opentext™ | Cybersecurity

ブローシャ

NetIQ as a Service

SaaS 型 ID およびアクセス管理

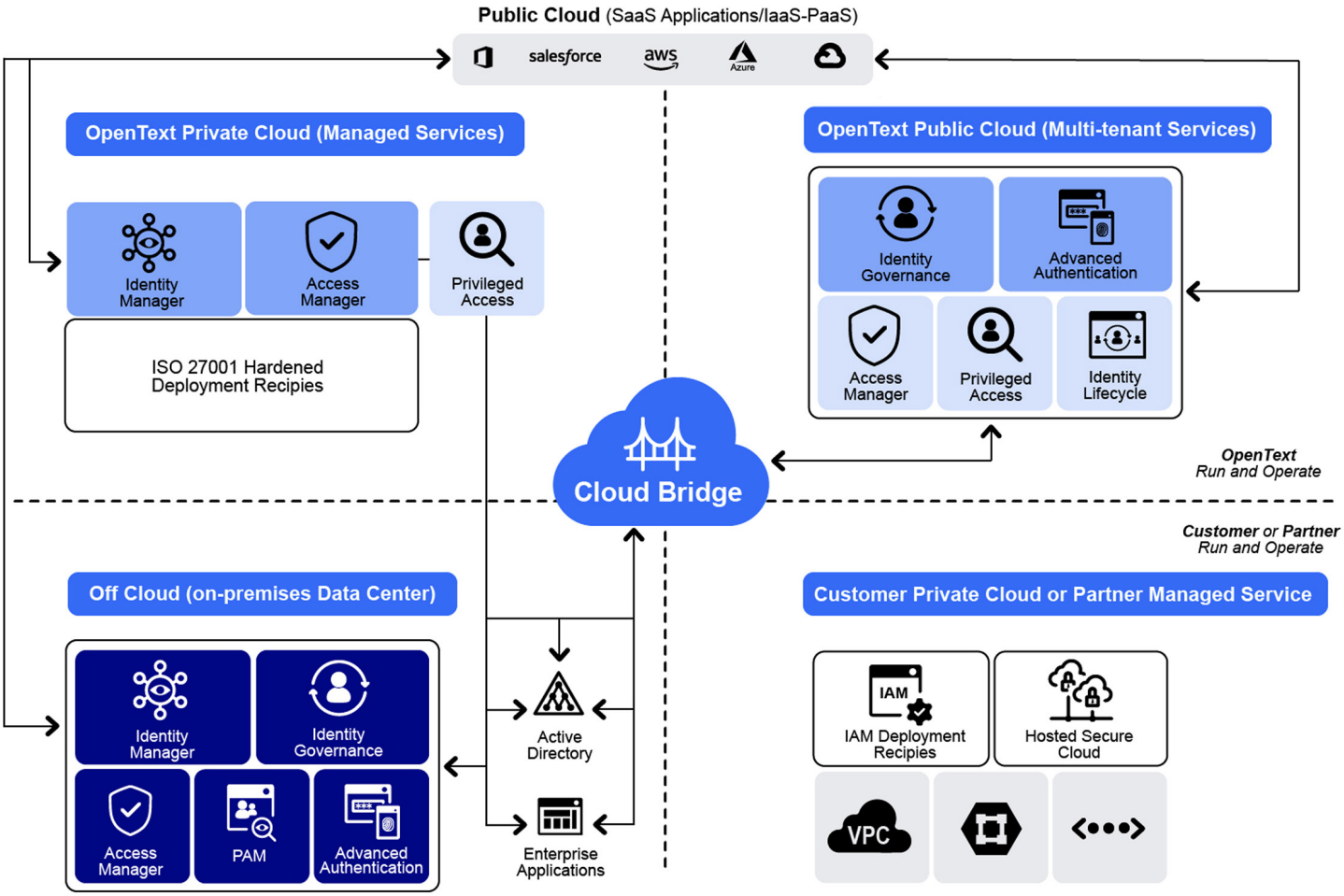
クラウドベースの IAM (ID およびアクセス管理) ソリューションは、どれも同じではありません。妥協や制限を強いられる企業もあります。特に、複雑な環境を持つ組織ではその傾向が強くなります。

大抵のことがそうであるように、ユーザーが自由かつ安全に運用できる ID 対応のデジタルサービスの実現には、決まった単一のアプローチはありません。それぞれ独自のアプリケーション、構成、文化的要件があるため、各組織に固有性があります。組織が確立しているほど、特定のニーズから伝統的なコアサービス群を維持する必要がある可能性が高くなります。そのため、純粋な SaaS 製品によるプラットフォームでビジネスを運営できる組織もありますが、多くの組織では、多年にわたる IT 投資や事業買収により、旧来のクラウドベースのマイクロサービスや SaaS ベースのデジタルリソースが混在する状況に追い込まれています。

一部の組織では、コアとなるサービスの確保に留まらず、IT の能力を競争上の差別化要因と見なし、生産性と消費者エンゲージメントを向上させるために投資しています。こうしたベストオブブリードの考え方から、結果として異質で複雑なデジタル環境ができる場合がよくあります。

すべてのデジタルモデルに対応する NetIQ

それぞれの組織に固有の性質があり変化するため、NetIQ by OpenText™ では、プラットフォームの実装について複数のオプションを用意しています。まず、NetIQ が提供するさまざまなタイプの IAM 製品とサービス、およびそれらで実現される環境について簡単に説明します。



Cloud Bridge によるハイブリッド IAM の実現
NetIQ Identity and Access Management (IAM) by OpenText™ は、組織のデジタルサービスモデルに関係なく、その機能全体を活用できるという点でユニークです。競合するソリューションはさまざまなカテゴリの機能を備えていますが、NetIQ は、組織のデータとサービスのモデル全体で同等の機能を備えた ID プラットフォームを提供します。これは時間の経過とともに進化するモデルであり、別の部門間では一致していない可能性があります。

NetIQ は Cloud Bridge ソリューションによってこのような柔軟性を得ています。これは、NetIQ by OpenText™ サービスと、データセンター、クラウド (パブリックおよびプライベート)、さまざまな ID プロバイダーを介して NetIQ にアクセスするエンティティの間の安全な通信を提供するための中心的な役割を果たします。Cloud Bridge は、従来の IAM ソリューションが提供する高度な機能と同様の機能を実現します。これにより、プラットフォームを継続的に構成、拡張して、固有の要件を解決できます。お客様の社内環境で実行することも、クラウドベースのサービスの一部として使用することもできます。多くの場合、IAM の専門能力を持ち、特定の要件に合わせて柔軟にカスタマイズできることを求める組織にこのような形態は好まれることが多いです。

プラットフォームメンテナンスのオーバーヘッドを削減する目的で、お客様はこれらの製品を AWS などの IaaS に配置することを選択できます。NetIQ ポートフォリオのほとんどは、自動化された Kubernetes 管理だけでなく、クラウド内構成も可能な Docker コンテナオプションが提供されています。

NetIQ SaaS 製品

NetIQ Identity Governance and Administration (IGA) の分析とリアルタイムの対応により、適切なレベルのアクセスを実現できます。多様な環境をサポートしており、強固な ID 基盤に基づいて構築されています。NetIQ IGA by OpenText™ は、大規模で複雑なハイブリッド環境で優位です。

NetIQ Advanced Authentication by OpenText™ は、パスワードレス認証テクノロジーを提供しており、煩雑さのない多要素認証を柔軟に実装できます。標準ベースのフレームワークにより、すべての認証サイロを単一のポリシーセットに統合できます。

NetIQ Identity Governance SaaS
NetIQ Identity Governance SaaS by OpenText™ の使用により、どのような組織でもリスクポリシーをより高いレベルのセキュリティと生産性に向上できます。自動化されたコンプライアンスチェックとレポート機能により、コンプライアンス目標の達成を支援します。

NetIQ Identity Governance は、数週間や数か月といった時間をかけることなく数時間で稼働できるように構築されており、エラーが発生しやすく時間のかかる手動方式に頼る必要はありません。手動方式では、コンプライアンス違反や過剰なアクセスによるリスクを招きがちです。NetIQ Identity Governance by OpenText™ では、社内でのユーザーの役職変更に伴い過度の権限が意図せずに付与された場合など、ユーザーに必要のないリソースへのアクセス権を迅速に特定して取り消すことができます。また、複数のシステム、アプリケーション、データからユーザーのエンタイトルメント情報が収集され、一括表示されます。その結果、LOB マネージャーにとってわかりやすいレポートが提供され、マネージャーはそのレポートに基づいて既存従業員のアクセス権が適切かどうかを確認し、必要に応じてアクセス権を取り消すアクションを即座に開始できます。NetIQ Identity Governance では、次のことが可能です。

- オンプレミス、ハイブリッド、クラウドのアプリケーションを含むインフラストラクチャ全体からエンタイトルメントデータを収集してレビューし、誰がどのリソースにアクセス可能かを正確に把握できます。
- 分析と役割マイニングを活用：エンタイトルメントの共通点を特定し、「what if」分析を実行して、コンプライアンスの測定基準とレポートを作成します。
- アクセス認証を実施：承認者の意思決定のサポートや管理者への問題のエスカレーションなど、自動通知や進捗報告によってアクセス認証プロセスがスケジュール通りに進むようにします。
- 違反や例外を検出し、それに対処する操作を定義：職務分掌 (SoD) 違反や放置されたアカウントなどを検出し、それに対処する操作を定義することで、リスクを低減できます。
- 業務に基づく役割と属性権限付与モデルを作成：これによってアクセス認証やアクセス要求の範囲と期間を縮小し、承認プロセスを短縮できます。これにより、すべてのエンタイトルメントではなく、例外に注目できるようになります。
- 修正作業の繰り返しを排除：ServiceNow や Remedy などのサービスデスクソリューションと統合することでチケット発行を自動化し、Identity Manager と統合することでフルフィルメントを自動化できます。
- リスク測定によりレビューを優先順位に基づいて実施：属性値、所属グループ、管理関係、アプリケーション、権限、コスト、リスクなどの基準に基づいたリスク測定により、最も必要性が高いものに注目を促すことで、レビューを優先順位に基づいて実施できます。
- ID ガバナンスに関するレポートを作成：エンタイトルメント、認証状況、要求と承認、ポリシー違反が盛り込まれた ID ガバナンスに関するレポートを作成できるため、監査報告が容易になります。スケジューリング機能や配布機能も標準でサポートされています。

NetIQ Identity Governance のリアルタイム適応型ガバナンスにより、継続的なリスク削減が可能です。競合他社のソリューションでは、特定の時点でのエンタイトルメントは収集されますが、次の収集が行われるまでの間、組織はリスクにさらされたままになります。NetIQ Identity Governance は、変更やイベントが発生したときにそれらに適応し、必要に応じてレビューをトリガーしてコンプライアンスを確保することにより、この空白を埋めます。これらのコストとリスクに関するインサイトから、多忙な承認者にビジネスレベルの情報が提供されるので、一貫した適切なエンタイトルメントの決定を簡単に実施できます。

NetIQ Advanced Authentication は、インテリジェントで適応性の高いテクノロジーでもあります。ユーザーのスマートフォンを使用して位置情報を活用し、目的とするレベルの利便性とセキュリティを提供する認証の種類を制御できます。また、測定されたリスクに基づいて、定義したタイプに認証のレベルを上げるために一般的に使用される他の指標も含まれています。

NetIQ Advanced Authentication SaaS
NetIQ では、Advanced Authentication (リスクサービスはオプション) と Identity Governance をフルサービスとして提供しています。リスクサービスの行動分析プラグインは、Interset テクノロジーに基づいており、サービスとして提供されます。サービスを有効にするには、お客様は資格情報とライセンスキーを指定するだけでよく、設定やメンテナンスは必要ありません。

統合 MFA アプローチのおかげで、NetIQ Advanced Authentication の構成や維持は他のソリューションほど複雑ではありません。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。当社製品を導入することで、企業全体のセキュリティとユーザビリティを向上させることができます。

また、MFA インフラストラクチャの新規構築、置き換え、統合を自由に行うことができるため、コストを管理し、投資を最大限に活用することができます。CTO やアーキテクトは長期にわたって、オープンスタンダードの利点を理解してきました。本質的に相互運用性を備えているため、アプリケーションやプラットフォームに依存することはなく、アーキテクチャの長期的な整合性を確保できます。しかし、独自のプロトコルで構築された認証ソリューションを導入すると、ニーズに最も適したデバイスを最良の価格で購入する自由はその組織にはもうありません。また、ベンダーロックインにも陥る可能性があります。

NetIQ は FIDO (Fast Identity Online) Alliance のメンバーであり、支援者です。FIDO U2F (Universal 2nd Factor) は、ユーザー自身が認証デバイスを管理する環境を組織がサポートできるようにします。NetIQ Advanced Authentication では、堅牢なフレームワークによって、開発を行わなくてもこうしたサポートがお使いのアプリケーションに提供されます。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だけでなく、ユーザーはデジタルライフの他の側面にも高いレベルのセキュリティを導入できるようになり、セキュリティ体制を向上できます。

IT グループは、今日の最新の認証規格を最低限しかサポートしていないソリューションを選択することには用心深くなる必要があります。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います。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ため、このことは重要です。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) を備えているため、既存の環境に幅広く対応できます。さらに、フレームワークが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、柔軟性に最適なオプションが提供されます。市場で最も広範なネイティブ統合を提供し、標準ベースのアプローチでベンダーロックインから保護します。

NetIQ Access Manager
NetIQ Access Manager by OpenText™ は、Web シングルサインオンソリューションをユーザーに提供するリーディングプロバイダーです。単にフェデレーション機能を統合するだけでは不十分なマルチプラットフォーム環境に特に適しています。多くの組織はアクセスの一元的な制御や、特別なユーザーエクスペリエンスのための設計を必要としています。複数のアプリケーションを 1 つのユーザーエクスペリエンスに統合する必要がある場合にも、NetIQ Access Manager は効果を発揮します。

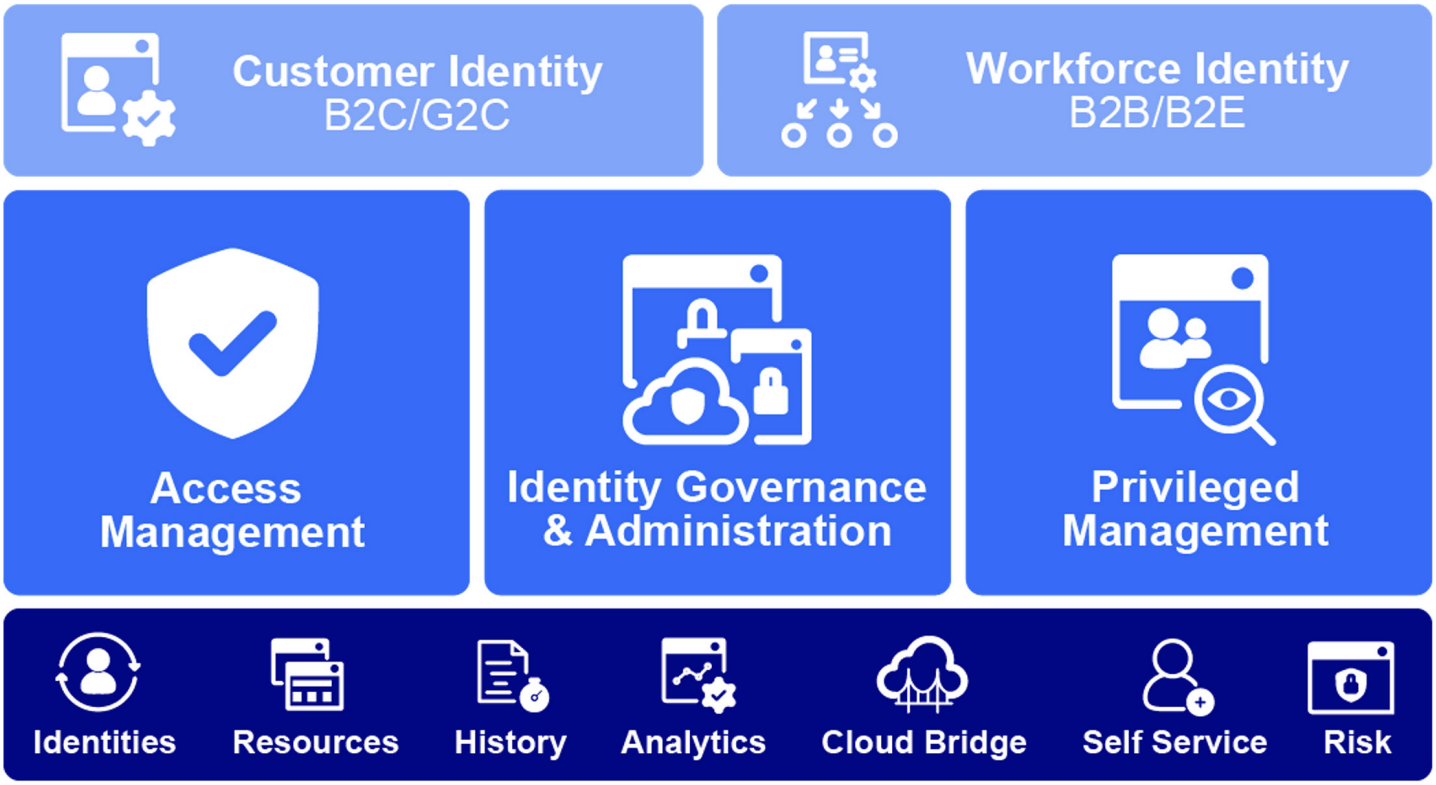
- **包括的でセキュアな Web アクセス管理**—NetIQ Access Manager は、企業全体でシングルサインオンとアクセス制御を実現します。クラウドベースまたは複雑なイントラネット環境に特化したソリューションは必要ありません。
- **パートナーとのより効果的な共同作業**—強力なシングルサインオンサポートに加えて、ミニポータル、モバイル SDK、さらにはモバイルゲートウェイを使用することで簡単にアクセスすることができます。パートナーとのデジタルインタラクションに適したアクセス管理ソリューションを選択すると、個人情報の共有が促進され、最終的にはコラボレーションがより効果的になります。
- **顧客のためのシンプルでセキュアなアクセス**—今日のデジタル顧客は、自分が利用したいサービスに自身で登録し、いつでもセルフヘルプや自己管理ができることを望んでいます。より高いレベルのセキュリティを必要とする組織では、NetIQ Access Manager を使用すると、ユーザーの利便性を維持しながら、リスクに合わせてセキュリティを強化できます。

NetIQ Identity Manager
NetIQ Identity Manager by OpenText™ は、ID 管理のライフサイクル全体を強化し、ID とそれに関連する属性を管理して権限の付与を最小限に抑えます。これにより、手作業でのアカウント管理に要するコストを削減し、コンプライアンスを実証できると同時に、不正アクセスのリスクを低減できます。組織全体の重要なステークホルダーにメリットがあります。NetIQ Identity Manager は、モジュール型でありながら統合的に ID ライフサイクル全体を管理できるように設計されているため、現在のニーズだけでなく将来発生するニーズにも対応できます。

- ユーザー等のプロビジョニング、デプロビジョニング、アカウント管理を自動化。
- オンボーディングからプロジェクトレベルの承認、アカウントの無効化に至るまで、完全なユーザーライフサイクル管理を実現する強力なルールエンジンと広範なコネクタ。
- イベント駆動型自動化エンジンによる、ID およびアクセスのガバナンス要件に基づく即時自動化。
- 監査またはコンプライアンスの要件を満たすために必要なレポートの提供。

NetIQ Privileged Account Manager
一般的なユーザーベースのアクセスを管理するだけでなく、このタイプの制御を、その情報を管理する基盤システムまで拡張することが重要です。NetIQ Privileged Account Manager by OpenText™ は、組織全体のシステムおよびデータソースへの特権アクセスに重点を置くことで、このニーズに対応します。多くの場合、最も大きな損害につながる侵害は、特権アカウントを悪用したものです。

NetIQ Privileged Account Manager は、特権ユーザーによる最も機密性の高い情報へのアクセスを保護するために必要な、特殊なレベルの監視と制御を提供します。より深いレベルの監視だけでなく、詳細なフォレンジックデータも提供します。



NetIQ SaaS のプラクティスとプロセス

NetIQ は、従業員と顧客の ID を管理するための SaaS 型 ID およびアクセス管理により、組織を保護します。保護する必要があるすべてのリソースの最新のカタログを維持し、インテリジェンスの追加により、それらへの適切なレベルのアクセスを保証します。また、組織全体向けに設計された堅牢な認証フレームワークも提供します。NetIQ は、こうしたサービスのお客様への提供において業界をリードすべく取り組んでいます。

データ処理

OpenText は、マルチティア、マルチデータセンターのデータ取り込みパイプラインを使用して、複数の入力からのデータを処理できるネットワークデバイスを介してデータをセキュアに処理します。このデータは NetIQ サービスの外に出ることはなく、適切に認定された資格を持つユーザーのみがアプリケーションを通じてアクセスできます。

OpenText サービスプラットフォーム

NetIQ SaaS サービスは、Amazon Web Services (AWS) 上で動作します。クラウドセキュリティは、AWS の最優先事項の 1 つです。この目的で、OpenText は AWS のインフラストラクチャを活用して、顧客のプライバシーを保護するための強力な保護策を実装します。すべてのデータは安全性の高い AWS データセンターに保存されており、これによってコンプライアンスプロファイルの中でデータセンターに関連する部分はすべて完備していることになります。これにより、最高水準のセキュリティを維持できます。OpenText はプラットフォームの弾力性とセキュリティ設計を活用して、どのような規模でもセキュリティを確保します。AWS インフラストラクチャは、お客様の規模によらずデータを安全に保つように設計されています。

AWS の主要機能の 1 つは、可用性ゾーンを使用して、同じリージョン内の複数のデータセンター間でアプリケーションとデータのレプリケーションを行うことにより、ビジネス継続性を実装できることです。その一方で OpenText は、データが物理的に配置されている地域に対する完全な制御と所有権を保持し、地域のコンプライアンスとデータレジデンシー要件を簡単に満たすことができます。

プライバシーを高め、ネットワークアクセスを制御するために、OpenText は AWS を活用して次のようなセキュリティ機能とサービスを提供しています。

- Amazon VPC に組み込まれたネットワークファイアウォールと AWS WAF の Web アプリケーションファイアウォール機能により、プライベートネットワークの作成や、インスタンスとアプリケーションへのアクセスの制御が可能。
- すべてのサービスで TLS を使用して転送中に暗号化。

NetIQ サービスの可用性は非常に重要です。そのため、OpenText チームは AWS に組み込まれているサービスとテクノロジーを基盤から活用し、DDoS 攻撃に直面したときの復元力を向上させます。さらに、プラットフォームの機能を活用して多層防御戦略を実現し、これにより攻撃を阻止し、さまざまなツールを使用して、クラウドサービスが OpenText の標準とベストプラクティスに準拠していることを確認しながら迅速に行動できます。

コンプライアンス

AWS で SaaS インフラストラクチャをホスティングすると、OpenText と AWS の間で責任共有モデルが作成されます。ホストオペレーティングシステムと仮想化レイヤーのレベルから、サービスが動作する施設の物理的なセキュリティまで、AWS がコンポーネントの運用、管理、制御を行うため、この共有モデルによって運用負荷が軽減されます。

AWS クラウドインフラストラクチャには非常に多くのセキュリティ機能が組み込まれているため、OpenText チームは、NetIQ 環境のセキュリティ (アップデートとセキュリティパッチを含む)、および Cloud Bridge の構成と操作などの AWS から提供されるセキュリティ機能の構成に集中しています。

セキュリティおよびリスク管理

ここまでで OpenText のコンプライアンスプログラムを詳細に確認しました。これらのプログラムでは、標準化されたコンプライアンスプロファイルが使用されます。この理由は、ソフトウェアベースのサービスに関する保証を表明するために業界が開発した方法であるからです。NetIQ サービスについては以下の状況です。

- ISO 27001:2013 の認証を取得済み。ISO 27001:2013 は最も高度なセキュリティ標準管理が実装および維持されていることを証明し、NetIQ SaaS 製品のセキュアなデリバリーが認定されます。
- ISO 27034-1 の認証を取得済み。ISO 27034-1 はアプリケーションのセキュリティ基準で、NetIQ 製品の開発ライフサイクルの一環として、セキュリティのプロアクティブな統合が認定されます。

NetIQ サービスのセキュリティおよびリスク管理

OpenText チームは、関連するコンプライアンスプログラムを詳細にレビューします。これらのプログラムは、標準化されたコンプライアンスプロファイルを使用し、ソフトウェアベースのサービスに関する保証を実現します。これらのコンプライアンスプロファイルには、OpenText がソリューションを開発および導入し、サービスを運用する方法について、一定の形式と厳密性が必要です。この形式を背景に、OpenText はこれらの要件を満たすために、サービスの提供について特定の行動を取りました。以下のセクションでは、「非形式な用語」で、OpenText SaaS チームが次のことを保証するために取る行動について説明します。

- システムはセキュリティ機能を備えるように設計されています。サービス拒否から脆弱性の悪用、マルウェアに至るまで、さまざまな形態のセキュリティ攻撃に耐えることができます。
- サービスが特定の顧客向けに構成される際には、SaaS チームは専門的に文書化されたプロセスでサービスを構築します。重要な決定は慎重に行われ、文書化されます。
- 顧客のデータのプライバシーを明示することは最も重要なことであり、いかなる場合も OpenText はその管理責任を放棄することはありません。
- NetIQ 製品は、高可用性を実現するように構成されています。お客様が必要なときに安心して使用できるようにするため、スピードと耐障害性は不可欠です。ハードウェアやネットワークの障害など予期しない問題が発生した場合、当社のプラットフォームチームはそれに対応し、ID とアクセスの機能を維持するための措置を講じます。
- OpenText SaaS チームは非常に誠実で、全員が自分の仕事を理解しており、サービスを提供するために必要な社内プロセスを迅速に進める方法を熟知しています。
- OpenText SaaS チームは、攻撃やパフォーマンスの低下に対してシステムを定期的に監視およびテストし、予防メカニズムが機能していることを確認します。

セキュアなソフトウェア設計ライフサイクル

セキュアな開発ライフサイクル (SDL) は、ソフトウェア開発に焦点を当てたセキュリティ保証プロセスです。これは全社的な取り組みで、必須のポリシーとして、セキュリティを最初から「設計に組み込んで」います。NetIQ チームにとっての SDL は、教育、継続的なプロセス改善、アカウンタビリティという 3 つのコアコンセプトに基づいています。

OpenText は、SaaS 対応のすべての製品のペネトレーションテストを実施しています。評価結果は SDLC プログラムの SLA に従って修正され、重要な指摘事項は直ちに緩和され、パッチがリリースされます。さらに、STAT と呼ばれる内部プラットフォームを使用して自動スキャンを実行します。

STAT は、アジャイルと DevOps を目指した自動セキュリティテストプラットフォームであり、日常的に使用してソースコードとアプリを自動的にスキャンし、ほぼリアルタイムで新しい脆弱性を遮断します。

これらのスキャンには、WebInspect、OWASP Dependency、Checker、CoreOS Clair、Fortify、Nessus などのツールを使用します。

アクセス管理

NetIQ プラットフォームへのアクセス制御は、コアとなるセキュリティ対策であるため、ポリシーによって制御および適用する必要があります。OpenText サービスは特定のプロセスを起動して、過度の管理者権限を防止し、管理者によってアクセスが承認された管理者の数を制限します。

アカウント所有者は root アクセスキーを保持しており、これは次のような考慮すべき点に関してセキュリティに影響します。

- アカウントの変更を監視し、確認すること。
- アカウントの数が最小限であり、放置アカウントを検出するために定常的にレビューする。
- 終了時にアカウントを無効にするまでの平均時間。

ID およびアクセス管理の専門家であるという観点から、OpenText は特殊なクラウド管理ツールを使用してアカウントへのアクセス管理と権限の委任を実施し、アカウント所有者がすべてのアクセスを管理できるようにします。

- アカウント管理者の委任は監視され、ユーザーに管理者アクセスが許可されるたびにアラートが発行されます。
- アカウント管理者の委任のリクエストは、SaaS セキュリティ担当者によって承認されます。

本番リソースやバックアップリソースなど、組織の個別のアカウントに対して複数の AWS アカウントを作成します。この分離により、さまざまな種類のリソースを明確に分離できて、優れたセキュリティ上の利点が得られます。

ユーザーアクセスレビュー手続き
OpenText チームは、アクセス管理のための定期的なレビューを実施して、必要な担当者が重要なシステムにアクセスでき、権限のない従業員 (あるいは悪意を持った者) がアクセスできないようにします。このプロセスには以下のような内容が含まれます。

- 従業員プロファイルのマネージャーレビュー
- 従業員の退職手続きの確認
- レビューとコンプライアンスの自動化
- 管理グループメンバーの確認
- 期限切れにならないパスワードを使用したプロファイルの確認

侵入および脆弱性のテスト
ペネトレーションテスト (またはペンテスト) は、システムの攻撃に対する耐性をテストするために、システムのセキュリティ制御をバイパスするように設計された一連の手順です。NetIQ SaaS 製品は非常に重要であると見なされており、すべてのメジャーリリースがテストされています。インフラストラクチャはほとんど変更されないため、運用ペネトレーションテストは毎年 1 回実施されます。
脆弱性スキャンは、インターネットに接続されたアセットに対して毎月実施され、その指摘事項はパッチ管理プログラムに従って修正されます。OpenText NOC チームは修正プロセスを監視し、パッチ適用 SLA が満たされていることを確認します。緊急アップデートは、パッチの安定性を確保した上で、できるだけ早く実行されます。これらのアップデートは、サーバーで発生している既知の問題を修正できる場合にのみ適用されます。

重要な更新は、パッチの安定性と緊急 CAB を確認した後、7 日間の期限内の運用時間外に適用されます。重要度の低いシステムに対する重要度の低い更新は、2 か月の期限内に定期的にスケジュールされたメンテナンスウィンドウで実行されます。

プラットフォームセキュリティチェック
OpenText チームは、数十万の AWS 顧客にサービスを提供してきた、運用履歴全体から学んだベストプラクティスを活用するアプリケーションを使用しています。このテクノロジーは、NetIQ 環境を検査し、システムパフォーマンスの向上とセキュリティギャップの解消につながる推奨事項を作成します。次の項目を確認します。

- 特定のポートまたはリソースへの無制限アクセス (0.0.0.0/0) を許可するルールを持つセキュリティグループ。
- 悪意のある活動 (ハッキング、DoS 攻撃、データ損失) の可能性を高める無制限アクセス。リスクが非常に高いポートには赤色のフラグ、リスクが低いポートには黄色のフラグを付与。
- 緑色のフラグが付いたポートは、一般的に HTTP や SMTP など無制限のアクセスを必要とするアプリケーションで使用されるもの。
- ルートアカウントである AWS IAM を使用し、MFA が有効になっていない場合に警告。
- すべてのユーザーにアップロード / 削除アクセス権を付与するオープンアクセス権限。これにより、誰もがアイテムを追加、変更、削除できるようになり、潜在的なセキュリティ脆弱性が発生する。
- 管理者アカウントのパスワードポリシー。パスワードポリシーが有効になっていない場合、またはパスワードコンテンツ要件が有効になっていない場合に警告する。

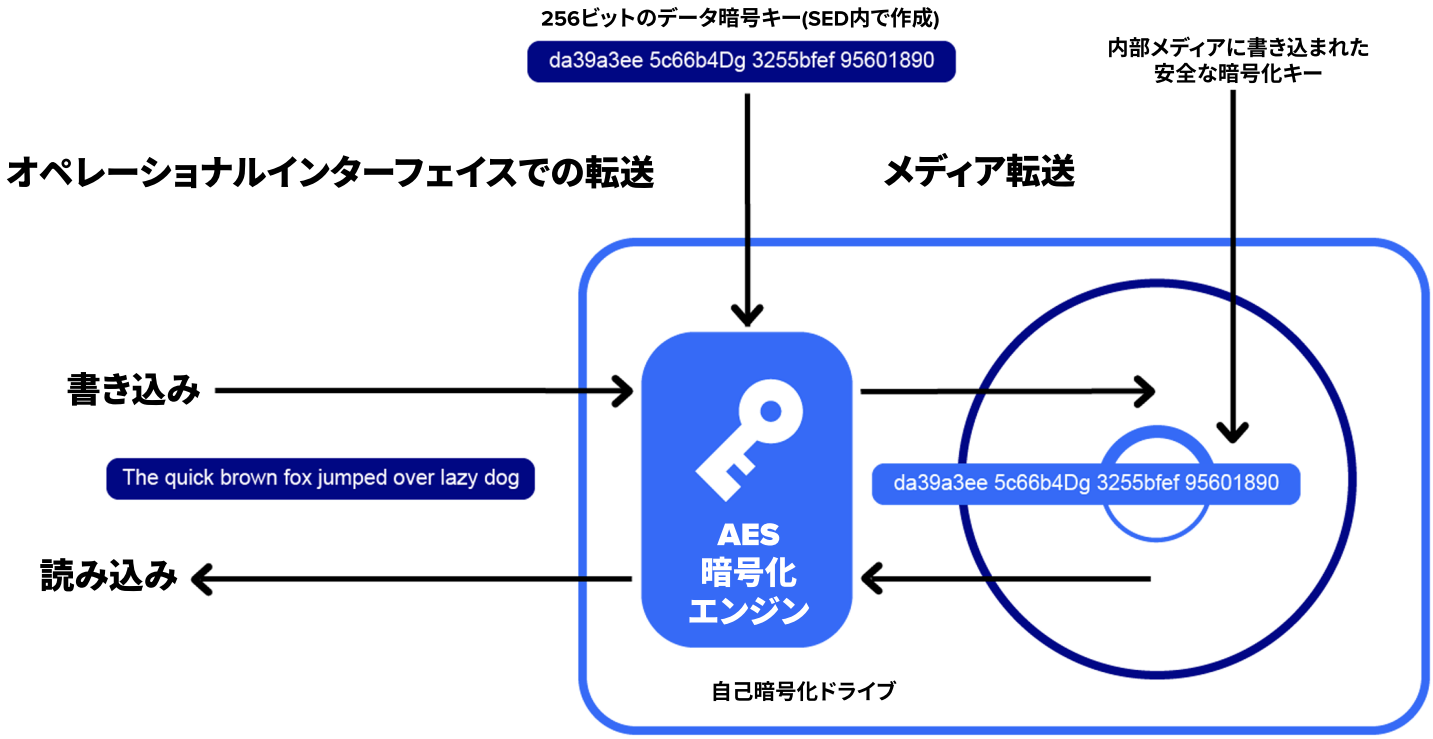
データ暗号化
NetIQ SaaS セキュリティには、サービス内に保存される機密データを保護する次のような技術が含まれています。

- 承認された暗号化の定義。
- 暗号化アーキテクチャと安全でないプロトコルのガイドラインの定義。
- データ転送中の暗号化。
- 保存データの暗号化。

転送中および保存時のデータ暗号化
OpenText は、データ転送中の暗号化に TLS1.2 を使用し (ブラウザー)、ストレージには HPE 3PAR デバイスを使用します。各 FIPS 1402 ディスクに書き込まれるすべてのデータに、Full Data Encryption を使用します。すべてのデータ暗号化はドライブレベルで処理されるため、データの暗号化に外部ソフトウェアやハードウェアは必要ありません。Full Data Encryption の利点は次のとおりです。

- 政府標準ベースの暗号化であり、業界全体の標準。
- AES-256 を使用。
- フルスピード暗号化専用エンジンを全ドライブに搭載。
- 暗号化キーは一意であり、メディア上で保護。
- 暗号化キー自体が暗号化されてメディアに保存されている。

SED ドライブでは、データは常にストレージメディア上で暗号化され、ライセンスは必要ありません。アレイで暗号化を有効にすると、暗号化が有効になっているアレイにディスクをロックすることにより、SED ドライブが悪意から保護されます。業界標準に従って、同じ暗号化ストレージアレイ内のすべてのディスクに、同じアレイ暗号化ロックキーが使用されます。



OpenText は、AWS のサーバー側暗号化を活用しており、これは、API 呼び出しをサービスが受信した「後」に、AWS KMS を活用してサーバーがデータを暗号化してくれます。Amazon S3 と EBS は、ユーザーデータのサーバー側暗号化 (SSE) をサポートしています。サーバー側の暗号処理は透過的です。当社のデータベースは EBS ストレージを使用しているため、すべてのデータベースストレージはこの方法で暗号化されます。AWS は、オブジェクトごとに一意の暗号化キーを生成し、AES-256 を使用して各オブジェクトを暗号化します。次に、安全な場所に保存されているマスターキーを使用して、暗号化キー自体が AES-256 を使用して暗号化されます。マスターキーは定期的にローテーションされます。

ログ記録と監視

ログ記録と監視は、セキュリティと運用のベストプラクティス、および業界の要件や規制へのコンプライアンスに対して重要なコンポーネントです。リソースに加えられた変更を理解することは、IT ガバナンスとセキュリティにおける重要要素です。ログデータへの変更や不正アクセスを防止することも同様に重要です。

OpenText はアカウントで行われた AWS API 呼び出しを記録し、指定された Amazon S3 バケットにログファイルを配信します。API の名前、呼び出し元の ID、API 呼び出しの時刻、リクエストパラメーター、AWS サービスが返したレスポンス要素など、各 API 呼び出しに関する重要な情報が記録されます。この情報は、AWS リソースに加えられた変更を追跡し、運用上の問題をトラブルシューティングするのに役立ちます。

API 呼び出しやリソースの変更を詳細に記録したログの構成ミスに対するほぼリアルタイムのアラートは、効果的な IT ガバナンスと社内外のコンプライアンス要件への準拠に向けて非常に重要です。管理者とリソースのアクティビティを監視するためにログ記録が適切に構成されていることが不可欠であるため、OpenText テクノロジーがログ管理に使用され、セキュリティオペレーションセンターチームによって監視されます。

ネットワークゼロトラストプラクティス
ネットワークアーキテクチャは、管理用とその他のサービス用の別々の VPC で構成されます。OpenText は IPS を使用して、ネットワークへの攻撃を防止し定期的な脆弱性スキャンを実施します。

- ディープパケットインスペクション、TCP セッションステート、スプーフィング防止を実行する FW。
- 厳密なグループポリシーによる管理された専用 Active Directory。
- すべてのコンポーネントを最新の状態に保つパッチ管理プロセスの配備。
- 転送中および保存中のクライアントデータの暗号化。
- TLS バージョン 1.2。
- すべてのサーバーとワークステーションにマルウェア検出エージェントをインストール。
- データと構成の両方のバックアップ。
- SOC チームによるインシデント監視とサービスの可用性追跡。

侵入防御システムは、総当たり攻撃やスプーフィング攻撃を検出してブロックします。システム構成は次のとおりです。

- このシステムの有効性は、攻撃履歴に基づいて毎年テストされます。
- IPS は、新しい攻撃シグネチャに対応して継続的に更新されています。

インシデント管理

OpenText のインシデントレスポンスは、ログとメトリクスの形を取る AWS の豊富な情報を活用して、潜在的なセキュリティインシデントを迅速に特定します。セキュリティイベントを分離するために、セキュリティ侵害の兆候に対する対応には、そのインスタンスに関連付けられたセキュリティグループの変更が含まれます。セキュリティチームは、このステップをさらに進め、新しいサブネットを作成して問題を分離し、一方では潜在的な脅威源や設定の脆弱性などの潜在的なリスクをさらに調査することができます。OpenText のインシデント対応戦略には、予測、抑止、検出、対応、回復の各フェーズが含まれます。

OpenText では、契約要件と適用される規制を満たすために、インシデント対応と通知プロセスも定義しています。インシデントが検出され、CSM に通知されると、SOC チームは、インシデントが解決されるまで、12 時間ごとに、または新しい情報を入手した時点で、CSM にアップデートを提供します。根本原因分析は、解決から 5 営業日以内にお客様に送信されます。このプログラムは、ISO27001 認証の一環として毎年監査を受けています。

ビジネスの継続性および耐障害性

ビジネス継続性 (BC) は、インシデントが発生した場合に、組織の重要なビジネス機能が継続的に稼働するか、あるいは迅速に回復することを保証します。これは、高可用性 (HA) と呼ばれることもあります。OpenText は世界中に複数のデータセンターを持っているため、データと構成に関する BCP リレーはリモートロケーションにバックアップされます。運用チームは、これらのバックアップをテストおよび検証するプログラムに従います。

まとめ

多くの組織が IAM サービスを SaaS モデルに移行する傾向はありますが、ニーズが減少しているとか簡素化しているということはありません。実際、デジタルトランスフォーメーションにより、強固な IAM インフラストラクチャへの依存度が高まっています。同時に、環境がますます複雑になるため、IT チームとセキュリティチームは組織に固有の要件を負うことになります。NetIQ の SaaS 設計により、組織は妥協することなくセキュリティをより高めることができます。

詳細については、NetIQ の Web サイトを参照してください。

お問い合わせ
www.opentext.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。

763-JA0012-002 | O | 07/24 |