Everpure and CDW Resilience Solution

This comprehensive overview details the synergistic relationship between the Everpure advanced data platform and CDW's strategic resilience services. In 2026, the industry has shifted from traditional "perimeter defence" to a holistic "business resilience" model designed to ensure organisations can withstand breaches, maintain essential functions, and recover rapidly.

1. The High Stakes of Business Disruption in 2026

Cyberattacks can halt operations for days or weeks, but modern organisations require the restoration of critical applications within hours. Delays in recovery lead to significant losses in customer trust and brand reputation, potentially allowing competitors to gain market share.

The Cost of Downtime

The Cost of Downtime: Enterprise-scale organisations can incur downtime costs of approximately **$9,000 per minute**, totalling roughly **$540,000 per hour**.

Regulatory Penalties

Failure to restore data quickly and securely can result in penalties from bodies such as HIPAA, GDPR, and the SEC.

Infrastructure Bottlenecks

Many organisations rely on legacy technology that fails to address the need for isolated recovery environments (IREs) and creates bottlenecks during data provisioning.

The UK Cyber Security and Resilience Bill

The UK Cyber Security and Resilience Bill is likely to start implementation in early 2027 (and in full force from 2028), shifting the focus from simple compliance to active resilience. Fines for non-compliance are eye-watering, with fines up to £17M or 4% of annual global turnover.

Everpure and CDW Resilience Solution

2. Everpure: The Cyber-Ready Foundation

Everpure transforms storage from a passive resource into an active and foundational layer of cyber defence. The Everpure platform is built to resist malicious access, detect threats faster, and recover with high confidence.

Built-In Security & Zero Trust

Data Immutability

Everpure indelible and immutable snapshots (called Safemode) ensure critical data cannot be altered, deleted, or encrypted by ransomware. This is your last line of defence.

Zero Trust Architecture

Everpure applies Zero Trust principles across every layer, ensuring every access request is verified and every action is authenticated.

Access Controls

The platform enforces role-based access control (RBAC), multi-factor authentication (MFA), and end-to-end encryption.

IAM 2.0

This identity and access control system introduces granular RBAC and federated identity integration to strengthen data security.

Hardware Security

Features such as Trusted Platform Module (TPM) and UEFI Secure Boot safeguard system integrity from start-up.

Connected Threat Detection

Real-Time Visibility

Everpure provides native threat detection to identify anomalies, unauthorized access, and suspicious activity using behavioural and heuristic analysis. Integration with key vendors such as Commvault, Veeam, Rubrik, provides unparalleled levels of resiliency.

AI Copilot & Assessment

Everpure Security Assessment 2.0, powered by the Everpure AI Copilot, identifies risks, vulnerabilities, and common vulnerabilities and exposures (CVEs).

Security Integration

Everpure integrates with SIEM, UEBA, and XDR solutions to provide real-time visibility into storage-level threats.

Everpure and CDW Resilience Solution

3. CDW: Strategic Cyber Resilience Services

CDW complements Everpure technology by categorising resilience offerings into four primary pillars: Advise, Transact, Transform, and Manage.

Cyber Resilience Advisory

CDW focuses on functional, tested strategies rather than “paper-only” plans, focusing on frameworks such as NIST

Minimum Viable Company (MVC) Planning

This 2026-specific methodology identifies the bare-bones IT requirements needed to keep a business operational during a catastrophic event.

Access Controls

The platform enforces role-based access control (RBAC), multi-factor authentication (MFA), and end-to-end encryption.

Incident Response Preparedness

CDW develops playbooks and conducts Tabletop Exercises to ensure leadership and technical teams are prepared for live breaches.

Managed Detection and Response (MDR)

CDW partners with vendors such as Sophos and CrowdStrike to provide 24/7 monitoring to neutralise threats before they become disasters.

Threat Hunting

Compromise assessments are used to identify “dwellers” – attackers already inside the network who have not yet triggered alerts.

Cloud & Hybrid Resilience

Designing multi-cloud architectures that avoid single points of failure, ensuring data sovereignty and federation across platforms.

Everpure and CDW Resilience Solution

4. Integrated Recovery Capabilities

The combined Everpure and CDW solution provides a seamless path from detection to full restoration.

Feature	Everpure Capability	CDW Capability
Recovery Environments	**Pure Protect** automatically provisions Isolated Recovery Environments (IREs) with compute, networking, and storage.	**ServiceWorks Assure (DRaaS)** provides continuous replication to UK data centres with a 60-minute recovery commitment.
Recovery Speed	**Everpure's FlashArray** and **FlashBlade** products provide unparalleled recovery at the speed of flash.	**CDW's experience** of deploying ultra-high speed recovery environments ensure that you're in safe hands.
Threat Mitigation	**Pure1** provides Al-driven anomaly detection and predicts vulnerabilities to reduce risk before attacks occur.	**Managed Detection and Response (MDR)** provides active threat hunting and containment through 24/7 monitoring.
Data Protection	**SafeMode Snapshots** provide secure, tamper-proof copies of data for rapid recovery.	**Immutable Backup Solutions** All CDW-delivered backup solutions support S3-compatible object lock immutability, securely locking data in "WORM" vaults.
Automation	Scripted workflows orchestrate failovers to ensure accurate, consistent setup across environments.	**Automated Resilience** implements SOAR to handle routine mitigation tasks without human intervention.
Integration with Alliance Vendors	Everpure's cyber resiliency capabilities have tight integration with Commvault, Veeam, Rubrik, and others.	CDW's breadth of knowledge and capability across many vendors ensures that all solutions will meet your cyber resiliency needs.

Everpure and CDW Resilience Solution

5. Unified Operations and Continuous Innovation

The Evergreen Model

The Everpure Evergreen subscription model enhances resilience through non-disruptive upgrades, firmware validation, and continuous innovation Disruptive tech refreshes are now a thing of the past.

Evergreen Replacement Service

The Cyber Resilience add-on to Everpure's Evergreen//One (consumption-based subscription model) guarantees that in the event of disaster or ransomware attack where the existing hardware becomes a "cordoned-off crime scene", Everpure will ship a new set of clean arrays next business day, with a defined recovery plan.

Performance and Scalability

The Everpure platform, featuring FlashArray and FlashBlade® systems, eliminates data silos and provides ultra-low latency (150µs to 1ms) for rapid data access and recovery.

Workforce Resilience

CDW provides specialised training programs and staff augmentation to equip internal IT teams with the skills to manage recovery operations, as well as providing specialised engineers to fill gaps in your security or infrastructure teams during high-risk periods.

Executive Summary

By combining Everpure's secure-by-default architecture and high-performance recovery with CDW's "Minimum Viable Company" planning and managed response, organizations can achieve a hardened foundation aligned with Zero Trust frameworks.

Take a closer look at Everpure **here**.