Gestärkte Verteidigung mit einer einheitlichen Plattform

Wichtigste Vorteile:

- Keine Resilienz-Lücke, vom strategischen Kern bis hin zum taktischen Edge
- Konsistente Plattform für missionskritische Anwendungen in nicht verbundenen Umgebungen
- Einheitlicher Ansatz für Autonomie und Sicherheit

Schließen der Resilienzlücke vom strategischen Kern bis hin zum taktischen Edge

Regierungsbehörden stehen vor einer zentralen Herausforderung: der Aufrechterhaltung zuverlässiger Operationen im gesamten Spektrum – vom strategischen Kern bis hin zum taktischen Edge. Aufgrund der dringenden Notwendigkeit von Agilität, robuster Sicherheit und strategischer Autonomie entwickelt sich der Verteidigungssektor rapide weiter. Die Richtung führt weg von traditionellen, zentralisierten Rechenzentren hin zu hochverteilten, einsatzbereiten Architekturen. Eine tiefgreifende Transformation ist unerlässlich, um Entscheidungshoheit zu erlangen – nämlich die Fähigkeit sämtlicher Kommandierender, in sämtlichen Bereichen schneller als jeder Gegner Erkenntnisse zu gewinnen, Wissen zu erlangen, Entscheidungen zu treffen und Maßnahmen zu ergreifen.

Die Notwendigkeit für eine durchgängige operative Resilienz

Moderne Missionen werden über ein ausuferndes Hybrid Cloud-Kontinuum abgewickelt, das private Air Gap-Clouds, bereitgestellte Mini-Rechenzentren sowie robuste taktische Geräte wie Drohnen und von Soldatinnen und Soldaten mitgeführte Systeme umfasst. Die Architektur ist für die Durchführung von Multi-Domain-Operationen (MDO) unerlässlich. Diese erfordern eine komplexe Integration und Koordination von Ressourcen in der Luft, zu Lande, zu Wasser, im Weltraum, im Cyberspace und im elektromagnetischen Spektrum.

Dieses erweiterte Spektrum führt jedoch auch zu kritischen Schwachstellen und erhöht die technische Komplexität erheblich. Isolierte Technologien und uneinheitliche Umgebungen können die operative Kontinuität beeinträchtigen, während sich Cybersicherheitsbedrohungen auf einer riesigen Angriffsfläche vermehren. Die Abhängigkeit von konstanter Konnektivität ist ein entscheidender Fehlerpunkt. In umkämpften Umgebungen müssen Edge-Geräte autonom funktionieren und dürfen Daten nur dann synchronisiert werden, wenn zuverlässige, unterbrochene Verbindungen verfügbar sind. Die zentrale Herausforderung besteht darin, echte Resilienz im gesamten Spektrum zu erreichen. Die Souveränität in einem zentralen Rechenzentrum reicht nicht aus, wenn der taktische Edge nicht unabhängig agieren kann.

Die größten Herausforderungen bei der digitalen Transformation in der Verteidigung

Obwohl die hybride Infrastruktur unbestreitbare Flexibilität bietet, stoßen Verteidigungsorganisationen bei ihrer digitalen Transformation auf mehrere entscheidende Hindernisse:

- **Cyberangriffe:** Verteidigungsorganisationen sind am meisten besorgt über die wachsende Bedrohung durch hochentwickelte Lieferketten und Cyberangriffe. So kann beispielsweise in Open Source-Libraries eingeschleuster Code ganze Flotten von Drohnen oder Fahrzeugen gefährden. In ähnlicher Weise können Man in the Middle-Angriffe (MitM) Firmware-Updates bei der Übertragung auf taktische Geräte verändern und so wichtige Missionen gefährden.
- **Isolierte Technologiestrukturen:** In verschiedenen Umgebungen – Core, Cloud und Edge – werden häufig inkompatible Technologie-Stacks verwendet. Diese Inkompatibilität zwingt Unternehmen dazu, Lösungen für die einzelnen Deployments neu zu erstellen, was zu einer Fragmentierung führt. Folglich müssen sich Streitkräfte und Engineers mit mehreren Plattformen vertraut machen, von Amazon Web Services (AWS) über Microsoft Azure bis hin zu speziellen taktischen Betriebssystemen, was die Einsatzbereitschaft erheblich verzögert.
- **Komplexität:** Manuelle Prozesse sorgen zwangsläufig für mehr Komplexität. So erfordert beispielsweise das Verschieben von Daten zwischen Kern- und Edge-Standorten benutzerdefinierte Workflows, wodurch sich die Bereitstellungszeiten erhöhen. Gleichzeitig lassen sich herkömmliche Sicherheitsmodelle nur schwer an verteilte Architekturen anpassen. So entstehen kritische Lücken, die Angreifende ausnutzen können.

Ein einheitlicher Ansatz für DevOps

Verteidigungsorganisationen benötigen dringend ein einheitliches, offenes Framework, das Autonomie und Sicherheit standortunabhängig stärkt. Ziel ist eine konsistente Plattform für die Ausführung wichtiger Anwendungen in einer Private Cloud, die Verarbeitung von KI-Workloads am Edge und die Bereitstellung von Echtzeitentscheidungen auf einem Edge-Gerät im Außeneinsatz. Echte moderne Resilienz ist die Fähigkeit, mit unerschütterlicher Integrität vom Kern bis zur Frontlinie zu funktionieren.

Wie Red Hat Sie unterstützt

Angesichts eines fragmentierten digitalen Raums benötigen Verteidigungsorganisationen eine einheitliche Basis und zuverlässige Beratung, um für Resilienz – vom strategischen Kern bis hin zum taktischen Edge – zu sorgen. Red Hat stellt diese wichtige, konsistente Plattform bereit. Mit dem Prinzip „Einmal bereitstellen, standortunabhängig ausführen" beschleunigt Red Hat die Einsatzbereitschaft. Dadurch können Teams vertraute Tools in verschiedenen Umgebungen nutzen. Neben dem konsistenten IT-Erlebnis basieren die Lösungen von Red Hat auf offenen Standards. Die Plattform verhindert Anbieterabhängigkeiten und ermöglicht dadurch bessere Integrationen mit einer skalierbaren und flexiblen Lösung.

Sicherheit auf Militärniveau: Red Hat setzt auf höchste Sicherheitsstandards: Wir stellen sicher, dass unsere wichtigsten Plattformen, wie etwa Red Hat® OpenShift®, strenge Compliance-Standards einhalten. Durch Red Hat Trusted Software Supply Chain sorgen wir kontinuierlich für Sicherheit und bieten einen ganzheitlichen und kontinuierlichen Sicherheitsansatz. Dieser Ansatz integriert DevSecOps-Praktiken, um die Produktkette zu stärken und zu verifizieren, dass die Software den erforderlichen Standards für Sicherheit, Compliance, Datenschutz und Transparenz entspricht.

Sicherheitssouveränität: Durch kryptografische Zertifizierung lässt sich überprüfen, ob Firmware und kritische Updates intakt sind. Dies unterstützt das allgemeinere Ziel der Sicherheitssouveränität. Mit diesem Prozess werden Integrität und Zuverlässigkeit digitaler Systeme überprüft. Er stellt ein Kernelement der Plattformstrategie von Red Hat dar, mit dem die Softwarelieferkette validiert und das Risiko des Einschleusens von bösartigem Code gemindert wird.

Getrennte Automatisierung: Getrennte Automatisierung ermöglicht das Patchen von Geräten im Außeninsatz und die Integration mit beliebigen spezifischen Prozessen, mit denen der Kunde bereits arbeitet, ohne dass eine Internetverbindung erforderlich ist. Red Hat unterstützt mit Red Hat Ansible® Automation Platform die Bereitstellung zuverlässiger autonomer Abläufe, die für eine moderne Verteidigung erforderlich sind. Mit der Plattform lassen sich Geräte unter den Bedingungen „Denied, Disrupted, Intermittent, Limited" (DDIL) verwalten, ohne von anfälliger externer Konnektivität abhängig zu sein. Diese Autonomie schützt die umfangreichen, langfristigen Investitionen in bereitgestellte Software-Assets, minimiert die Sicherheitsrisiken im Zusammenhang mit dem Einschleusen von bösartigem Code und garantiert einen kontinuierlichen, geschäftskritischen Betrieb, wenn externe Unterstützung nicht möglich ist.

Im strategischen Kern sorgen zuverlässige Lösungen wie Red Hat OpenShift für eine skalierbare, souveräne Infrastruktur. Am bereitgestellten Edge verarbeiten kompakte OpenShift-Cluster wichtige Informationen und KI-Workloads. An der taktischen Frontlinie bietet das schlanke Red Hat Device Edge hochportierbare, nicht vernetzte Operationen auf robusten Systemen.

Bewährte Use Cases in der Verteidigungsbranche

Mehrere Verteidigungsorganisationen haben erfolgreich Lösungen von Red Hat implementiert, um kritische operative Herausforderungen zu bewältigen und bedeutende Fortschritte zu erzielen:

Optimierte Außeneinsätze für eine europäische Luftwaffe: Eine europäische Luftwaffe sah sich mit anhaltenden Einsatzstörungen konfrontiert, die durch Netzwerkausfälle bei Außeneinsätzen verursacht wurden. Durch die Implementierung von Red Hat OpenShift in mobilen Edge-Rechenzentren konnte die IT-Abteilung der Luftwaffe lokale KI-Verarbeitungsfunktionen einführen, die unabhängig vom Verbindungsstatus für einen kontinuierlichen Betrieb sorgen und gleichzeitig den Bandbreitenbedarf erheblich reduzieren.

Software-Updates während des Flugs für unbemannte Luftsysteme: In einer weiteren Demonstration führender Funktionen demonstrierte ein großes Verteidigungsunternehmen seine Fähigkeit, Software-Updates auf unbemannten Luftsystemen während des Flugs durchzuführen. Mithilfe von Red Hat Device Edge konnte das Unternehmen während aktiver Missionen erfolgreich KI-Modell-Upgrades für Drohnen bereitstellen und so die Zielerkennung in Echtzeit verbessern, ohne dass eine Unterbrechung der Mission oder Systemausfallzeiten erforderlich waren.

Beschleunigte Infrastruktur und Bereitstellung für eine nationale Verteidigungsorganisation: Eine nationale Verteidigungsorganisation konnte durch die Automatisierung ihrer PaaS-Prozesse (Platform as a Service) mit Ansible Automation Platform und Red Hat OpenShift deutliche Effizienzsteigerungen erzielen. Die Organisationen konnten die Bereitstellungszeiten ihrer Infrastruktur von mehreren Wochen auf nur 24 Stunden reduzieren und sind dadurch für den Kampfeinsatz bereit. Gleichzeitig konnte die Entwicklungskapazität des Unternehmens innerhalb von nur einem Jahr auf das nahezu Vierfache gesteigert werden, und das unter Einhaltung strenger Sicherheitsprotokolle.

Erste Schritte

Kontaktieren Sie Red Hat, um mehr darüber zu erfahren, wie Sie Ihre Verteidigungsoperationen vom Kern bis zum Edge schützen können.

Über Red Hat

Red Hat unterstützt Kunden dabei, ihre Umgebungen zu standardisieren, cloudnative Anwendungen zu entwickeln und komplexe Umgebungen mit vielfach ausgezeichnetem Support, Training und Consulting Services zu integrieren, zu automatisieren, zu sichern und zu verwalten.

EUROPA, NAHOST, UND AFRIKA (EMEA)
00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

de.redhat.com
Nr. 3134353_1225