Fortalecimiento de la defensa con una plataforma unificada

Principales beneficios:

- integración de la capacidad de recuperación desde la infraestructura principal estratégica hasta el extremo táctico;
- plataforma uniforme para las aplicaciones esenciales en los entornos desconectados;
- enfoque unificado para la autonomía y la seguridad.

Integración de la capacidad de recuperación desde la infraestructura principal estratégica hasta el extremo táctico

Los organismos gubernamentales de defensa enfrentan un desafío fundamental: mantener operaciones confiables en todos los entornos, desde la infraestructura principal estratégica hasta el extremo de red táctico. Debido a la necesidad fundamental de contar con agilidad, seguridad sólida y autonomía estratégica, el sector de defensa evoluciona rápidamente: deja los centros de datos concentrados y tradicionales y adopta arquitecturas altamente distribuidas y listas para la misión. Es fundamental llevar a cabo una transformación profunda para dominar la toma de decisiones, es decir, lograr que todos los comandantes perciban, comprendan, decidan y actúen con mayor rapidez que cualquier adversario en todos los dominios.

La necesidad de la resistencia operativa integral

Las misiones modernas se ejecutan en una nube híbrida en constante expansión, que incluye nubes privadas aisladas, minicentros de datos implementados y dispositivos tácticos reforzados como los drones y los sistemas que portan los soldados. La arquitectura desempeña un papel clave en la ejecución de operaciones multidominio (MDO), lo cual exige una integración y coordinación complejas de los recursos en los dominios electromagnéticos, aéreos, terrestres, marítimos, espaciales y cibernéticos.

Sin embargo, la expansión de los dominios también genera puntos vulnerables graves y aumenta considerablemente la complejidad técnica. Las tecnologías aisladas y los entornos diferentes pueden dificultar la continuidad operativa, mientras que las amenazas a la ciberseguridad se multiplican en una amplia superficie de ataque. Depender de la conectividad constante es un punto de falla importante. En los entornos conflictivos, los dispositivos del extremo de la red deben funcionar de manera autónoma y sincronizar los datos solo cuando haya enlaces confiables e intermitentes disponibles. El desafío principal es adquirir una verdadera capacidad de recuperación en todos los dominios. La soberanía en un centro de datos central no es suficiente si el extremo táctico no puede funcionar de forma independiente.

Desafíos clave en la transformación digital de la defensa

Si bien la infraestructura híbrida ofrece una gran flexibilidad, los organismos de defensa enfrentan varios obstáculos importantes en su proceso de transformación digital:

- **Ataques cibernéticos:** Los organismos de defensa temen por la creciente amenaza de las cadenas de suministro sofisticadas y los ataques cibernéticos. Por ejemplo, el código malicioso que se introduce en las bibliotecas open source puede comprometer flotas completas de vehículos o drones. De manera similar, los ataques de intermediarios (MitM) pueden afectar a las actualizaciones de firmware en tránsito hacia los dispositivos tácticos, lo que podría sabotear las misiones más importantes.
- **Estructuras tecnológicas aisladas:** Los distintos entornos (infraestructura principal, nube y extremo de la red) suelen utilizar stacks tecnológicas incompatibles, lo que obliga a los organismos a volver a diseñar soluciones para cada implementación y provoca fragmentación. Por lo tanto, los soldados y los ingenieros deben aprender a utilizar varias plataformas, desde Amazon Web Service (AWS) y Microsoft Azure hasta sistemas operativos tácticos especializados, lo cual ralentiza notablemente la preparación para las misiones.
- **Complejidad:** La dependencia de los procesos manuales genera un mayor nivel de complejidad. Por ejemplo, el traslado de los datos entre la infraestructura principal y el extremo de la red y viceversa requiere flujos de trabajo personalizados, lo cual implica tiempos de implementación más prolongados. Al mismo tiempo, los modelos de seguridad tradicionales tienen dificultades para adaptarse a las arquitecturas distribuidas y generan fallas importantes que los agentes malintencionados pueden aprovechar.

Adopción de un enfoque unificado

Los organismos de defensa necesitan con urgencia un marco abierto y unificado que refuerce la autonomía y la seguridad en todos los ámbitos. El objetivo es contar con una plataforma uniforme que permita ejecutar las aplicaciones más importantes en una nube privada, procesar las cargas de trabajo de inteligencia artificial en el extremo de la red y brindar decisiones inmediatas en un dispositivo del extremo de la red en el campo. La verdadera capacidad de recuperación moderna consiste en la posibilidad de funcionar con una firme integridad desde el nivel estratégico hasta el táctico.

El respaldo de Red Hat

Los organismos de defensa, que se enfrentan a un entorno digital fragmentado, necesitan una base unificada y un asesor de confianza que garanticen la capacidad de recuperación desde la infraestructura principal estratégica hasta el extremo de red táctico. Red Hat ofrece esta plataforma esencial y uniforme. Al adoptar la práctica de "implementación única y ejecución en cualquier lugar", Red Hat agiliza la preparación para las misiones, de modo que el personal puede utilizar herramientas conocidas en todos los entornos. Además de contar con una experiencia uniforme, las soluciones de Red Hat se basan en estándares abiertos, y la plataforma evita la dependencia de un solo proveedor, lo cual permite lograr mejores integraciones con una solución expandible y flexible.

Seguridad de nivel militar: Red Hat incorpora seguridad de nivel militar al garantizar que sus plataformas principales, como Red Hat® OpenShift®, se ajustan a los estrictos estándares de cumplimiento normativo. La seguridad se aplica permanentemente a través de Red Hat Trusted Software Supply Chain para ofrecer un enfoque integral y permanente. Este enfoque integra las prácticas de DevSecOps para fortalecer la cadena de custodia y verificar que el software respete los estándares del organismo en materia de seguridad, cumplimiento normativo, privacidad y transparencia.

Garantía de seguridad: La autenticación criptográfica verifica que el firmware y las actualizaciones importantes no se hayan modificado, lo cual responde al objetivo general de soberanía de seguridad. Este proceso verifica la integridad y la confiabilidad de los sistemas digitales, y constituye una parte fundamental de la estrategia de plataforma de Red Hat para validar la cadena de suministro de software y reducir el riesgo de presencia de código malicioso.

Automatización desconectada: Esta función permite aplicar parches en los dispositivos de campo e integrarlos a cualquier proceso específico que el cliente ya tenga, sin necesidad de conectarse a Internet. Red Hat ayuda a ofrecer las operaciones autónomas y confiables que se necesitan para la defensa moderna mediante Red Hat Ansible® Automation Platform. La plataforma permite gestionar los dispositivos en entornos denegados, desconectados, intermitentes y con bajo ancho de banda (DDIL) sin depender de una conectividad externa vulnerable. Esta autonomía protege la enorme inversión a largo plazo en los recursos de software implementados, disminuye los riesgos de seguridad asociados con la presencia de código malicioso y garantiza el funcionamiento permanente de los sistemas esenciales cuando no es posible contar con soporte externo.

En la infraestructura principal estratégica, las soluciones confiables como Red Hat OpenShift ofrecen una infraestructura soberana y expansible. En el extremo de la red implementado, los clústeres compactos de OpenShift procesan las cargas de trabajo de inteligencia artificial más importantes. En la primera línea táctica, la solución ligera Red Hat Device Edge ofrece operaciones desconectadas y ultraportátiles en sistemas reforzados.

Casos prácticos comprobados del sector de defensa

Varios organismos de defensa han implementado con éxito las soluciones de Red Hat para superar los desafíos operativos más importantes y lograr grandes avances:

Optimización de las operaciones de campo para una fuerza aérea europea: Una fuerza aérea de Europa enfrentaba constantes obstáculos en las misiones causados por las interrupciones de la red en las operaciones de campo. Al implementar Red Hat OpenShift en centros de datos del extremo de la red portátiles, el departamento de TI de la fuerza área adoptó funciones locales de procesamiento de inteligencia artificial que mantuvieron la continuidad operativa con independencia del estado de la conectividad. Al mismo tiempo, se redujeron considerablemente los requisitos de ancho de banda.

Actualizaciones de software durante el vuelo para los sistemas aéreos no tripulados: En otra demostración de funciones destacadas, un importante contratista del sector de defensa presentó la posibilidad de realizar actualizaciones de software durante el vuelo en los sistemas aéreos no tripulados. La empresa contratante utilizó Red Hat Device Edge para implementar con éxito las actualizaciones de los modelos de inteligencia artificial en los drones durante las misiones activas, lo que permitió mejorar las funciones de reconocimiento de objetivos en tiempo real sin interrumpir las tareas ni ocasionar tiempo de inactividad del sistema.

Agilización de la infraestructura y la implementación para un organismo de defensa nacional: Un organismo de defensa nacional aumentó notablemente su eficiencia al automatizar los procesos de plataforma como servicio (PaaS) con Ansible Automation Platform y Red Hat OpenShift. Los tiempos de implementación de la infraestructura del organismo se redujeron de varias semanas a tan solo 24 horas, lo que permitió que estuviera preparado para las operaciones de combate. Paralelamente, su capacidad de desarrollo se multiplicó casi por cuatro en un solo año, sin comprometer los estrictos protocolos de seguridad.

Para comenzar

Comunícate con un representante de Red Hat para aprender a proteger tus operaciones de defensa desde la infraestructura principal hasta el extremo de la red.

Acerca de Red Hat

Con Red Hat, los clientes pueden llevar la estandarización a todos los entornos; desarrollar aplicaciones directamente en la nube; e integrar, automatizar, proteger y gestionar los entornos complejos a través de servicios galardonados de soporte, capacitación y consultoría.

facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

ARGENTINA
+54 11 4329 7300

CHILE
+562 2597 7000

COLOMBIA
+571 508 8631
+52 55 8851 6400

MÉXICO
+52 55 8851 6400

ESPAÑA
+34 914 148 800

es.redhat.com
#3134353_1225