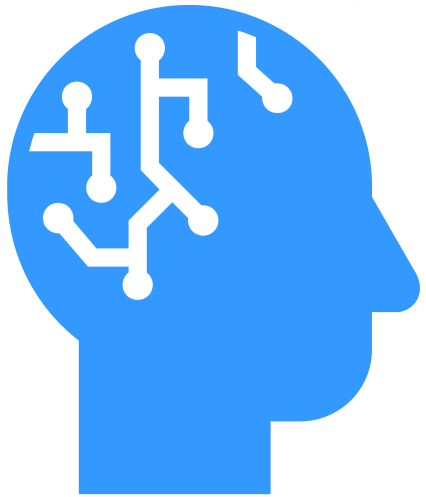
1. 中小企業でも、EDRの導入は必要になってきます。

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！