

The Border

クララオンラインの自社IT戦略と エンドポイント入れ替え実録



株式会社クララオンライン
ビジネスストラテジー部
コーポレートIT

山崎隼人

前半：クララオンライン 山崎

- クララオンラインの自社の取り組みについて
- 次世代型エンドポイント保護(NGAV/EPP+EDR)の
導入時の検証(PoC)や製品選定のポイント

後半：東京エレクトロンデバイス 三吉様

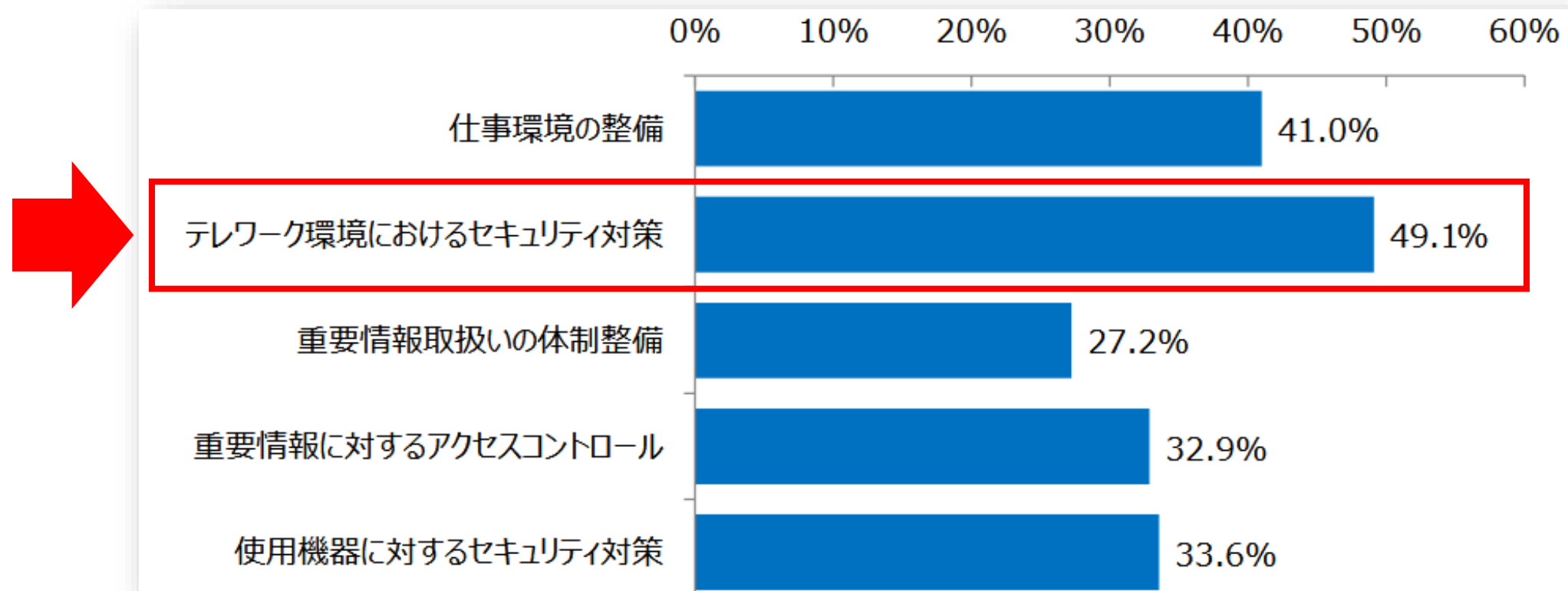
「SentinelOne」について

- **国内販売までの背景や製品の評価ポイント**
- **導入・運用トピックス**

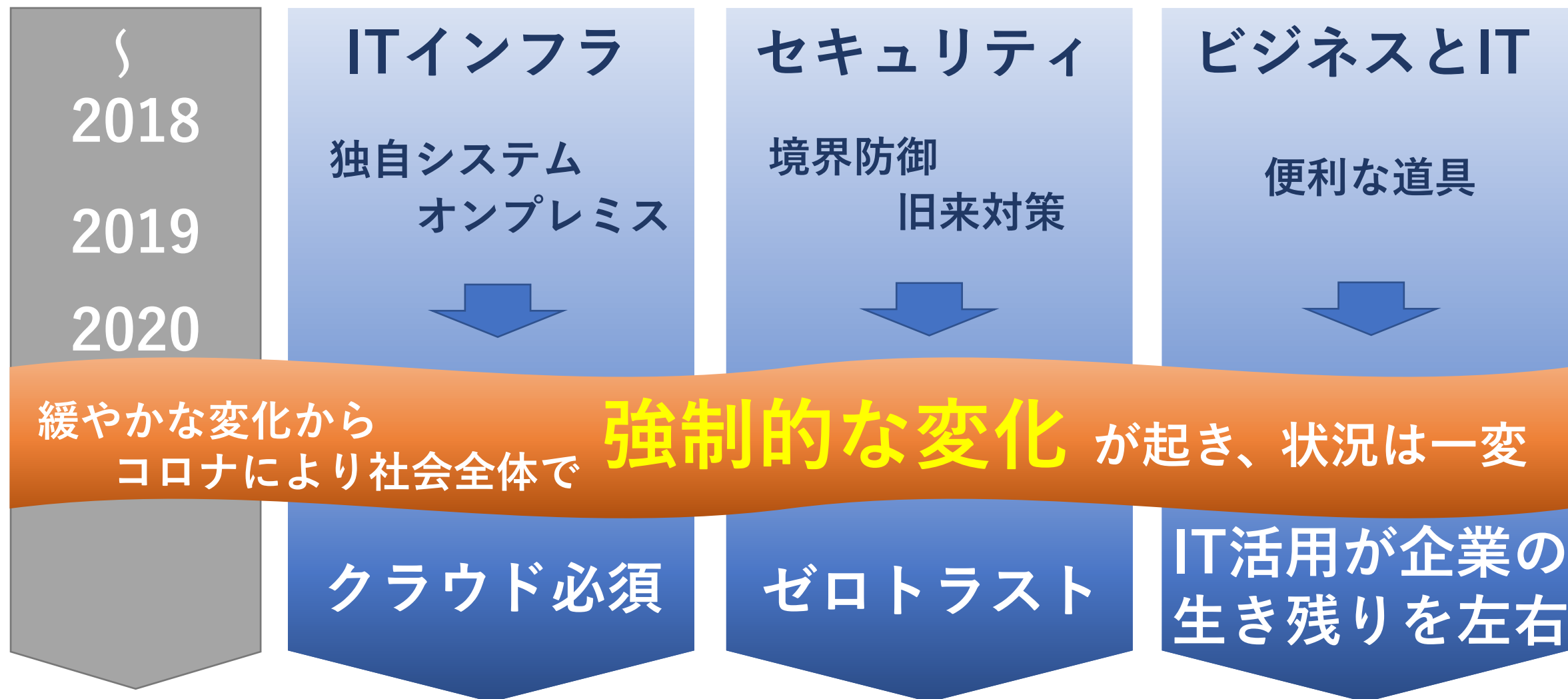
- コロナ禍による変化
- 当社の取り組み
- 次世代型エンドポイント保護の導入のポイント
 - 課題意識／比較検討
 - 導入検証のコツ
 - 製品評価・選定ポイント

コロナ禍による変化

緊急事態宣言下で業務を円滑に遂行するために重視した点として
「セキュリティ対策」が半数を占めている



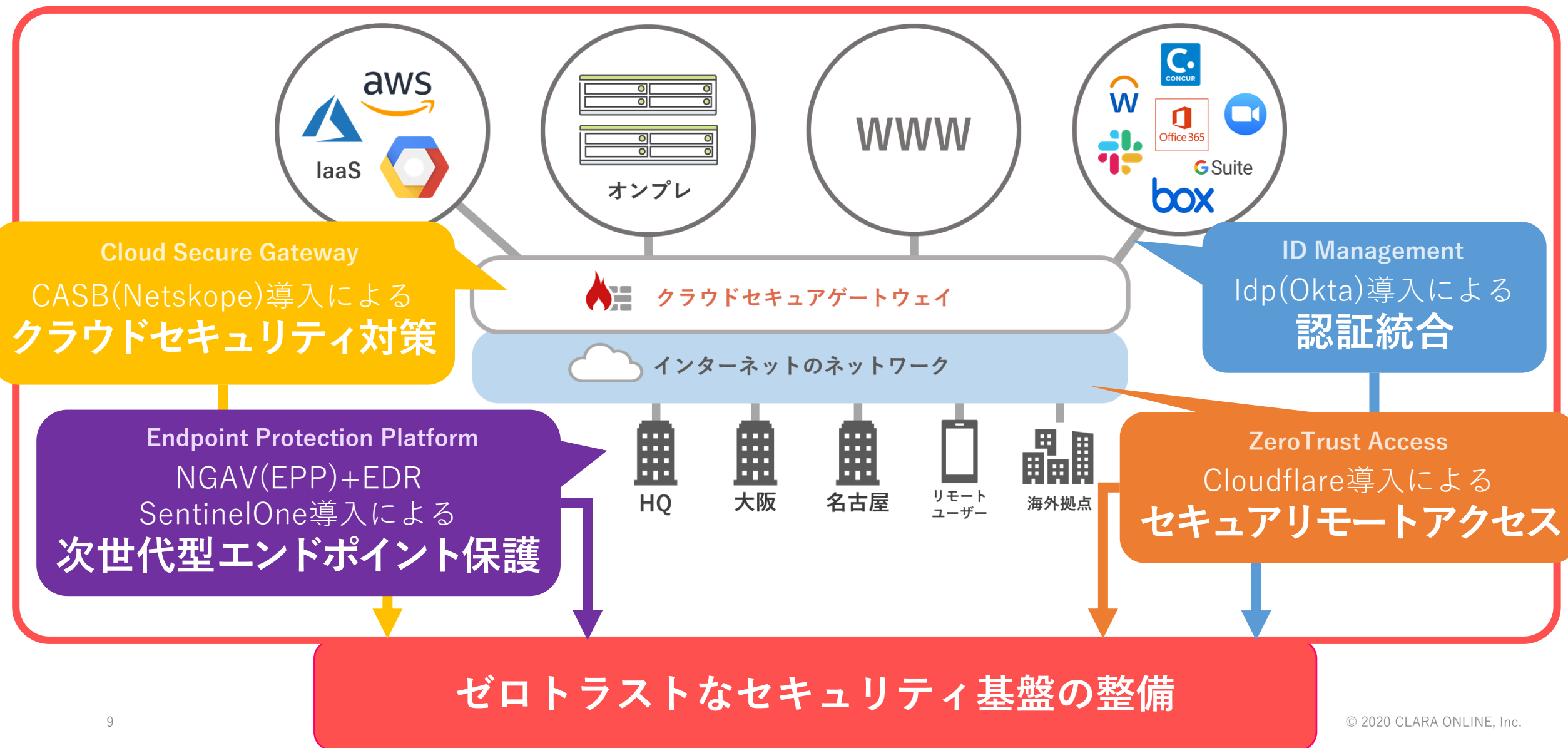
出典：「企業IT利活用動向追跡調査2020」調査結果 - JIPDEC／株式会社アイ・ティ・アール
<https://www.jipdec.or.jp/topics/news/20200924.html>

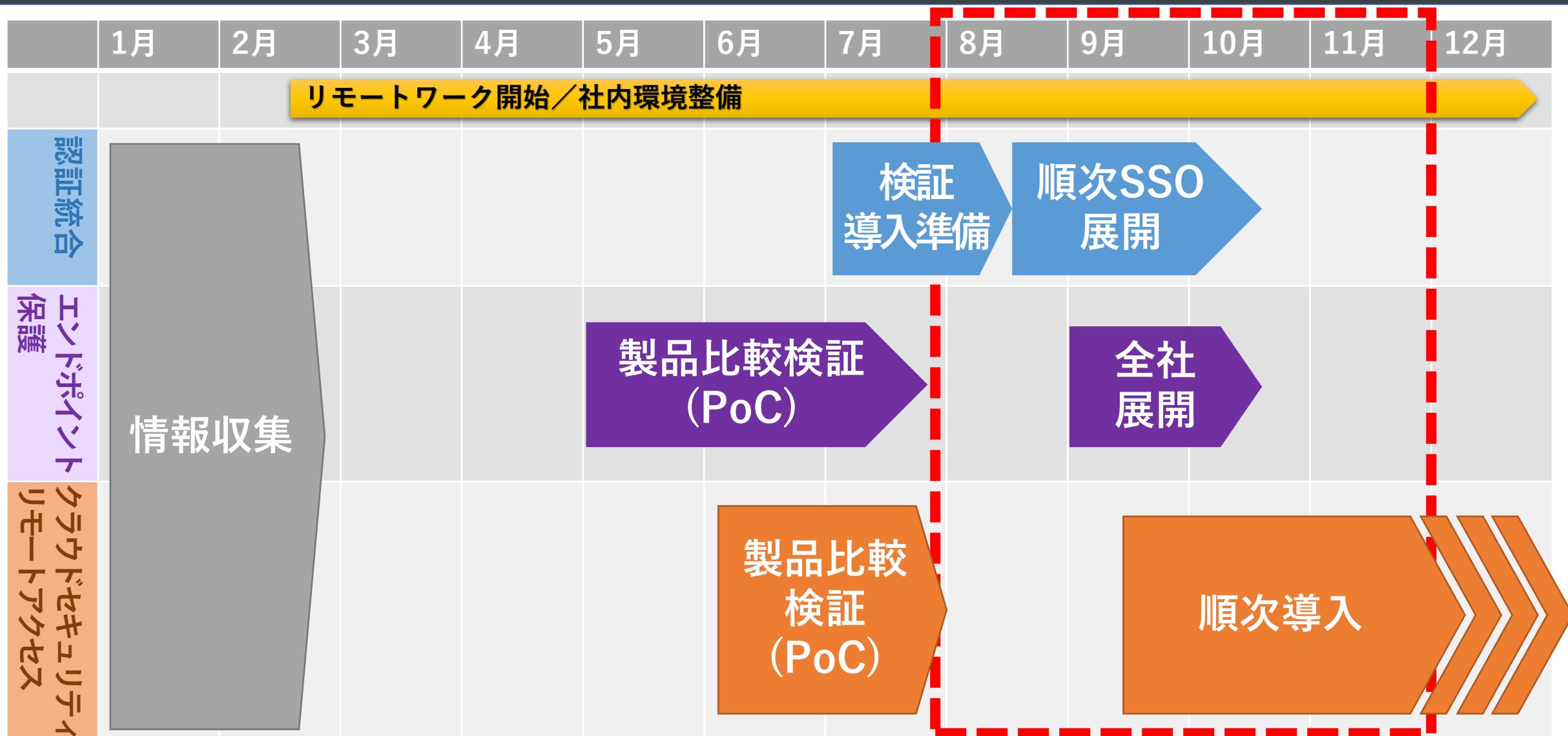


当社の取り組み



コーポレートITの活動が **事業サービスの強み、競争力** に
(自社の経験とノウハウをサービスに還元)





次世代型エンドポイント保護の 導入のポイント

課題意識

- 従来型の仕組みでは防ぎきれない現状
 - 攻撃の約8割が、未知のマルウェアやファイルレス攻撃
 - 攻撃を受け、感染する前提での環境整備の必要性
- **次世代環境(EDR)の運用コスト**
 - 高度なセキュリティスキル、人的リソース

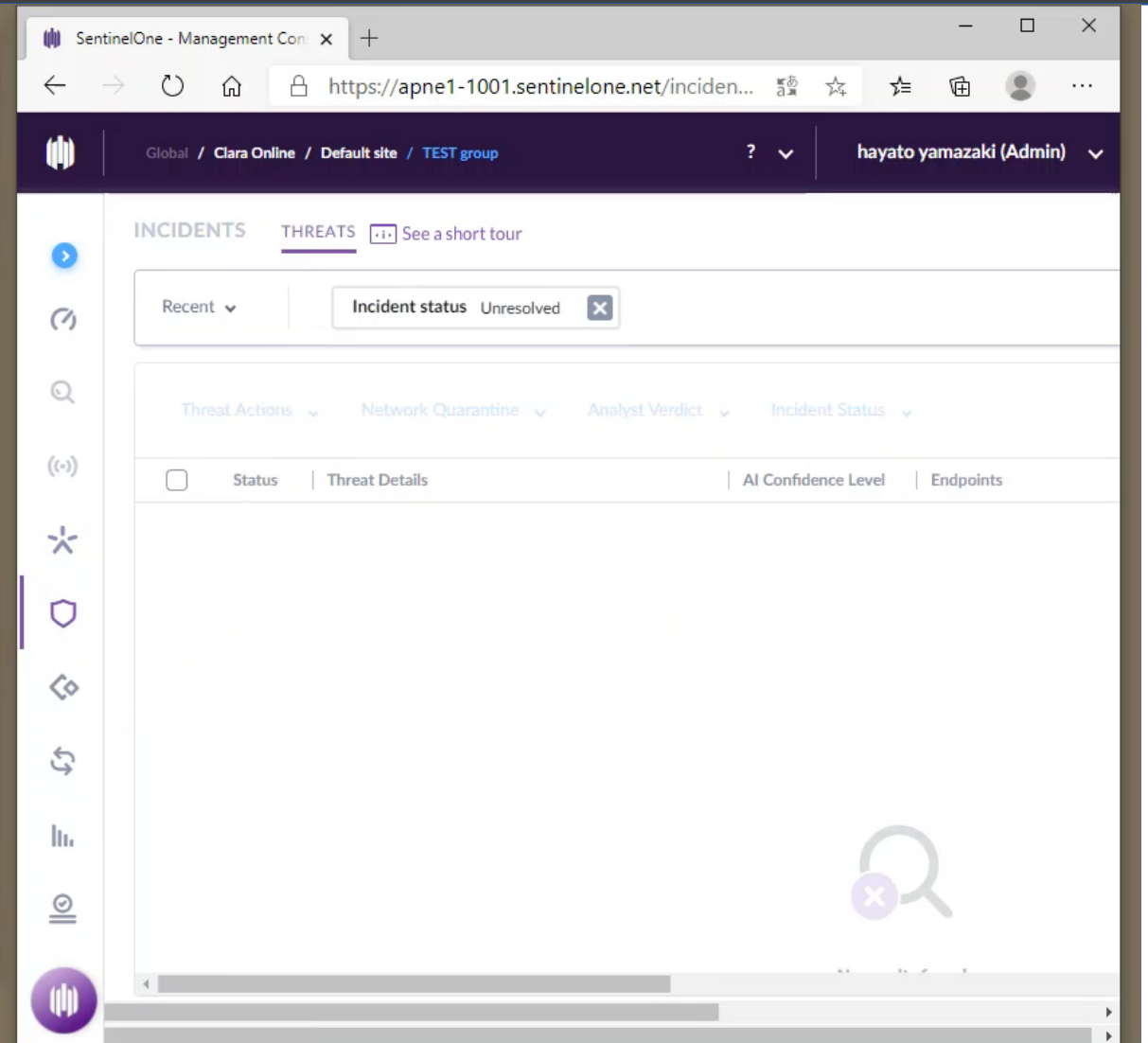
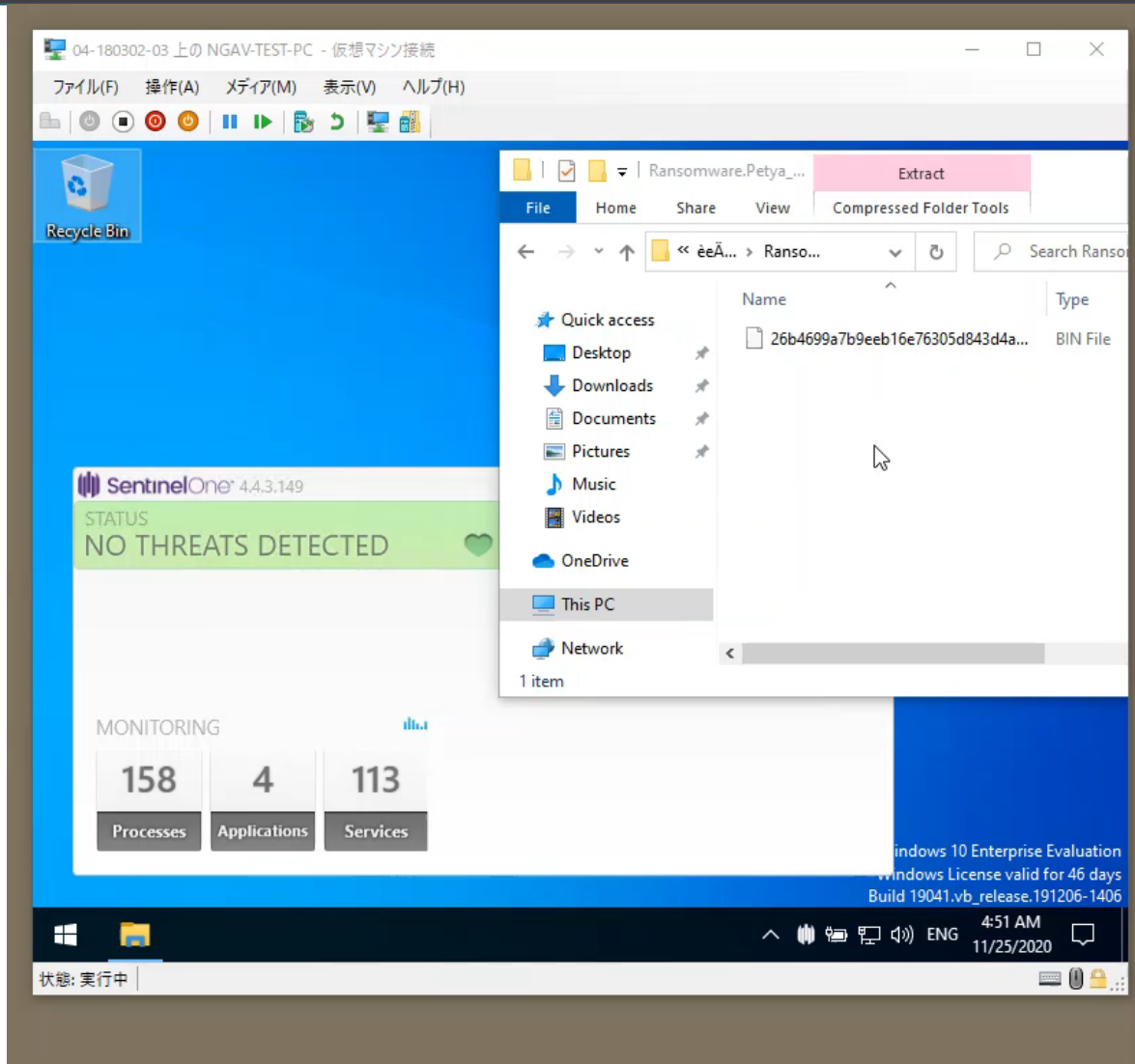
比較検討

- 従来型、次世代型より約10製品を比較
- 価格、機能、**運用、サポート品質**、カルチャー、など

1) 本物のウィルスを使い感染と対処

- スマホのテザリング接続したPCに仮想マシンを構築して検証
- ふるまい検知や、その時の自動防御の理解
- **実際に感染した際の対処方法の把握**

導入検証のコツ - 本物のウィルスを動作させる(自動防御)



1) 本物のウィルスを使い感染と対処

- スマホのテザリング接続したPCに仮想マシンを構築して検証
- ふるまい検知や、その時の自動防御の理解
- 実際に感染した際の対処方法の把握

2) 実業務の環境で検証

- 業務環境下での干渉問題の有無
- 誤検知(頻度)の体験と、検知内容や対処方法の把握

• 一般

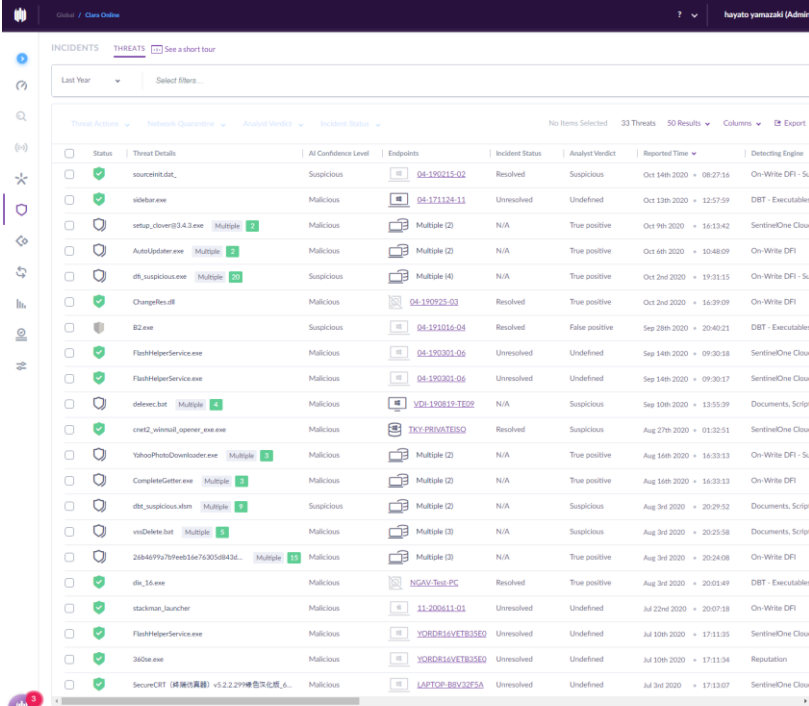
- Windowsデスクトップガジェット
- PCメーカーのプリインストールアプリ
- 広告系アプリ(e.g. JWord)

• エンジニア関連

- XAMPPに含まれるランチャーモジュール
- ハッシュファイルを変換するプログラム

• 中国関連

- 中華圏のセキュリティソフトウェア(e.g. 360)
- 国境を超える特殊なネットワーク系ソフトウェア
- 中華圏で取得されたFlashプレイヤー



The screenshot displays the 'THREATS' tab in the The Border interface. It shows a table of detected threats with columns for Status, Threat Details, AI Confidence Level, Endpoints, Incident Status, Analyst Verdict, Reported Time, and Detecting Engine. The table lists various threats such as 'sourceinit.dat', 'vulnar.exe', 'setup_clover@3.4.3.exe', 'AutoUpdater.exe', 'dft_suspicious.exe', 'Changefiles.dll', 'E2.exe', 'FlashHelperService.exe', 'FlashHelperService.exe', 'delvec.bat', 'cmd2_winnet_opener.exe', 'YahooPhotoDownloader.exe', 'CompleterGetter.exe', 'dft_suspicious.com', 'cmdDelete.bat', '20440P9z70red51e7a305d843d...', 'dlx_3d.exe', 'stackman_launcher', 'FlashHelperService.exe', '3dbox.exe', and 'SecureCRT (誤検出漢語) v5.2.2.2999绿色汉化版_6...'. Each entry includes a status icon (e.g., green checkmark for resolved, red X for unresolved), a threat name, an AI confidence level (e.g., Suspicious, Malicious), a list of endpoints, an incident status, an analyst verdict, a reported time, and the detecting engine (e.g., SentinelOne Cloud, DBT - Executables).

Status	Threat Details	AI Confidence Level	Endpoints	Incident Status	Analyst Verdict	Reported Time	Detecting Engine
Resolved	sourceinit.dat	Suspicious	04-190215-02	Resolved	Suspicious	Oct 14th 2020 + 08:27:56	On-Write DFI - Su
Unresolved	vulnar.exe	Malicious	04-171124-11	Unresolved	Undefined	Oct 13th 2020 + 12:57:59	DBT - Executables
True positive	setup_clover@3.4.3.exe	Malicious	Multiple (2)	N/A	True positive	Oct 9th 2020 + 16:13:42	SentinelOne Cloud
True positive	AutoUpdater.exe	Malicious	Multiple (2)	N/A	True positive	Oct 6th 2020 + 10:48:09	On-Write DFI
True positive	dft_suspicious.exe	Suspicious	Multiple (4)	N/A	True positive	Oct 2nd 2020 + 19:31:15	On-Write DFI - Su
Resolved	Changefiles.dll	Malicious	04-190723-03	Resolved	True positive	Oct 2nd 2020 + 16:39:09	On-Write DFI
Resolved	E2.exe	Suspicious	04-191016-04	Resolved	False positive	Sep 28th 2020 + 20:40:21	DBT - Executables
Unresolved	FlashHelperService.exe	Malicious	04-190301-06	Unresolved	Undefined	Sep 14th 2020 + 09:30:18	SentinelOne Cloud
Unresolved	FlashHelperService.exe	Malicious	04-190301-06	Unresolved	Undefined	Sep 14th 2020 + 09:30:17	SentinelOne Cloud
Suspicious	delvec.bat	Malicious	V01-190815-TE09	N/A	Suspicious	Sep 10th 2020 + 13:55:39	Documents, Script
Resolved	cmd2_winnet_opener.exe	Malicious	TKY-P00A7E5Q	Resolved	Suspicious	Aug 27th 2020 + 01:32:51	SentinelOne Cloud
True positive	YahooPhotoDownloader.exe	Malicious	Multiple (2)	N/A	True positive	Aug 16th 2020 + 16:33:13	On-Write DFI - Su
True positive	CompleterGetter.exe	Malicious	Multiple (2)	N/A	True positive	Aug 16th 2020 + 16:33:13	On-Write DFI
Suspicious	dft_suspicious.com	Suspicious	Multiple (2)	N/A	Suspicious	Aug 3rd 2020 + 20:29:52	Documents, Script
Suspicious	cmdDelete.bat	Malicious	Multiple (3)	N/A	Suspicious	Aug 3rd 2020 + 20:25:58	Documents, Script
True positive	20440P9z70red51e7a305d843d...	Malicious	Multiple (3)	N/A	True positive	Aug 3rd 2020 + 20:24:08	On-Write DFI
Resolved	dlx_3d.exe	Malicious	NGAV-Test-PC	Resolved	True positive	Aug 3rd 2020 + 20:01:49	DBT - Executables
Unresolved	stackman_launcher	Malicious	11-200611-01	Unresolved	Undefined	Jul 22nd 2020 + 20:07:18	On-Write DFI
Unresolved	FlashHelperService.exe	Malicious	YORD816VET8360	Unresolved	Undefined	Jul 10th 2020 + 17:11:35	SentinelOne Cloud
Unresolved	3dbox.exe	Malicious	YORD816VET8360	Unresolved	Undefined	Jul 10th 2020 + 17:11:34	Reputation
Unresolved	SecureCRT (誤検出漢語) v5.2.2.2999绿色汉化版_6...	Malicious	LAPTOP-BRV32F5A	Unresolved	Undefined	Jul 3rd 2020 + 17:13:07	SentinelOne Cloud

1) 本物のウィルスを使い感染と対処

2) 実業務の環境で検証

- 製品ごとの違いが明確になり、比較は容易
- 運用の負荷についても予めの想定が可能
(運用イメージを具体化)

自社の運用環境に適した製品を選定

1. 既存EDRの課題をクリア

効率的な運用、負荷の軽減

- 自律的(Autonomous)、能動的(Active)EDRとして**できる限りの自動化**
- 専門性の高い操作を減らし、脅威発生から対応までの**工数削減**

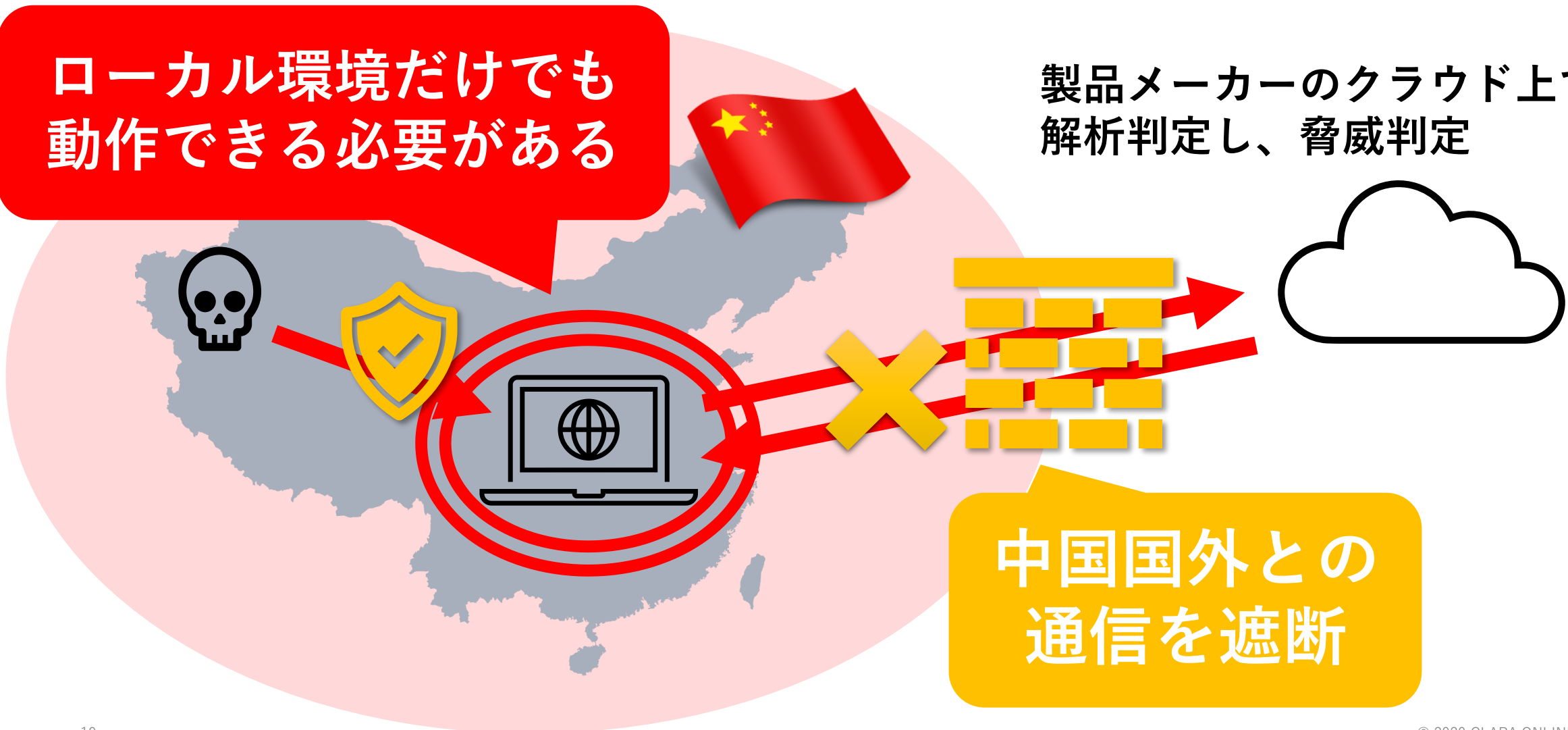
2. 次世代型の弱点をクリア

- **ディスクスキャン**によるウィルス隔離
- **オフラインでの動作**



ローカル環境だけでも
動作できる必要がある

製品メーカーのクラウド上で
解析判定し、脅威判定



• 既存EDRの課題をクリア

効率的な運用、負荷の軽減

- 自律的(Autonomous)、能動的(Active)EDRとして**できる限りの自動化**
- 専門性の高い操作を減らし、脅威発生から対応までの**工数削減**

• 次世代型の弱点をクリア

既存環境からの移行にスムーズ

- ディスクスキャンによるウィルス隔離
- オフラインでの動作



<https://www.clara.jp/wsi/>



WSI / Work
Style
Innovation

WSIとは？

ソリューション

プラン

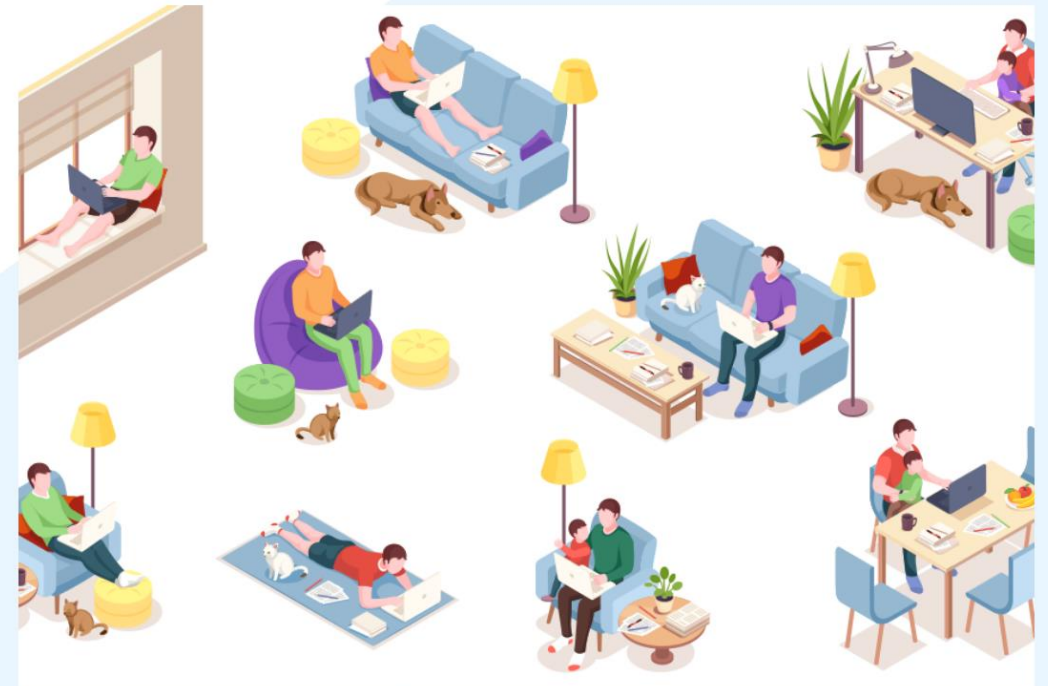
ゼロトラストとは

提供機能一覧 →

Work Style Innovation

ゼロトラストベースのセキュアなテレワーク環境を実現する
クラウド活用ソリューションをワンパッケージで提供しま
す。

30日間無料トライアル
お申し込み



SCROLL

The Border

ご視聴ありがとうございました

