DATA SHEET

Technical solutions overview for the CANES program

What if PMW 160 could accelerate deployment of the CANES program and empower sailors in Active Directory administrator roles to build and maintain a secure, efficient and resilient network, as well as implement identity management strategy? What if you could not only support enhanced naval operations today, but meet evolving mission requirements long into the future?

These objectives are within reach. Here's how:

Integration and consolidation – You can deliver to the fleet unified identity management capabilities that align with CANES' objectives.

- Hardened cybersecurity with robust privileged access management (PAM) protections, real-time monitoring and comprehensive auditing.
- Implementing increased agility in system upgrades through Cyber Threat Upgrade (CTU) tech refresh strategy
- Rapidly addressing cyber vulnerabilities, maintaining operational availability and pacing warfighting threats

Enhanced sailor self-sufficiency – You can automate Active Directory (AD) administrative tasks to reduce redundancy and lower operational costs, allowing IT personnel to focus on strategic initiatives.

- Improving sailors' ability to fight and defend their network
- Expand access to CANES Training Virtual Environment (TVE)
- Increase operational readiness through automation and network insight

Tactical network remote monitoring – Scalability and flexibility ensures quick adaptation to evolving mission requirements.

Cost-efficient zero trust architectures and tactical network remote monitoring.

Quest Software solutions – ideally suited for CANES deployment

Quest Change Auditor – Comprehensive change auditing and compliance

- Real-time monitoring: provides real-time auditing, alerting, and reporting on changes made to AD, ensuring rapid detection and response to unauthorized changes.
- Enhanced security: ensures compliance with security policies by tracking and reporting all critical changes, thereby reducing the risk of malicious activities.
- Centralized console: offers a single, centralized console for event logging and change reporting, simplifying compliance and security management.

*The Total Economic Impact™ Of Quest Recovery Manager for Active Directory Disaster Recovery Edition – Forrester, February 2023

Quest GPOAdmin – Streamline and Secure Group Policy Management

- Change tracking: monitors and tracks every change made to Group Policy Objects (GPOs), providing real-time visibility and control.
- Version control: offers a robust check-in/check-out system for GPOs, preventing unauthorized changes and ensuring compliance with security policies.
- Automated workflows: facilitates automated workflows for common GPO tasks, reducing the burden on IT staff and enhancing operational efficiency.

Quest Recovery Manager for Active Directory – Ensure business continuity and data protection

- Rapid recovery: enables swift restoration of Active Directory (AD) environments in case of cyberattacks or disasters, minimizing downtime and ensuring operational continuity.
- Bare Metal recovery: automates the restoration of domain controllers to bare metal, VMs or clean OS, ensuring systems are free from potential threats.
- Disaster resilience: with downtime costs estimated at $730,000 per hour*, Recovery Manager significantly reduces financial risks by enabling phased recovery and clean OS recovery methods.

One Identity Active Roles – Efficient and Secure Account Management

- Automation: automates provisioning, de-provisioning, and access right management, reducing manual efforts and minimizing errors.
- Least-privilege model: enforces a least-privilege access model, ensuring users have only the necessary permissions, enhancing security.

One Identity Safeguard – Advanced Privileged Access Management

- Privileged credential management: automates, controls, and secures the process of granting privileged credentials, a critical aspect of cybersecurity.
- Session monitoring: monitors and records privileged sessions, detecting suspicious activities and enforcing security policies in real time.

Integrating Quest Software's and One Identity's advanced identity management and cybersecurity solutions into the CANES program will significantly bolster the U.S. Navy's ability to manage, secure and optimize its shipboard IT environments. These tools enhance cybersecurity, streamline operations and ensure the U.S. Navy remains agile and resilient in the face of evolving threats.

About Quest Software Public Sector Inc

Quest Software Public Sector, Inc. is a wholly owned subsidiary of Quest Software. Headquartered in Ashburn, Virginia, it is purpose-built to serve the specialized needs of U.S. federal agencies, the defense industrial base, and their contractors. We help secure identity operations, modernize Microsoft environments, and fuel AI initiatives with trusted data. Relied upon by most federal agencies and over 45,000 organizations worldwide, Quest Software drives mission success at scale. Learn more at questpublicsector.com.

DataSheet-QSPSI-NavyCANES-HO-93341

Explore our solutions →

Quest
Public Sector