株式会社アンドパッド 様

マルチOS環境でのエンドポイント脅威を統合管理 EPP+EDR でセキュリティレベルの向上と運用しやすい UX が魅力の SentinelOne

建築・建設現場向けの施工管理ソリューションを提供している株式会社アンドパッドでは、ビジネスの拡大に応じて社員数が増えるなか、Windows や MacOS などマルチ OS で展開しているエンドポイントのセキュリティを強化するべく、SentinelOne Endpoint Protection Platform（以下、SentinelOne）を導入。エンドポイントセキュリティにおける統合管理を可能にし、脅威の可視化によってセキュアな環境整備を実現しています。

情報システム部　高橋 洋平 氏　　情報システム部　部長 青木 勝則 氏

検知率の低いシグニチャベースの仕組みだけでは経営的なリスクが回避できない

「幸せを築く人を、幸せに。」をミッションに掲げ、2014 年 4 月に設立された株式会社アンドパッド。建築・建設現場における円滑な情報共有を支援するクラウド型の施工管理アプリ「ANDPAD」を提供しており、ユーザー数は 14 万人、現場で利用している企業は 5 万社を超えるまでに事業を拡大させています。施工現場に必要な図面や工程表をアプリ上で共有でき、チャットアプリによって電話や FAX が主体だった現場のコミュニケーションを円滑化するなど、施工現場の効率化から経営改善まで一元管理できる仕組みとして重宝されています。

そんな同社では、以前から業務に利用するエンドポイントに対してシグニチャベースの EPP を導入していましたが、Windows や MacOS などマルチ OS 環境だったことで、それぞれ個別最適化された対策が中心でした。しかし、事業拡大に応じてメンバーが増えるなか、マルチ OS 環境でも統合的に管理できる環境が求められていたのです。

「統合管理できていなかったことで、実際の検知状況などがすぐに可視化できる状況にはありませんでした。パターンマッチングに頼ったシグニチャベースの仕組みでは検知率の面で限界があるため、経営的なリスクとしてセキュリティに関する課題意識を以前から持っていたのです」（青木氏）。

検知精度に関するユーザー評価が高く、運用しやすい UX が大きな魅力に

そこで、エンドポイント環境のセキュリティ強化に向けて、新たな環境づくりに着手することに。そこで求められたのは、マルチ OS であっても統合的に管理できるものを前提に、シグニチャだけでなく振る舞いによってインシデントが検知でき、対策が実施できる環境づくりでした。

「セキュリティレベルの向上は第一の優先事項でしたが、部内の業務効率化も考慮し、管理画面のスムーズな遷移やインシデント検知の状況把握がしやすい、運用性の高いものが必要でした。また、NGAV や EDR を中心とした新しいテクノロジーを検討したため、第三

ANDPAD

会 社 名：株式会社アンドパッド
従業員数：173名（2020年5月1日時点）
導入済エンドポイント数：数百台
所 在 地：〒101-0022
東京都千代田区神田練塀町300
住友不動産秋葉原駅前ビル8階
他合計4拠点
U R L：andpad.co.jp

導入前の課題

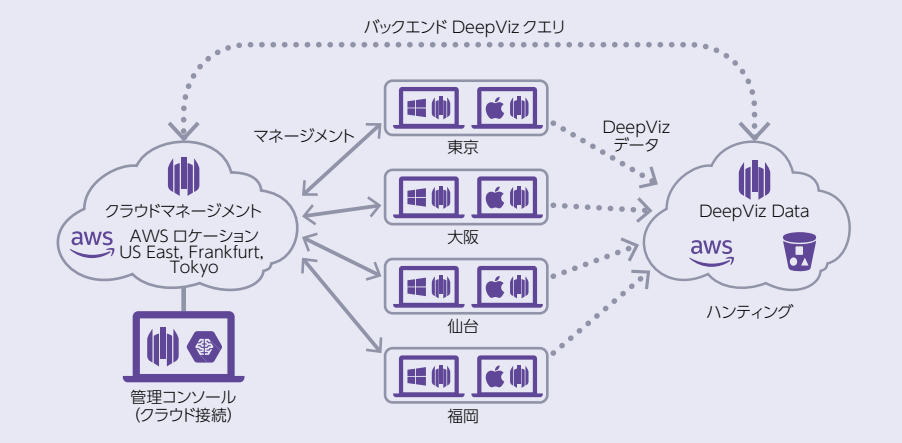
+ マルチ OS 環境のために個別最適化された形でしか運用できていない
+ 統合管理できておらず、状況の可視化が不十分
+ 検知率の低いシグニチャベースの EPP では経営リスクを回避できない

ソリューションの利点

+ マルチ OS での統合管理が可能、EPP と EDR 双方の機能を併せ持っている
+ 運用しやすい UX
+ 第三者機関の調査でユーザー評価が高い
+ MITRE ATT&CK の結果から検知率の高さを実感

導入後の効果

+ 検討開始から PoC を経てわずか 4 か月で展開できた
+ 統合管理が可能なだけでなく、運用
+ 負荷が上がらない環境を整備
+ 状況の可視化が可能になり、担当者の安心感醸成に貢献



者評価を中心に検知精度が優れているものを希望したのです」（青木氏）。

そこで注目したのが、調査会社が行った EDR 関連のレポートにおいてユーザー評価の高かった SentinelOne でした。実際の検知率については、サイバー攻撃のライフサイクルに基づくフレームワークとして著名な「MITRE ATT&CK」の結果から、その能力を高く評価したのです。

「ユーザー評価で初めて SentinelOne を知ったのですが、海外製品ではあるもののユーザーからの評価が非常に高いことが分かりました。そこで検討候補の 1 つに加えたのです」（高橋氏）。

そんな折、コロナ禍においてラインセスの貸与が発表されたことで、使い勝手を確認するべく PoC を実施することに。一部の部署にも展開してみたところ、端末の負荷増大もなく、動きも安定している環境で、セキュリティ対策ができると好評だったのです。

「管理者の立場では、設定をグループごとにバインドさせる作業がしやすく、ダッシュボードから脅威判定された情報へアクセスしやすいなど、直感的な操作性が備わっており、非常に運用しやすいものでした。情報システム部の業務ボリュームを考慮すると運用では手離れのいいものが必要不可欠で、まさに我々に最適だと考えたのです」（高橋氏）。

PoC の段階から Web 会議での定例ミーティングにて情報がやり取りできるなど、サポート体制についても安心感が得られた点が大きいと高橋氏。機能面でもランサムウェア対策用のロールバックといったユニークな機能が備わっていたことで、将来的な活用の幅も広がると判断。結果として、新たなエンドポイント対策の仕組みとして、EPP と EDR 双方の機能を併せ持った SentinelOne が同社のセキュリティ強化策として採用されたのです。

統合的な管理で エンドポイント対策を強化、 可視化によって安心感が得られる

既存環境のリスクからいち早く脱却するべく、検討開始から PoC を経てわずか 4 か月で SentinelOne の展開をスタート、現在では開発用の検証機を含めて全社員が使う数百台の PC にエージェントを導入しており、検知を中心に運用を行っています。

「導入して間もない状況ですが、順調に検知が行われており、アラートがあれば私がダッシュボードから確認しています。運用負荷が上がらない状況で統合管理できるのは、現状のリソースを考えると大きな効果の 1 つです」（高橋氏）。

新たな環境を整備したことで、マルチ OS 環境であっても統合的に可視化できるようになり、リスク軽減につながっていると評価します。

「以前は正直何が起きているのか把握が難しく、見えていないことが何よりも怖かった。最近では Emotet のようなマルウェアが話題になっていましたが、今なら自社にどの程度脅威があったのか、実際に感染していないかどうかが迅速に把握できるため、セキュリティ担当者として安心感が得られています」（青木氏）。

今後については、現状検知を中心とした運用から、実際の対応まで含めて範囲を広げていきながら、セキュリティ関連業務のさらなる省力化につなげていきたい考えです。また、クラウド上に蓄積された振る舞いに関するログを活用し、脅威ハンティングといったさらなるセキュリティ強化策にも活用していきたいと語ります。

「SIEM のような統合ログ管理の仕組みを導入し、SentinelOne のログも含めて状況把握の迅速化に役立てながら、ログから新たな示唆が得られるような環境づくりも進めていきたい」（青木氏）。

SentinelOne Japan株式会社

〒103-0027
東京都中央区日本橋2-1-3
アーバンネット日本橋2丁目ビル10F
https://jp.sentinelone.com
sales-japan@sentinelone.com