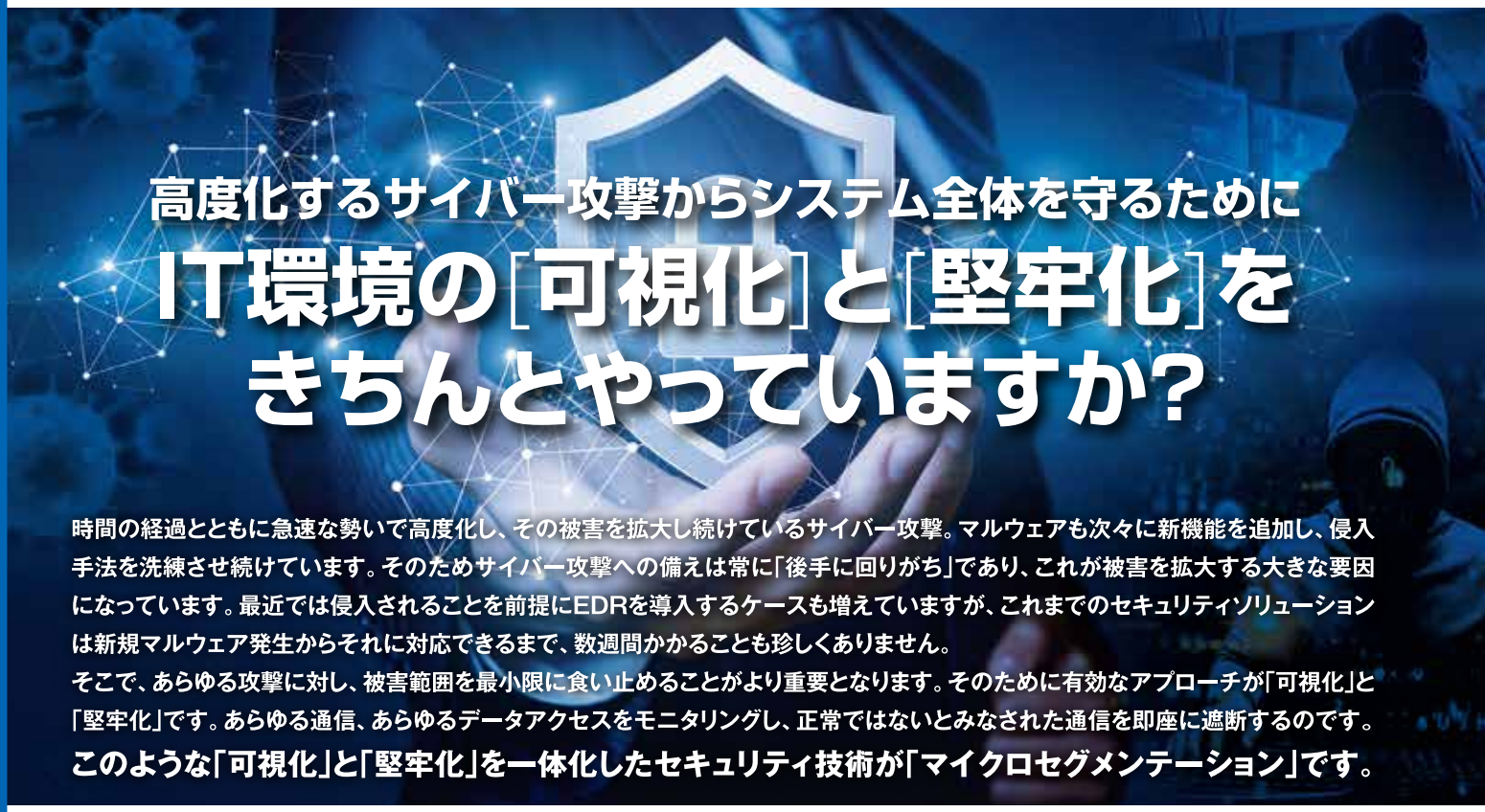
illumio

デジタルテクノロジー株式会社



高度化するサイバー攻撃からシステム全体を守るために

IT環境の[可視化]と[堅牢化]をきちんとやっていますか?

時間の経過とともに急速な勢いで高度化し、その被害を拡大し続けているサイバー攻撃。マルウェアも次々に新機能を追加し、侵入手法を洗練させ続けています。そのためサイバー攻撃への備えは常に「後手に回りがち」であり、これが被害を拡大する大きな要因になっています。最近では侵入されることを前提にEDRを導入するケースも増えていますが、これまでのセキュリティソリューションは新規マルウェア発生からそれに対応できるまで、数週間かかることも珍しくありません。

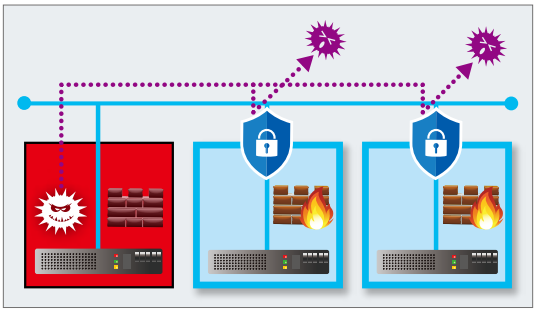
そこで、あらゆる攻撃に対し、被害範囲を最小限に食い止めることがより重要となります。そのために有効なアプローチが「可視化」と「堅牢化」です。あらゆる通信、あらゆるデータアクセスをモニタリングし、正常ではないとみなされた通信を即座に遮断するのです。

このような「可視化」と「堅牢化」を一体化したセキュリティ技術が「マイクロセグメンテーション」です。

マイクロセグメンテーション技術を使って効果がある主なセキュリティ脅威

通信をきめ細かい単位で監視・制御する
マイクロセグメンテーション

マイクロセグメンテーションとは、近年大きな注目を集めるようになった、ネットワークセキュリティ技術の1つ。インターネットと内部ネットワークのように、ネットワークセグメントの間にファイアウォールなどを設置してセキュリティ制御を行う手法を「ネットワークセグメンテーション」と言いますが、これをマシン単位、アプリケーション単位で行うのがマイクロセグメンテーションです。これにより、特定のマシンやアプリケーションがマルウェアに感染しても、その影響を他のマシンやアプリケーションに及ぼさない環境を実現できます。



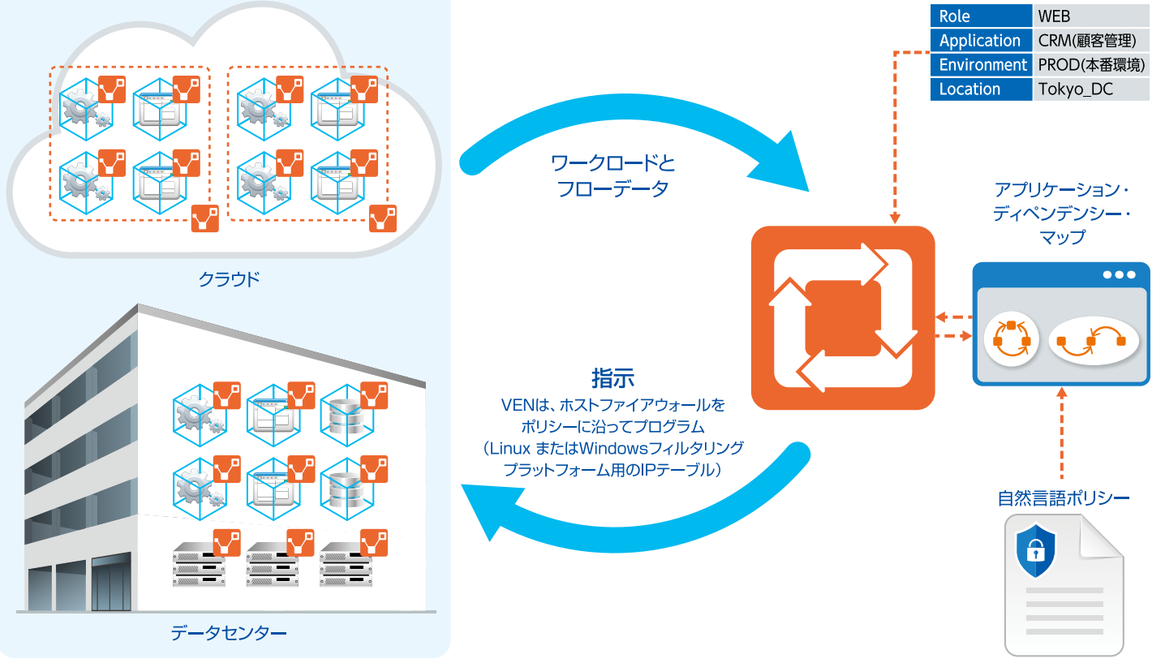
マイクロセグメンテーションの技術はすでに確立されており、Windows OSやVMwareの仮想ネットワークなどに実装されています。しかしこれらは設定が煩雑で、特定のOSや仮想環境に利用範囲が限定される、という問題がありました。このままではマイクロセグメンテーションのポテンシャルを引き出すことは困難です。できるだけシンプルに設定・管理を行うことができ、しかも幅広い環境に適用できることが求められます。

これを実現しているのが「Illumio」です。

4種類のタグ+ポリシーで設定・管理をシンプル化。

データセンターからクラウド、コンテナ環境までカバーします。

Illumioは、データセンターやクラウドで発生するワークロードやデータフローのデータを収集し、あらかじめ決められたポリシーに従って、データセンターやクラウド内に実装された仮想ファイアウォールなどに通信遮断などの指示を行います。そのためにデータセンターやクラウドの各マシン/アプリケーションには、アンテナの役割を果たすVirtual Environment Node(VEN)を実装。これらのアンテナから送られるデータをPolicy Compute Engine(PCE)で収集し、ポリシーに基づいた指示をPCEからVENへと発行する、というコアアーキテクチャとなっています。



Virtual Enforcement Node(VEN)
アンテナのような役割

Policy Compute Engine(PCE)
セントラルブレインのような役割

Illumioの特徴 1 4種類のタグとポリシーで設定をシンプル化

Illumioの最大の特徴は、わずか4種類のタグでマシンやアプリケーションの属性を定義し、それに基づいたポリシーを設定するだけで利用できる点にあります。管理者は個々のマシンやアプリケーションに対して、個別の設定を行う必要がありません。そのため膨大な数のマイクロセグメンテーションの設定を、極めてシンプルに実施できるようになります。

Illumioの特徴 2 マシン間/アプリ間の通信をすべて可視化

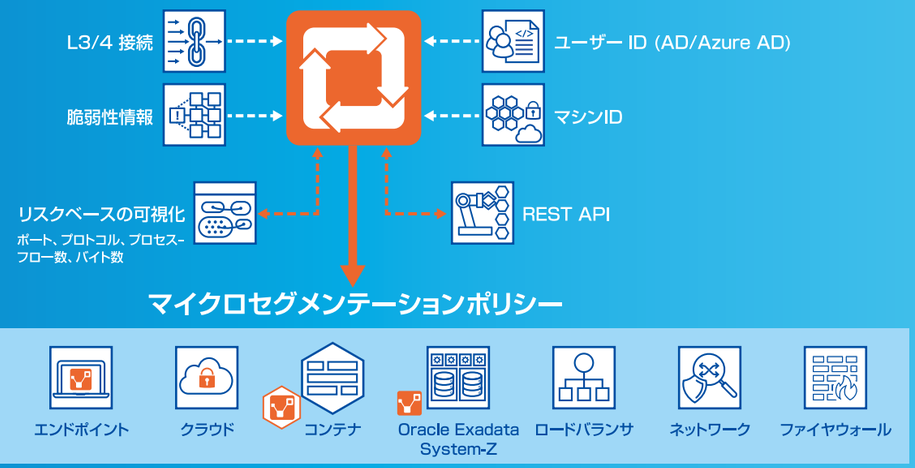
VENによって収集された通信の情報は、Illumioのダッシュボード上で可視化されます。これを見ることで、どこからどこへの通信がどれだけ行われているのかが、直感的に把握できるようになっています。また通信経路を意味する画面上の「ライン」をクリックすることで、その詳細な通信状況を確認することも可能です。

Illumioの特徴 3 漏れのない通信ポリシーの適用が容易

通信の制御を行う場合には、通信元ノードと通信先ノードの属性タグを選択し、どのような通信制御を行うかを選択するだけで設定が完了。各ノードの名称が変更された場合や、ノードが追加された場合でも、これらのノードに適切なタグを設定しておくことで、通信制御のポリシーが自動的に適用されます。そのためポリシーを漏れなく適用することが容易になります。

Illumioの特徴 4 幅広いカバレッジ

Illumioは特定のOSや仮想マシンだけではなく、様々なエンドポイントやアプリケーション、クラウド環境、コンテナ環境など、幅広いカバレッジを持っています。そのためマルチクラウド環境・ハイブリッドクラウド環境でも、一貫性のあるポリシーでマイクロセグメンテーションを運用できます。



Illumioをお勧めしたいお客様

デジタルテクノロジーは、以下のようなお客様にIllumioをお勧めします。

タイプ1 IT環境の可視化と最低限の「緊急対応能力」を確保したいお客様

将来に向けたセキュリティ戦略を明確化していくには、IT環境全体を可視化し、そこに存在するリスクや課題を理解しなければなりません。また、いつ襲いかかってくるかわからないランサムウェアなどに対処するには、最低限の緊急対応能力も不可欠です。このような「可視化と堅牢化への第一歩」を踏み出したいお客様にとって、Illumioは極めて有効な選択肢となります。

タイプ2 重要システムを優先的に短期間で堅牢化したいお客様

IT環境の中には、侵害されると事業継続に大きな影響を与えるシステムもあれば、そうでないシステムもあります。これらのうち、侵害の影響が大きいミッションクリティカルなシステムやアプリケーションを明確にし、それらに関連する通信を可視化・精査するとともに、最小限の権限のみ設定したいというお客様もいらっしゃいます。Illumioならこのようなニーズに対しても、短期間で対応できます。

タイプ3 重要システムを中心に長期計画でIT環境全体の堅牢化を図りたいお客様

IT環境の堅牢性を継続的に維持・向上させていくには、長期的な計画にもとづいた取り組みも求められます。このような長期戦略を立案し、その実現を着実に推進したいお客様にとっても、Illumioの活用は大きな効果をもたらします。これによって常にIT環境全体を可視化し、継続的にポリシーを改善していくことで、最新のサイバー攻撃への高い耐性を確保できるようになります。

Illumioの導入・活用はデジタルテクノロジーにご相談ください。

デジタルテクノロジーは、Illumioの特徴や活用方法を熟知しており、その知見にもとづくサポートを提供しています。また検討段階におけるコンサルティングから、初期導入に必要な各種作業、運用フェーズにおける監視・設定に至るまでを一貫して支援。Illumioの導入・活用は、ぜひデジタルテクノロジーにご相談ください。

デジタルテクノロジー株式会社

https://www.dtc.co.jp/

[東京] 〒104-0032 東京都中央区八丁堀 2-23-1 エンパイヤビル
MAIL：sales@dtc.co.jp

[大阪] 〒530-0001 大阪市北区梅田1-13-1
大阪梅田ツインタワーズ・サウス 15F
MAIL：osaka@dtc.co.jp

2024.02