opentext™ | Cybersecurity

ポジションペーパー

ゼロトラストのための アプリケーションセキュリティ フレームワーク

目次

概要 1
OpenTextのアプリケーションセキュリティサービス 2
データ保護フレームワーク 17
エッジでの共有ゼロトラストサービス 20
主なメリットの概要 21
NetIQ by OpenTextについて 21

概要

OpenText™ の政府機関向けソリューションのセキュリティサービスは、ネットワーク境界でゼロトラストの原則を実現するよう設計された、サイバーセキュリティ製品の統合サービスです。このサービスを利用して高度なアプリケーションセキュリティ機能を提供することにより、環境の成熟度を迅速に高めることができます。このサービスは、独立しても、または既存のツールと連携しても機能する優れたツールとサービスのセットです。SD-WAN テクノロジーパートナーと緊密に連携した当社のアプリケーションセキュリティサービスは、現在のゼロトラスト要件を満たすだけでなく、共有エンタープライズゼロトラストサービスを通じて環境の成熟度をより広範に高めます。

ゼロトラストプログラムの主なメリットは次のとおりです。

- 極めて高度なリスク分析を継続的なアクセスの決定に適用します。
- エッジにおけるユーザーアプリケーションとデータを対象にしたゼロトラストサービスを実現します。
- 高度な脅威検知および修復機能 (初回アクセス、特権昇格、ラテラルムーブメント、多数の追加の MITRE ATT&CK TTP など) により、ゼロトラストアーキテクチャ (ZTA) の成熟度を高めます。
- 機密データをエンドツーエンドで検知して保護します。
- レガシーアプリケーションの統合パスを作成します。

組織は、ゼロトラストレベルのセキュリティに到達するために、アプリケーションセキュリティに対する新たなアプローチを必要としています。つまり、好ましくない環境がデフォルトの前提です。エッジに継続的な認証を実装することで、次のようにして真の適応型アクセスが構築されます。

- ユーザーセッションのライフサイクル全体にわたって監視と制御を拡張します。
- セッション開始時からリスクレベルが変化したことを検出し、追加の認証要求を開始します。
- 特定されたリスクと利用可能な ID 検証に基づいて、認証レベルを調整 (引き下げまたは引き上げ) します。

環境内の適応型セキュリティインフラストラクチャを効果的に運用するためには、エッジのセキュリティ制御を規範的なリスクポリシーよりも拡張し、より詳細な要求のコンテキストと行動分析を活用する必要があります。ベストプラクティスが示唆するように、規範的なアクセスポリシーをデフォルトで適用するものの、個々には特定のユーザーの行動情報としての重みをそれほど重視しないハイブリッドアプローチを採用するのが最も効果的です。さまざまなシナリオに対応するため、通常は強力な認証方法とパッシブ認証方法を組み合わせて使用することが必須です。それにより、特定のニーズと関連するリスク (情報の機密性の程度と要求のコンテキスト) に基づいて最適な方法を適用できるようになります。

OpenText は、ZTA へのスムーズな移行、既存の義務化期限の遵守、より効果的なセキュリティ運用を支援します。

OpenText のアプリケーションセキュリティサービス

ゼロトラストは、アプリケーションセキュリティスタックにぜひとも追加すべきものですが、そのためにはアクセスの提供方法を根本的に変える必要があるというのが当社の見解です。ゼロトラストの場合、ユーザーのデバイスと要求の発信元のどちらも、サービスへのアクセスを自動的に許可しません。むしろ、要求のコンテキストの理解を深め、アクセスを要求する ID の検証レベルを高めることが必要になります。これは、厳格で適応性の高いレベルのセキュリティです。

継続的な認証では、サービスへのアクセスを継続すべきかどうかについて、システムの評価が繰り返し行われます。アクセスメトリックが継続的に収集され、リスクが頻繁に再計算されます。IT セキュリティチームがミッションに適したリスクモデルを定義する場合、ゼロトラストパラダイムは、オープンなものではなく、クローズドループと見なされます。クローズドループの監視と制御のほうが高度なセキュリティアプローチを提供するだけでなく、行動分析にも適しています。これにより、現在一般的に使用されている標準的なリスクメトリックをはるかに超えるレベルの ID 中心のメトリックが提供されます。アクセス制御の許可 / 忘却モデルは、従来のポリシーを適用するうえではそれなりの役割を果たしますが、昨今の脅威環境においてはこれではまったく不十分です。

継続的なユーザートラッキングを実施すると、各セッションのアクセス制御を保持できるというセキュリティ上の利点に加えて、資産を保護する能力を強化できるだけでなく、はるかに大規模なユーザーコンテキストのライブラリを構築することができます。こうしたコンテキスト情報のリポジトリは、一般的なリスクベースの認証をはるかに超える、より深いレベルのリスクインテリジェンスを構築するために、ユーザー / エンティティ行動分析 (UEBA) の適用を可能にする基盤となります。

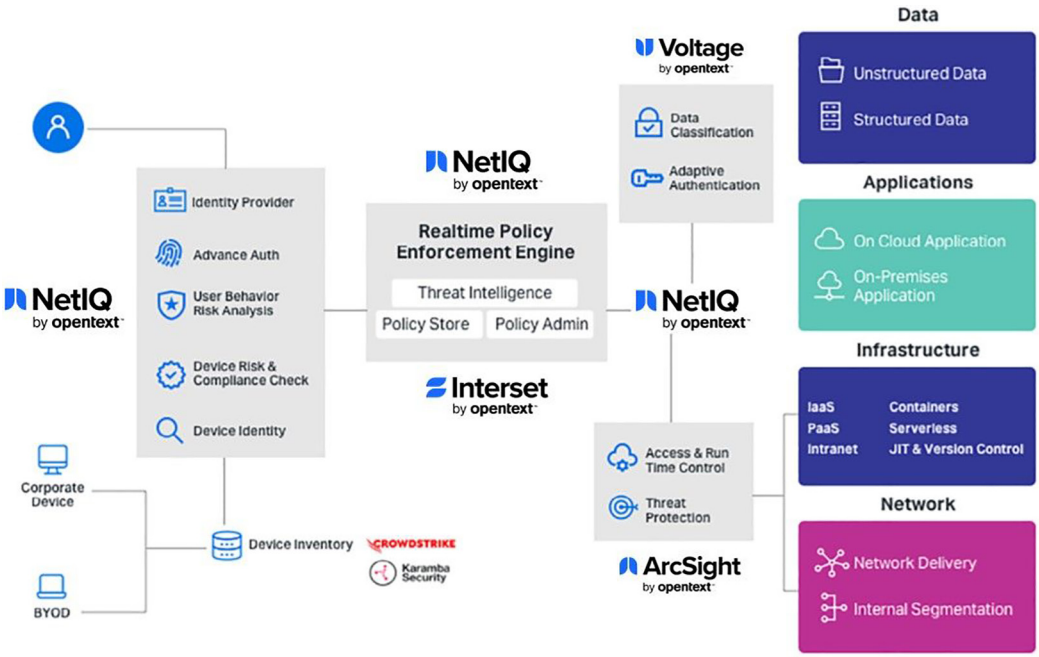


図 1. ゼロトラストアーキテクチャ | アプリケーションセキュリティフレームワーク

要約すると、環境内のエッジに継続的な認証機能を組み込むことにより、以下のようなセキュリティ上の利点とより高度な保護を即座に実現できます。

- アクションを測定して認証レベルの変更が必要かどうかを判断することで、即座に保護が強化されます。
- リスクの高い行動を迅速に特定して、計算されたリスクレベルにより正当化された適切なポリシーアクション (要求の承認、追加認証の呼び出し、セッションの終了) を実行します。
- 保護されたデータにアクセスするたびにコンテキスト情報を収集することにより、ユーザーの通常の行動に関するより完全なプロファイルが構築されます。
- コンテキストデータの分析を継続的に実行することにより、予想される行動をより正確に把握できるようになり、リスクの高いイベントを特定する能力が向上します。
- データの流れの大部分を占める、さまざまなタイプの入力ソース (API、マイクロサービスなど) のすべてを監視し、リスクがないか確認します。
- 外部パラメータには、UEBA ベースのメトリックなど、より高度なコンテキスト情報が含まれます。
- 継続的な認証により、継続的なスコアリングとアクティブなセッション制御が可能になります。

多要素認証フレームワーク

認証の新規導入は通常はプログラム内で提案されるため、多くの場合、特定の戦術的観点から行われます。こうしたアプローチでは、組織は認証において複数のサイロ (アクセスの構築、リモートアクセス、コンプライアンス要件など) を抱えることになります。このようにばらばらの実装が行われると、管理オーバーヘッドが高くなり、プロセスが非効率になります。しかし、さらに重要な点は、一貫性のない認証ポリシーが原因で脆弱性が発生することです。

つまり、認証フレームワークで以下のことを実現できることが必要です。

- 統合によるコストの削減と複雑さの軽減
- ポリシーの一元化によるセキュリティの強化
- より多くの多要素認証オプションの提供

また、MFA フレームワークは幅広い組織上のニーズを満たす必要があります。以下に例を挙げます。

- 小規模な組織にとっては導入や管理が簡単であり、一方で大規模な組織にとってはスケーラビリティの要件を満たすものでなければなりません。
- 特定の地域に集中している組織か、世界中に広く分布している組織かに関わらず、組織全体の相違点に適応できる必要があります。組織の形態に関係なく、フレームワークは認証要求に迅速に応答しなければなりません。
- フレームワークでサポートされる方式が多ければ多いほど、認証のサイロを 1 つに統合するための組織の柔軟性が増します。また、新しい認証技術が市場に投入された際に、フレームワークを容易に拡張できる必要もあります。

環境への導入を実施するうえでは、ミッションパートナーに現在と将来の MFA のニーズに対応するオプションと柔軟性を提供する必要があります。NetIQ Advanced Authentication by OpenText は、認証のサイロや古いテクノロジーに縛られることはありません。OpenText は、FIDO U2F ベースのデバイスとの互換性など、新しいテクノロジーの出現に伴って積極的にアップデートを行うオープンなフレームワークを提供します。

FIDO Universal 2nd Factor (U2F) は、ユーザー自身が認証デバイスを管理する環境をサポートします。NetIQ Advanced Authentication は、開発の必要なく、アプリケーションにそのサポートを提供する強固なフレームワークを提供します。トークンコストを先送りできるというメリットを得られるばかりか、ユーザーが、使用を許可された代替トークンオプションを組み込むことができます。NetIQ Advanced Authentication が提供する高度なサポートを考慮に入れれば、前進し続ける U2F 認証環境を提供するフレームワークとして、これほど優れたものはありません。

OAuth2	Microsoft OATH	Kerberos
OATH認証	NFC ISO/IEC	PKSCS7およびPKCS11FIPS 140.2
Google Authenticator	RADIUS	

NetIQ Advanced Authentication では、RADIUS で使用できる認証タイプ以外にも、市場に出回っている他のどのソリューションよりも多くの認証方式がネイティブで用意されており、現在は 37 種類の MFA 方式がサポートされています。それがなぜ重要なのかと言えば、社内外のユーザーが、さまざまな状況下で複数のデバイスから機密情報にアクセスするからです。NetIQ Advanced Authentication は、導入後すぐに使用可能な一連のアプリケーション統合機能 (RADIUS、OpenID、OATH、FIDO、RACF、z/OS、Windows、Mac OS、Linux、Citrix、VMware など多数) を備えているため、既存のアプリケーションセキュリティスタックに幅広く対応できます。さらに、多様な認証リーダーや認証方式を広範にサポートしているため、かつてないレベルの柔軟性が提供されます。

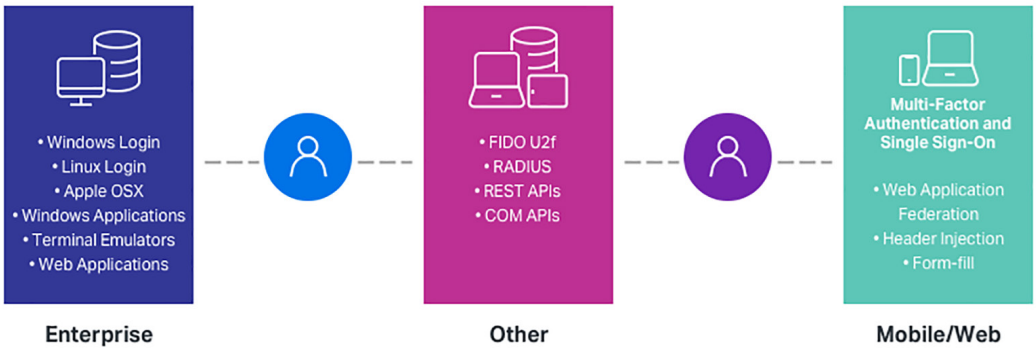


図 2. 高度な多要素認証フレームワーク

アプリケーション層における ID の観点からゼロトラストを環境に適用する場合、重要な機能は継続的な認証と権限付与です。

- 継続的な認証とは、セッション内で急上昇したリスクスコアに応じて、必要な回数だけ ID を再検証する機能です。認証方式の強度によっては、リスクスコアを下げるために 1 回以上認証に成功することが必要になる場合があります。
- セッション内の任意の時点でリスクスコアが上がった場合、アクセス要求が制限されるか、終了する可能性があります。
- ミッションパートナーが自由に使える MFA 方式が多ければ多いほど、生産性を低下させないゼロトラスト環境を採用できる可能性が高くなります。

NetIQ Advanced Authentication は、既存の数多いソリューションよりも構成と保守の複雑さが軽減されています。また、導入後すぐに統合できるため、構成可能な認証オプションを豊富に利用できる点も強みです。NetIQ Advanced Authentication を環境に適したエンタープライズアプリケーションセキュリティの一部として使用すると、セキュリティ、柔軟性、ユーザビリティの向上により、アプリケーションアクセスのあらゆる面においてメリットが得られます。

継続的なリスクサービス

NetIQ Risk Service by OpenText を導入すると、複雑なインフラストラクチャを必要とせずに、適応型アクセス制御を導入できます。適応型アクセスとは、コンテキスト、ユーザーの過去の行動、アプリケーションの機密性を評価してアプリケーションにアクセスするために必要な認証を決定するプロセスです。適応型アクセスの目的は、機密リソースにアクセスするために、リスクを軽減する適切な保証レベルを提供することです。この際、ユーザーは自分が誰であるかをさらに証明する必要があります。

NetIQ Risk Service は、アプリケーションやサービスへのユーザーアクセスのリスク評価を通じて、適応型アクセスを提供します。アクセスアクティビティに関連するさまざまな指標を分析して、そのアクティビティが不正である確率を判断します。ユーザーのいる場所、アクセス時間、プロファイルなどのコンテキスト情報や、履歴レコード、ユーザーとエンティティの行動データなどの要因を使用して、リスク指標が計算されます。

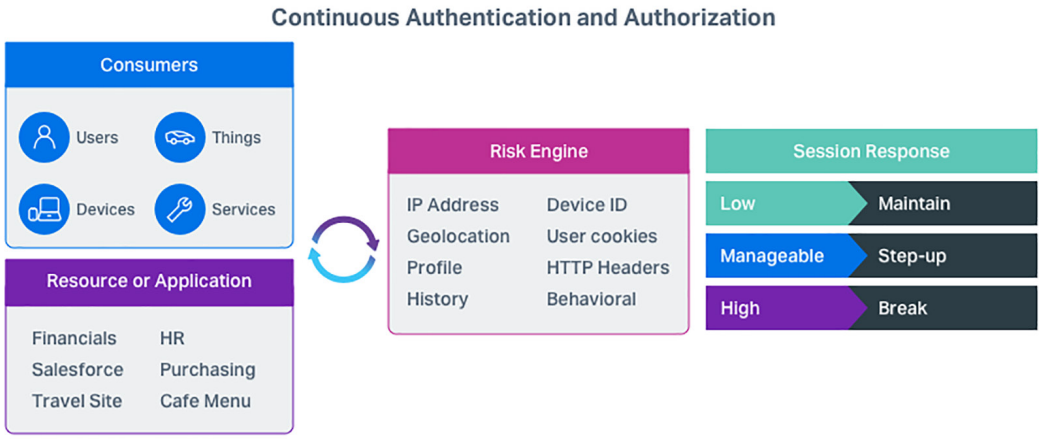


図 3. Riskn フレームワークのレベルに基づくさまざまなアクセスポリシーの適用

アプリケーションセキュリティスタックの一部として NetIQ Risk Service を使用すると、ユーザーを認証する前に、特定のログイン試行の潜在的なリスクを評価できます。事前認証リスク評価により、潜在的なリスクを軽減するための詳細な認証要素を微調整できます。また、NetIQ Access Manager by OpenText および NetIQ Advanced Authentication とすぐに統合できるため、スムーズでリスクを意識した、適応型の継続的な認証が可能になります。特に重要な点は、NetIQ Risk Service では、Interset または ArcSight Intelligence (AI) のリスク分析をネイティブに取り込み、組み合わせたリスク計算に行動分析を直接利用できることです。

Interset/AI は、教師なし機械学習アルゴリズムを使用してユーザーアクセスのパターンを検出し、脅威を特定します。数百の組み込み学習アルゴリズムが、アクセス情報とログファイルからエンティティ (個々のユーザー、マシン、IP アドレス、Web サーバー、プリンターなど) を抽出し、それらのエンティティに関するイベントを観察して、どのような行動が通常行われるか、または予期されるかを判定します。分析プロセスで得られた新しい情報を収集して、以前に観察した行動や動的に測定された統計的ピアグループと比較し、潜在的リスクを評価します。

Interset/AI は NetIQ by OpenText 製品ラインの一部ではありませんが、最先端の機械学習を適用して高度なユーザー行動分析を作成する OpenText のサイバーセキュリティソリューションです。セッション全体でユーザーメトリックを収集し、そこからユーザーレベルできめ細かいリスク評価基準を作成します。NetIQ Risk Service の組み込みエンジンと組み合わせて使用すると、Interset/AI は、ユーザビリティを向上させるとともにセキュリティを大幅に強化する独自の機能を提供します。

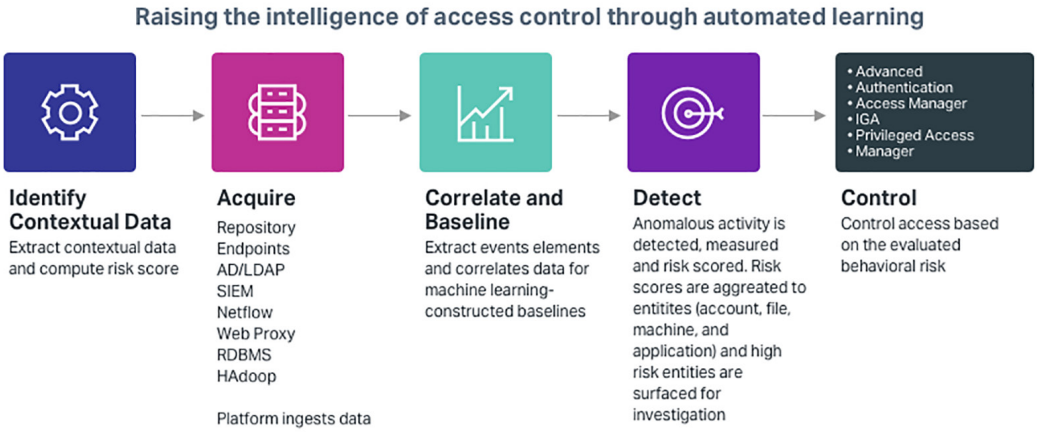


図 4. アクセスリスクサービスは高度な行動分析を使用

なりすまし詐欺の加害者は、デジタル防御を通り抜ける、より高度な方法を使うようになってきています。NetIQ Risk Service は、ハイリスク認証とアプリケーションアクセス要求に対し、リスクスコアがより高度な ID 検証が必要だと示した場合に多要素ステップアップ認証を使用することで保護を行います。NetIQ Risk Service には、メトリックが組み込まれたシンプルなルールエンジンが備わっているため、最小限の労力ですばやく作業を開始できます。また、ユーザーアクセスに加えて、モバイルサービスやマイクロサービスなどの API に対するリスクベースのアクセスにも保護を提供します。NetIQ Risk Service は、静的な認証およびアクセスから継続的な適応型認証へと、環境を進化できるようにします。また、コンテキストに関する測定値をさまざまなソースから使用できます。管理者は、すぐに使用できるメトリックを使用して NetIQ Risk Service を開始できます。このメトリックは、管理者による調整や設定が可能です。

既知の脅威の検知

NetIQ Risk Service は、IP アドレスとレピュテーション、ジオロケーション、ユーザーの ID、ロール、プロファイル情報、デバイス ID、一意に作成されたデバイスのフィンガープリント、Cookie やブラウザー情報、ヘッダー情報、履歴、アクセスパターン、外部ソースからの情報など、さまざまなソースからリスク情報を計算します。入力範囲の幅が広いため、きめ細かなリスク計算が可能になり、潜在的な脅威を迅速に特定し、ルールベースのポリシーを適用してリスクの増加を軽減できます。こうした規範的なコンテキストルールは、リスクベースのアクセス制御の基盤となっています。ただし、これらのアクセス要件は政府機関のセキュリティポリシー適用において不可欠ですが、残念ながらそれだけでは十分ではありません。多くの場合、時間が経つにつれて内部ユーザーや執拗な攻撃者の両方が、このような静的なリスクポリシーを回避する方法を習得します。これらの未知の脅威に対し、動的なリスクポリシーに基づくさらなる制御が必要になります。

未知の脅威の検知

巧妙な攻撃者や執拗な攻撃者を把握するには、既知の脅威を検知するだけでなく、すべてのエンティティの行動プロファイリングができるようにする必要があります。なりすましや悪意のある内部ユーザーの攻撃に対する最も効果的な防御策は、企業内すべてのユーザーそれぞれの通常の行動を知ることです。こうしたベースラインにより、NetIQ Risk Service は、悪意のある行動、偶発的な行動、疑わしい行動のいずれであっても、ほとんどの異常で疑わしい行動を検知できます。

NetIQ Risk Service は Interset/AI オプションを提供しており、リスク計算に行動分析を組み込むことができます。Interset/AI は教師なし機械学習を使用するほか、ユーザーアクセスパターンとアクティビティパターンを検出して数十億のイベントから優先的な脅威を特定する何百ものアルゴリズムが組み込まれています。NetIQ Risk Service はまた、リスクポリシーの評価と適用のために使用する異常なユーザーアクセスパターンを特定するためのデータベースの作成もサポートしています。環境に実装する NetIQ 製品ラインのコンポーネントの数が多いほど、Interset エンジンには豊富な分析機能が提供されます。

MITRE の ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) フレームワークは、エンタープライズネットワークに対して現実に行われた攻撃で観察された脅威の戦術と技術の生きたナレッジベースであり、行動分析において極めて重要な役割を果たします。現在、Interset/AI は、これまでの ATT&CK フレームワークの 75% をカバーしており、その範囲は今後も拡大する予定です。450 を超える機械学習モデルを活用して、環境内のすべてのユーザーとエンティティの行動のベースラインを作成し、それらのベースラインから逸脱したものを潜在的にリスクのある行動として評価します。当社の機械学習モデルは、ATT&CK の 219 種類の技術に慎重にマッピングされており、価値の高い情報の流出や詐欺などを促進するさまざまな脅威に対して効果的に対応します。

正確なリスクスコアを作成するために、Interset/AI の分析エンジンは不確実な推論に対する確率論的手法、クラスタリングアルゴリズム、分類アルゴリズムと統計的学習手法、およびニューラルネットワークを含む人工知能の手法を活用しています。また、統計的アプローチを採用して、さまざまな異常の可能性を単一のエンティティのリスクスコア、つまり有効で実用的なセキュリティ分析の重要な要素に圧縮します。

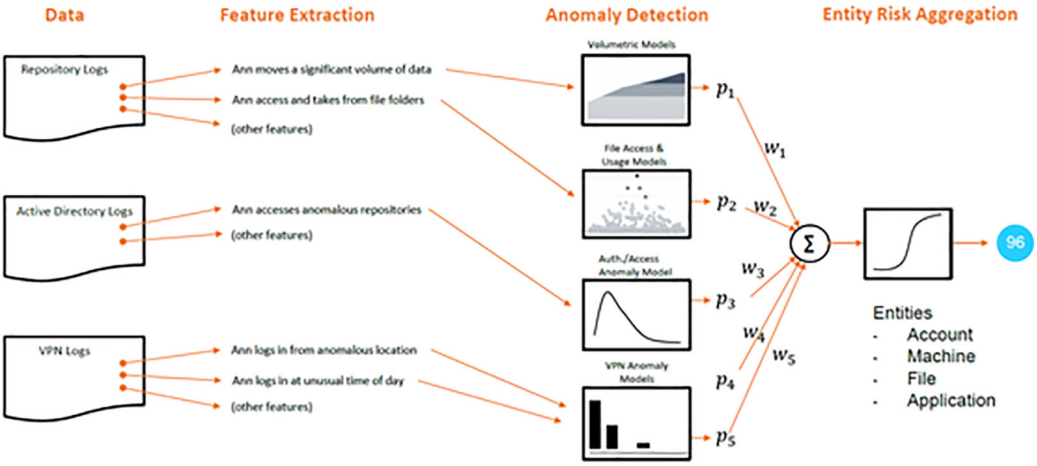


図 5. 分析フレームワーク | ログデータからリスクのあるエンティティへ

スコアは、異常を定量化するためにイベントごとに計算されます。Interset/AI は、エンティティの過去のリスクスコアと、従業員ウォッチリスト、脅威インテリジェンス、他のセキュリティツールが提供するデータなどエンティティに影響を与える可能性のある外部インテリジェンスを考慮したうえで、関連するエンティティにこのようなイベントの可能性を集約します。これにより、Interset/AI が収集できるすべてのコンテキストに基づいて、あるイベントに関連するすべてのエンティティを考慮したリスクスコアが作成されます。

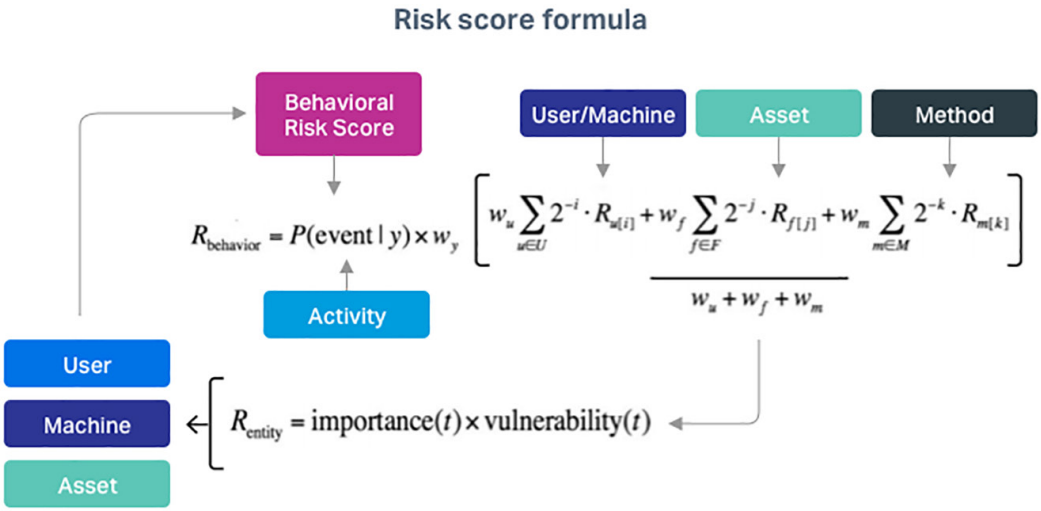


図 6. 行動リスクスコアの背後にある数式

分析エンジンは、高いリスクのユーザー、特に大きなリスクにさらされているファイル、高リスクのアクティビティによく使用されているマシンについて学習して、異常パターンを調整します。また、統計的分析により、観察された行動の異常度を定量化します。エンティティが高リスクで異常なアクティビティに関与するほど、リスクスコアは上昇します。逆に、エンティティが高リスクなアクティビティに関与することなく、それ自体や他の類似エンティティと比較して一般的な行動をしている場合、リスクスコアは徐々に低下します。このリスクスコアはすべての単一エンティティ、つまりすべてのユーザー、マシン、IP アドレス、プリンター、Web サーバー、ファイル共有などごとに計算されます。こうした多数の個別化されたリスクスコアに関して、機械学習はそれらをすべて正確に相互比較できるように正規化し、ランク付けされた脅威のヒントリスト 1 つに集約します。セキュリティチームは、これに基づいて時間と作業の優先度を決定することができます。

NetIQ Risk Service は、すぐに利用可能な統合機能だけでなく、コンテキスト属性、リスクスコアリング、行動に関する情報を提供するサードパーティの SASE サービスや CASB サービスと統合するためのインターフェイスや API も備えています。

統合アクセス制御フレームワーク

認証と権限付与を単一のソリューションにまとめると、統合されたポリシーとプロセスのセットでアクセスを保護し、制御できます。このアプローチは特に、モバイルユーザーに適しています。サイロ化されたモバイルアプリは本質的にセキュリティが低いことに加え、セキュリティや使用するシステムではなくモバイルアプリ自体に集中する必要がある開発者からすると、そうしたアプリは余計な仕事を増やす原因でもあります。デスクトップユーザーやラップトップユーザーと同様に、単一のアクセス制御フレームワークを使用すると、余分な資格情報管理やつながりのないその他の各種アクセス制御ポリシーが不要になります。

環境に適した統合アクセス制御の主な機能は、以下のとおりです。

- 簡素化されたアプリケーションとサービスポータル：NetIQ Access Manager のビルトインポータルを使用することで、管理者はユーザーがラップトップ、タブレット、スマートフォンからアプリケーションやサービスにアクセスする際のユーザーエクスペリエンスを簡単に設定することができます。このポータルは、各フォームファクターのビューを最適化し、迅速で容易なナビゲーションを可能にします。また、ポータルを独自の外観とスタイルでカスタマイズし、ブランド化することもできます。
- SaaS および Web アプリケーション SSO をモバイルユーザーに拡張：動的クラウドと Web ベースのアプリをモバイルユーザー向けに拡張したい場合には、NetIQ Access Manager がそれを実現します。NetIQ Access Manager は、Web アプリケーションにセキュアかつシンプルにアクセス可能な NetIQ MobileAccess アプリ (Apple App Store または Google Play で入手可能) に対応しています。このアプリ内で、企業のミニポータルがユーザーに表示され、アイコンを 1 回タッチするだけで SSO が利用できます。何より重要な点として、管理者は通常、半日でこれらのアプリケーションを構築できます。
- モバイルシングルサインオン：NetIQ Access Manager はネイティブでモバイル SDK をサポートしているため、シングルサインオン時のユーザーの負担を軽減できます。モバイルのネイティブアプリでサービスを提供している場合にも、NetIQ Accesss Manager では、iOS 用の SDK、OpenID Connect、または OAuth 認証が用意されています。
- ユーザーのオンボーディング：NetIQ Access Manager を使用すると、ユーザーは各自でアカウントの登録と設定を行うことができます。また、Advanced Authentication Framework を使用してセルフサービスのオンボーディングとアカウントのメンテナンスプロセスを自動化できます。
- ユーザーとミッションパートナーの完全なアクセスおよびアクセスポリシー管理：NetIQ Access Manager の堅牢なフェデレーションは、IdP または SP としてのサービスなど、現在使用されている最新のフェデレーション標準をすべてサポートしているため、パートナーの ID プロバイダーを信頼することができます。モバイルデバイスを使用しているすべての担当者に安全なアクセスを提供して、ネイティブアプリを有効にすることも、既存の Web ベースアプリケーションをその担当者のデバイスまで拡張することもできます。

NetIQ Access Manager は、ユーザーとミッションパートナーのためのフェデレーションとシングルサインオンを備えた、モバイル、Web、レガシーアプリケーションのフルアクセスゲートウェイソリューションです。これは、単なるフェデレーション以上のものが求められる混在環境や、さまざまなエンタープライズアプリケーションを安全で一貫性のある単一のユーザーエクスペリエンスに統合する必要がある環境に特に適しています。

NetIQ Access Manager は、アプリケーションおよびサービスゲートウェイとして機能するリバースプロキシ機能を備えています。NetIQ Access Gateway を使用すると、複数のプラットフォームにわたってアプリケーションにアクセスできるようになり、デバイス間でのユーザーエクスペリエンスが簡素化されます。また、既存のアプリケーションにセキュリティ層を追加するためによく使用される一方、シングルサインオンフェデレーションと組み合わせて使用することで最高のユーザーエクスペリエンスを提供することもできます。

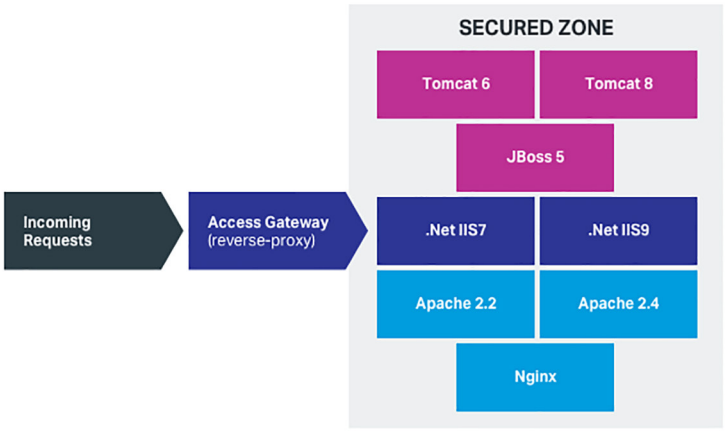


図 7. Access Gateway によるアプリケーション保護

さらに、NetIQ Access Gateway のリバースプロキシを使用して、アクセス要求の一元的なロギングを行うこともできます。このロギングは、バックエンドアプリケーションプラットフォームで行われたロギングを補完することも、置き換えることもできます。ゲートウェイでの要求ログのキャプチャは、ほとんどの環境で使用されている複数のアプリケーションプラットフォームのログを統合するよりも簡単です。ゲートウェイのログには、アプリケーションのログでは使用できない可能性のある要求に関する情報も記録されます。

NetIQ Access Manager には、アクセスゲートウェイや ID プロバイダーからデータを収集して視覚化するために使用できる分析サービスが含まれています。下の図は、すぐに使用できる監視およびレポート作成ダッシュボードの 1 つです。

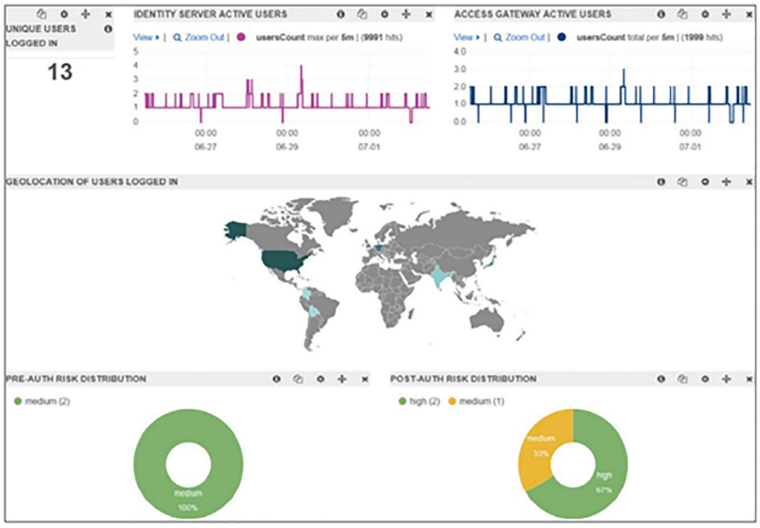


図 8. アクセスダッシュボードの例

類似のテクノロジーは他にもありますが、NetIQ Access Manager では柔軟でコンパクトなアプローチにより構成が簡素化されており、大規模な環境や分散環境に必要な優れたパフォーマンスが提供されます。そのため、管理に必要なシステムリソースと人材が少なくて済みます。

資格情報とエンドポイントセキュリティの制御
当社の適切に設計されたアクセスセキュリティレイヤー (ASL) は、多要素認証、動的アクセス制御、アプリケーションへのシングルサインオンを提供し、あらゆる場所から使用するあらゆる承認済みデバイスに対応できるようにします。この「あらゆる」の原則を考慮すると、保護された情報を要求するさまざまなリモートアクセスシナリオに対応できる環境が必要であることは明らかです。アクセスの利便性を可能な限り保つことが求められていますが、呼び出されるセキュリティレベルが現状の既存のリスクと一致する必要もあります。想定される場所から既知のデバイスでアクセスを要求するリモートユーザーは、外部や管理対象外の場所から未知のデバイスで要求してくる場合よりも、リスクは低くなります。

NetIQ Access Manager は、測定されたリスクに基づいて、アプリケーションやサービスに対するユーザーの認証を動的に変更し、特定の脅威に即座に対応できるようにします。NetIQ Access Manager は、代替トークンを使用して即時の多要素ステップアップ認証を実施したり、リアルタイムのエンドポイントとユーザー属性に基づいてアクセスを拒否したりする機能を備えているため、適応型のアクセスシステムを確立するうえで不可欠な要素となります。

Interset/AI の分析エンジンは、高度なエンドポイントでの検知および対応 (EDR) の脅威データを、組み合わせたリスク評価に利用することもできます。たとえば、CrowdStrike Falcon EDR は、ネイティブな統合を通じて、検知、応答、フォレンジックにまたがり、継続的かつ包括的にエンドポイントを可視化します。Interset/AI の分析エンジンは、Falcon センサーデータを使用して、エンドポイントの脅威ベクトルに関連するリスクを即座に特定できます。そのため、CrowdStrike の豊富なエンドポイントデータの可視性がさらに向上し、持続的脅威 (APT) などの検知が困難な脅威を発見できます。他の EDR サービスプロバイダーとの統合も可能です。

当社はパートナーの Karamba Security と共同で、OT ネットワークと脆弱な IoT デバイスの保護を向上させるための共同セキュリティソリューション、IoT SmartGuard をリリースしました。IoT SmartGuard は、レベルアップした IoT セキュリティを提供し、悪意のあるコードの実行をトラッキングして阻止するほか、組織内の高リスクのデバイスを透過的に表示します。

IoT SmartGuard は、Karamba Security の XGuard が提供する効率的なピンポイントログ生成機能と決定論的保護機能に、OpenText Cybersecurity が提供する強力な行動分析エンジンが組み合わさることで、SOC のセキュリティアナリストを強力にサポートします。

このソリューションは、見つけにくい脅威を迅速に検知し、各 IoT デバイスでの悪意のある実行を阻止する、効率的な IoT セキュリティを実現します。XGuard は、図 9 に示すように、XGuard プラットフォームの機能と構成に基づいて、さまざまなデバイスやオペレーティングシステムに容易に導入できます。独自のクラウドデバイスエッジアーキテクチャを使用しており、リソースに制約のある環境でのセキュリティを最適化します。

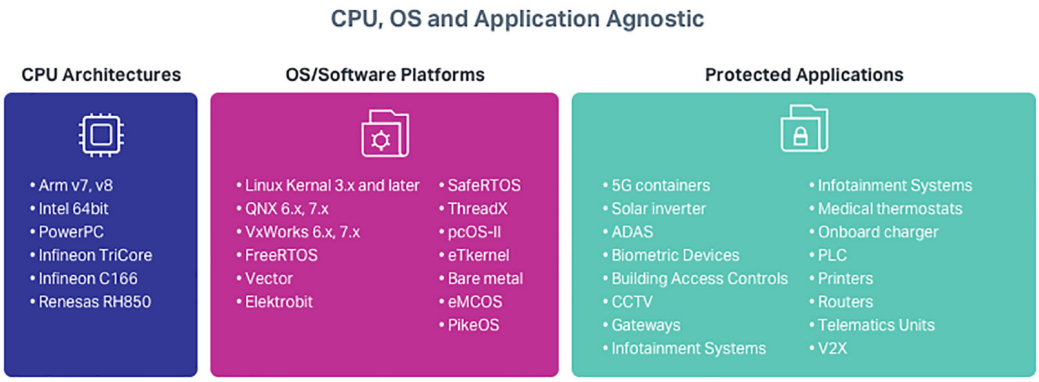


図 9. IoT SmartGuard で提供されるネイティブのプラットフォームサポート

アプリケーションセキュリティの制御

お客様の環境に当社のアプリケーションセキュリティサービスを導入する最大のメリットの 1 つは、認証サービスを直接使用できないレガシーアプリケーションを保護する新しい統合ポイントを利用できるようになることです。ゲートウェイは、ポリシー適用ポイントとなる可能性があり、アプリケーションにデータを送信するための統合オプションを提供するプロキシとして機能します。こうしたサービスは、レガシーアプリケーションにとって、または保護やアクセス制御がいかなるレベルでも含まれない小規模な専用サービスにとって必要です。

もう 1 つのメリットは、複数のバックエンドアプリケーションが 1 つのアプリケーションのように見えるため、シームレスなユーザーエクスペリエンスを享受できることです。こうした「仮想化」を行うには、要求をルーティングし、要求と応答の両方をインフローで変更する複雑で強力な機能が必要です。ゲートウェイは、使用しているデバイスの種類に関係なく、同じタイプのアクセスサービスを提供します。

これらのゲートウェイ機能を境界で活用することにより、お客様の環境でセキュリティとアプリケーションチェックポイントの追加レイヤーが提供されるようになります。このゲートウェイの、外部に向けた一貫性の高い強固なインターフェイスの背後に、さまざまなネイティブアプリケーションプラットフォームが隠れています。こうした保護機能の追加により、アプリケーションやサービスに含まれている可能性がある脆弱性にさらされるのを防ぐことができます。また、このゲートウェイは、アプリケーション自体の機能を強化するか置き換えるため、大まかな認証を実行することもできます。これにより、アプリケーションアクセスポリシーのユニバーサルな適用が可能になります。

レガシーアプリケーションの制御と統合

OpenText™ Host Access Management and Security Server (HA-MSS) は、ホストされている IBM z/OS、Unisys 2200、Linux、UNIX、および Windows ベースのアプリケーションにアクセスするユーザーとデバイスのためのアプリケーションセキュリティ層です。これらの環境に適したユーザーセッション認証機能とユニバーサルアクセス制御機能が、それぞれ HA-MSS 製品によって提供されます。そこに含まれる多要素認証フレームワークは、業界で最もネイティブな統合方式を提供します。

HA-MSS は、既存の IAM システムを活用してそれぞれのユーザーを認証し、システムへのアクセスを許可します。そのため、すべてのアクティビティが 1 か所に記録されます。HA-MSS を使用すると、アプリケーション自体やユーザーワークフローに変更を加えることなく、IAM 承認スキームをアプリケーションに拡張できます。また、HA-MSS では、ユーザーが実行できる操作と実行できない操作を指定することもできます。たとえば、端末エミュレーションクライアントのセキュリティを強化できます。ユーザーがマクロを編集できる機能を削除したり、TLS 1.2 または 1.3 の接続設定をロックしたり、ユーザーデバイスに表示されるアプリケーションの機密データをマスキングしたりすることができます。

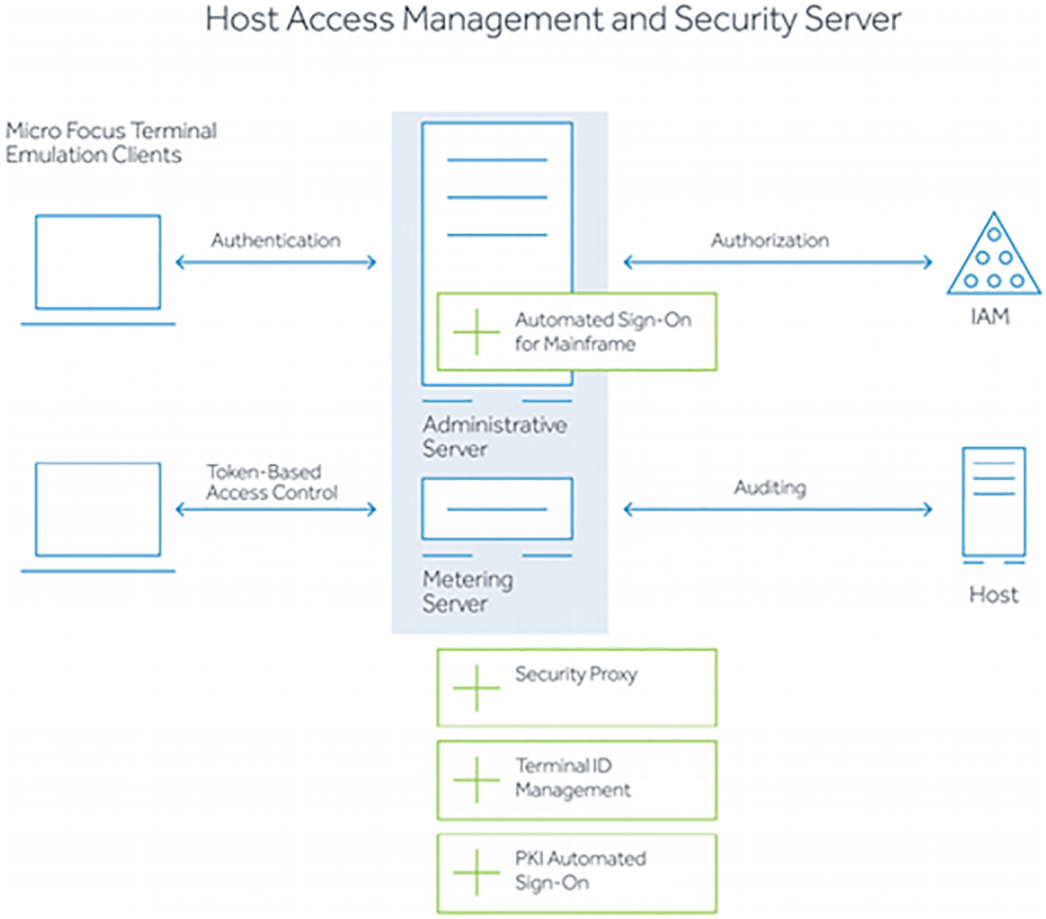


図 10. 端末 / レガシーアプリケーションのアクセス制御フレームワーク

最新リリースの HA-MSS は、ここに記載されている当社のアプリケーションセキュリティサービスとネイティブに統合されており、既存のレガシーシステム環境とゼロトラストイニシアチブとのシームレスな連携を提供します。そのため、お客様の環境向けに開発されているゼロトラスト機能を、レガシーアプリケーションに迅速に拡張できます。

API セキュリティの制御

最新のアプリケーションセキュリティスタックを使用することにより、ミッションパートナーやユーザーの API アクセスを保護しながら、アプリケーションインフラストラクチャを公開することなく、複数の API を容易に組み合わせて新しい機能を作成できます。包括的なソリューションである NetIQ Secure API Manager by OpenText は、開発、ライフサイクル管理、セキュリティに加え、REST、SOAP、IoT、レガシーカスタム API などのあらゆるタイプの API の統合と監視を目的に導入できます。NetIQ Secure API Manager には、拡張性の極めて高い API Gateway が備わっており、あらゆるタイプの API の保護、制御、変換、管理を行うためのオプションを提供します。API Gateway を使用すると、トラフィックを制御しながら、どこからでも API に安全にアクセスできます。

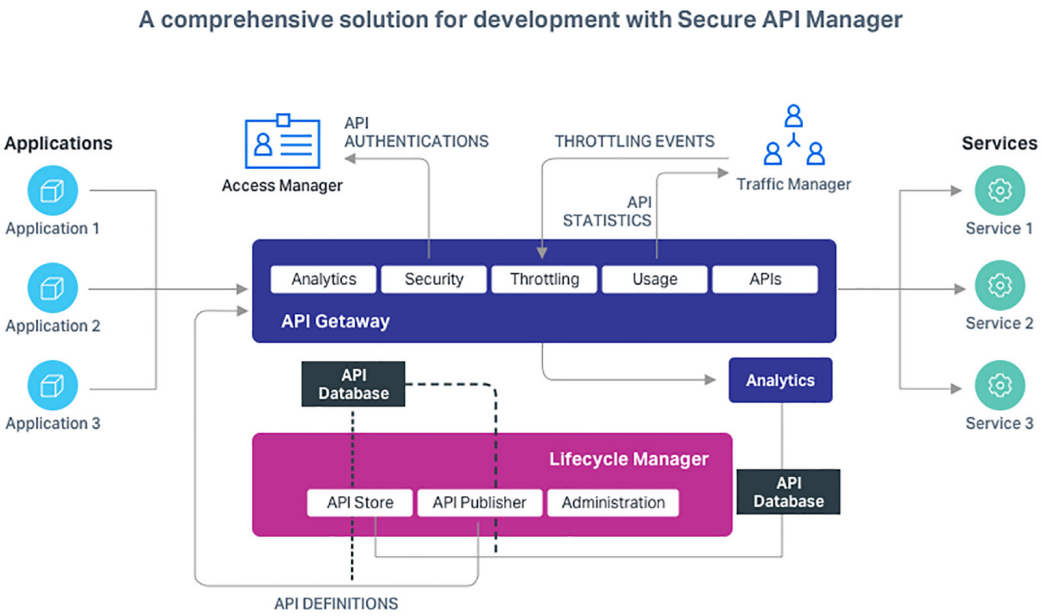


図 11. API およびマイクロサービスのアクセス制御フレームワーク

NetIQ Secure API Manager は NetIQ Access Manager と統合されており、NetIQ Access Manager が提供する堅牢な認証および権限付与機能を最大限に活用する API 管理およびセキュリティ機能を提供します。クラウド、Web、モバイル、レガシーアプリケーションの保護に使用されるのと同じインフラストラクチャを拡張して、API やマイクロサービスを保護できます。また、すべてのフェデレーション認証を利用することもできます。さらに、NetIQ Advanced Authentication と組み合わせることにより、サービスベースのアプリケーションでリスクベースの多要素認証を使用できます。

NetIQ Secure API Manager は、次の 2 つの主要な機能領域で構成されています。

- API Gateway は、サービス要求を処理するランタイム機能を提供します。セキュリティを強化し、API の使用を管理および制限するほか、バックエンドサービスとの間で要求と応答を変換します。これを実行する際には、API の使用状況の監視および分析用のデータを収集します。

- Lifecycle Manager では、API の実装と管理を行います。Lifecycle Manager は、新しいサービスの公開を処理し、既存のサービスの更新を制御しますが、最も重要なのは、API の廃止を管理できる機能です。また、Lifecycle Manager は監視および分析用に広範なデータを収集します。

NetIQ Secure API Manager は、アクセスおよび認証環境を拡張し、ミッションパートナーのあらゆるニーズに対応するセキュアな API 配信を実現します。API の管理性と実装時間の短縮に必要なアクセス制御と一元管理を行うことができます。そのため、従来および既存のセキュリティ強化方法と比較して、より優れたセキュリティを実現できます。

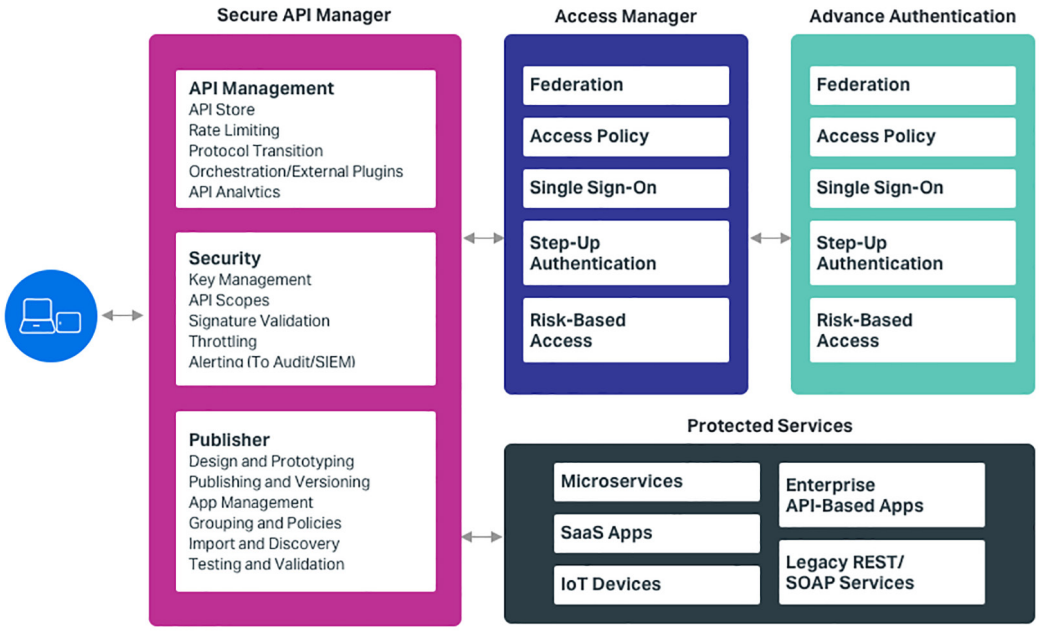


図 12. NetIQ コンポーネントの連携方法

NetIQ Secure API Manager を使用すると、アプリケーションがサービスを呼び出すレートを制限できます。レートはアプリケーションごとに制限でき、API ごとに合計トランザクションボリュームを適用することもできます。この機能を使用すると、リソースが過剰に使用されないようにすることができます。あるいは、差別化されたレベルのサービスを提供するためにこの機能を使用することもできます。NetIQ Secure API Manager の設定により、バックエンドサービスを呼び出すサービスのフローを制御することもできます。この機能を使用すると、バックエンドサービスに過度な負担がかからず、ユーザーがスムーズなパフォーマンスを体験できるようになります。応答内のデータがやや静的な場合は、バックエンドサービスからの情報をキャッシュすることもできます。

NetIQ Secure API Manager のゲートウェイを使用するもう 1 つのメリットは、API の使用状況とパフォーマンスに関する情報を容易にかつ一元的に収集できることです。NetIQ Secure API Manager には組み込みの分析機能がいくつかあり、このような情報を管理者とミッションパートナーのユーザーの両方に提示できます。

データ保護フレームワーク

データがより部門横断的に利用されるようになり、モバイルでのデータ利用も増えている今、既存の IT インフラストラクチャに広く組み込まれている従来型のデータセキュリティ対策は効果を次第に失いつつあることが証明されています。ハイブリッド IT への移行が進み、SaaS アプリケーションへの依存度が高まっていますが、自社開発のアプリケーションを API レベルで連携させることができない、またはそのような連携を実現できるだけの開発リソースがない組織もあるでしょう。

Voltage SecureData Sentry by OpenText は、オンプレミス、クラウド、ビッグデータ分析プラットフォームのどこに機密データが転送されても、そのデータを保護できます。Voltage SecureData Sentry の暗号化により、データプライバシー保護、データ漏えいの防止、安全なデータ利用による革新的なビジネス推進を実現します。

Voltage SecureData Sentry は、プライバシーのコンプライアンスを確保できるため価値実現までの時間を短縮でき、またエンドツーエンドで一貫した形でデータ保護を提供します。Voltage SecureData Sentry はオンプレミスにもクラウドにも導入でき、HTTP プロキシやロードバランサーなどの ICAP (Internet Content Adaptation Protocol) 対応のネットワークインフラストラクチャと通信し、クラウドとの間を行き来するデータにセキュリティポリシーを適用します。また、JDBC (Java Database Connectivity) や ODBC (Open Database Connectivity) API 呼び出しを代行受信して、データベースとの間を行き来するデータにセキュリティポリシーを適用します。導入先に関わらず、企業はインフラストラクチャを完全に制御できます。暗号化キーやトークン保管庫を他の関係者と共有する必要はありません。Voltage SecureData Sentry の検査モードでは、機密情報を含む特定のデータフィールドと添付ファイルをセキュリティポリシーの対象にすることができます。

Voltage SecureData Sentry は、クラウドソフトウェアサービスおよびオンプレミスアプリケーションのデータ保護に特化した製品です。Voltage SecureData Sentry のデータ保護テクノロジーは、Salesforce、ServiceNow、OpenText ALM Octane、Microsoft Dynamics 365 などの SaaS アプリケーションや、商用アプリケーション (COTS) に拡張することができます。Voltage SecureData Sentry は、データフロー傍受の手法を使用してネットワークを流れる機密データを保護します。そのため、SaaS アプリケーションや COTS アプリケーションで使用されるデータのセキュリティも確保できます。

Voltage SecureData Sentry は、ユーザーと、そのデータが使用され通常は保存されるターゲットアプリケーションまたはシステムの間のデータトラフィックを傍受します。この保護の目的は、ターゲットアプリケーションのコア機能を妨害することなく、ターゲットアプリケーションやデータベースから機密情報を隠すことです。保護されたシステムのユーザーは、保護が行われていることに気づかない場合があります。また、データが保護されていることをユーザーが識別できるように、意図的にデータを保護または変換するような保護機能を設定することもできます。大まかに言うと、コンテンツと関連メタデータは、ICAP プロキシまたはデータベースラッパーから、Voltage SecureData Sentry Engine によって受信されます。Voltage SecureData Sentry は、管理者が設定したプロファイルを使用してデータを分析し、保護が必要なデータを特定します。保護フローにより、データの保護方法と、データがソースアプリケーションに返される形式が決定されます。

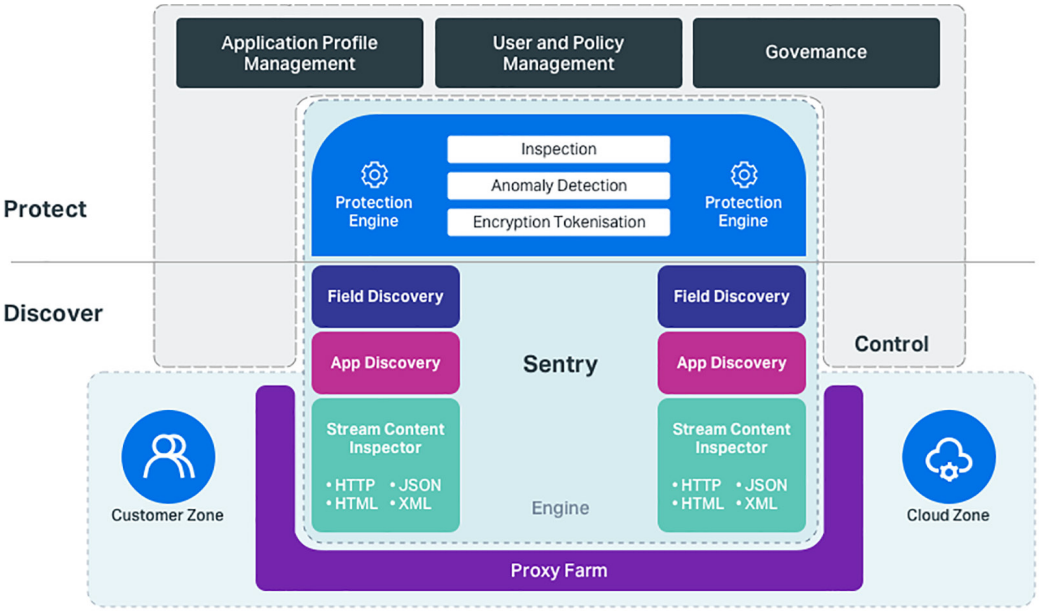


図 13. Voltage SecureData Sentry のデータフロー

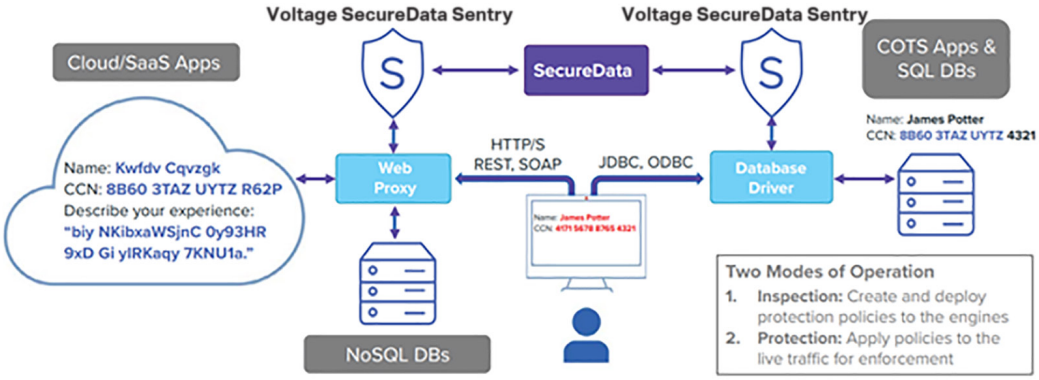
Voltage SecureData Sentry は、アクセス時にデータをマスキングするためにも使用できます。保護フローが柔軟性に富んでいるため、Voltage SecureData Sentry は、アクセス時にデータを復号化するのではなく、データを保護 / マスキングできます。たとえば、海外からアプリケーションにアクセスするユーザーは、機密データにアクセスできません。これらのユーザーのトラフィックが Voltage SecureData Sentry を介してルーティングされると、応答内の機密フィールドを検出して保護できます。データ自体は暗号化されない状態で保存されます。

Voltage SecureData Sentry は、保護が必要なデータについて、ユーザーとリモートサーバー間の HTTP および HTTPS トラフィックを検査します。これは、クラウドアプリケーションやカスタムまたはオンプレミスの Web アプリケーションに送信されるデータを保護するための一般的なシナリオです。通常、Web ブラウザーやユーザーのシステムが、Web アプリケーションへの HTTP 要求を準備します。この要求は、ICAP プロキシを経由して Voltage SecureData Sentry Engine に渡されます。

または、プロキシチェーンを使用して、Voltage SecureData Sentry Engine に要求を転送することもできます。この場合、外部プロキシが、保護されたアプリケーションの要求と応答を、ICAP をサポートする親プロキシに転送します。親プロキシは、Voltage SecureData Sentry Engine に要求を転送します。

Voltage SecureData Sentry Engine は、要求のヘッダーとコンテンツを使用して、要求の保護を行うかどうか、そしてどのように保護するかを決定します。要求内の個々のデータフィールドは、個人情報を暗号化された同等の情報に置き換えるなどの方法で保護できます。保護フィールドを含む完全な要求は、元のプロキシに転送され、次にターゲット Web アプリケーションに転送されます。

同様に、Web アプリケーションはユーザーに応答を返し、プロキシを介して送信され、分析のために Voltage SecureData Sentry Engine に提示されます。応答のヘッダーと内容は分析され、通常は元の要求とは異なるプロパティを使用して保護できます。また、応答内に暗号化されたデータが含まれている場合もありますが、これは復号化できます。これは高度にカスタマイズ可能で、必要なセキュリティを確実に維持できます。復号化されたフィールドや変更されたフィールドを含む完全な応答が生成され、最終的に元のプロキシを介してエンドユーザーに転送されます。



Voltage SecureData Sentry consistent and transparent data protection, on premises and in the cloud.

図 14. エッジでのハイブリッドアプリケーションデータ保護

SQL データベースから取得された挿入データは、Voltage SecureData Sentry を使用して分析し、保護することもできます。これは、JDBC と ODBC で利用可能なカスタムドライバーを使用して行われます。このカスタムドライバーは、クエリーと関連パラメータを Voltage SecureData Sentry Engine に転送します。Voltage SecureData Sentry Engine でアクティブになっているプロファイルに応じて、クエリーとパラメータが分析され、保護されます。たとえば、データベースに入力されるデータ値の暗号化が行われます。変更されたクエリーとパラメータは、ドライバーに再び返されます。それらを組み合わせて、保護されたデータをデータベースに配信する新しいデータベース呼び出しにすることができます。

データベースから値を取得する場合は、その逆も可能です。値は Voltage SecureData Sentry に転送して再度保護することができます。通常は復号化されます。復号化された値は、ユーザーに提示できる状態になります。

柔軟な導入オプション

チーム編成やミッションの優先順位によって、導入する最適なオプションは決まりますが、OpenText はお客様の成功を確実にするため、市場で最も幅広いテクノロジーオプションを提供していますのでご安心ください。

Deployment options	physical	virtual	containers	SaaS*	public cloud	private cloud	hybrid
NetIQ Advanced Authentication	✓	✓	✓	✓	✓	✓	✓
NetIQ Access Manager	✓	✓	✓	✓	✓	✓	✓
NetIQ Risk Service	✓	✓	✓	✓	✓	✓	✓
ArcSight Intelligence	✓	✓		✓	✓	✓	✓
Voltage SecureData	✓	✓		✓	✓	✓	✓

図 15. ミッションに応じた導入オプション

エッジでの共有ゼロトラストサービス

OpenTextのアプリケーションセキュリティサービスは、サードパーティのSD-WANソリューションが環境要件を満たすのに役立つだけでなく、以下のような共有ゼロトラストサービスを通じて、選択されたSD-WANソリューションと環境の両方の成熟度をより広範に加速させるうえでも役立ちます。

- ダイナミックな多要素認証サービス：30以上のMFA方式、ステップアップ認証。
- 継続的なリスク分析サービス：属性と行動を組み合わせたリスクポリシー。
- 高度なエンティティ行動分析サービス：MITRE ATT&CKおよびEDR脅威分析。
- アプリケーションおよびAPIセキュリティポータル：ユーザーセルフサービス、シングルサインオン、一元管理。
- アプリケーションデータ保護サービス：機密データの漏洩を防ぎ、フィールドレベルのデータを検知して保護。
- 主要なアクセスインテリジェンスデータのセキュリティ運用との共有：リスクダッシュボード、データフィードへのアクセス、優先脅威アラート。

主なメリットの概要

OpenText のアプリケーションセキュリティサービスは、エッジでのゼロトラストに対応するよう設計された統合製品セットであり、高度なエンタープライズアプリケーションセキュリティ機能をエッジなどに提供することにより、環境の成熟度を迅速に向上させる機会を提供します。

これらのサービスが提供する独自のメリットは、次のとおりです。

- 極めて高度なリスク分析を継続的なアクセスの決定に適用。
- エッジでユーザーアプリケーションとデータを対象にした主要なゼロトラストサービスを実現。
- 高度な脅威検知機能 (初回アクセス、特権昇格、ラテラルムーブメント、その他の TTP) により、ZTA の成熟度を向上。
- 機密データをエンドツーエンドで検知して保護。
- レガシーアプリケーションとの統合パスの提供。
- 実証済みのスケーラビリティを備えた、極めて柔軟性の高いハイブリッド導入オプション。
- アプリケーションセキュリティスタックの統合に伴うリスクとコストを最小限に抑制。ゼロトラスト機能の幅広いセットを提供する唯一のベンダー。
- 過去の実績と政府機関での導入事例を有する、米国政府機関向けの定評があり信頼できるソフトウェアメーカー。
- ゼロトラストの専門知識、政府機関での経験が豊富なエンジニア、確立されたパートナーエコシステム。

OpenText の政府機関向けソリューションを、ぜひお客様のゼロトラストチームに加えてください。ZTA への円滑な移行とより効果的なセキュリティ運用を促進するため、ミッション目標を可能な限り迅速に達成できるよう積極的に貢献します。

NetIQ by OpenText について

このたび、OpenText による、CyberRes を含む Micro Focus の買収が完了しました。両社の専門知識の融合によって、セキュリティ製品 / サービスの提供が拡張され、権限とアクセスの制御の自動化を通じて、アプリケーション、データ、リソースへの適切なアクセスを確保することにより、お客様の機密情報の保護を支援します。NetIQ Identity and Access Management は OpenText Cybersecurity の一部であり、あらゆる規模の企業やパートナーに包括的なセキュリティソリューションを提供します。

お問い合わせ
www.opentext.com

OpenText 政府機関向けソリューション
Rockville Office
One Irvington Center
700 King Farm Boulevard
Suite 125
Rockville, MD 20850-5736
米国
電話：+1-301-838-5000

お問い合わせ先情報とオフィスの所在地：
www.microfocusgov.com

opentext™ | Cybersecurity

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurity のお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。

762-JA0088-002 | O | 08/24 |