Solution brief

DELIVER UNINTERRUPTED OPERATIONS

Enabling mobility and resilience for U.S. federal agencies

U.S. federal agencies manage a broad array of tasks that touch virtually every aspect of Americans' lives. IT, civilian, defence, and intelligence agencies are all currently facing the requirement to modernize their systems. This drive is aimed at providing a better user experience and fulfilling agency objectives. New services must be deployed quickly with a secure, pragmatic, cloud-first approach to leverage the scalability, flexibility, and cost-effectiveness of cloud infrastructures, all while complying with strict standards for managing vital operations and handling highly sensitive and protected data.

Though this is a large undertaking, HPE Zerto Software can significantly ease much of the burden by delivering the protection and mobility that federal agencies need to manage their environments and enable mission-critical results. HPE Zerto is purpose-built to protect and move applications and data for agencies' ultra-sensitive and demanding IT environments. **By combining continuous data protection and enterprise-grade security, HPE Zerto helps federal agencies to recover quickly and safely from disruptions—enabling mission continuity when failure is not an option.**

Continuity of operations

The rise of cyber threats, including a growing number of state-sponsored attacks, make U.S. federal agencies particularly vulnerable targets. However, HPE Zerto enables federal agencies to sustain uninterrupted operations to provide critical services and uphold national security objectives.

By offering a range of advanced capabilities that strengthen resilience and accelerate recovery, HPE Zerto promotes data protection across complex federal environments:

— **Continuous data protection (CDP)** captures every change in real time, enabling near-zero data loss and instant recovery—even from sophisticated, fast-moving cyberattacks.

  Granular journaling allows agencies to rewind to a precise point in time mere seconds before a disruption, enabling forensic analysis and clean recovery from cyber threats. The result is aggressive recovery time objectives (RTOs) measured in minutes and recovery point objectives (RPOs) measured in seconds.

— **Application-centric protection** ensures that mission-critical services—like citizen-facing portals or intelligence systems—are recovered as cohesive units, not just individual virtual machines (VMs), minimizing chaos and downtime.

  Policy-based protection tiers allow agencies to prioritize recovery for essential services like emergency response systems or secure communications, aligning with Continuity of Operations (COOP) and Continuity of Government (COG) frameworks.

— **Real-time encryption detection** alerts agencies instantly to suspicious anomalies, enabling proactive containment before threats spread. With the earliest warning, organizations can respond immediately.

— **Rapid recovery across hybrid environments** enables seamless data mobility across on-prem and cloud environments, enhancing operational continuity regardless of architecture or location. When deployed in AWS GovCloud regions, HPE Zerto leverages AWS infrastructure to help agencies meet FedRAMP, ITAR, and other federal compliance standards.

— **Non-disruptive testing and multi-site analytics and reporting** enables agencies to regularly validate continuity plans without impacting live operations, while providing central visibility into resilience postures across geographically distributed data centers. This provides readiness for real-world scenarios like natural disasters, coordinated cyberattacks, and data migrations, while supporting compliance with federal continuity mandates.

— **The HPE Cyber Resilience Vault** provides an additional security layer and is a last line of defense that combines an isolated recovery environment with an immutable data vault to deliver the ultimate air-gapped solution through zero-trust architecture.

  The vault leverages the unique strengths of continuous data protection offered by HPE Zerto, combined with industry-leading hardware from HPE, to enable rapid air-gapped recovery unlike anything else on the market. No matter how devastating a cyberattack may be, you can always return to the vault to recover.

Take ownership of your data and applications

As they adapt to ever-evolving IT strategies, most agencies find it challenging to migrate IT infrastructure. Factors like platform lock-in, the speed of technological change, and constantly emerging cloud technologies make migrations complex.

HPE Zerto eliminates these challenges by offering a simple, scalable, and risk-free migration experience. CDP with HPE Zerto has built-in orchestration and automation, it can migrate between any infrastructure, including cross-hypervisor, cross-cloud, and even between on-premises and the cloud. Additionally, you can test your recovery or mobility at any time with fewer resources and without production impact, giving you time to focus on your mission objectives.

Aiding with compliance

HPE Zerto helps federal agencies comply with and adhere to the 325+ controls within the NIST framework. Our easy-to-use automated disaster recovery (DR) testing and reporting can help you meet compliance and pass audits. Additionally, a significant number of other requirements, including contingency planning, incident response, and recovery objectives, can be fulfilled with HPE Zerto. We assist in compliance with some of the most widely recognized standards and regulations, including:

FISMA (Low-High) | FIPS 140-2/3 | CISA Attestation | DFARS 800-171 | NIST 800-53 | CIS Level 1 | ISO 27001 & 9001 Certified | HIPAA | PCI | GDPR

Multiple federal agencies, including the Federal Aviation Administration (FAA), the U.S. Army, NASA, and the Federal Deposit Insurance Corporation (FDIC) rely on HPE Zerto to modernize their operations. Whether you need the ability to support granular recovery to ensure uninterrupted operations, move between, to, or from clouds with ease, or test without disruption, HPE Zerto helps agencies achieve efficiency, control costs, and improve agility to achieve their mission objectives.

FIPS compliance

Federal Information Processing Standard (FIPS) is a U.S. government standard for cryptography required on federal systems. With FIPS-validated encryption as of version 10 update 7, HPE Zerto satisfies federal standards for encrypted data, helping to reduce risk across critical IT environments for federal agencies, contractors, and other security-conscious organizations.

CISA attestation

With the Cybersecurity and Infrastructure Security Agency (CISA) attestation, HPE Zerto formally declares alignment with the National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF) as of version 10 update 8. It is now required for software suppliers to federal agencies, and affirms that HPE Zerto is developed in accordance with rigorous security practices designed to reduce cyber risk across U.S. government systems and their supply chains. The SSDF framework outlines best practices that include secure coding, vulnerability management, implementation of security controls, and maintaining a Software Bill of Materials (SBOM).

Enterprise security built for federal agencies

In addition to incorporating FIPS-validated encryption and completing CISA attestation, HPE Zerto delivers enterprise-grade secure access controls—including SSO, MFA, RBAC, and a built-in identity provider via Keycloak—helping agencies strengthen resilience and demonstrate compliance with confidence.

These capabilities are further reinforced by a suite of advanced security practices that protect critical workloads, support regulatory compliance, and enhance overall cyber resilience:

— **Audit and logging:** With comprehensive visibility into system activity and user behavior, HPE Zerto enables robust traceability, monitoring, and compliance auditing.

  All REST API are tracked and RBAC-enforced for permitted roles only, enabling strict control of administrative access.

  As of version 10 update 8, HPE Zerto also supports Syslog forwarding, enabling integration with leading Security Information and Event Management (SIEM) platforms for centralized security oversight.

— **Network security:** HPE Zerto architecture is designed with network security in mind, supporting secure multi-site and hybrid deployments through network segmentation, secure communication, and firewall compatibility support.

  By following a minimal exposure principle, only required and documented ports are used by HPE Zerto components, keeping all communication paths clearly defined. Administrators can further enhance security by restricting inbound and outbound traffic to trusted IP ranges or internal network segments.

— **Secure Development and Operations (SDLC):** HPE Zerto adheres to a secure code development lifecycle that incorporates rigorous peer review, automated static code scanning, and vulnerability management across all components. To further minimize exposure and strengthen resilience, HPE Zerto uses secure default configurations and hardening appliances. Additionally, security patches are applied promptly, and customers running older product versions are strongly encouraged to upgrade to remain protected against any newly-discovered vulnerabilities.

— **Scanning and vulnerability management process:** Security is a core pillar of HPE Zerto's development and release practices, with automated scanning integrated throughout the software stack. This includes source code scanning in Git repositories, operating system level inventory scanning, and checks on deployed containers to identify and address potential vulnerabilities.

— **Advanced detection with CrowdStrike Falcon:** The CrowdStrike-Zerto strategic partnership strengthens cyber resilience by combining real-time threat detection with rapid cyber recovery.

  CrowdStrike Falcon monitors critical workloads for malicious activity— including ransomware and advanced threats—and when a threat is discovered, HPE Zerto can automatically restore applications and VMs to a clean recovery point just seconds before the attack, minimizing business impact.

HPE Zerto feature	How does HPE Zerto help federal IT?
Mitigate disruptions.	Protect your agency from outages and disruptions by dramatically limiting data loss and downtime.
Detect and neutralize cyberthreats.	Detect in seconds and recover in minutes, at scale, to a state seconds before an attack.
Modernize infrastructure.	Remove complexity to support disparate infrastructures and enable true modernization.
Unlock hybrid and multi-cloud.	Drive digital transformation with cross-platform protection for IaaS, PaaS, and SaaS.
Simplify migrations.	Reduce resources and speed up data center consolidations with hassle-free migrations across on-premises and the cloud.
Improve operational efficiency.	Streamline IT operations with automation, orchestration, and consumer-level simplicity.
Demonstrate compliance.	Continuously align with industry-leading compliance guidelines to maintain customer trust and meet regulatory obligations.

Learn more about how HPE Zerto delivers unparalleled data protection for the federal government

Visit HPE.com

Chat now

a50012149ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com