

통합 플랫폼을 통한 국방 강화

주요 장점:

- 전략적 핵심 지대에서 전술적 엣지까지 회복 탄력성 격차 해소
- 네트워크 연결이 단절된 환경의 미션 크리티컬 애플리케이션을 위한 일관된 플랫폼
- 자율성과 보안을 위한 통합된 접근 방식

전략적 핵심 지대에서 전술적 엣지까지 회복 탄력성 격차 해소

정부 국방 조직은 전략적 핵심 지대부터 전술적 엣지에 이르기까지 전 영역에 걸쳐 신뢰할 수 있는 운영을 유지해야 하는 중대한 과제에 직면해 있습니다. 또한 민첩성, 강력한 보안, 전략적 자율성에 대한 요구가 크게 증가하면서 국방 분야가 빠르게 발전하고 있습니다. 기존의 중앙화된 데이터센터를 넘어 고도의 분산형 작전 수행 가능 아키텍처로 전환 중입니다. 모든 지휘관이 모든 영역에서 적보다 더 빠르게 감지하고 이해하며 결정하고 행동할 수 있는 능력, 즉 결정 우위를 달성하기 위해서는 근본적인 트랜스포메이션이 필수적입니다.

포괄적 작전 회복 탄력성을 위한 필수 과제

현대적인 작전은 폐쇄형 프라이빗 클라우드부터 현장 전개형 미니 데이터센터, 그리고 드론이나 착용형 시스템과 같은 강화된 전술 장비에 이르기까지 광범위하게 펼쳐진 하이브리드 클라우드 연속체 전반에서 수행됩니다. 이러한 아키텍처는 육해공, 우주, 사이버, 전자기 스펙트럼에 이르는 모든 영역에서 자산의 복잡한 통합 및 조정을 요구하는 다영역 작전(Multi-Domain Operation, MDO)을 수행하는 데 필수적입니다.

그러나 전장 영역의 확장은 중대한 취약점을 야기할 뿐만 아니라 기술적 복잡성을 현저히 증대시키는 것도 사실입니다. 격리된 기술과 서로 다른 환경은 작전 연속성을 단절시킬 수 있으며, 동시에 사이버 보안 위협이 광범위한 공격 표면 전반에서 기하급수적으로 증가합니다. 이때 네트워크에 대한 상시 연결에 의존할 경우 치명적인 실패로 이어질 수 있습니다. 분쟁 환경에서 엣지 기기는 자율적으로 작동해야 하며, 신뢰할 수 있는 간헐적 통신망이 확보된 경우에만 데이터를 동기화해야 합니다. 핵심 과제는 전 영역에 걸쳐 진정한 회복 탄력성을 실현하는 것입니다. 전술적 엣지가 독립적으로 작동하지 못하는 경우에는 중앙 데이터센터의 주권 확보만으로는 충분하지 않습니다.

국방 디지털 트랜스포메이션의 주요 과제

하이브리드 인프라가 거부할 수 없는 유연성을 제공하는 것은 사실이지만 국방 조직은 디지털 트랜스포메이션 여정에서 다음과 같은 몇 가지 중대한 난관에 봉착합니다.

- ▶ **사이버 공격:** 국방 조직은 고도화되는 공급망 공격과 사이버 공격의 위협의 증대를 가장 우려하고 있습니다. 예를 들어 악성 코드가 오픈소스 라이브러리에 삽입될 경우 모든 드론 또는 전투 차량 전체가 무력화될 수 있습니다. 마찬가지로 중간자(Man-in-the-Middle, MitM) 공격은 전술 기기로 전송되는 펌웨어 업데이트를 변조하여 핵심 작전을 무력화시킬 수 있습니다.
- ▶ **격리된 기술 구조:** 코어, 클라우드, 엣지 등 서로 다른 환경에서는 호환되지 않는 기술 스택을 사용하는 경우가 많습니다. 이러한 상호 불호환성으로 인해 조직은 각 전개 시 솔루션을 재구축해야 하므로 파편화가 발생합니다. 그 결과 장비와 기술 요원은 AWS(Amazon Web Service)와 Microsoft Azure부터 특수 전술용 운영 체제에 이르기까지 여러 플랫폼을 익혀야만 하므로 작전 투입 준비 속도가 현저히 저하됩니다.
- ▶ **복잡성:** 수동 프로세스에 의존하면 복잡성이 초래될 수밖에 없습니다. 가령, 본부와 현장 간에 데이터를 이동하려면 사용자 정의 워크플로우가 필요하며, 이로 인해 배치 시간이 증가합니다. 동시에 기존의 보안 모델은 분산형 아키텍처에 적응하는 데 어려움을 겪고 있어 적군이 악용할 수 있는 치명적인 공백을 야기합니다.

통합된 접근 방식 활용

국방 조직에는 어디서나 자율성과 보안을 강화하는 통합된 개방형 프레임워크가 시급합니다. 목표는 프라이빗 클라우드에서 중요 애플리케이션을 실행하고 엣지에서 AI 워크로드를 처리하며 전장 현장의 엣지 기기에서 실시간 의사 결정을 지원하는 일관된 플랫폼을 구축하는 것입니다. 진정한 현대적인 회복 탄력성은 핵심 지대에서 최전방까지 일관된 무결성을 유지하며 기능할 수 있는 능력입니다.

Red Hat의 지원 방법

디지털 전장의 파편화에 맞서 국방 조직이 전략적 핵심 지대에서 전술적 엣지까지 회복 탄력성을 보장하려면 통합된 기반과 신뢰할 수 있는 조연자가 필요합니다. Red Hat은 이러한 필수적이고 일관된 플랫폼을 제공합니다. '1회 배포로 어디서나 실행'하는 방식을 통해 Red Hat은 작전 투입 준비를 가속화하고 인력이 어느 환경에서나 익숙한 툴을 사용할 수 있도록 지원합니다. Red Hat 솔루션은 일관된 경험을 제공할 뿐만 아니라 오픈 표준을 토대로 설계되었습니다. 또한 플랫폼은 벤더 종속성을 방지하여 확장 가능하고 유연한 솔루션과의 원활한 통합을 촉진합니다.

군사 등급 보안: Red Hat은 Red Hat® OpenShift®와 같은 핵심 플랫폼이 엄격한 컴플라이언스 표준을 준수하도록 보장함으로써 군사 등급 보안을 구현합니다. Red Hat Trusted Software Supply Chain을 통해 보안이 상시 적용되며, 총체적이고 지속적인 보안 접근 방식이 실현됩니다. 이러한 접근 방식에서는 DevSecOps 사례를 통합해 관리 연속성을 강화하고 보안, 컴플라이언스, 개인정보 보호 및 투명성을 위한 국방 기관 표준에 소프트웨어가 부합하는지 확인할 수 있습니다.

보장 주권(assurance sovereignty): 암호화 증명, 펌웨어와 중요 업데이트가 변경되지 않았음을 검증하여 보장 주권이라는 더욱 광범위한 목표를 지원합니다. 이 프로세스는 디지털 시스템의 무결성과 신뢰성을 검증하며, 소프트웨어 공급망을 검증하고 악성 코드 삽입의 위험을 완화하기 위한 Red Hat 플랫폼 전략의 핵심 부분입니다.

인터넷 연결이 필요 없는 자동화: 인터넷 연결이 필요 없는 자동화를 통해 인터넷 연결 없이도 현장 기기의 패치를 수행하고, 고객이 운용 중인 특정 프로세스와 통합할 수 있습니다. Red Hat은 Red Hat Ansible® Automation Platform을 사용하여 현대적인 국방에 필요한 신뢰할 수 있는 자율적 운영을 제공하도록 지원합니다. 이 플랫폼은 취약한 외부 연결에 의존할 필요 없이 통신이 거부되거나, 교란되거나, 간헐적이거나, 제한적인(Denied, Disrupted, Intermittent, and Limited, DDIL) 환경에서 기기를 관리하는 데 도움이 됩니다. 이러한 자율성은 배포된 소프트웨어 자산에 대한 막대한 장기 투자를 보호하고, 악성 코드 삽입과 관련된 보안 리스크를 최소화하고, 외부 지원이 불가능한 상황에서 핵심 임무 작전의 지속적 수행을 보장합니다.

전략적 핵심부에서는 Red Hat OpenShift와 같은 신뢰할 수 있는 솔루션이 확장 가능한 주권적 인프라를 제공합니다. 그리고 현장에 배치된 엣지에서는 소형 OpenShift 클러스터가 중요 인텔리전스와 AI 워크로드를 처리합니다. 전술적 최전방의 경우 경량화 Red Hat Device Edge가 강화된 시스템에서 이식성이 뛰어난 네트워크 단절 모드 운영 역량을 제공합니다.

입증된 방위 산업 활용 사례

여러 국방 조직들이 중요한 작전상 과제를 해결하고 괄목할 만한 발전을 이루기 위해 Red Hat 솔루션을 성공적으로 구현했습니다.

유럽 공군을 위한 현장 운영 최적화: 한 유럽 공군이 현장 작전 중 네트워크 중단으로 인해 작전 수행에 반복적으로 차질을 겪었습니다. 해당 공군의 IT 부서는 휴대용 엣지 데이터센터에 Red Hat OpenShift를 구현함으로써 네트워크 연결에 관계없이 지속적인 운영을 유지하는 로컬 AI 처리 기능을 도입하는 동시에 대역폭 요구 사항을 크게 줄였습니다.

무인 항공 체계를 위한 비행 중 소프트웨어 업데이트: 선도적 역량을 증명하는 또 다른 활용 사례로, 한 대형 방위 산업체에서는 무인 항공 체계에서 비행 중 소프트웨어 업데이트를 수행하는 역량을 발휘했습니다. 이 방위 산업체는 Red Hat Device Edge를 사용하여 작전 수행 중 드론에 AI 모델 업그레이드를 성공적으로 배포해 작전 중단이나 시스템 다운타임 없이 실시간 목표물 인식 역량을 강화했습니다.

국방 조직을 위한 인프라 배포 가속화: 한 국방 조직이 Ansible Automation Platform과 Red Hat OpenShift를 통해 Platform-as-a-Service(PaaS) 프로세스를 자동화하여 괄목할 만한 효율성 증대를 실현했습니다. 이 조직의 인프라 배포 시간은 수 주에서 24시간으로 크게 단축되었으며, 이를 통해 즉각적인 전투 작전 수행 능력을 갖추게 되었습니다. 동시에 개발자 역량이 단 1년 만에 4배 가량 확대되었고, 그 과정에서도 엄격한 보안 프로토콜을 유지할 수 있었습니다.

시작하기

[Red Hatter](#)에게 문의하여 핵심 지역에서 옛지까지 국방 작전을 보호하는 방법에 대해 알아보세요.

한국레드햇 홈페이지 <https://www.redhat.com/ko>



Red Hat 소개

Red Hat은 전 세계 고객에게 높은 수준의 지원과 교육 및 컨설팅 서비스를 제공하여 [권위 있는 어워드를 수상](#)한 바 있으며 이를 통해 고객 환경 전반의 표준화, 클라우드 네이티브 애플리케이션 개발, 복잡한 환경의 통합, 자동화, 보안 및 관리를 지원합니다.

f www.facebook.com/redhatkorea
구매했던 02-6105-4390
buy-kr@redhat.com