統合プラットフォームで防衛を強化する

主な利点：

- 戦略的コアから戦術的エッジまでのレジリエンスのギャップがない
- オフライン環境におけるミッションクリティカルなアプリケーションのための一貫したプラットフォーム
- 自律性とセキュリティへの統一されたアプローチ

戦略的コアから戦術的エッジまでのレジリエンスのギャップを埋める

政府防衛機関は、戦略的コアから戦術的エッジに至るまで、その全範囲にわたって信頼性の高い運用を維持するという極めて重要な課題に直面しています。アジリティ、堅牢なセキュリティ、戦略的自律性に対する重大なニーズを受けて、防衛部門は急速に進化しています。従来型の一元化されたデータセンターから、高度に分散されたミッション対応型アーキテクチャへと移行しています。決断の優位性を得ること、つまり、すべての指揮官があらゆる領域でどのような敵よりも迅速に検知し、理解し、決定し、行動できるようにするためには、大幅な変革が不可欠です。

エンドツーエンドのオペレーショナル・レジリエンスの必要性

先進的なミッションは、エアギャップされたプライベートクラウド、デプロイされたミニデータセンター、堅牢な戦術的デバイス (ドローンや兵士が身に付けるシステムなど) を網羅した、無秩序に広がるハイブリッドクラウドの連続体で実行されています。このアーキテクチャはマルチドメイン作戦 (MDO) を実行するための基盤であり、空、陸、海、宇宙、サイバー、電子波の各領域にわたるアセットの複雑な統合と調整が必要になります。

しかし、ドメインの拡張によって重大な脆弱性も生じ、技術的な複雑さが大幅に増します。分離したテクノロジーや統合されていない環境では、運用の継続性が損なわれる可能性があります。一方、サイバーセキュリティの脅威は広大な攻撃対象領域上で増大します。常時接続への依存は、重大な障害点となります。紛争中の環境においては、エッジデバイスは自律的に機能する必要があり、信頼できる断続的なリンクが利用可能な場合にのみデータを同期します。主な課題は、あらゆる領域にわたって真のレジリエンスを実現することです。戦術的エッジが独立して機能できないのであれば、中央データセンターの主権は不十分です。

防衛デジタル・トランスフォーメーションにおける主な課題

ハイブリッド・インフラストラクチャがもたらす柔軟性は明白である一方、防衛組織はデジタル・トランスフォーメーションの過程でいくつかの重大な障壁に突き当たります。

- **サイバー攻撃：**防衛組織が最も懸念しているのは、高度なサプライチェーン攻撃やサイバー攻撃による脅威の増大です。たとえば、オープンソース・ライブラリに悪意のあるコードが埋め込まれていると、ドローンや車両の部隊全体が侵害される可能性があります。同様に、中間者 (MitM) 攻撃では戦術的デバイスへの送信中にファームウェアのアップデートが改変され、重要なミッションが妨害される可能性があります。
- **分離されたテクノロジー構造：**コア、クラウド、エッジなど、異なる環境で互換性のないテクノロジースタックが使用されることがよくあります。互換性がないと、組織はデプロイごとにソリューションを再構築しなければならず、断片化が生じます。その結果、兵士とエンジニアは Amazon Web Services (AWS) や Microsoft Azure から特殊な戦術的オペレーティングシステムまで、複数のプラットフォームを習得しなければならず、ミッションに対する準備が大幅に遅れます。
- **複雑度：**手作業によるプロセスに頼っていると、その性質上複雑さが増してきます。たとえば、コアとエッジロケーション間でデータをやり取りするにはカスタムワークフローが必要になり、デプロイメント時間が長くなります。同時に、従来のセキュリティモデルを分散アーキテクチャに適応させるのは困難であるため、攻撃者が悪用できる重大なギャップが生じています。

統一されたアプローチを採用する

防衛組織は、あらゆる場所で自律性とセキュリティを強化する、統一されたオープンなフレームワークを早急に必要としています。目標とするのは、重要なアプリケーションをプライベートクラウドで実行し、AI ワークロードをエッジで処理し、現場のエッジデバイス上でリアルタイムの意思決定を行うための、一貫したプラットフォームです。真の先進的レジリエンスとは、コアから最前線に至るまで、揺るぎない整合性を維持しながら機能できることです。

Red Hat にできること

断片化したデジタル戦闘空間に直面する防衛組織には、戦略的コアから戦術的エッジまでのレジリエンスを維持するために、統合基盤と信頼できるアドバイザーが必要です。Red Hat は、そのような極めて重要で一貫したプラットフォームを提供します。Red Hat は「一度デプロイすれば、どこでも実行できる」というプラクティスにより、ミッションへの対応準備を迅速化し、防衛組織の人員は環境を問わず使い慣れたツールを使用できます。一貫したエクスペリエンスを提供するだけでなく、Red Hat のソリューションはオープンスタンダードに基づいて構築されており、プラットフォームはベンダーに依存しないため、スケーラブルで柔軟なソリューションとのより良い統合が可能です。

軍用レベルのセキュリティ：Red Hat は、Red Hat® OpenShift® などのコア・プラットフォームを厳格なコンプライアンス基準に準拠させることで、軍用レベルのセキュリティを実現します。セキュリティは Red Hat Trusted Software Supply Chain を通じて継続的に適用され、セキュリティに対する包括的で継続的なアプローチが実現します。このアプローチでは、DevSecOps のプラクティスを統合して証拠保全を強化し、ソフトウェアがセキュリティ、コンプライアンス、プライバシー、透明性に関する機関の基準を満たしていることを検証します。

保証主権：暗号証明によって、ファームウェアや重要なアップデートが変更されていないことが検証され、保証主権のより広範な目標がサポートされます。このプロセスはデジタルシステムの整合性と信頼性を検証するもので、ソフトウェア・サプライチェーンを検証して悪意のあるコードが挿入されるリスクを軽減するという、Red Hat のプラットフォーム戦略の中核を成すものです。

オフラインでの自動化：オフラインでの自動化により、インターネット接続を必要とせずに、フィールドデバイスのパッチ適用が可能になり、すでに使用しているあらゆる種類のプロセスと統合できます。Red Hat は Red Hat Ansible® Automation Platform を使用して、先進的な防衛に必要な信頼できる自律的運用の実現を支援します。このプラットフォームは、拒否される、中断する、断続的になる、制限される (DDIL) 状況において、脆弱な外部接続に依存することなくデバイスを管理するのに役立ちます。この自律性により、デプロイされたソフトウェア資産への大規模かつ長期的な投資が保護され、悪意のあるコードのインジェクションに関連するセキュリティリスクが最小限に抑えられ、外部サポートが不可能な場合でも継続的でミッションクリティカルな運用が保証されます。

戦略的コアでは、Red Hat OpenShift などの信頼性の高いソリューションが、スケーラブルなソブリン・インフラストラクチャを提供します。デプロイされたエッジでは、コンパクトな OpenShift クラスタが重要なインテリジェンスと AI ワークロードを処理します。戦術的な前線では、軽量の Red Hat Device Edge が、堅牢なシステム上での極めて可搬性の高いオフライン操作を可能にします。

防衛業界の実証済みのユースケース

複数の防衛組織が Red Hat ソリューションを導入して運用上の重大な課題を克服し、大幅な進歩を達成しています。

欧州空軍の現場運用の最適化：欧州の空軍は、現場での作戦中にネットワークの停止が発生し、ミッションが幾度も中断されるという問題に直面していました。移動式のエッジデータセンターに Red Hat OpenShift を実装することで、空軍の IT 部門はローカル AI 処理機能を導入し、接続状況に関係なく継続的な運用を維持すると同時に、帯域幅の要件を大幅に削減しました。

無人航空機システムの飛行中におけるソフトウェアアップデート：先進的な機能を示すもう 1 つの例として、大手防衛関連企業が無人航空機システムのソフトウェアアップデートを飛行中に行う機能を披露しました。この企業は Red Hat Device Edge を使用して、実際のミッション遂行中に AI モデルのアップグレードをドローンにデプロイすることに成功し、ミッションの中断やシステムのダウンタイムを必要とせずに、リアルタイムのターゲット認識機能を強化しました。

国防機関のインフラストラクチャとデプロイメントの迅速化：ある国防機関では、Ansible Automation Platform と Red Hat OpenShift を使用して Platform-as-a-Service (PaaS) プロセスを自動化することで、大幅な効率化を実現しました。インフラストラクチャのデプロイ時間が数週間からわずか 24 時間に短縮され、戦闘に使える状態になりました。それと同時に、厳格なセキュリティプロトコルを維持しながら、開発者の能力が 1 年間で約 4 倍に増加しました。

今すぐ始める

コアからエッジまで防衛活動を保護する方法について、Red Hat の担当者までお問い合わせください。

Red Hat について

Red Hat は、受賞歴のあるサポート、トレーニング、コンサルティング・サービスをお客様に提供し、複数の環境にわたる標準化、クラウドネイティブ・アプリケーションの開発、複雑な環境の統合、自動化、セキュリティ保護、運用管理を支援します。

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

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

jp.redhat.com
#3134353_1225