Red Hat

エッジにおけるセキュリティ

エッジデバイス、アプリケーション、ネットワークのセキュリティ強化ガイド

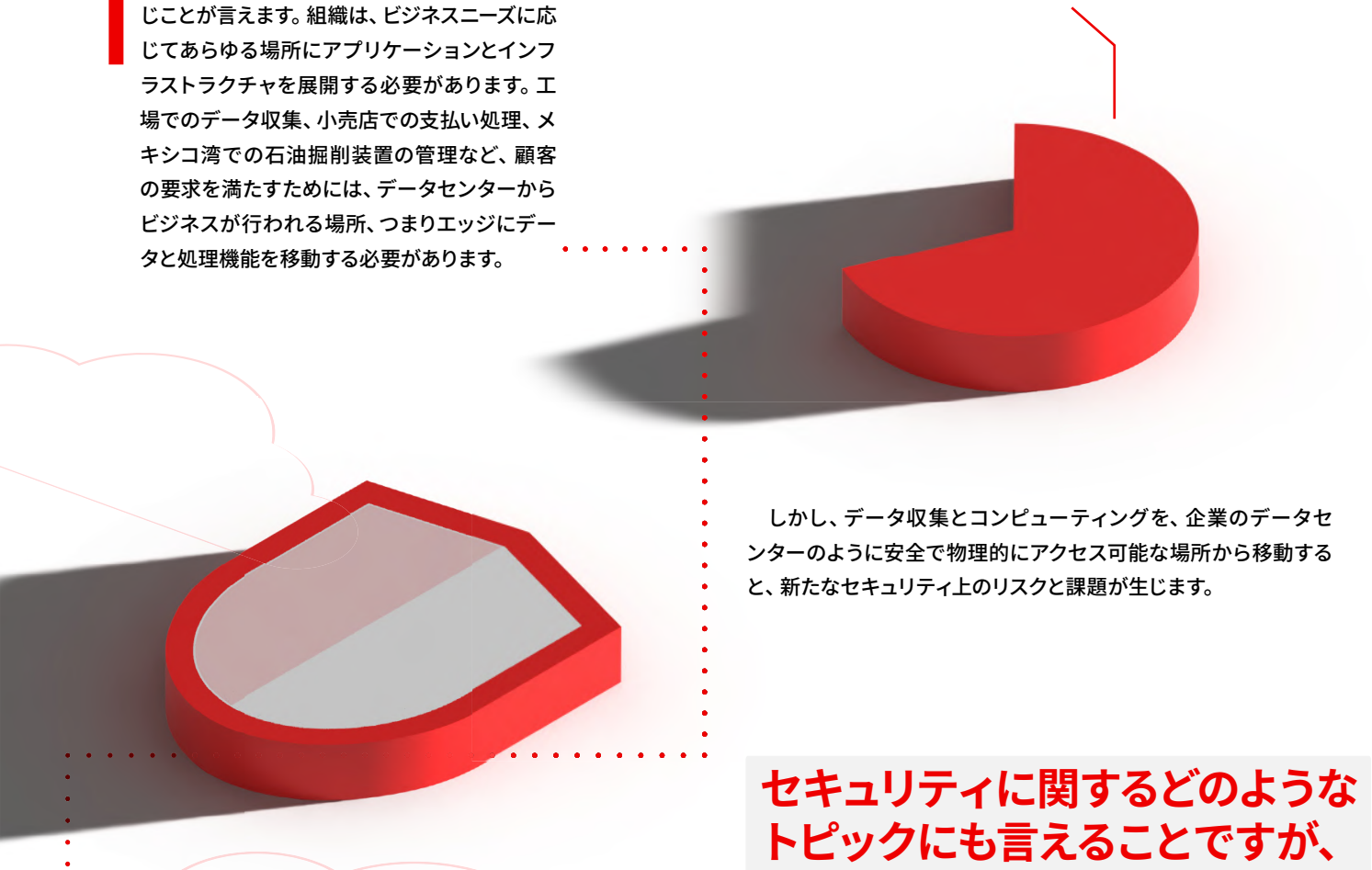
目次

はじめに

セキュリティに注力するのは容易なことではない

現在のグローバル組織は、地理や国境に縛られません。インフラストラクチャについても同じことが言えます。組織は、ビジネスニーズに応じてあらゆる場所にアプリケーションとインフラストラクチャを展開する必要があります。工場でのデータ収集、小売店での支払い処理、メキシコ湾での石油掘削装置の管理など、顧客の要求を満たすためには、データセンターからビジネスが行われる場所、つまりエッジにデータと処理機能を移動する必要があります。

70% の組織が、エッジ関連投資の中で最も重要な要因の 1 つとしてセキュリティを挙げています（他のすべての要因を上回ってトップ）。[1]



しかし、データ収集とコンピューティングを、企業のデータセンターのように安全で物理的にアクセス可能な場所から移動すると、新たなセキュリティ上のリスクと課題が生じます。

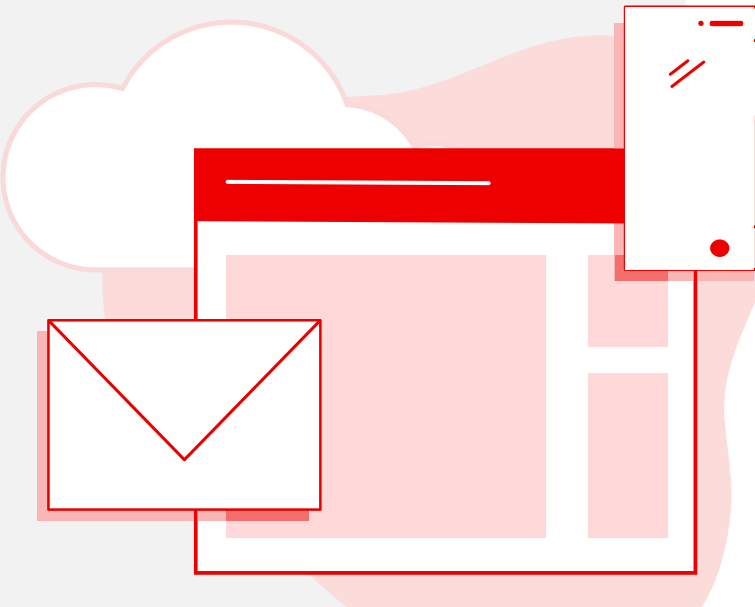
セキュリティに関するどのようなトピックにも言えることですが、単純な答えはありません。

[1] IDC、「Securing the Edge: How Edge Is Architected Will Determine How Security Is Designed」、Document #US48547722、2022 年 2 月。

サイバーセキュリティと NetOps の担当者は、アプリケーションと情報のセキュリティ、認証とアクセス制御、システム更新といった基本要件を満たした上で、さらにエッジの保護という課題にも対処しなければなりません。そうした課題には、断続的なインターネット接続、エッジサイトへのアクセス、IoT (モノのインターネット) エッジデバイスのセキュリティなどがあります。

エッジでのセキュリティを機能させるためには、コアデータセンターやクラウド・インフラストラクチャからエッジに至るまで、セキュリティツール、ポリシー、プロセスを適応させ、進化させる必要があります。これは、組織が強力なセキュリティ体制、ガバナンス、コンプライアンスを維持するために不可欠です。

セキュリティチームは、ソフトウェアが一貫して更新されるようにする、リスクを事前に予測し、検出し、それに対処するためのリソースを得るなど、断続的なネットワーク接続という不確実性を伴うリモートのエッジロケーションであらゆることを管理できるツールとリソースを備える必要があります。



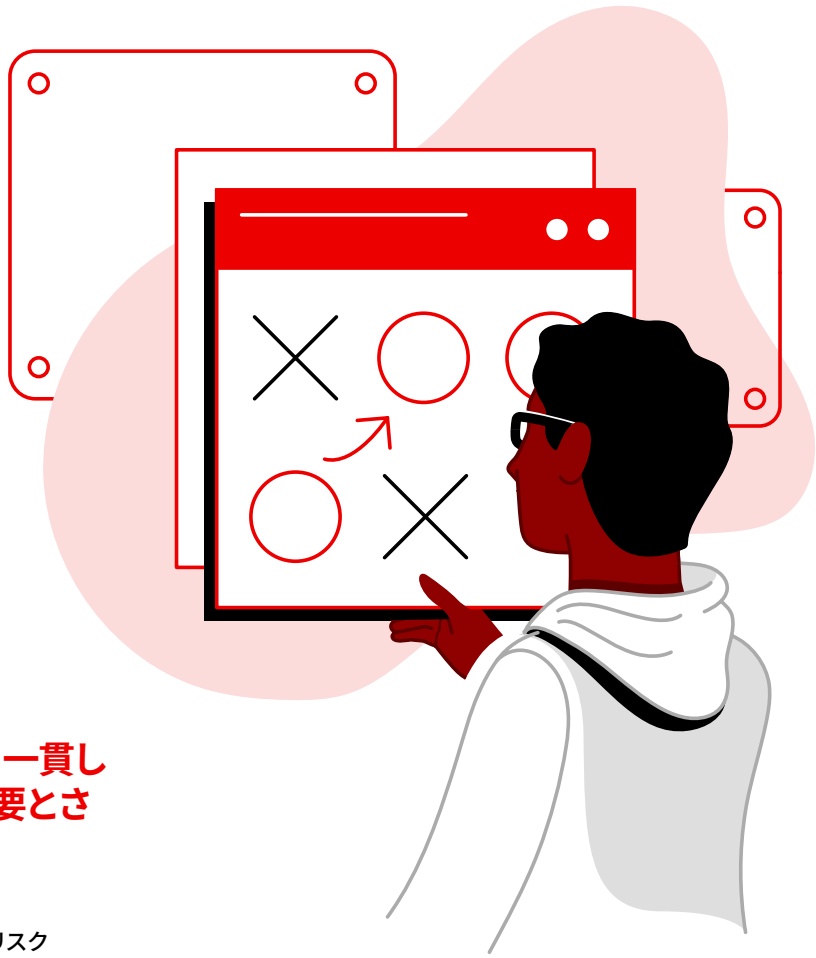
エッジでのセキュリティ向上における課題とは

一般的なデータセンターでは、ネットワークエンジニアやシステム管理者が物理的な再起動、故障したユニットの交換、必要なセキュリティ更新の適用などを実行するのは簡単です。クラウド・インフラストラクチャでは、管理者、DevOps エンジニア、またはサイト信頼性エンジニアが同様のタスクを管理できます。

ここで、小売店でのエッジデバイスの管理について考えてみましょう。デバイスを再起動できる人はいるかもしれませんが、セキュリティインシデントやセキュリティ侵害が発生した場合にセキュリティパッチを適用したり、介入したりすることができる人はいません。デバイスが盗まれた場合は、小売店の本社がそのことを知るまでに数日あるいは数週間かかる場合があり、悪意のある人物がデータを取得するリスクが高まります。

エッジでのコンピューティングには、多くの場合レガシーソフトウェアおよびハードウェアが使用され、それがセキュリティポリシーとプロセスをさらに複雑にします。これらのシステムの多くは、セキュリティ更新やパッチが適用されなくなった古いオペレーティングシステムで実行されています。

セキュリティをエッジにまで拡張する際の課題は、業界、ソリューション、場所によって異なります。



エッジデプロイメントの規模も、一貫したエンタープライズ自動化が必要とされる要因となります。

組織は、エッジデバイスを追跡し、セキュリティリスクを予測し、対応策を推奨するために、エッジ環境を継続的に分析する必要があります。

ここでは、エッジを保護するためのアプローチを策定する際に考慮すべき５つの課題について説明します。

1.

限定的または断続的なネットワークアクセス

リモートサイトでデータの収集と処理を行えることは、エッジの最も重要な利点の１つであり、主要な潜在的障害点の１つでもあります。石油掘削装置、ガスポンプ場など、遠隔施設でのファーエッジ・デプロイメントでは、インターネット接続が不十分であったり、断続的であったりする場合があります。これにより、エッジデバイスにパッチや更新を一貫して確実にダウンロードすることが困難になる可能性があります。

エッジデバイスへの接続が失われることによるもう１つの課題は、オフライン中にデバイスが改ざんされてしまうリスクです。エッジデバイスの接続が切断された場合、ネットワークに再接続するために物理的な介入が必要になることがあります。そして、このような場合の再接続は、多くの場合、店舗や工場の現場で IT 担当ではない従業員が行っています。場合によっては、これらのデバイスは、オンラインに戻ってもセキュリティ体制が確認できるまでネットワークリソースからの隔離が必要になります。

もう１つの重要な考慮事項は、証明書キーのローテーションです。月内の特定の日だけ接続が利用できるエッジサイトがあるとします。証明書のローテーションの予定日がそのサイトがオフラインになる日に当たってしまうと、そのデバイスへの接続が失われる可能性があります。接続が失われるとそのエッジデバイスは信頼できるデバイスではなくなるため、現場にエンジニアを派遣して手動で更新することが必要になる場合があります。

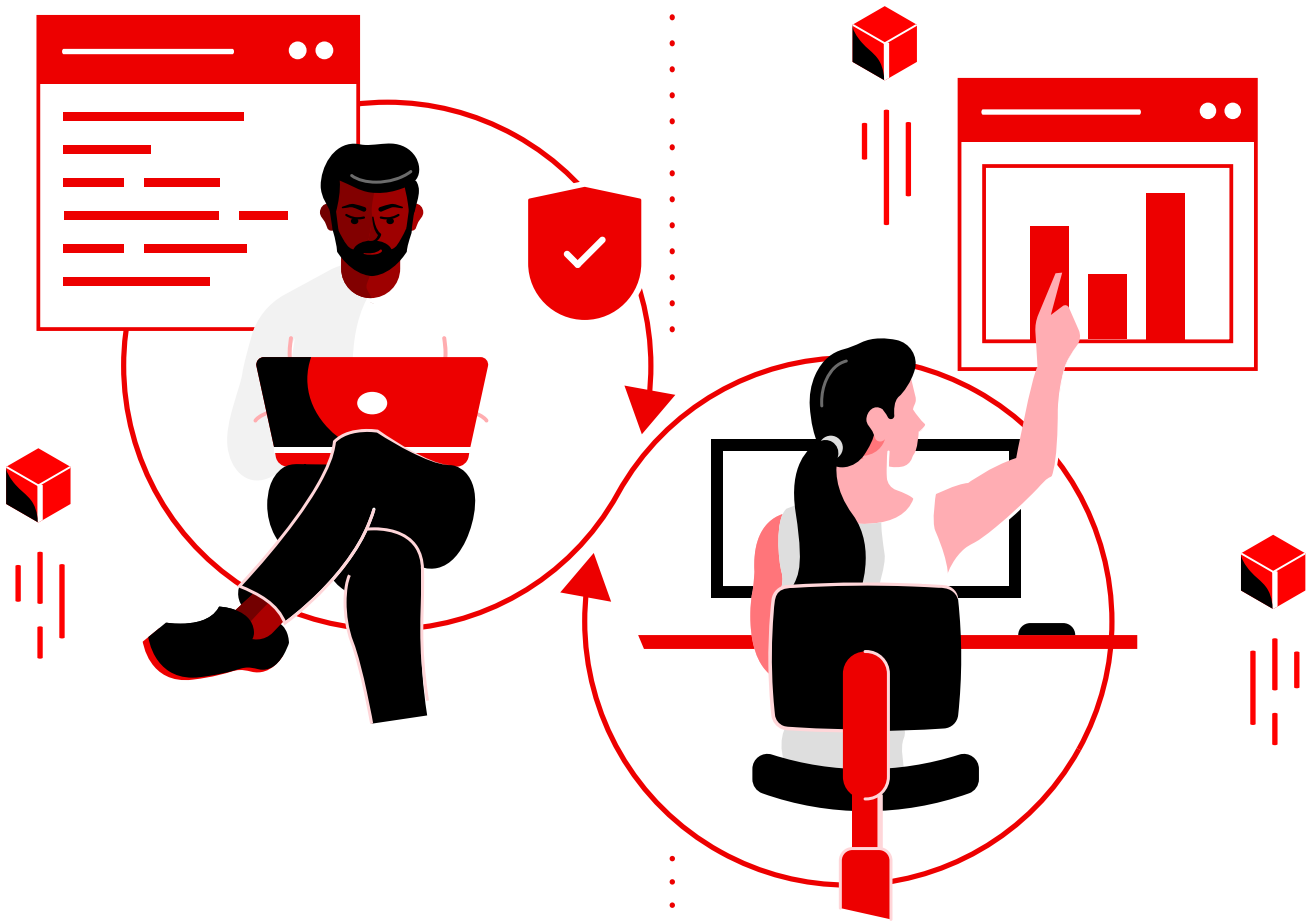
2.

物理的な改ざんと攻撃

組織がエッジで展開するデバイスの数は、数百から数千に及ぶ可能性があり、多くの場合、そのベンダーはさまざまです。エッジにおける最初の攻撃ベクトルの1つは、デバイスの侵害です。

侵害されたデバイスが設置されると、それによって攻撃ベクトルが広がる可能性があります。エッジ環境は遠隔地にあるため、エッジロケーションではデバイスの物理的なセキュリティを常に確保できるとは限りません。エッジデバイスを使用すると、悪意のある人物が USB ドングルやその他の攻撃ベクトルを介してデバイスを侵害する可能性が生じます。これらの侵害されたデバイスは、企業ネットワークやその他のエッジデバイスまたはアプリケーションへのバックドアアクセスを得るために使用されることがあります。

また、エッジロケーションでは、長期間にわたって人員がいないこともよくあります。適切なセキュリティがなければ、エッジデバイスが盗まれ、新たなセキュリティリスクが生じることがあります。デバイスが盗まれた場合、ネットワークアクセス用の秘密鍵や顧客データ、ビジネスデータなどの機密情報がサイバー犯罪者の手に渡る可能性があります。

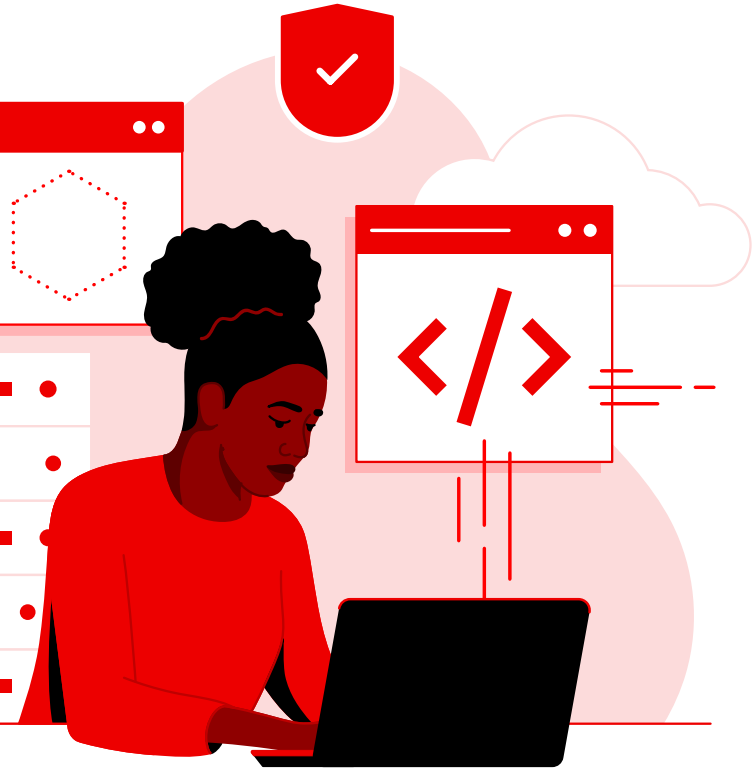


3.

エッジデバイスのリモート管理に関する課題

オンサイトのデータセンターでは、デバイスを再起動したり更新を適用したりするために従業員を派遣するのは簡単です。クラウドでは、システム管理者や DevOps チームがこれらのプロセスを管理します。エッジでは、多くの場合、再起動が必要な場合にエッジデバイスをリセットしたり、その他のセキュリティ問題に対処したりする担当者が現場にいません。

エッジ環境同士が物理的に離れており、接続が不十分あるいは存在しないことが多いため、エッジデバイスへのパッチと更新の適用は、リモート管理での最も重要な課題の 1 つです。この作業に含まれるのは、デバイスのオペレーティングシステムのセキュリティ更新だけではありません。デバイスの基本入出力システム (BIOS)、オペレーティングシステム (OS)、WiFi またはセルラースタック、およびあらゆるアプリケーションを含む、デバイススタック全体を考慮する必要があります。



4.

エッジでのトラフィック傍受の防止

エッジデバイスは、ネットワーク接続が限定的または断続的であるという問題に加えて、悪意のある人物にネットワークトラフィックを傍受されてしまうおそれもあります。このトラフィックには、顧客データやビジネスデータ、SSL (Secure Sockets Layer) および SSH (Secure Shell Protocol) キー、または中央のインフラストラクチャをさらなる攻撃にさらす可能性のあるデータが含まれる場合があります。

もう 1 つの課題が、エッジでの WiFi 接続に関するセキュリティの強化です。組織は、エッジデバイスから WiFi アクセスポイントまで、WiFi 無線パッチを確実に適用し、アクセス ポイントのサービスセット識別子 (SSID) を頻繁にローテーションして、セキュリティが不十分なエッジの WiFi ネットワークから悪意のある人物が企業ネットワークに侵入する可能性を減らす必要があります。

5.

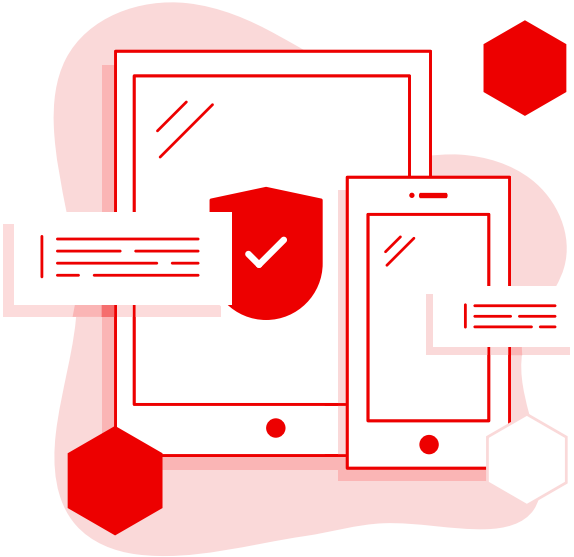
エッジセキュリティにおけるヒューマンエラーの防止

セキュリティに関しては常にそうですが、エッジセキュリティの弱点も人です。2022 年の Verizon Data Breach Investigations Report によると、侵害の 82% に、ソーシャルアタック、エラー、誤用などの人的攻撃ベクトルが関与していました。[2] 多くのエッジロケーションには、IT やネットワークの専門家が配置されていません。これにより、ログイン資格情報のセキュリティが緩かったり、必要な場合にデバイスをより迅速に再起動できるようにエッジデバイスのパスワードを製造元のデフォルトのままにしていたりと、多数の潜在的な攻撃ベクトルが生じます。

さらに、エッジロケーションの人員は、組織の IT チームやセキュリティ運用チームが承認していないデバイス、アプリケーション、またはツールを使用する「シャドー IT」を利用していることがよくあります。制御されていない、または管理されていないテクノロジーが使用されると、ただでさえリスクの高いインフラストラクチャ内の攻撃ベクトルがさらに増加してしまいます。

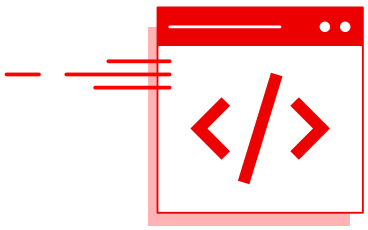
82% の侵害に、人的攻撃ベクトルが関与しています。[2]

エッジデバイスやその他の IoT デバイスは軽量で持ち運びやすいという性質を持つことから、これらを使用する現場で適切な認識が共有されない場合があります。従業員がそのデバイスをインフラストラクチャの重要な一部分であると認識せず、改ざんや盗難の危険にさらす可能性があります。



[2]Verizon、「2022 Data Breach Investigations Report」、2022 年 5 月 25 日。

エッジのセキュリティ向上のベストプラクティス



エッジハードウェアとファームウェアの管理を自動化

エッジデバイスは、しばしば最初の攻撃ベクトルになります。自動化ツールを使用して、ブート ROM などのデバイスパッチやデバイスファームウェアが、ネットワーク接続が限定的あるいは断続的であっても一貫性のある自動化された方法で適用されるようにすることで、リスクを軽減できます。可能であれば、物理的な障壁を使用してデバイスへのアクセスを制限すれば、USB やその他のポートを介した改ざんを防げます。

アプリケーション・ライフサイクル全体でセキュリティを統合

エッジセキュリティに関与するのは、デバイスだけではありません。あらゆるデバイスで実行されるアプリケーションには、アプリケーション開発ライフサイクルのすべての段階で継続的なセキュリティが必要です。これには、開発と構築、デプロイ、ランタイムが含まれます。さらに、監査、監視、ロギングを実施して、アプリケーションがプロダクション環境にデプロイされ、稼働を開始した後に重要なセキュリティインシデントを通知してログに記録し、それに応じて修正できるようにする必要があります。

自動化されたデバイスのオンボーディングとプロビジョニングでヒューマンエラーを削減

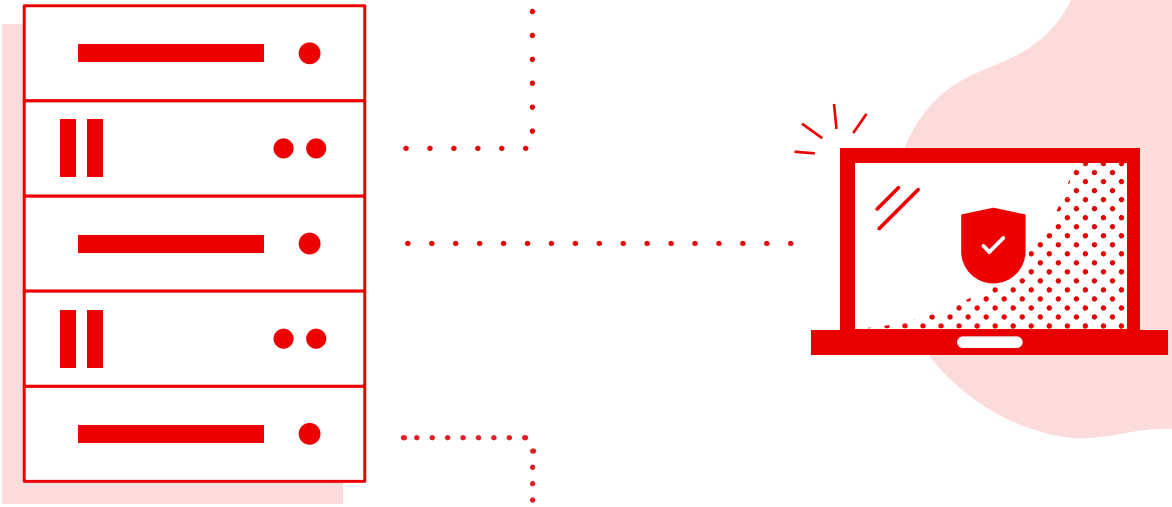
ゼロタッチ・プロビジョニングにより、ネットワーク内でエッジデバイスを自動的にプロビジョニングできるため、システム管理者は専門的なタスクの実行に時間を使えるようになり、必要な手動構成作業、ダウンタイム、物理的な場所への移動時間がなくなることで、ヒューマンエラーが減少します。さらに、ゼロタッチ・プロビジョニングは大規模かつ極めて迅速に実行できます。これらはすべて、エッジセキュリティを大規模に実行するための鍵です。

ネットワークのセキュリティをエンドツーエンドで暗号化

エッジデバイスが侵害される可能性は高いです。ネットワークトラフィックをより適切に制御し、転送中の機密データを保護してセキュリティを向上させるために、ネットワークのセグメント化とポリシーベースの復号化 (PBD) の使用を検討するべきです。また、自動化と監視ツールを使用して、疑わしいトラフィック・アクティビティについてネットワークを分析し、自動化された方法で大規模に問題を修正する必要があります。

エッジのセキュリティに対する Red Hat のアプローチ

Red Hat のオープンソース・エッジコンピューティング・ソリューションは、プロビジョニングとハードニング、管理、事前定義の構成、オーケストレーションの自動化により、組織が運用を効率化し、エッジ環境全体のセキュリティを向上させるのに役立ちます。



安定した基盤を使用してエッジにデプロイ

エッジのプロジェクトでは、ハードウェアが侵害されていないことの確認、リモート管理の問題への対処など、複数の課題が生じます。安定した基盤を持つことは、エッジデータの収集とコンピューティングにとって不可欠です。Red Hat® Enterprise Linux® を使用すると、エッジの軽量ハードウェアにミニサーバールームをデプロイし、一貫性のある強化された運用環境を得ることができます。これは、認定済みのハードウェア、ソフトウェア、クラウド、およびサービスプロバイダーでの長期的な安定性とセキュリティサービスを必要とするワークロード向けに構築されています。

「Red Hat は、エッジコンピューティングへのロードマップを含め、我々がビジネス上の課題と技術上の課題に対処できるよう、人材と製品の適切な組み合わせを提示してくれます」[3]

イスラエル国防軍中佐

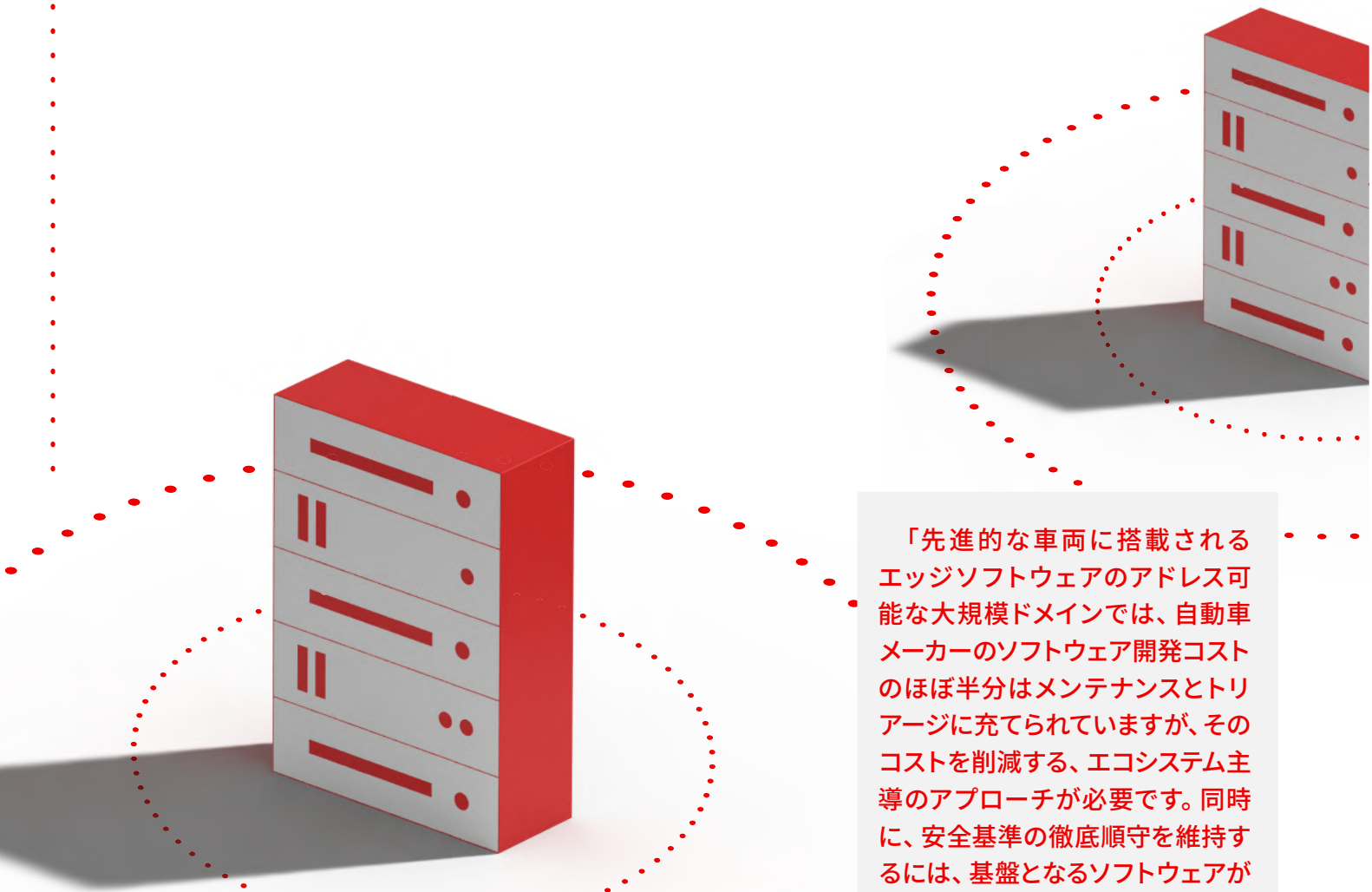
C4i およびサイバー防衛局 Mamram エッジクラウドプラットフォーム R & D 統括責任者

[3] Red Hat、「イスラエル国防軍の IT 部門、Red Hat を使用して as-a-Service 機能の提供を迅速化」、2022 年 4 月 26 日。

エッジの複雑さを管理

エッジのプロジェクトには数百から数千のエッジデバイスが関与する可能性があり、セキュリティ上の課題を多数もたらします。そうした課題には、デバイスに正しいセキュリティパッチが適用されるようにすることや、紛失または盗難の可能性があるデバイスのデバイスインベントリーを管理することなどがあります。

Red Hat Ansible® Automation Platform は、オンプレミス、クラウド、ハイブリッドクラウド、およびエッジの自動化機能を提供します。また、サードパーティ製ソリューションおよびコンテンツをサポートする、開発からプロダクションまでの共通自動化言語を提供します。環境を最新の状態に保ち、エッジデバイスのセキュリティ上の問題を大規模に修正するには、一貫したエンタープライズ自動化が不可欠です。



「先進的な車両に搭載されるエッジソフトウェアのアドレス可能な大規模ドメインでは、自動車メーカーのソフトウェア開発コストのほぼ半分はメンテナンスとトリアージに充てられていますが、そのコストを削減する、エコシステム主導のアプローチが必要です。同時に、安全基準の徹底順守を維持するには、基盤となるソフトウェアが高レベルの確実性を備えていることが必要です」[4]

Alex Oyler 氏
SBD Automotive 北米担当取締役

[4] Red Hat プレスリリース、「Red Hat とゼネラルモーターズが協業ソフトウェア・デファインド・ビークルの未来を拓く」、2022 年 5 月 10 日。

毎日 24 時間、エッジを監視

セキュリティのための強力な基盤を備えても、組織がエッジ環境を継続的に分析してリスクを予測し、対応策を推奨しなければ意味がありません。

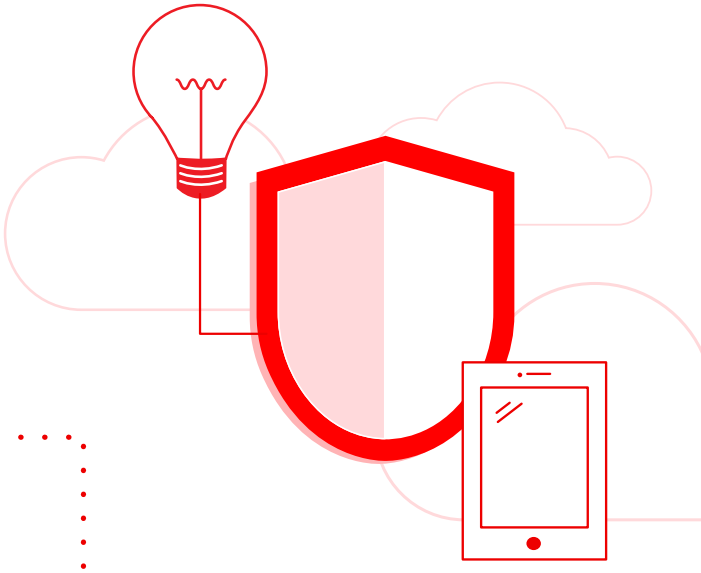
Red Hat Insights は、エッジに配置された Red Hat Enterprise Linux システムの脆弱性、構成の問題、その他の潜在的なセキュリティの問題を監視し、Ansible Playbook を生成することができます。この Playbook を使用して、リスクを広範囲にわたって修正できます。エッジ環境は、パートナープロバイダーが提供する SIEM (Security Information and Event Management) ツールや SOAR (Security Orchestration Automation and Response) ツールを使用して監視および管理することもできます。Ansible Automation Platform Certified Content Collections は、SIEM、SOAR、エンドポイント保護、その他のサードパーティ製ソリューションと統合してサポートする、認定済みの Ansible 自動化コンテンツを提供するために利用できます。[5]

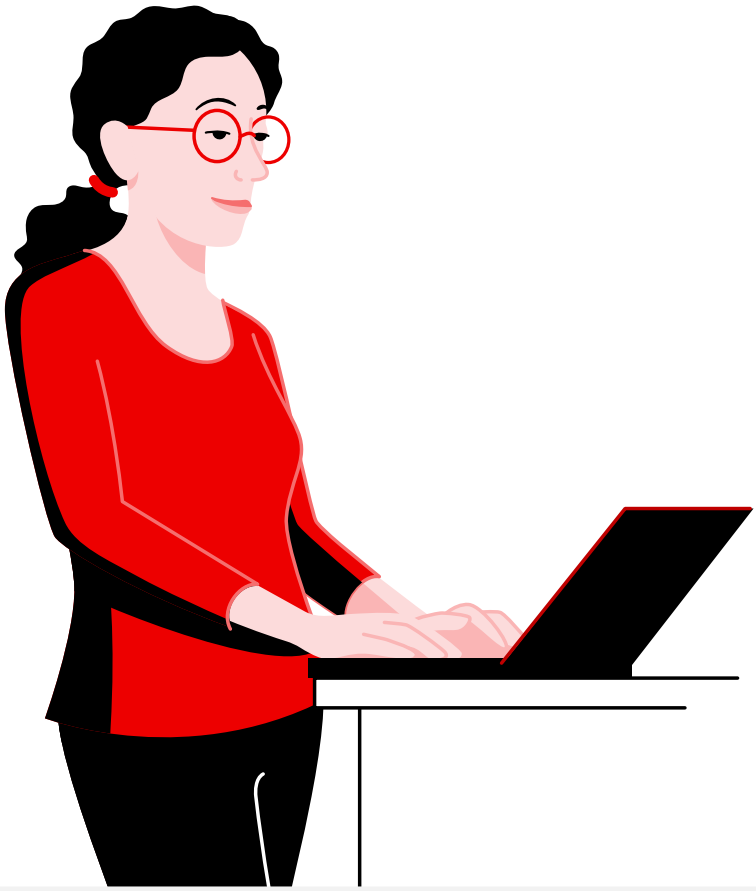
従来の環境とコンテナ化環境の両方のセキュリティを強化

エッジセキュリティの問題はデバイス管理に影響を与えますが、その同じ問題によって、エッジデバイスでのコンテナベースのアプリケーションの構築、デプロイ、実行、管理が困難になる可能性があります。Red Hat OpenShift® は Kubernetes プラットフォームであり、Red Hat OpenShift で実行されているコンテナ化されたワークロードに詳細なアクセス制御、監査、ロギング、および監視機能を提供します。また、エッジデバイスの通信をエンドツーエンドで暗号化することもできます。

[5] Red Hat、「Ansible Automation Platform Certified Content」、Red Hat カスタマーポータル、2022 年 7 月 28 日。

また、Red Hat Advanced Cluster Management for Kubernetes、Ansible Automation Platform、Red Hat Insights を使用すれば、セキュリティリスクを特定し、対応することができます。Red Hat テクノロジーには、連邦情報セキュリティマネジメント法 (FISMA)、医療保険の相互運用性と説明責任に関する法律 (HIPAA)、PCI SSC (Payment Card Industry Security Standards Council) など、業界標準のセキュリティ・フレームワークに準拠するための堅牢なポリシー機能とコンプライアンス機能が組み込まれており、従来の環境とコンテナ化された環境の両方に対応します。





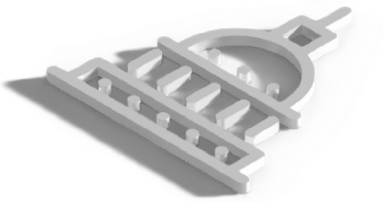
さらに、Red Hat Advanced Cluster Security for Kubernetes と Red Hat OpenShift は、コンテナベースのアプリケーションの DevSecOps ワークフローを自動化し、エッジにデプロイされたこれらのアプリケーションを構築からデプロイ、実行まで、アプリケーション・ライフサイクル全体で保護するのに役立ちます。

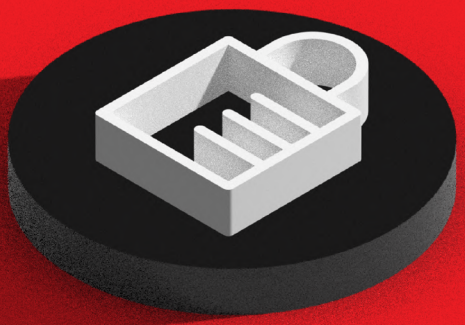
さらに詳しく

エッジのセキュリティ強化を始めましょう

Red Hat には、データセンターからエッジに至るまでセキュリティを実現するために役立つソリューションと専門知識があります。

- 資料を読む：Red Hat のアプローチ：ハイブリッドクラウド・セキュリティ
- 詳細を見る：Red Hat Enterprise Linux のセキュリティとコンプライアンス
- 試用を開始する：Red Hat Ansible Automation Platform、Red Hat OpenShift





Red Hat について

エンタープライズ・オープンソース・ソフトウェア・ソリューションのプロバイダーとして世界をリードする Red Hat は、コミュニティとの協業により高い信頼性と性能を備える Linux、ハイブリッドクラウド、コンテナ、および Kubernetes テクノロジーを提供しています。Red Hat は、クラウドネイティブ・アプリケーションの開発、既存および新規 IT アプリケーションの統合、複雑な環境の自動化および運用管理を支援します。受賞歴のあるサポート、トレーニング、コンサルティングサービスを提供する Red Hat は、フォーチュン 500 企業に信頼されるアドバイザーであり、オープンな技術革新によるメリットをあらゆる業界に提供します。Red Hat は企業、パートナー、およびコミュニティのグローバルネットワークの中核として、企業の成長と変革を支え、デジタル化が進む将来に備える支援を提供しています。

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

アジア太平洋
+65 6490 4200
apac@redhat.com

オーストラリア
1 800 733 428

インド
+91 22 3987 8888

インドネシア
001 803 440 224

日本
03 4590 7472

韓国
080 708 0880

マレーシア
1 800 812 678

ニュージーランド
0800 450 503

シンガポール
800 448 1430

中国
800 810 2100

香港
800 901 222

台湾
0800 666 052

jp.redhat.com