Rafforza la difesa con una piattaforma unificata

Vantaggi principali:

- Nessun divario di resilienza tra il core strategico e l'edge tattico
- Piattaforma coerente per applicazioni di importanza critica in ambienti disconnessi
- Approccio unificato all'autonomia e alla sicurezza

Colmare il divario di resilienza tra il core strategico e l'edge tattico

Gli enti governativi che si occupano di difesa devono affrontare una sfida cruciale: garantire l'affidabilità delle operazioni nell'intero spettro, dal core strategico all'edge tattico. Per via di esigenze fondamentali come agilità, sicurezza affidabile e autonomia strategica, il settore della difesa è in rapida evoluzione. Sta passando dai datacenter centralizzati tradizionali ad architetture mission ready altamente distribuite. Una profonda trasformazione è essenziale per far sì che tutti i leader siano in grado di percepire, comprendere, decidere e agire più rapidamente di qualsiasi altro avversario in tutti i domini.

L'imperativo per la resilienza operativa end to end

Le missioni moderne si svolgono in un ampio spettro di soluzioni di cloud ibrido in continua espansione, che comprende cloud air gap privati, mini datacenter distribuiti e dispositivi tattici ottimizzati come droni e sistemi indossati dai soldati. L'architettura è fondamentale per l'esecuzione di operazioni multidominio (MDO), che richiedono un'integrazione e un coordinamento complessi delle risorse in ambito aereo, terrestre, marittimo, spaziale, informatico ed elettromagnetico.

Tuttavia, l'espansione dei domini dà adito a vulnerabilità critiche e aumenta notevolmente la complessità tecnica. Impiegare tecnologie isolate in ambienti diversificati può compromettere la continuità operativa, mentre le minacce alla sicurezza informatica si moltiplicano su una vasta superficie di attacco. Affidarsi a una connettività costante è un errore critico. Negli ambienti in conflitto, i dispositivi edge devono funzionare in modo autonomo, sincronizzando i dati solo quando sono disponibili collegamenti intermittenti e affidabili. La sfida principale è raggiungere una resilienza effettiva nell'intero spettro. La sovranità in un datacenter centrale non è sufficiente se l'edge tattico non può operare in modo indipendente.

Sfide principali nella trasformazione digitale della difesa

Sebbene l'infrastruttura ibrida offra una flessibilità innegabile, gli enti che si occupano di difesa devono affrontare diversi ostacoli critici lungo il percorso di trasformazione digitale.

- **Attacchi informatici:** la principale preoccupazione degli enti di difesa è la crescente minaccia rappresentata dagli attacchi sofisticati alla sicurezza informatica e alla catena di distribuzione. Ad esempio, l'introduzione di codice dannoso nelle librerie open source può compromettere intere flotte di droni o veicoli. Allo stesso modo, gli attacchi man-in-the-middle (MitM) possono alterare gli aggiornamenti del firmware in transito verso dispositivi tattici, e quindi potenzialmente sabotare missioni critiche.
- **Strutture tecnologiche isolate:** ambienti diversi (core, cloud ed edge) utilizzano spesso stack tecnologici incompatibili. Questa incompatibilità costringe le organizzazioni a realizzare le soluzioni da zero per ogni deployment, causandone la frammentazione. Di conseguenza, soldati e ingegneri devono imparare a utilizzare più piattaforme, da Amazon Web Services (AWS) e Microsoft Azure a sistemi operativi tattici specializzati, rallentando notevolmente la preparazione alla missione.
- **Complessità:** affidarsi a processi manuali implica una maggiore complessità. Ad esempio, lo spostamento dei dati da e verso la posizione core-to-edge richiede flussi di lavoro ad hoc, il che aumenta i tempi di deployment. Allo stesso tempo, i modelli di sicurezza tradizionali faticano ad adattarsi alle architetture distribuite, generando lacune critiche che gli avversari possono sfruttare.

Un approccio unificato

Gli enti di difesa hanno urgente bisogno di un framework unificato e aperto che rafforzi l'autonomia e la sicurezza ovunque. L'obiettivo è ottenere una piattaforma coerente per eseguire le applicazioni critiche in un cloud privato, elaborare i carichi di lavoro dell'IA all'edge e prendere decisioni in tempo reale con un dispositivo edge sul campo. La vera resilienza moderna è la capacità di operare con un'integrità costante dal core alla prima linea.

Il ruolo di Red Hat

Di fronte a un ambiente di battaglia digitale frammentato, gli enti che si occupano di difesa necessitano di una base unificata e di un consulente affidabile per garantire la resilienza dal core strategico all'edge tattico. Red Hat offre proprio questa piattaforma coerente essenziale. Adottando un approccio che prevede la distribuzione delle soluzioni una volta sola per eseguirle ovunque, Red Hat accelera la preparazione alle missioni offrendo al personale strumenti familiari in tutti gli ambienti. Oltre a garantire coerenza, le soluzioni Red Hat si basano su standard open source ed evitano i vincoli a un solo fornitore, consentendo integrazioni migliori con una soluzione scalabile e flessibile.

Sicurezza di livello militare: Red Hat integra una sicurezza di livello militare garantendo che le sue piattaforme principali, come Red Hat® OpenShift®, rispettino rigorosi standard di conformità. La sicurezza viene applicata in modo costante con Red Hat Trusted Software Supply Chain, che offre un approccio olistico e continuo integrando le pratiche DevSecOps per rafforzare la catena di custodia e verificare che il software soddisfi gli standard di sicurezza, conformità, privacy e trasparenza.

Sovranità della sicurezza: l'attestazione crittografica verifica che il firmware e gli aggiornamenti critici siano intatti, a favore di un più ampio obiettivo di sovranità della sicurezza. Questo processo verifica l'integrità e l'affidabilità dei sistemi digitali ed è una parte fondamentale della strategia della piattaforma di Red Hat che ha lo scopo di convalidare la catena di distribuzione del software e ridurre il rischio che venga introdotto codice dannoso.

Automazione disconnessa: l'automazione disconnessa consente di applicare le patch ai dispositivi sul campo, integrandosi con qualsiasi processo specifico già in uso, senza richiedere alcuna connessione a Internet. Red Hat consente di svolgere le operazioni autonome e affidabili necessarie per una difesa moderna utilizzando Red Hat Ansible® Automation Platform. La piattaforma aiuta a gestire i dispositivi in condizioni DDIL (Denied, Disrupted, Intermittent, and Limited) senza dipendere dalla connettività esterna vulnerabile. Questa autonomia protegge gli ingenti investimenti a lungo termine nelle risorse software distribuite, riduce al minimo i rischi per la sicurezza associati all'introduzione di codice dannoso e garantisce operazioni mission-critical continue quando non è disponibile supporto esterno.

Nel core strategico, le soluzioni affidabili come Red Hat OpenShift offrono un'infrastruttura sovrana e scalabile. Nei deployment all'edge, i cluster OpenShift compatti elaborano le informazioni critiche e i carichi di lavoro di IA. In prima linea tattica, il leggero Red Hat Device Edge consente di svolgere operazioni ultraportatili e disconnesse su sistemi ottimizzati.

Scenari di utilizzo comprovati nel settore della difesa

Diversi enti che operano nel settore della difesa sono riusciti a superare le sfide operative critiche e ottenere progressi significativi adottando le soluzioni Red Hat.

Operazioni sul campo ottimizzate per una forza aerea europea: una forza aerea europea ha dovuto far fronte a interruzioni persistenti delle missioni a causa di guasti di rete durante le operazioni sul campo. Con l'implementazione di Red Hat OpenShift nei datacenter portatili all'edge, il reparto IT dell'aeronautica ha adottato capacità di elaborazione dell'IA in loco che hanno consentito lo svolgimento continuo delle operazioni indipendentemente dallo stato della connettività, riducendo al contempo i requisiti di larghezza della banda.

Aggiornamenti software in volo per sistemi aerei senza pilota: un'altra dimostrazione di capacità all'avanguardia è l'esempio di un importante appaltatore della difesa che è riuscito a eseguire aggiornamenti software in volo su sistemi aerei senza pilota. Utilizzando Red Hat Device Edge, l'azienda appaltatrice ha potuto implementare gli upgrade dei modelli di IA sui droni durante missioni attive, migliorando le capacità di riconoscimento dei bersagli in tempo reale senza dover interrompere le missioni o l'operatività dei sistemi.

Infrastruttura e deployment accelerati per un ente di difesa nazionale: un ente di difesa nazionale ha ottenuto notevoli miglioramenti in termini di efficienza automatizzando i processi Platform-as-a-Service (PaaS) con Ansible Automation Platform e Red Hat OpenShift. I tempi di deployment dell'infrastruttura sono stati ridotti da alcune settimane a sole 24 ore, il che l'ha resa pronta per le operazioni di combattimento. Allo stesso tempo, l'ente ha aumentato la capacità di sviluppo di quasi 4 volte in un solo anno, pur mantenendo rigidi protocolli di sicurezza.

Per iniziare

Contatta un esperto di Red Hat per scoprire come proteggere le operazioni di difesa dal core all'edge.

Informazioni su Red Hat

Red Hat consente la standardizzazione in diversi ambienti e lo sviluppo di applicazioni cloud native, oltre a favorire l'integrazione, l'automazione, la protezione e la gestione di ambienti complessi grazie a pluripremiati servizi di consulenza, formazione e supporto.

ITALIA
it.redhat.com
italy@redhat.com

EUROPA, MEDIO ORIENTE, E AFRICA (EMEA)
00800 7334 2835
it.redhat.com
europe@redhat.com

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

it.redhat.com
#3134353_1225