政府機関向け ゼロトラストセキュリティモデルの

導入ガイド

クラウドとリモートワークの時代の
セキュリティ戦略

splunk>
turn data into doing™

日本政府に求められるゼロトラスト「常時診断・対応型のセキュリティアーキテクチャ」

政府においては、コロナ禍の中、国民からの様々な期待の高まりを受けるとともに、デジタル庁設立、リモートワーク導入、クラウド導入、DX推進など大きな変化要求・変化要因があります。さらに、攻撃者の戦術・技術の進展は目覚ましく脅威度は高まっており、特に自組織の変化部分については新しい脅威にさらされるようになりました。また、ウクライナ情勢による緊張の高まり、ランサムウエアによる工場停止、また内部犯行による情報漏洩といった最近の事案にも注目が集まっています。

技術面の変化としては、ゼロトラストというキャッチフレーズを聞く機会が増えました。ゼロトラストは非常に簡単に言えば、「確認・検証していないものを信じるな。まずは確認・検証しよう。」という考え方です。外から入ってくるデータも、従業員の行いも確認が必要です。（なお、ゼロトラストの格式ある定義は本レポート内にありますのでご参照ください。）

では、その「確認・検証」は具体的にどうするのか。日本政府はサイバーセキュリティ戦略（2021年7月）において常時診断・対応型のセキュリティアーキテクチャの導入を可能なところから率先して導入を進める方針を掲げています。この常時診断・対応型のセキュリティアーキテクチャと原点となっているのが米国政府で採用されるCDMアーキテクチャです。CDMにおいては、まず、自組織の人（アカウント）及びモノ（ハード・ソフト）をきちんと検証します。承認された人（アカウント）だけが承認されたモノ（ハード・ソフト）を利用できる環境を確保します。そこからさらにセキュリティを固めるとともに、リアルタイム監視・対処を行います。米政府の基準では、全システムを72時間以内に点検することになっていますが、CDMを実装すれば難しい要求ではありません。

また、CDMは、様々な企業の優れた製品・サービスを組み合わせるアーキテクチャです。一社単独のセキュリティ製品ではないというのは、官公庁に向いていると言えます。また、現在のセキュリティ市場には、資産管理ソフト、マルウェア対策ソフト、多要素認証ソフトなど、様々な企業の優れたセキュリティ製品があふれています。自組織の状況に合わせた最高の製品を組み合わせられることは性能面・コスト面で優れたメリットとなります。

Splunkは、CDMにおいて様々な製品を有機的に統合するため重要な役割を果たしています。各種製品のログを相関分析しやすい状態でデータを蓄積することで、CDMを構成する様々な機能を一元的に管理し、システム全体のリアルタイムでの監視・分析を可能にします。

本レポート「政府におけるゼロトラストセキュリティモデルの手引き」は、「A Guide to Embracing a Zero Trust Security Model in Government」の抄訳です。政府のゼロトラスト導入にあたって参考となる情報が多く含まれています。本レポートが我が国のセキュリティ強化の一助になれば幸いです。

Splunk Services Japan合同会社
公共政策統括部長 **仲間　力**

政府機関は現在、大規模なデジタルトランスフォーメーションの真っただ中にあります。クラウド、モバイル、マイクロサービスをはじめとするテクノロジーの進歩がもたらす変革は、政府機関の以下のような取り組みを後押しします。

- 企業のように効率的なサービス提供
- 増大するミッションクリティカルな要求への対応
- 市場の期待への対応とさらなる効率化

その結果としてリモートワークが可能になり、政府機関の職員と関係者が場所や時間を問わず、組織のアプリケーションやサービスにアクセスできるようになります。

デジタルトランスフォーメーションとクラウド移行により政府機関が得られるメリットは、効率、俊敏性、利用者の満足など、多数あります。しかし一方で、これまでに一定の安全性が認識されているオンプレミス型システムの外へ大切なデータを移動することにもなります。これは、従来型セキュリティの要として機能してきた「組織とインターネットを隔てる境界」が消えることにつながります。

また、この変革により、サイバー脅威に新たな攻撃経路が開かれ、攻撃にさらされる範囲が広がります。こうした脅威に係る懸念と、クラウド移行に際して予想される課題は、政府機関における移行と最新ツールの導入を遅らせており、政府機関がいまだ多くのレガシーシステムを運用している大きな理由の1つです。

バイデン政権は、サイバーインシデントへの準備及び対応の改善を指示する「国家サイバーセキュリティ改善に関する大統領命令(EO)」を発行しました。

この大統領令を受けたメモランダムOMB M-21-31では、省庁に対して、政府プロセスにおけるハイレベルな要求を設定し、義務化しています。本メモランダムには、組織全体におけるログ管理の成熟度を4段階に区分したイベントログ管理成熟度モデルと、省庁の成熟度が各段階に達するまでの期限が示されています。イベントログ管理成熟度モデルでは、段階が上がるごとに高度化して多くのデータソースと長期間の保持が求められるようになり、最終的にはビジネス分析機能およびセキュリティのオーケストレーションと自動化(SOAR)機能が必要になります。

このような状況に対応するには、どうすればよいのでしょうか?懸念や課題はあるものの、もう先送りにはできません。連邦政府機関はセキュリティ運用を刷新し、ネットワークを強化し、利用できる専門技術を活用することで、新たなサイバー攻撃に対処するための情報と体制を整える必要があります。

新型コロナウイルスにより
新たな時代への対応を迫られる政府機関

パンデミックが契機となり、多くの政府機関では変革への取り組みが加速しています。一夜にして、政府職員はリモートワークを余儀なくされ、既存のキャパシティしかないIT部門やセキュリティ部門には多大な負荷がかかっています。

政府機関は一般に、VPNソリューションを利用して組織へのリモートアクセスを管理し、セキュリティ体制を維持しています。しかしVPNソリューションは、リモートワークロードの爆発的な増加を想定して設計されていないため、拡張して対応することが困難です。

さらに、この急激な変化によって、政府機関はこれまでにないセキュリティ脅威にさらされることにもなりました。これまで政府機関が利用してきたツールは古いタイプの「多層防御」アプローチを採用するものが大半であり、このアプローチでは、組織を守るために組織の境界を定義することが必要となります。しかし、パンデミックによって働き方が急激に変わったことで、このような従来型のアプローチではもはやサイバーセキュリティに対応しきれなくなっています。

これまでのアプローチでは、いったん脅威がネットワークに侵入し、境界が破られてしまえば、ハッカーはそこにある脆弱性を悪用することができます。アクセス権限を手に入れ、ネットワーク内を縦横無尽に移動し、ネットワークに接続するシステムに侵入して資産を侵害できるため、甚大な被害につながる可能性があります。

クラウドへ移行するとユーザーのアクセスは境界の外に移動することになり、このことがデータの可視性や制御、セキュリティの確保について新たな課題を政府機関に突きつけます。

ネットワーク上のデバイスと、そこからアクセスできるデータは、それ自体を保護する必要があります。従来のように境界に頼るのではなく、保護と認証はデバイスレベルとユーザーレベルで継続的に適用しなければなりません。

それらの課題に加え、脅威や敵の背景を考慮すると、政府機関は、すでに侵害を受けたという前提に立って自組織を守るために必要な手段を講じていかなければなりません。

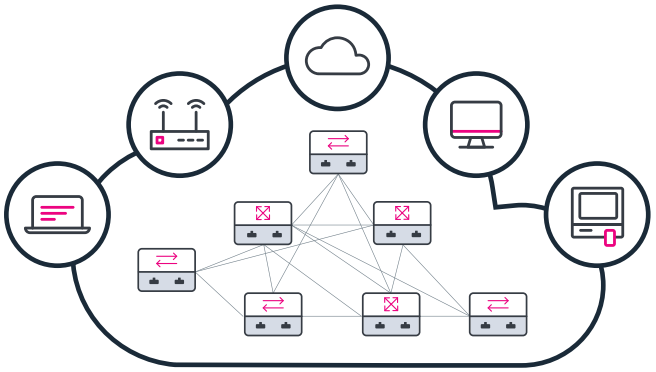
そして、この考え方に立つのであれば、アクセス権を与えられたユーザー、デバイス、サービスは、たとえそれが既知の承認されたデバイスやユーザーであっても、すべて潜在的に悪意があると見なす必要があります。

さらに、データと一口に言ってもその価値はさまざまです。組織を守ろうと格闘する中で、セキュリティチームが必ず気づくことが 1 つあります。それは、すべての資産を同じレベルで保護することは不可能であり、またそうする必要もないということです。組織の境界が消え、データが組織の壁の外へと移行する中、本当に意味のある効果的なセキュリティ対策を行っていくには、まず、各データの機密性と重要度を正確に評価することが不可欠です。

こうした課題に取り組むことなく、単にクラウドへ移行したり、インフラの最新化を図ったりするだけでは、政府機関のキャパシティおよびセキュリティに実のある成果をもたらすことはできません。そのようなやり方では、資産を適切に保護することができず、技術の進化がもたらす潜在的なメリットを実際に活用することはできないでしょう。

新型コロナウイルスの時代とその先を生き抜くには、境界を前提とするセキュリティ戦略の先を見通すことのできる、先進的なアプローチが必要なのです。

従来のネットワーク



セキュリティに対する新しいアプローチ：Trust No One（信頼しない）

政府機関のデータやシステムの保護を改善する可能性のあるセキュリティアプローチの1つが、**ゼロトラスト**と呼ばれる概念です。

ゼロトラストは、境界ベースの保護のみに依存する状態を解消することで、セキュリティを強化します。ゼロトラストでは、ネットワークセキュリティへの依存度が実質的に下がり、代わりにエンドポイントやバックエンドアプリケーションを保護します。

これにより、一定の信頼が確保され、リモートオフィスの安全性に対する不安がある程度解消します。また、職員が自分のデバイスにダウンロードした機密性の高い業務データを誤って失ってしまうといった「データ漏えい」のリスクも軽減します。

このアプローチでは、保護と認証をトランザクションごとにデバイスレベルおよびユーザーレベルで常に実施し、継続的な適応認証を徹底します。

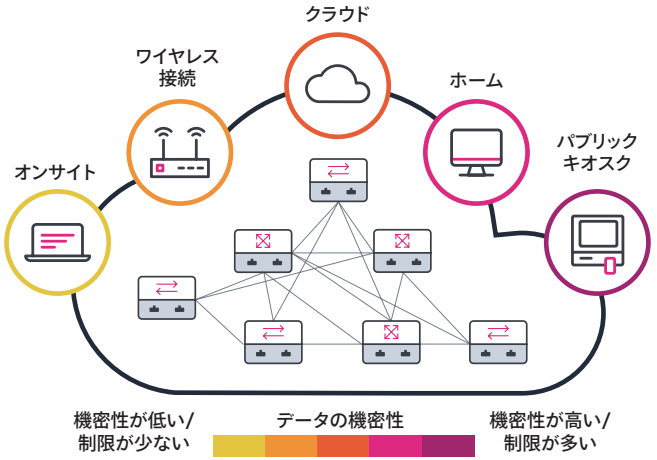
実際にどのようになるのか、簡単な例で説明しましょう。管理対象デバイスから、組織のケース管理システムにアクセスする職員がいるとします。この職員にはアクセス権が付与されています。

しばらくしてこの職員は、仕事に役立つと考えて、あるWebサイトからドライバをダウンロードします。すると、職員のデバイスはゼロトラスト戦略で継続的に監視されているため、組織のシステムへのアクセス権が取り消されます。このデバイスには現在、未知のコンポーネントがあり、組織のリソースに対するリスクが高くなっているからです。

この例からわかるとおり、ゼロトラスト戦略では、職員のアクセス権がITチームの管理するデバイスに関連付けられます。さらに、個人デバイスから機密情報へのアクセスについては、組織のリスクへの許容度に応じて、禁止されるか、少なくとも情報量が制限されます。

Forrester社のレポートは、今組織が置かれている状況を次のように表現しています。「私たちは、すでに侵害されているのにそのことに気づいていないだけ、という前提に立たなければなりません。これは、現在のように悪意に満ちた環境では必要な考え方です。検証しなくとも信頼するという方法では、不意を突かれ、危機管理に追われることになります。ゼロトラストは厳しすぎるように聞こえるかもしれませんが、重要なミッションを果たす素地を整える、プロアクティブで構造的なアプローチなのです」

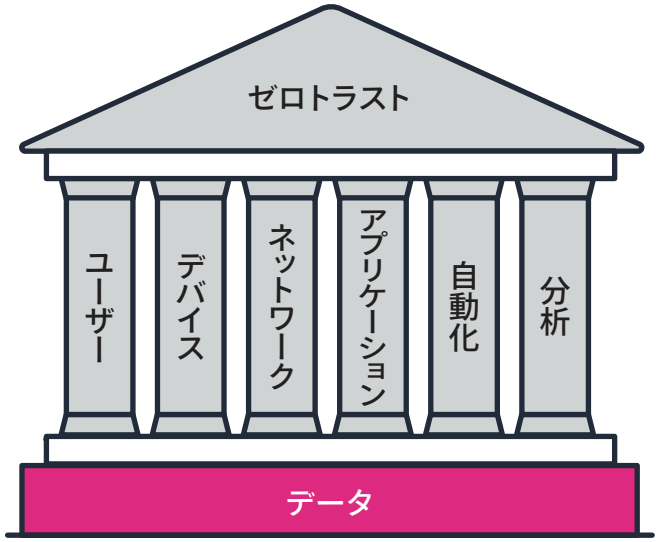
Forrester社はゼロトラストを「組織とブランドを守る最善の方法」とも述べています。



ゼロトラストモデルの構築

ゼロトラストモデルは、新型コロナウイルスが世界的に流行している現在、そしてその収束後も含めて組織を保護する有効なアプローチとして、業界およびセキュリティのエキスパートの間で認められています。

たとえばACT-IACは、ゼロトラストについて「戦略的なイニシアチブと考えることができる。系統立ったフレームワークと組み合わせることで、意思決定者とセキュリティリーダーは実用的かつ効果的にセキュリティを実装できる」と述べています。



出典：Zero Trust Cybersecurity Current Trends、2019年4月18日、ACT-IAC

ACT-IACは、データという基盤上に構築されたゼロトラストセキュリティモデルには6つの柱があるとしています。その内容を大まかにまとめると、次のようになります。

ユーザー	信頼済みのユーザーを継続的に認証し、ユーザーの信頼性を継続的に監視、確認して、アクセスと権限を管理する。
デバイス	デバイスのサイバーセキュリティ対策と信頼性をリアルタイムで評価する。
ネットワーク	ネットワーク(ソフトウェア定義のネットワーク、ソフトウェア定義の広域ネットワーク、インターネットベースの技術を含む)をセグメント化、分離、制御できる。
アプリケーション	アプリケーションレイヤー、コンテナ、仮想マシンを保護し、適切に管理する。
自動化	SOAR(セキュリティのオーケストレーションと自動化によるレスポンス)によって、いくつもの製品にまたがるタスクをワークフローで自動化し、エンドユーザーをインタラクティブに監督する。
分析	セキュリティエキスパートが、SIEM(セキュリティ情報/イベント管理)、高度なセキュリティ分析プラットフォーム、UEBA(ユーザーとエンティティの行動分析)など、可視化や分析を可能にするツールを利用して、起こっていることを観測し、状況をインテリジェントに判断して、防御を実行できる。

ゼロトラストセキュリティプログラムを成功させるための必須要件：

- ネットワークには常に悪意が潜んでいると見なす。
- ネットワークには常に外部および内部からの脅威があるものとする。
- ネットワークローカリティが示す場所だけでは信頼性を判断してはならない。
- あらゆるデバイス、ユーザー、ネットワークフローの認証と許可を必須とする。
- ポリシーは動的で、かつできるだけ多くのデータソースから導き出すものとする。
- さまざまな条件と属性に基づいて、アクセスを要求しているエンティティのリスクスコアを動的に算出でき、一連の情報によって常に信頼が確保される。

同様に、NISTも、ゼロトラスト戦略の実装を成功させるための独自のガイドラインを打ち出しています。

- すべてのデータソースとコンピューティングサービスは、リソースと見なす必要がある。
- すべての通信は、ネットワークの場所に関係なく保護しなければならない。
- 個々の組織リソースへのアクセスは、セッション単位で許可する。
- リソースへのアクセスは、動的なポリシーによって判断される。動的なポリシーとは、クライアント識別、アプリケーション、及び要求中の資産についての観測状態が含まれる。その他の振る舞い属性を含めてもよい。
- 保有デバイスと関連デバイスがすべて可能な限り安全な状態にあることを徹底する。資産の監視を行い、それらを可能な限り安全な状態に保つ。
- あらゆるリソースで、認証と許可を動的かつ厳密に行ってからアクセスを許可する。
- 組織は、ネットワークインフラと通信の現状について、できるだけ多くの情報を収集し、集めた情報をセキュリティ対策の改善に活用する。

出典：Zero trust cybersecurity current trends、ACT-IAC、2019年4月

ここに取り上げたすべてのレポートから浮かび上がるのは、組織のサイバーセキュリティに対する考え方が自然に進化した結果、ネットワークの防御と静的な境界に焦点を当てた防御ベースのアプローチから、ユーザー、資産、利用可能なリソースに焦点を当てるゼロトラストへの移行が起きている現状です。とりわけ新型コロナウイルス時代の今、世界中でゼロトラストへの移行が避けられなくなっています。

ゼロトラストアプローチによって成果を上げるには、その基盤となる組織全体のデータの活用に注力すること、そしてあらゆるデータがセキュリティに関わる、と理解することが重要です。データを監視および保護した上で防衛範囲を拡大し、デバイス、インフラ、ユーザーなど、すべての資産を対象にすることができます。

従来	これから
静的、境界ベース	資産、ユーザー、リソースの保護
境界内を全面的に信頼	侵害されていることが前提/継続的に評価
許可されるとネットワークに接続できる	許可されるとリソースに接続できる
製品/ツールベース	「組織全体」でのアプローチ

Splunkとゼロトラストモデル

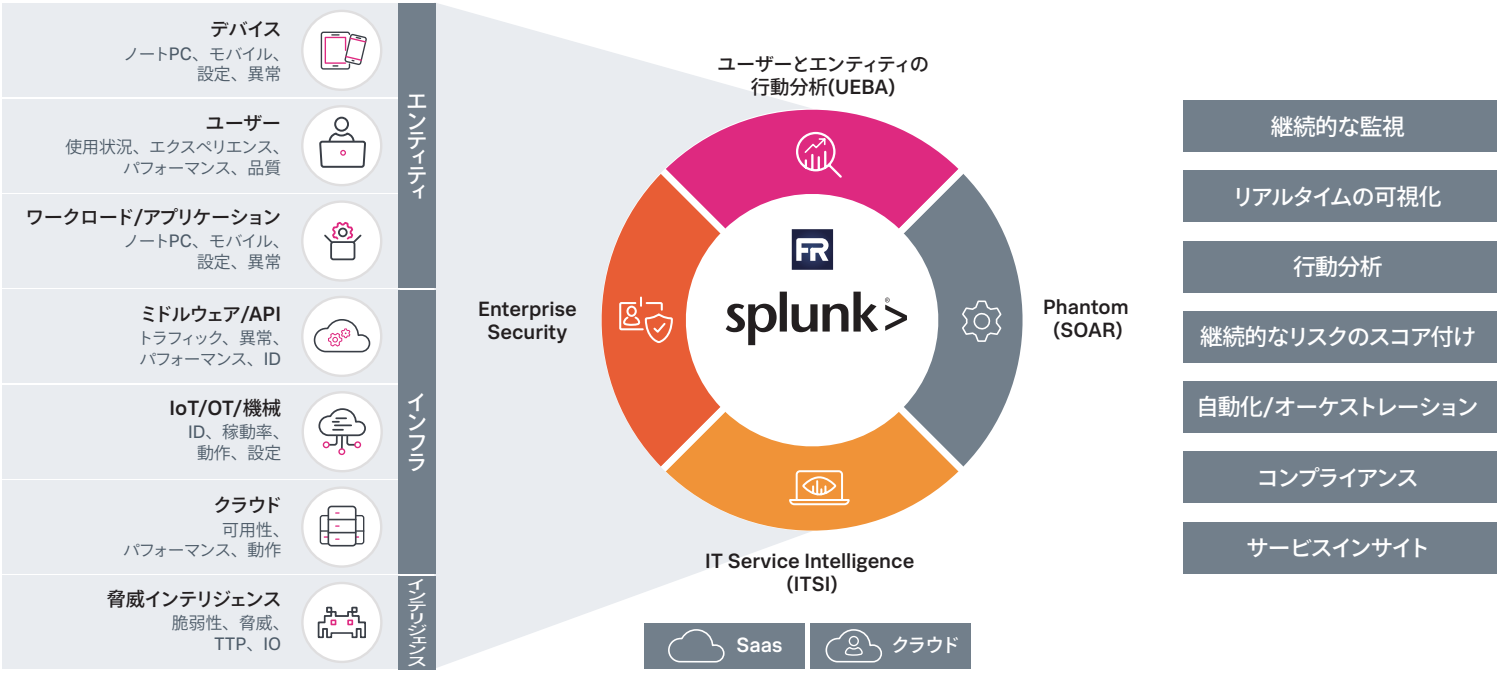
Splunkプラットフォームは、境界のない現代の組織においてデータやアプリケーションへのアクセスの安全性を確保しなければならないCISO(最高情報セキュリティ責任者)やセキュリティ担当者に、継続的な監視ソリューションと分析ソリューションを提供します。

Splunkのプラットフォームを使うことで、アクセスに関する決定の確実性と継続的な信頼性を高め、ゼロトラストエコシステム全体でコンポーネントのパフォーマンスと可用性を維持し、ポリシーの遵守を徹底できます。

また、ほぼあらゆるソースからデータを取り込み、インフラをエンドツーエンドで監視して、ゼロトラストエコシステムを最適化し、その有効性を高めることができます。

Splunkは、具体的には次の3つの方法でゼロトラストモデルを実現します。

1. ユーザー、資産、サービスの信頼性を継続的に監視することで、組織のリソースへのアクセス権限の確実性と信頼性を高める。
2. サービスの健全性、コンポーネント同士の関係、インフラをスタック全体にわたって可視化し、パフォーマンスと可用性を確保するとともに、機械学習によって問題をその発生前に予測する。
3. タスクの自動化とワークフローのオーケストレーションによってゼロトラストポリシーを適用し、手作業やアナリストの負担を軽減して、コストを削減する。



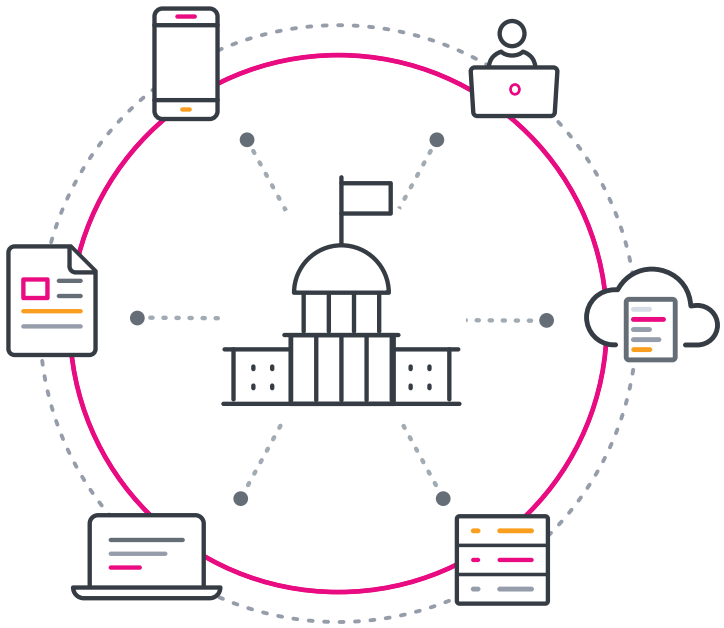
確実性を高め、リスクを軽減

ゼロトラストの大前提は、組織のデータをその場所に関係なく保護しながら、正当なアクセスを必要としているエンティティにアクセスを許可することです。Splunkのプラットフォームは、すべてのユーザー、デバイス、サービス、インフラの継続的な監視を通じて、組織リソースに対するユーザー認証を確実かつ高い信頼性で行えるようにします。Splunkのポリシーエンジンは、収集した情報を基にユーザー、資産、サービスの信頼性を検証し、組織のセキュリティポリシーに従ってアクセスと権限を各段階で管理します。

Splunkのソフトウェアなら、組織リソースへのアクセスを要求しているあらゆるユーザー、資産、サービスに関する内容の濃い詳細なコンテキスト情報を組織のポリシーで定めた間隔で取得し、その情報に基づいて決定を迅速に下せます。

また、このソリューションにはイベント管理、セキュリティ分析、行動分析といった高度な機能に加えて、こうした機能を強化する機械学習機能も備わっているため、ポリシーエンジンを活用して組織データへのアクセスを要求するエンティティの信頼性やリスクを常に見極めることができます。

続いて、有効なゼロトラストモデルの構築を支援する、Splunkの各ソリューションについて見ていきましょう。



Splunkとともにある安心

Splunkのセキュリティスイートは、組織のセキュリティの中枢として機能し、データをインサイトに変え、インサイトを行動に変えます。組織全体のデータをセキュリティへの関連性を問わずに活用して脅威の検出と対応を強化でき、CDM（常時診断・対応型）アーキテクチャにおいて重要な統合レイヤーとして機能します。

Splunkのソフトウェアは複数のソースから脅威インテリジェンスを収集して集約し、重複排除と優先順位付けを行うことで、コンテキストを提供し、セキュリティ運用を合理化します。また、実用的なユースケースコンテンツで継続的に強化されるため、常に最新のサイバーセキュリティ脅威の情報に基づいて組織を守り、リスクプロファイルやアクティビティのステータスを評価して、結果を組織全体で共有することができます。

中核となるセキュリティソリューションは、Splunk Enterprise Security (ES)、Splunk User Behavior Analytics (UBA)、Splunk SOARで構成されています。機能拡張および価値の早期実現のためにアプリケーションを追加することも可能です。

Splunk Enterprise Securityは、組織のセキュリティ状況（Security Posture）をエンドツーエンドで可視化して実用的なインテリジェンスを提供し、インシデントに優先順位を付けて適切に対応できるようにする、業界をリードするSIEMソリューションです。

Splunk ESでは、セキュリティの観点からデータを包括的に把握できるため、セキュリティチームはサイバー脅威をすばやく検出して、インシデントへの対応を最適化できます。また、調査も迅速に行えるため、悪意あるアクティビティを特定し、侵害を検出して、脅威や攻撃の影響範囲を調査できます。さらに、情報保証の状況や対策の遵守状況を詳細に可視化して、インサイトをリアルタイムで得ることで、リスクを継続的に評価することも可能です。

Splunk UBAは、UEBA(ユーザーとエンティティの行動分析)ソリューションで、教師なしの機械学習を使用した高度な内部脅威検出機能を提供します。デバイス、ユーザー、アプリケーションにわたって未知の脅威や異常行動を検出できます。

Splunk UBAは、脅威の検出を最適化し、的を絞ったインシデント対応を可能にして、組織が精度の高い脅威インテリジェンスに基づいて行動できるように、Splunk ESの機能を拡張します。Splunk UBAでは、アクセス制御とユーザーの行動を、それが内部のものか外部のものかに関わらず継続的に監視して、あらゆる異常行動や不正なアクティビティを検出し、リスクを動的に評価することができます。ユーザー、アカウント、デバイス、アプリケーションといった複数のエンティティにまたがるいくつもの異常を1つの脅威として自動で関連付けることができるため、分析が容易になり、脅威への対処が加速されます。

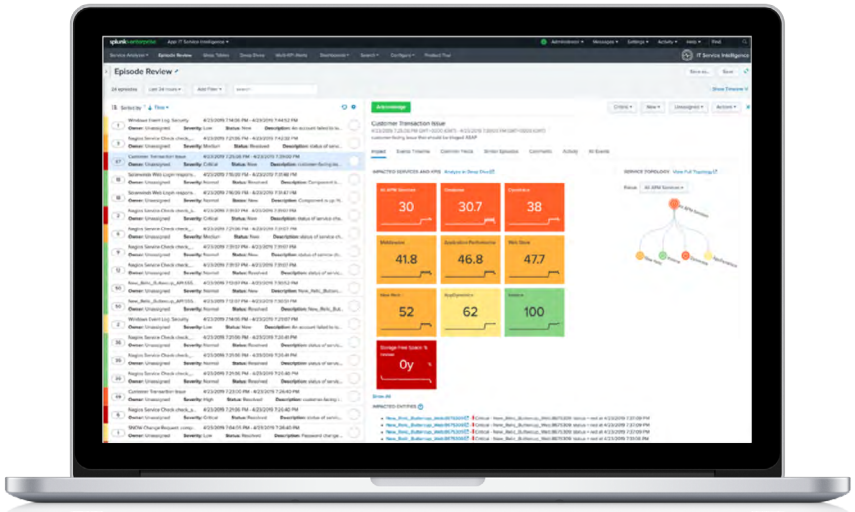
稼働時間の増加とストレスの軽減

Splunkは、ゼロトラストエコシステム全体を最適化し、その有効性を高めます。サービスの健全性、コンポーネント同士の関係、およびインフラをスタック全体にわたって継続的に可視化することで、パフォーマンスと可用性を確保し、機械学習によって問題をその発生前に予測します。コンポーネントがダウンしたり、期待どおりに稼働していない場合は、即座にITとセキュリティの担当者にアラートが送信され、問題がピンポイントで示されるため、トラブルシューティングにかかる時間を場合によっては何時間も短縮でき、失われたデータの復旧も容易になります。

さらに、ネットワーク、エンドポイント、アプリケーションスタック全体をリアルタイムで詳細に可視化できるため、コンプライアンスが徹底され、監査を短時間で終えられるほか、設定のずれも全体で調整しつつ修正できます。このように、組織はゼロトラストインフラのコンポーネントを継続的に監視できるため、各ポリシーに従った評価ができ、資産の安全を最大限確保できます。

Splunk IT Service Intelligence (ITSI)は、サービスの中断を招くインシデントを発生前に防止し、データに機械学習を適用することによって、サービスの全面的な監視や予測分析、効率的なインシデント管理を実現するソリューションです。サービス品質の低下が事前に予測されるため、チームは先手を打って調査を行い、実際に影響が出る前にすばやく対処できます。

ITSIは、メトリクス、ログ、トレースデータを相関付けて機械学習を適用するとともに、監視、イベント管理、インシデント対応を1つのプラットフォームに統合します。アラート管理機能と分析機能を基盤とする、予測機能を取り入れたほぼリアルタイムのパフォーマンスダッシュボードでは、サービスの健全性を監視できます。VictorOpsやSplunk SOARなどのITサービス管理(ITSM)ツールやオーケストレーションツールとも統合されるため、インシデントを一元的に監視、検出、対応、解決することもできます。



アナリストの負担や手作業を軽減

Splunkのプラットフォームは、タスクを自動化し、ワークフローをオーケストレーションすることで、ゼロトラストポリシーの適用をサポートします。セキュリティインフラが複雑で人材がひっ迫していても、システムへのパッチ適用をはじめとする繰り返し行うタスクを自動化し、リソースへのアクセスを要求する個人デバイスのリスクを判断するワークフローをオーケストレーションすることで、負担を軽減できます。

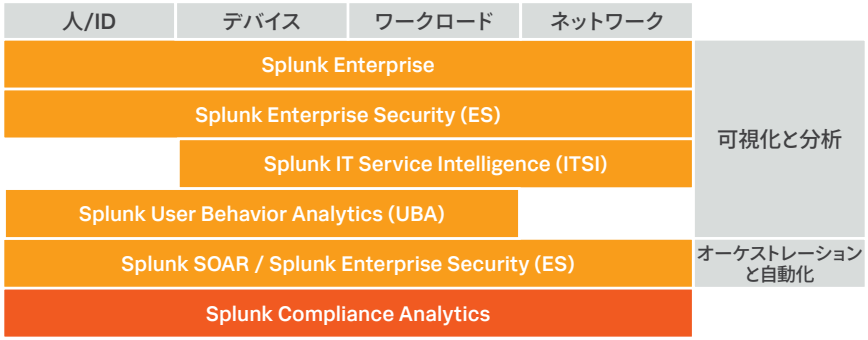
自動化とオーケストレーションで手作業の大幅な削減が見込めるため、脅威への先手を打った対応、セキュリティ運用センター (SOC)のアナリストの負担軽減、イベントへの早期対応が可能です。これにより、コストを削減できる上、アナリストはその時間をサイバー脅威へのプロアクティブな対処や、異常イベントへの対応に使えるようになります。

Splunk SOARは業界をリードするSOARソリューションです。Splunk SOARの拡張性に優れた自動化機能とオーケストレーション機能により、組織は業務を効率化し、脅威に迅速に対応し、サイバー防御を強化できます。Splunk SOARの柔軟なアプリケーションモデルでは数百ものツールと数千ものAPIがサポートされており、チームとツールを横断する複雑なワークフローをつなぎ合わせて調整することができます。

またSplunk SOARでは、セキュリティインフラ全体で、手作業で行えば数時間以上かかるようなファイルのデトネーション(仮想領域での実行)からデバイスの隔離に至る一連のアクションを、わずか数秒で実行できます。Splunk SOARを活用して複数あるチーム、プロセス、既存のセキュリティツールを統合することで、イベント管理やケース管理、コラボレーション、レポートなど、幅広いセキュリティ運用機能に対応可能です。

ゼロトラストの原則を実装するには、テクノロジーだけでは不十分です。ゼロトラストはプロセスに組み込まれ、組織を支える全チームで実践されなければなりません。Splunk SOARは、標準運用手順を再利用可能なテンプレートにコード化し、人とマシンのタスクをオーケストレーションするとともに、関連するすべてのデータとアクティビティを1つの場所に集めることで、一貫性を高めます。

Splunkとゼロトラストの柱



Turn Data Into Doing
データを行動に変える

成功するゼロトラスト戦略の中心に例外なくあるもの、それはデータです。ソースや種類は関係ありません。データの可能性を最大限に引き出す上で最大の障壁となるのが、その価値を閉じ込めているシステムや構造です。

こうした障害を取り除くことができれば、政府機関にとって貴重な情報源となりうる宝の山が解き放たれます。関連のないように見えるデータ同士を組み合わせることが可能になるため、組織全体でリアルタイムなアクションが促進され、有効なゼロトラスト戦略に必要な確固たる基盤形成にも寄与します。

Splunkは、データと行動を隔てる障壁を解消するために、データを行動に変える世界初のプラットフォームである「Data-Into-Doingプラットフォーム」を構築しました。このプラットフォームを導入すれば、あらゆる問題解決、意思決定、行動にデータを活用できるようになります。

Splunkのプラットフォームは、業界トップクラスのSIEM、UEBA、SOARソフトウェアソリューションを統合した業界唯一のスイートです。市場で実証された拡張性のあるビッグデータプラットフォームであるこのスイートは、実用的なユースケースのコンテンツで継続的に補強されます。

詳細情報

ゼロトラストポリシーの構築にSplunkのData-Into-Doingプラットフォームがどのように役立つか、ご興味のある方はぜひこちらをご覧ください。

また、Splunkが新たに発表したGovernment Logging Modernization Programと、Splunkのゼロトラストアーキテクチャツールが、バイデン政権の定めたサイバーインシデント対応に関する新たな要件(OMB M-21-31)の遵守にどのように役立つかをこちらでご確認いただけます。

Splunkのエキスパートまでご相談ください。お客様の環境について検討し、要件を評価して、現在のような厳しい状況を乗り切るためにSplunkをどのように役立てられるかをご案内いたします。

21-21617-Splunk-Zero Trust Security Model in Government-EB-JA-202203

splunk> turn data into doing™