



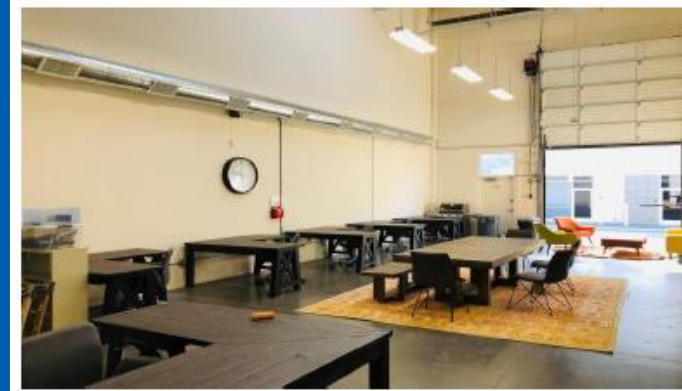
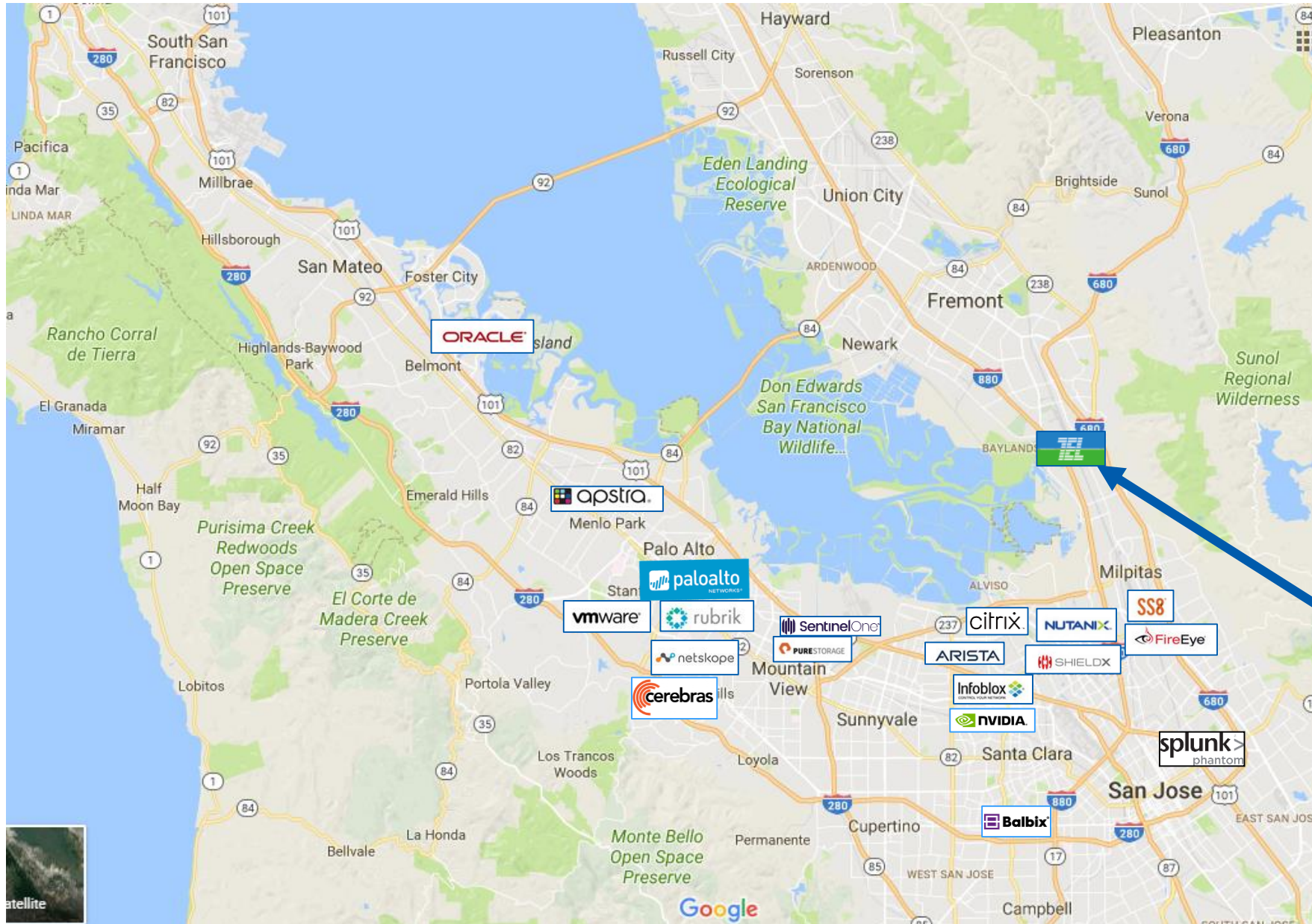
The Border2020

2020年12月
東京エレクトロン デバイス株式会社
クラウド技術部サイバーセキュリティ技術グループ
三吉 徹



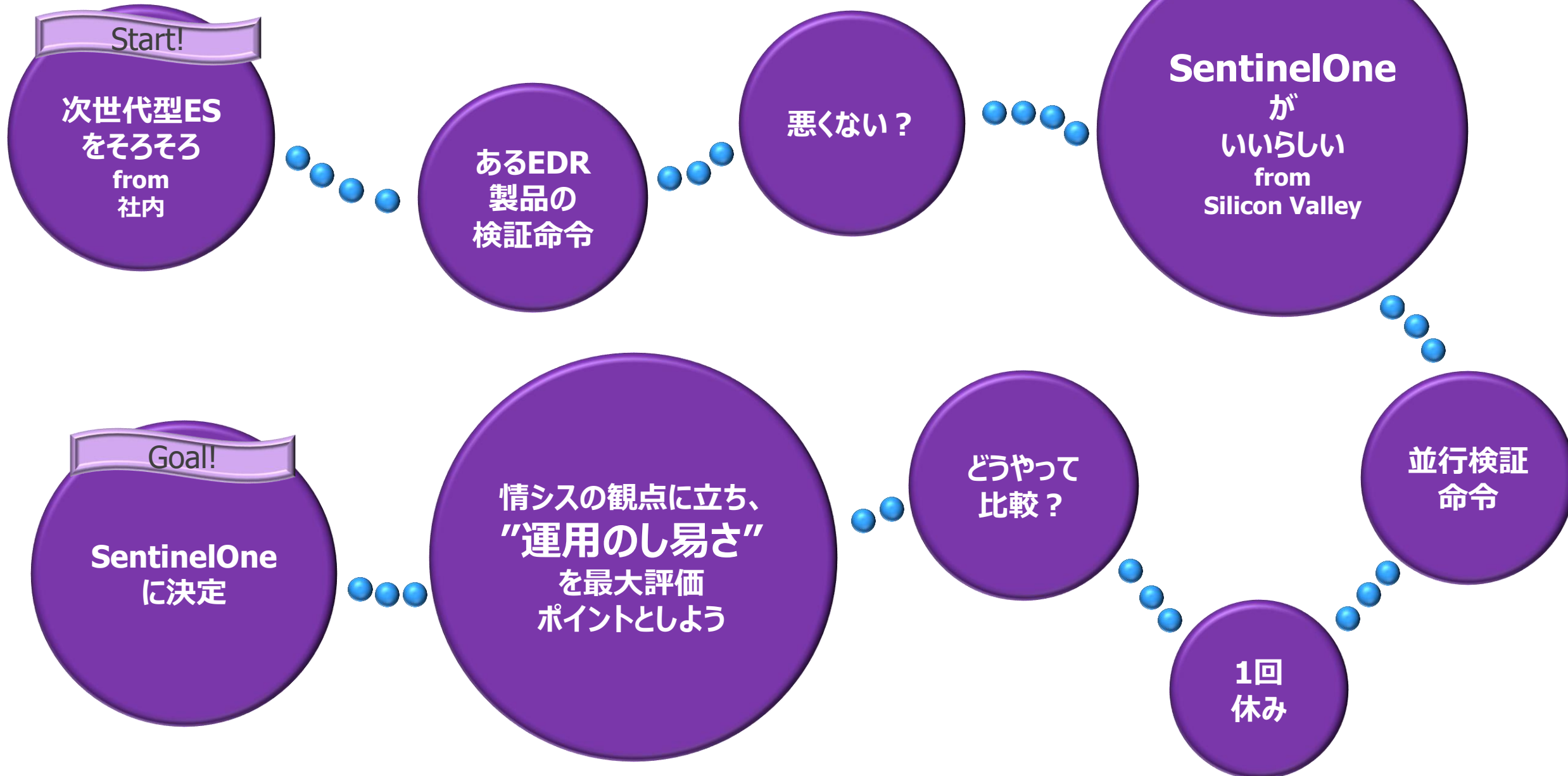
TED? / Why SentinelOne??

Tokyo Electron Device Americaにて情報収集

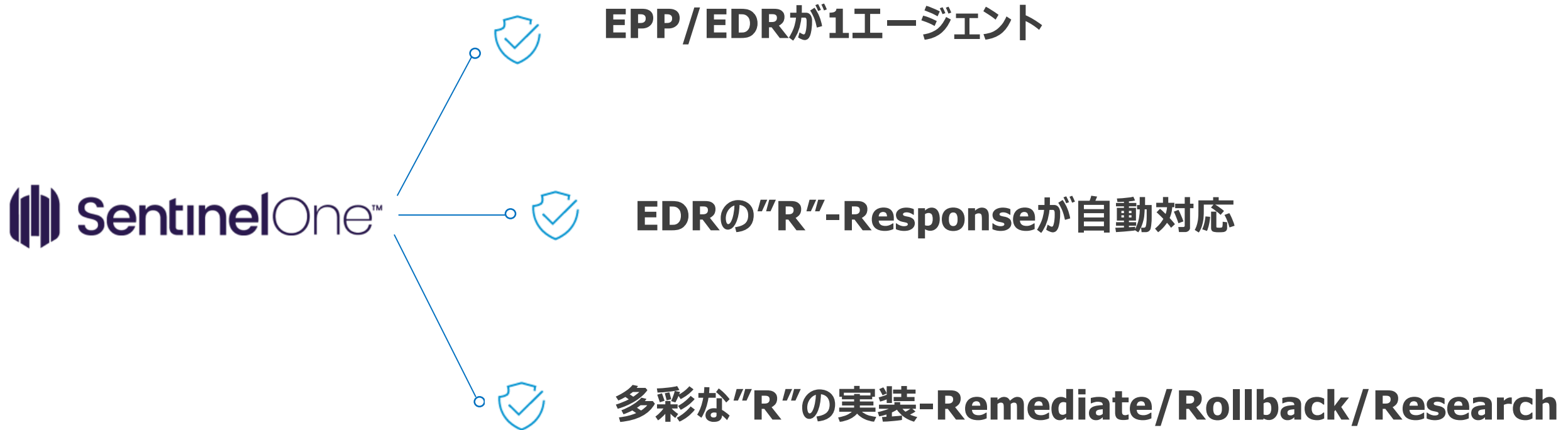


- 設立：2016年4月1日
- 所在地：Fremont, CA
- 従業員数：9名
- 資本金：\$300,000

TEDがSentinelOneを取り扱うに至った経緯



TEDがSentinelOneを取り扱う決め手になった要因



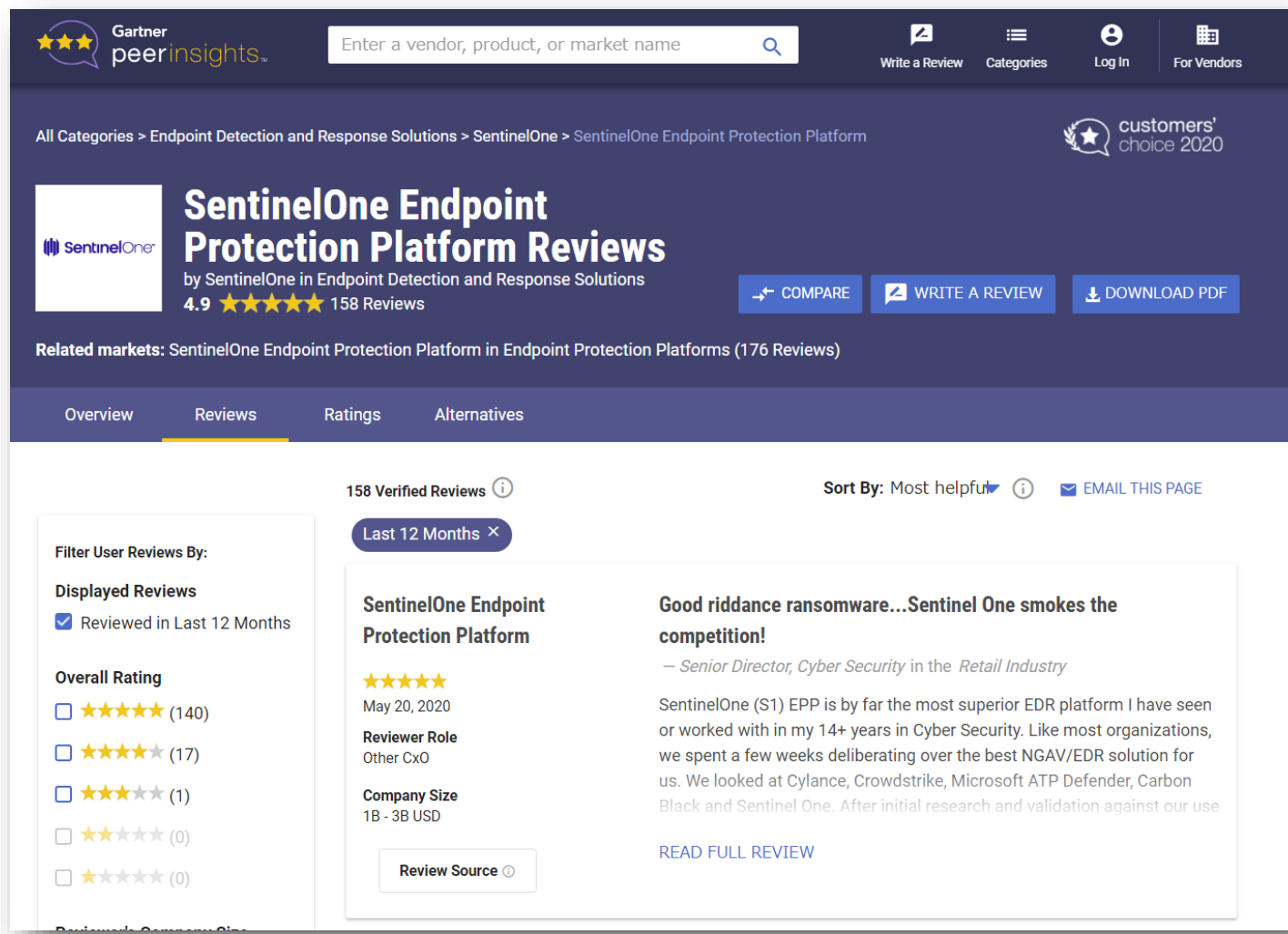
考えるプロセスを”極小化”出来るソリューション = 運用が楽に違いない、という確信



SentinelOneに対する第三者評価



“(SentinelOne) gives them the ability to do actual Security work instead of Administering an AV product for 90% of the time.”



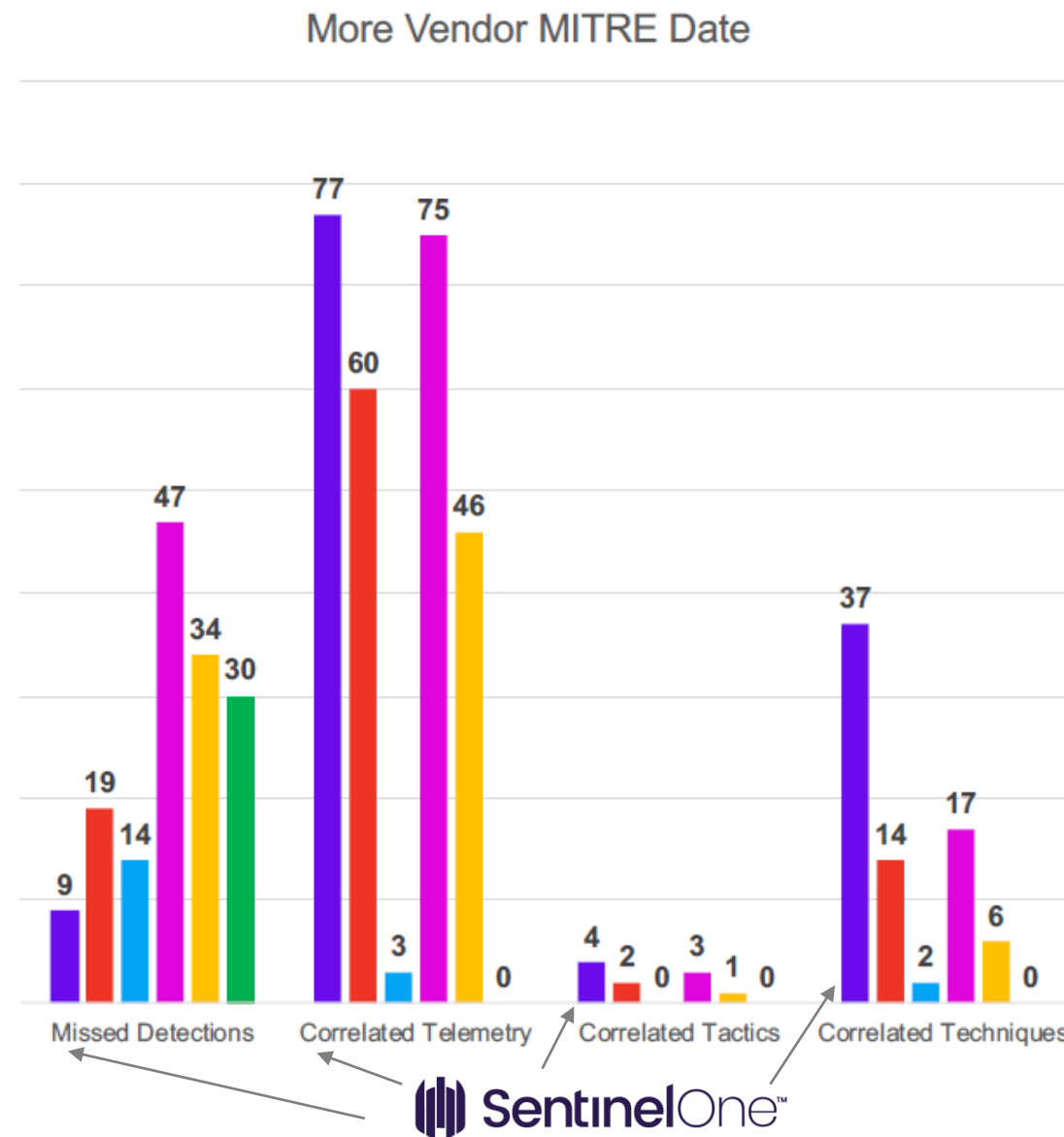
The screenshot shows the Gartner peer insights page for SentinelOne Endpoint Protection Platform. The page features a dark blue header with the Gartner peer insights logo, a search bar, and navigation links for 'Write a Review', 'Categories', 'Log In', and 'For Vendors'. Below the header, the breadcrumb trail reads: 'All Categories > Endpoint Detection and Response Solutions > SentinelOne > SentinelOne Endpoint Protection Platform'. A 'customers' choice 2020' badge is visible on the right. The main content area displays the product name 'SentinelOne Endpoint Protection Platform Reviews' with a 4.9 star rating and 158 reviews. Action buttons for 'COMPARE', 'WRITE A REVIEW', and 'DOWNLOAD PDF' are present. A 'Related markets' section indicates the product is in the 'Endpoint Protection Platforms' category with 176 reviews. A navigation bar at the bottom of the main content area includes 'Overview', 'Reviews' (selected), 'Ratings', and 'Alternatives'. The 'Reviews' section shows '158 Verified Reviews' and a 'Sort By: Most helpful' dropdown. A filter for 'Reviewed in Last 12 Months' is active. A list of star ratings is provided: 5 stars (140), 4 stars (17), 3 stars (1), 2 stars (0), and 1 star (0). A sample review is displayed, titled 'Good riddance ransomware...Sentinel One smokes the competition!' by a Senior Director in the Retail Industry, dated May 20, 2020. The reviewer's role is 'Other CxO' and their company size is '1B - 3B USD'. A 'Review Source' link is also visible.

運用負荷軽減に関するコメントが多数見受けられる

引用元: <https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions/vendor/sentinelone/product/sentinelone-endpoint-protection-platform/reviews>

MITRE ATT&CK Evaluations

- ✓ APT29(別名:The Dukes)の攻撃手法をエミュレートしてEPP/EDR製品をテスト
- ✓ SentinelOneが最も詳細に検知
 - ✓ Missed→未検知数(9)
 - ✓ Telemetry→痕跡のログ保存(77)
 - ✓ Tactics→検知理由として攻撃フェーズを表示(4)
 - ✓ Techniques→検知理由として攻撃フェーズ並びに攻撃手法を表示(37)
- ✓ 運用に叶っていることが客観的にも証明



引用元：SentinelOne社資料 "MITRE ATT&CK Round 2 - SentinelOne results v2.1.pdf"

東京エレクトロン デバイス



運用に関するエピソード

Registration form fields:

- First Name: *
- Last Name: *
- Business Email: *
- Company Name
- Phone Number: *
- Employee Range: Select...
- Country: * (Select... dropdown)
- Submit button

By clicking Submit, I agree to the use of my personal data in accordance with the Privacy Policy. SentinelOne will not sell, trade, lease, or rent your personal data to third parties.

東京エレクトロン デバイス株式会社

製品情報 | ソリューション | 導入事例 | セミナー | ホワイトペーパー | 技術サポート

SentinelOne Remote Work Program (リモートワーク支援プログラム)

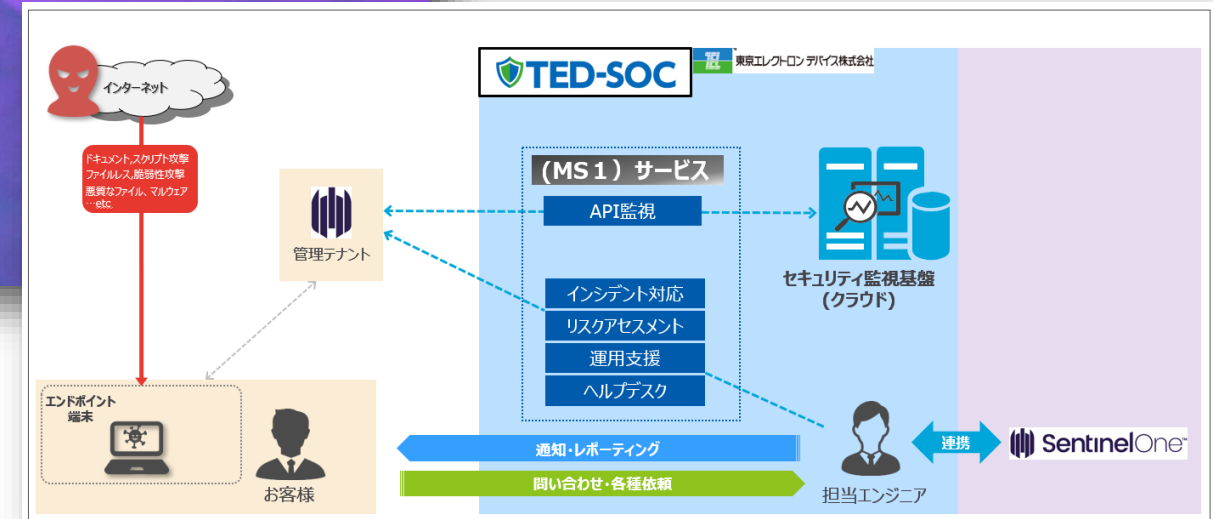
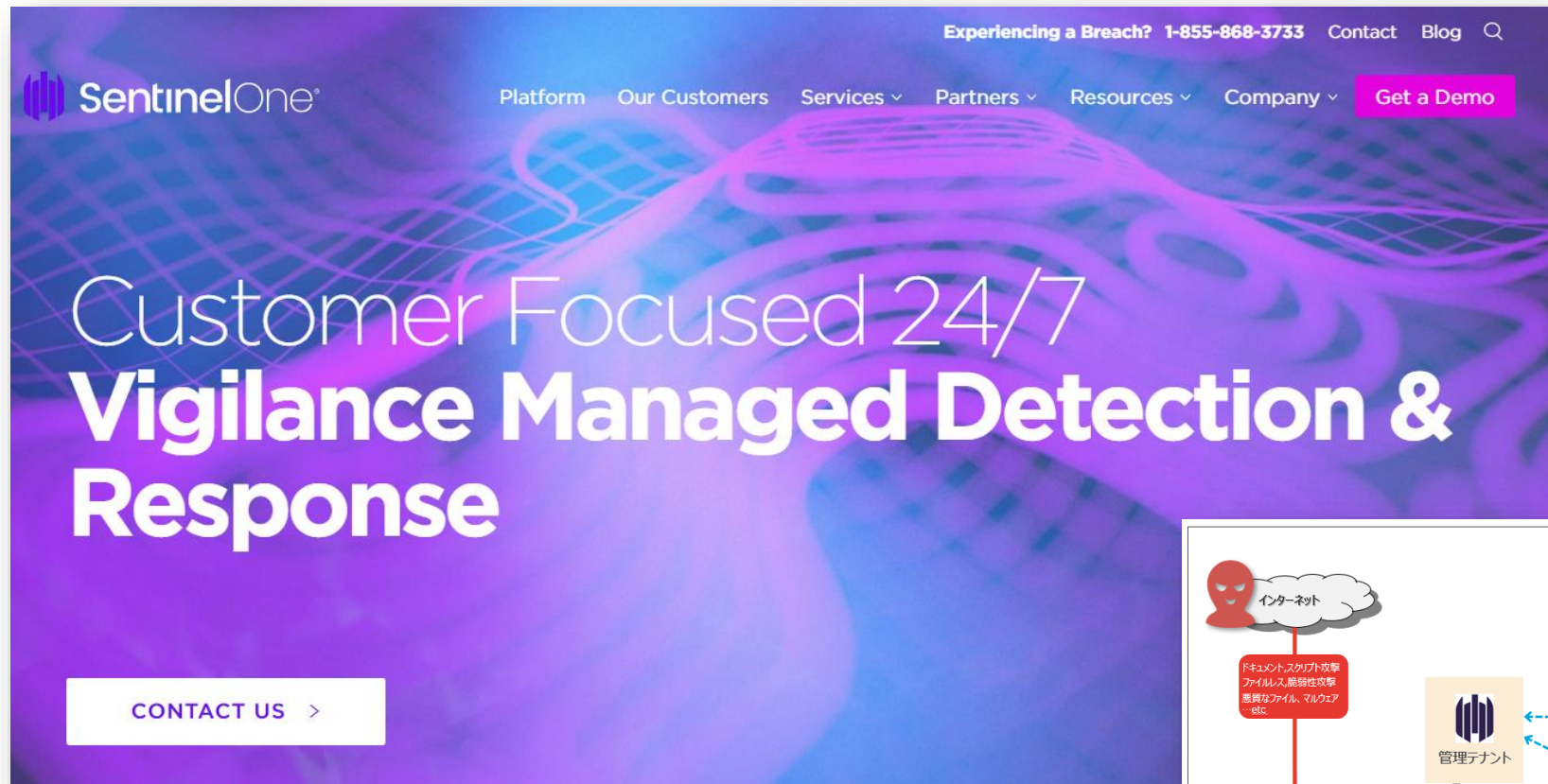
EPP/EDRベンダーのSentinelOneは、コロナウイルス（COVID-19）の感染拡大防止に配慮したテレワークを支援するため、自律型エンドポイントセキュリティ製品「SentinelOne Endpoint Protection Platform」のライセンスを期間限定で無償にて提供する「Remote Work Program（リモートワーク支援プログラム）」を提供しています。

SentinelOneの国内販売代理店である東京エレクトロンデバイスはこの活動に賛同し、お客様企業のキャンペーン登録を支援いたします。

SentinelOne Remote Work Program (リモートワーク支援プログラム)	
適用期間	2020年10月1日～2021年1月31日
お申込対象	テレワークを推進する企業・団体の情報セキュリティ担当者（個人従業員の方からの申し込みはご遠慮ください）
お申込み方法	社名、担当者名、連絡先、従業員数（規模）等 必要事項を下記フォームにて入力・お申し込み

素早く展開出来、必ずしもSOCを必要としないSentinelOneならではのキャンペーン

SOC-MDR(Managed Detection & Response)の採用率



SOC採用率はWorldwideで10%弱、Japanで21%。他は全て自社運用



クララオンライン様へのご紹介に際して



“Good PoC is Good Deal.
Let’s use real malware!”

JARED PHIPPS
VP Worldwide Sales Engineering
ex US Air Force - MITRE

実際に存在するマルウェアファイルを検査検体としてご提供

クララオンライン様へのご支援(2)評価項目表のご提供

■ SentinelOne PoC 実施項目一覧表

9	静的検知/防御	シグネチャマッチングによる既知のマルウェアファイルの検知、隔離ができる
10		ファイル構造解析によるマルウェアファイルの実行前検知、隔離ができる
11		端末がオフライン状態の場合も、シグネチャマッチング・ファイル構造解析によるマルウェアファイルの検知、隔離ができる
12	動的検知/防御	動的解析エンジンにより、悪意ある挙動(Powershellによるファイルレス攻撃など)の検知、防御ができる
13		端末がオフライン状態の場合も、動的解析エンジンにより悪意ある挙動の検知、防御ができる
14	軽減	管理画面より、端末のネットワーク隔離ができる
15		マルウェア検知時に、感染端末をポリシーにて自動的に隔離処理ができる
16		隔離したファイルに対して、隔離解除やダウンロード操作ができる
17		ハッシュ値を利用したブラックリスト登録ができる
18		静的エンジンに対するホホワイトリスト登録ができる (ハッシュ、証明書、拡張子)
19		動的エンジンに対するホホワイトリスト登録ができる (パス指定、ブラウザ)
20	修復	マルウェア感染時に一時作成されたファイル、改変されたレジストリキー等を元の状態に修復できる
21		ランサムウェアに暗号化された感染端末内のファイルを復旧できる
22		管理画面より、隔離していた端末のネットワーク復帰ができる
23		実行されたコマンドラインの内容が確認できる
24		別プロセスへのインジェクション状況の確認ができる
25		プロセスが実行したディスク、レジストリ上の書き込み/読み込みの確認ができる
26		プロセスが実行したネットワークオペレーション (DNS、IPアドレス) の確認ができる
27		静的エンジンでの検知理由が確認ができる

運用面を重視したPoC評価項目のご提示



ロジカルな選定プロセス→迅速な意思決定



企業風土さえも評価対象-カルチャーフィット



全てリモート(非対面)で完遂-製品紹介からPoC、ご発注まで



今後の展開 with クララオンライン様



東京エレクトロン デバイス



Withコロナ/Afterコロナ- リモートワークへの訴求



一人情シスのお客様(特にSMB)へ寄り添う



来年もTheBorderに参加！？



SentinelOneに続く新規ソリューションのご提案・協業



共に創る 新たな価値を



東京エレクトロン デバイス