Enhance cyber resilience in the DoD

Build enduring advantage with automated response and interoperability

"Cyber resilience: The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."

National Institute of Standards and Technology (NIST)

"The Department [of Defense] will enhance the cyber resilience of the Joint Force and ensure its ability to fight in and through contested and congested cyberspace. We will prioritize those cyber capabilities that support the Joint Force's military mission assurance and commit to training the force to operate amid network and warfighting platform degradation."

2023 Cyber Strategy of the Department of Defense[1]

The great power competition requires cyber resilience

Cyber resilience is the bedrock of continuous operational readiness throughout the Department of Defense (DoD). To fight in and through contested and congested cyberspace, forces need the following capabilities:

- **Maneuverability.** Cyber operators must be able to rapidly restore destroyed or degraded applications in the same or another location—public cloud, garrison or base datacenter, or tactical edge (e.g., aircraft, ships, vehicles, and portable fly-away kits).
- **Interoperability, for unity of effort and multicapable forces.** Each service component uses servers and network devices from multiple vendors. In multi-domain operations (MDO), cyber operators need the ability to manage any vendor's device without knowing vendor-specific commands for software updates, configuration changes, capacity additions, and other actions needed for resilience.
- **Rapid application deployment and scaling.** DoD science teams and developers continually retrain and tune artificial intelligence and machine learning (AI/ML) models and applications used for offensive and defensive cyber operations and decision dominance. Resilience in the face of new threats requires the ability to rapidly scale capacity for model training and to deploy new models in the location closest to warfighters, without specific training on the hardware in that location.
- **Visibility across the cyber terrain.** Operators need robust visibility into the cyber terrain so that they can identify the source of new threats to deploy effective countermeasures.

Red Hat technologies accelerate cyber resilience

The DoD can accelerate cyber resilience using Red Hat® technologies for automation and interoperability. Red Hat Ansible® Automation Platform automates recovery of destroyed or degraded capabilities at mission speed. Cyber operators do not need to learn vendor-specific commands to configure, deploy, and scale services because Ansible Automation Platform translates an intent expressed in natural language (e.g., "add a new route") into the appropriate commands for each device.

A hybrid cloud application platform powered by Kubernetes, Red Hat OpenShift® accelerates resilience by allowing containerized applications and virtual machines (VMs) to be moved to different vendors' server hardware in any location, with little or no modification. If a base datacenter is destroyed, for example, its applications can be restored to a public cloud, and vice versa. Workloads can also run on small, resource-constrained devices at the tactical edge (e.g., aircraft, vehicles, ships, and portable fly-away kits) running Red Hat Device Edge. Edge devices running Red Hat Device Edge can operate in denied, disrupted, intermittent, and limited (DDIL) network conditions, continuing to collect and analyze data even when a connection is not available.

1 *"2023 Cyber Strategy of the Department of Defense." media.defense.gov, accessed 13 Jan. 2025.*

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

redhat.com

"Secure and resilient C3 [command, control, and communications] capabilities are essential for assured and trusted battlefield information exchange."

Department of Defense[2]

Cyber resilience scenarios

Automated maneuverability

Mission challenge. When a primary site is under attack, traditional failover to a secondary or tertiary site can take an hour or more, threatening mission survivability.

How Red Hat can help. Detecting an event that puts the mission at risk, Ansible Automation Platform automatically executes a playbook of predefined actions to confront the risk in near real-time. If the primary site is inoperable, Ansible Automation Platform and Red Hat OpenShift work together to automatically transition mission-critical workloads to a secondary site or recovery point, which might be a base, public cloud, or edge server. No human intervention is needed. Instead, a feature called Event-Driven Ansible monitors for conditions such as failure of the communications line or servers, and then executes automated actions to reconstitute services from the alternate location (Table 1). Red Hat OpenShift ensures that applications operate consistently regardless of where they are running. Mature, automated workflows support goals for continuity of operations (COOP).

Table 1. Examples of adverse events that Ansible Automation Platform can recognize and remediate

Threat	Sample playbook actions to confront the threat
Failed communications line	Transition workloads to an alternate site
Malware discovery	Take the infected system offline and stand up a new one in real time Scale application services up or down Close a firewall port
Cluster node stops responding	Reconstitute workloads on another node
Configuration drift on a VM or container, causing a security vulnerability	Identify and execute self-healing actions

Unity of effort across the cyber terrain

Mission challenge. Each service component uses servers and networking devices from many original equipment manufacturers (OEMs), each with its own management tools, operating systems, and commands. Even within a single department, cyber operators need to be trained on different toolsets to manage deployments.

How Red Hat can help. With Red Hat OpenShift, applications can be built once and then deployed anywhere from the hybrid cloud to the edge. This means that ML models and AI-based applications developed by a single department or component can be deployed on any other department's or component's servers, promoting unity of effort and a multicapable IT workforce. Automation also

2 *"DoD Releases the Fulcrum: DoD Information Technology (IT) Advancement Strategy."* defense.gov, 25 June 2024.

contributes to unity of effort because IT specialists in each department can work toward a common operational capability without having to learn specific technology commands for each of many IT systems. Ansible Automation Platform can automate any action that can be initiated from a command-line interface (CLI) or application programming interface (API).

Rapid building and deployment of warfighting capabilities, at scale

Mission challenge. DoD software teams continually add software capabilities, harden security, and tune ML models in response to stresses and attacks. Today, software update cycles are delayed because each domain uses multiple hardware platforms, some operating in DDIL environments. To accelerate cyber resilience, service components need the ability to deploy new and updated applications to disparate endpoints more rapidly, at scale, and with confidence that the applications will behave consistently on every platform.

How Red Hat can help. With Red Hat OpenShift, joint operations teams can build applications once and then deploy them to any environment, from the datacenter or cloud to the mission edge. VMs can run alongside containers on the same node, which simplifies operations and maximizes resource use. When confronted by threats or adverse conditions, forces can autoscale capacity at the time of need.

Joint operations teams can deploy standardized AI capabilities in geographically constrained areas by using Red Hat OpenShift, Ansible Automation Platform, and Red Hat Device Edge in combination. For example, picture a forward operating base (FOB) that needs to update an ML model that captures and characterizes drone imagery. With Red Hat Device Edge, U.S. military platforms like the Stalker unmanned aerial system (UAS) can be equipped with advanced software that lets small platforms handle large AI workloads, driving faster, data-based decision making in the field. In this scenario, Ansible Automation Platform allows operators to run a playbook to simultaneously deploy updated models to large numbers of drones or other edge devices. The effect is to accelerate mission outcomes by reducing errors, improving operational consistency, and adjusting to real-world threat information and mission needs with increased speed.

> "...the Department will increase unity of effort between defensive cyberspace and DODIN [Department of Defense Information Network] operations by integrating the visibility, capabilities, and operations of relevant mission elements. We will align intelligence, acquisition and sustainment, and other functions to ensure that the DODIN can rapidly adapt to counter evolving cyber threats."
>
> 2023 Cyber Strategy of the Department of Defense[3]

Visibility and observability across the cyber terrain

Mission challenge. The DoD is working to streamline compliance processes, reduce risk, and automate critical tasks such as Security Technology Implementation Guide (STIG) deployment, patch management, configuration management, and incident responses. Barriers to success include the cyber exposure caused by massive surface attacks, ongoing changes to the security environment and the DoD's force posture, and rapidly changing technology.

How Red Hat can help. Ansible Automation Platform provides a comprehensive inventory of the IT estate, allowing visibility across the cyber terrain (hybrid cloud, on-premise, and at the edge). An accurate, up-to-date inventory helps DoD IT teams accelerate resilience by scaling more quickly, reducing compliance risks, and swiftly identifying threats to availability so that they can be remediated.

To observe real-time events across the cyber terrain, use Event-Driven Ansible, included with Ansible Automation Platform. Event-Driven Ansible constantly looks for specified events, automatically invoking predefined actions when an event is detected.

3 *"2023 Cyber Strategy of the Department of Defense." media.defense.gov, accessed 4 Feb. 2025.*

Summary: Resilience demands automation and interoperability

To dominate in the great power competition, DoD forces need superior capabilities for anticipating, withstanding, and recovering from adverse conditions. Learn more about Red Hat's work with the DoD.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#1666167_0225

Copyright © 2025 Red Hat, Inc. Red Hat, the Red Hat logo, Ansible, and OpenShift are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.