Fortaleça a defesa com uma plataforma unificada

Principais benefícios:

- Sem lacuna de resiliência do núcleo estratégico à edge tática
- Plataforma consistente para aplicações de importância crítica em ambientes desconectados
- Abordagem unificada de autonomia e segurança

Elimine a lacuna de resiliência do núcleo estratégico à edge tática

Os órgãos governamentais de defesa enfrentam um desafio decisivo: manter operações confiáveis em todas as frentes de atuação, do núcleo estratégico à edge tática. Devido à necessidade de agilidade, segurança robusta e autonomia estratégica, o setor de defesa está evoluindo rapidamente. O setor está migrando de data centers centralizados tradicionais para arquiteturas altamente distribuídas e prontas para missão. Uma transformação profunda é essencial para alcançar superioridade na tomada de decisão: a capacidade de todos os comandantes perceberem, compreenderem, decidirem e agirem mais rápido que todos os adversários em todos os domínios.

A importância da resiliência operacional de ponta a ponta

As missões modernas atuam em uma extensa nuvem híbrida distribuída, abrangendo nuvens privadas isoladas, data centers pequenos implantados e dispositivos táticos robustos, como drones e sistemas usados por soldados. A arquitetura é fundamental para a execução de operações multidomínio (MDO), que exigem integração complexa e coordenação de ativos nos domínios do espectro eletromagnético, aéreo, terrestre, marítimo, espacial e cibernético.

No entanto, a expansão de domínios também gera vulnerabilidades críticas e aumenta significativamente a complexidade técnica. Tecnologias isoladas e ambientes distintos podem prejudicar a continuidade operacional enquanto ameaças de cibersegurança se multiplicam em uma ampla superfície de ataque. A dependência de conectividade constante é um ponto de falha crítico. Em ambientes disputados, dispositivos de edge precisam funcionar com autonomia, sincronizando dados somente quando vínculos confiáveis e intermitentes estão disponíveis. O principal desafio é alcançar uma resiliência real em toda a operação. A soberania em um data center central não será suficiente se a edge tática não contar com operação independente.

Principais desafios da transformação digital no setor de defesa

A infraestrutura híbrida oferece flexibilidade inegável. No entanto, os órgãos de defesa enfrentam vários obstáculos críticos na jornada de transformação digital:

- **Ataques cibernéticos:** os órgãos de defesa estão mais preocupados com a ameaça crescente de ataques cibernéticos e cadeias de suprimentos sofisticadas. Por exemplo, código mal-intencionado injetado em bibliotecas open source pode comprometer frotas inteiras de drones ou veículos. Da mesma forma, ataques man-in-the-middle (MitM) podem comprometer atualizações de firmware em trânsito para dispositivos táticos e sabotar missões importantes.
- **Estruturas de tecnologia isoladas:** ambientes diferentes (núcleo, nuvem e edge) costumam usar stacks de tecnologia incompatíveis. Essa incompatibilidade força as organizações a desenvolver novamente soluções para cada implantação, gerando fragmentação. Consequentemente, soldados e engenheiros precisam aprender a usar várias plataformas, como Amazon Web Services (AWS) e Microsoft Azure, e até sistemas operacionais táticos especializados. Isso atrasa significativamente a prontidão da missão.
- **Complexidade:** depender de processos manuais gera mais complexidade. Por exemplo, mover dados do núcleo ao local da edge e de volta para o núcleo requer fluxos de trabalho personalizados, que aumentam os tempos de implantação. Ao mesmo tempo, os modelos de segurança tradicionais são difíceis de adaptar a arquiteturas distribuídas, gerando lacunas críticas que adversários podem explorar.

Adote uma abordagem unificada

Os órgãos de defesa precisam urgentemente de um framework unificado e aberto que fortaleça a autonomia e a segurança em todos os ambientes. O objetivo é ter uma plataforma consistente para executar aplicações críticas em uma nuvem privada, processando cargas de trabalho de IA na edge e oferecendo decisões em tempo real em um dispositivo de edge em campo. A verdadeira resiliência moderna é a capacidade de trabalhar com integridade inabalável, do núcleo à linha de frente.

Como a Red Hat pode ajudar

Ao enfrentar um espaço de batalha digital fragmentado, os órgãos de defesa precisam de uma base unificada e um consultor de confiança para garantir resiliência, do núcleo estratégico à edge tática. A Red Hat oferece essa plataforma consistente e essencial. Com a prática "implante uma vez, execute em qualquer lugar", a Red Hat acelera a prontidão da missão, permitindo que funcionários usem ferramentas familiares em diferentes ambientes. Além da experiência consistente, as soluções da Red Hat são baseadas em padrões abertos, e a plataforma impede a dependência de fornecedor, possibilitando integrações melhores com uma solução escalável e flexível.

Segurança de nível militar: a Red Hat incorpora segurança de nível militar garantindo que suas plataformas principais, como o Red Hat® OpenShift®, sigam rigorosos padrões de conformidade. A segurança é reforçada constantemente pelo Red Hat Trusted Software Supply Chain, que oferece uma abordagem holística e contínua. Essa abordagem integra práticas de DevSecOps para fortalecer a cadeia de custódia e verificar se o software atende aos padrões de segurança, conformidade, privacidade e transparência do órgão.

Soberania de confiabilidade: o atestado criptográfico confirma que o firmware e as atualizações críticas permanecem intactos, apoiando o objetivo mais amplo de soberania de confiabilidade. Esse processo verifica a integridade e a confiabilidade dos sistemas digitais, e é parte essencial da estratégia de plataforma da Red Hat para validar a cadeia de suprimentos de software e mitigar o risco de injeção de código mal-intencionado.

Automação desconectada: a automação desconectada permite a aplicação de patches em dispositivos de campo, se integrando a qualquer processo específico que o cliente já tenha, sem necessidade de conexão com a internet. A Red Hat ajuda a entregar as operações autônomas confiáveis para a defesa moderna usando o Red Hat Ansible® Automation Platform. A plataforma ajuda a gerenciar dispositivos em condições de rede negadas, interrompidas, intermitentes e limitadas (DDIL), sem depender de conectividade externa vulnerável. Essa autonomia protege investimentos de longo prazo em ativos de software implantados, minimiza riscos de segurança ligados à injeção de código mal-intencionado e assegura a continuidade de operações de importância crítica mesmo sem suporte externo.

No núcleo estratégico, soluções confiáveis como o Red Hat OpenShift oferecem infraestrutura soberana e escalável. Na edge implantada, os clusters compactos do OpenShift processam cargas de trabalho críticas de inteligência e IA. Na linha de frente tática, o Red Hat Device Edge leve oferece operações ultraportáteis e desconectadas em sistemas robustos.

Casos de uso comprovados no setor de defesa

Vários órgãos de defesa implementaram soluções da Red Hat com sucesso para superar desafios operacionais e alcançar avanços significativos:

Operações de campo otimizadas para uma força aérea europeia: uma força aérea europeia enfrentava disrupções persistentes nas missões causadas por interrupções da rede em operações de campo. Com a implementação do Red Hat OpenShift em data centers de edge portáteis, o departamento de TI da força aérea adotou recursos locais de processamento da IA que mantêm operações contínuas sem depender do status de conectividade, além de reduzir significativamente os requisitos de largura de banda.

Atualizações de software de bordo em sistemas aéreos não tripulados: em mais uma demonstração de recursos líderes do setor, um grande prestador de serviços do setor de defesa mostrou a capacidade de realizar atualizações de software de bordo em sistemas aéreos não tripulados. Com o Red Hat Device Edge, a empresa contratante conseguiu implantar upgrades de modelos de IA em drones durante missões ativas, aprimorando os recursos de reconhecimento de alvos em tempo real sem interromper a missão nem gerar tempo de inatividade do sistema.

Infraestrutura e implantação aceleradas para uma agência de defesa nacional: uma agência de defesa nacional melhorou a eficiência ao automatizar seus processos de Plataforma como Serviço (PaaS) com o Ansible Automation Platform e o Red Hat OpenShift. Os tempos de implantação de infraestrutura foram reduzidos de várias semanas para apenas 24 horas, preparando a agência para as operações de combate. Ao mesmo tempo, a capacidade de desenvolvimento aumentou quase quatro vezes em um ano, com protocolos de segurança rigorosos.

Veja por onde começar

Contate um consultor da Red Hat para descobrir como proteger suas operações de defesa, do núcleo à edge.

Sobre a Red Hat

A Red Hat ajuda os clientes a definirem padrões entre diferentes ambientes e a desenvolver aplicações nativas em nuvem, além de integrar, automatizar, proteger e gerenciar ambientes complexos com serviços de consultoria, treinamento e suporte premiados.

facebook.com/redhatinc
@redhatbr
linkedin.com/company/red-hat-brasil

AMÉRICA LATINA
+54 11 4329 7300
latammktg@redhat.com

BRASIL
+55 11 3629 6000
marketing-br@redhat.com

br.redhat.com
#3134353_1225