Build defense resilience and strategic autonomy

The imperative for strategic autonomy

True mission survival for defense organizations requires resilience that goes beyond digital sovereignty, ensuring continuous operations in an evolving and more complex threat landscape.

Defense organizations need resilience beyond sovereignty

In a complex global technology landscape, digital sovereignty is a critical concern for nations and enterprises. However, for defense organizations, sovereignty alone is not enough. True mission survival demands resilience that goes beyond jurisdictional control, establishing operational continuity even in the face of crisis. This necessity means achieving strategic autonomy—the capacity to function independently when external support is unavailable or compromised.

Dynamic threats and complex defense challenges

The defense industry faces an array of complicated and rapidly developing challenges that highlight the urgent need for comprehensive digital transformation and resilience strategies. Primarily, there must be a clear, well-communicated vision with executive support to encourage adoption of these digital transformation efforts. Organizations cannot embark on a transformation without clearly defined success metrics, a strategic roadmap, or identifying key challenges:

- **Geopolitical climate:** In peacetime, reliance on hyperscale cloud providers and distributed IT infrastructure is manageable. But in conflict, the requirements shift substantially. Physical destruction can render datacenters inoperable, while internet outages cripple cloud-dependent operations. The ability to maintain operational resilience when facing conflict or severe geopolitical disruption requires the capacity to act independently when cooperation is impossible.
- **Cybersecurity and data security:** Digital transformation, while essential, opens the door to cyberattacks, spying, and sabotage. Defense organizations handle highly sensitive data about military strategies, personnel, and classified communications. Failed digital transformations can expose this data to hackers, who exploit vulnerabilities in new or partially modernized systems. The risk of cyber intrusion or data leaks often slows the adoption of new platforms. Cyberattacks can occur at unprecedented speed, demanding machine-speed responses rather than human speed.
- **Traditional system integration:** Many defense programs are still supported by decades-old computer-aided design (CAD) tools, enterprise resource planning (ERP) systems, and paper-based processes. Creating interoperability between these outdated systems and modern digital platforms is technically challenging and organizationally disruptive, yet it is essential for building a true end-to-end digital thread. Managing this complexity with existing processes leads to delays, cost overruns, and operational vulnerabilities.
- **Supply chain complexity and security:** Contractors depend on thousands of suppliers, many of whom are small businesses with limited resources to adopt advanced digital platforms. Establishing a security-focused and collaborative supply chain ecosystem is difficult when collaborating organizations have vastly different levels of digital maturity. The growing threat of supply chain attacks, where malicious code can be inserted into software updates in transit, poses a significant risk to critical missions.

- **Talent gaps and cultural resistance:** The defense industry is facing a shortage of engineers and technicians with the expertise in model-based systems engineering, AI, machine learning (ML), and digital twin technologies. Attracting and retaining digital-native talent is increasingly difficult because of competition from commercial tech companies. Furthermore, defense programs are inherently reluctant to take risks, and engineers and technicians often rely on traditional workflows. Shifting from burdensome and document-focused processes to model-based approaches demands new tools and a change in how engineering, manufacturing, and service-focused teams work.
- **Operational complexity:** Defense operations span a vast spectrum, from strategic core datacenters to deployed edge locations. Different environments often use incompatible technology stacks, forcing organizations to rebuild solutions for each deployment. This situation creates isolated technology structures and hinders uninterrupted operations.
- **Standalone operations and poor communication:** Effective digital transformation requires consistent collaboration between IT, operations, and leadership. In large, hierarchical organizations like defense organizations, standalone operations, and poor communication often hinder cross-functional collaboration.

3 strategic autonomy pillars to overcome defense challenges

3 pillars of resilience

To overcome complex challenges in the threat landscape, defense must focus on 3 crucial pillars of strategic autonomy: people, processes, and technology.

Strategic autonomy is not only about where the hardware is located but also about maintaining strict control over critical processes and intellectual property. Releasing proprietary solutions as fully open source is not often an option, as it could expose sensitive methodologies and vulnerabilities. To overcome these challenges and achieve true mission survival, defense organizations must focus on these 3 crucial pillars:

- **People:** Defense IT teams must be trained to manage disruptions, adapt to systems, codevelop, innovate, and maintain operations without external assistance. Cultivating DevSecOps and cloud-native expertise is necessary to deploy and manage distributed systems effectively. Internal collaboration models, such as InnerSource, can foster agility by applying open source principles within closed environments. Open leadership is equally necessary, breaking down isolated structures and accelerating decision-making in high-pressure scenarios. Investing in personnel training and skills development is a key strategy as advanced technologies are integrated.
- **Processes:** Clear, tested procedures are essential for responding to crises. Defense organizations need disaster recovery plans that account for times of conflict and deliver continuity even if central systems fail. Decentralized workflows allow operations to persist in fragmented environments, while open methodologies allow continuous adaptation as threats evolve. Adopting agile methodologies in project management is crucial, fostering flexibility and responsiveness.
- **Technology:** A truly autonomous IT ecosystem must be versatile enough to run anywhere, whether in central datacenters, the cloud, or disconnected edge locations. It should support multiple hardware architectures, from x86 to Arm and RISC-V, avoiding vendor dependency. Most importantly, it must handle any workload, from traditional systems to modern AI-enabled applications, allowing uninterrupted operation across all mission-critical functions.

Empowering people through training and enablement

Red Hat addresses the strategic autonomy pillar, people, by providing comprehensive training and enablement programs. For example, InnerSource is a global software development strategy that applies open source best practices within a single organization, helping defense sector entities to accelerate development and increase code reuse. It allows different departments within a defense organization, such as a field operations unit and a datacenter team, to collaborate as if they were in an open source community, but within the organization's boundaries.

A department can develop a software solution and share its source code internally. Other departments can then use, improve, and contribute features back to this internal project. This fosters collaboration, reduces redundant development, and accelerates innovation. Crucially, it builds internal expertise and ensures that personnel, from soldiers to commanders, are trained on and intimately familiar with the systems and processes, creating a self-sufficient force capable of operating critical infrastructure even if external support is severed. Red Hat empowers organizations' internal teams to acquire the necessary skills to operate, maintain, and collaboratively develop the infrastructure, including training on Red Hat technologies and best practices for open source development.

Red Hat's guidance on InnerSource practices helps cultivate a culture of continuous learning and improvement within defense organizations. By allowing different departments to collaborate as if they were in an open source community, but within security-focused organizational boundaries, InnerSource fosters innovation and reduces redundant development.

By investing in the skills of defense personnel, Red Hat helps ensure that the military builds and retains the sovereign capability to be resilient in both peace and wartime. This internal expertise is invaluable for adapting to new challenges and maintaining operational integrity independently.

Red Hat: The foundation for digital autonomy

Red Hat addresses these pillars by providing foundational open source technology, comprehensive training, and guidance on DevSecOps-focused processes to help improve operational versatility and autonomy.

Allowing effective processes for agility and security

Red Hat offers critical guidance on the procedural shifts required to effectively adopt and implement development methods focused on security. We help establish strong governance frameworks, defining clear contribution models and fostering effective collaboration. Teams can share code, accelerate innovation, and align development with open source best practices, while maintaining security posture and control.

Red Hat helps defense organizations implement DevSecOps practices, integrating security throughout the entire software development lifecycle. This proactive approach is vital for protecting defense systems from evolving threats and cybersecurity challenges. By automating security checks and integrating them into development workflows, DevSecOps helps mitigate vulnerabilities early in the process.

The integration of AI into DevSecOps is transforming software development by introducing intelligent automation and proactive defense throughout the entire software lifecycle. Integration is crucial to building resilience, enabling them to function effectively despite disruption or advanced cyber threats. AI shifts DevSecOps from reactive security to a more proactive and adaptive defense, anticipating and mitigating threats before deployment or during operation.

Red Hat® Ansible® Automation Platform supports sovereign strategies through an automated approach to device, network, and application lifecycle management. Automation plays a key role

in managing complex environments, ensuring software updates, patching, configuration, and deployment are minimized at the tactical edge. Automation is critical for responding to cyber threats at machine speed and making sure to provide operational continuity during crises.

Red Hat OpenShift®, when paired with Ansible Automation Platform, dramatically reduces the burden by automating the entire application lifecycle.

Providing advanced technology solutions for digital autonomy

Red Hat provides the foundational open source technology platforms that help defense organizations to modernize their IT infrastructure, address legacy system integration, and achieve operational versatility across all environments. The open hybrid cloud portfolio gives organizations the solutions needed to achieve resilience, autonomy, and independence. Defense organizations can deploy and manage applications consistently across various environments, from on-premise to the edge.

Modernize infrastructure on a unified platform with Red Hat Enterprise Linux® and Red Hat OpenShift. Red Hat Enterprise Linux provides a consistent, flexible, and security-focused platform for enterprise workloads, laying the foundation for building sovereign cloud environments. Red Hat OpenShift helps apply sovereign controls over data and infrastructure with consistent operations to deploy and support workloads anywhere. This simplifies development, deployment, and management of containerized applications, ensuring reliability even in Denied, Disrupted, Intermittent, and Limited (DDIL) environments.

For example, a European air force used Red Hat OpenShift on portable edge datacenters to overcome mission disruptions caused by network outages. This deployed edge benefits by using compact OpenShift clusters, allowing local AI processing capabilities that maintain continuous operations regardless of connectivity status, while significantly reducing bandwidth requirements.

Lightweight Red Hat Device Edge supports ultra-portable operations for devices like drones and autonomous vehicles, allowing real-time data collection, analysis, and action even when disconnected. It has been used to deploy AI model upgrades to drones during active missions, enhancing target recognition without interruption.

Red Hat's solutions include advanced security measures like cryptographic attestation for firmware and update verifications, and disconnected automation for security-focused patching of field devices. Red Hat OpenShift is hardened for security to meet Security Technical Implementation Guides (STIGs), Federal Information Processing Standards (FIPS), and zero trust requirements, offering microsegmentation, security-focused zones, and policy-based access control even in disconnected environments.

Red Hat AI delivers sovereign AI capabilities, helping defense organizations build and run AI solutions by providing the tools to train custom models or adapt existing ones, ensuring they work exactly how their operations require, from initial experiments to full production. This capability allows the defense industry to use the power of AI while maintaining strict control over its data and models.

Open source is the foundation of strategic autonomy

Open source is uniquely suited to strategic autonomy. It provides transparency, allowing defense organizations to audit and modify code as needed. This transparency ensures independence as systems can be maintained and extended even if the original vendor is unavailable due to mature and well-established permissive and copyleft licensing models.

The flexibility of open source also means the same platform can run on everything from large-scale datacenters to mobile field deployments, making it ideal for defense environments where adaptability is paramount. For defense organizations, this flexibility translates to true self-reliance, the ability to sustain operations regardless of geopolitical disruptions.

Defense organizations can incorporate third-party solutions without vendor dependence, maintaining flexibility for future needs. This is crucial for supporting multiple hardware architectures and avoiding reliance on a single provider.

Defense organizations adopting open source principles seek a balance between collaboration and control. While they recognize the immense value in open source technology, practices, and the communities that foster them, they cannot operate with completely open technology. Therefore, the goal in defense is to use the innovation and agility of open source within a controlled environment, ensuring they are not dependent on external entities that could be compromised during a conflict.

The comprehensive role of Red Hat in enhancing defense resilience

Red Hat is working with numerous defense organizations globally to increase open source solution adoption for digital autonomy, playing a multifaceted role across people, process, and technology. Our open hybrid cloud approach and adherence to open source principles provide a foundation of trust, choice, and protection.

Red Hat is a trusted partner, helping defense organizations to build strong, adaptable, and self-reliant digital foundations essential for national advanced security. The unified platform approach, using an open framework based on open standards, strengthens autonomy, security, and uninterrupted operations across all environments. Complete digital sovereignty, unified operations, and proactive security measures is an approach that gives defense organizations the confidence to deploy, update, and operate anywhere, supporting mission success under increasingly complex threats.

Several defense organizations have established dedicated development services that provide standardised platforms for building and deploying applications at varying security levels. Others are replacing existing virtualization platforms with open source container solutions to improve performance and reduce dependencies. These efforts highlight a broader shift toward modular, interoperable architectures that support rapid innovation while preserving operational sovereignty.

Beyond providing the trusted open source technology platforms, Red Hat offers critical guidance on the cultural and procedural shifts required, including governance frameworks, contribution models, and collaboration methods that allow teams to share code, accelerate innovation, and align internal development with best open source practices.

redhat.com
#3091145_1225