Everpure

Accelerate Recovery with Everpure Cyber Resilience

Reduce the risk and impact of cyber disruptions.

Cyberattacks may halt operations for days or even weeks, but most organizations need to recover critical applications and services within hours. The longer an organization takes to recover, the greater the loss of customer trust and brand reputation, and competitors may gain market share if services remain unavailable. Adding to the problem is that downtime is extremely costly, especially to enterprise-scale organizations. Organizations can incur downtime costs of approximately $9,000 per minute, which translates to roughly $540,000 per hour. And regulatory penalties (such as those associated with HIPAA, GDPR, and SEC) can be imposed if organizations fail to restore data quickly and securely.

From passive to proactive: A new cyber resilience foundation

Many organizations rely on legacy disaster recovery technology, processes, and policies to recover from ransomware attacks. These fail to address the complexities of cyber recovery, including the need to quickly provision isolated recovery environments (IREs) critical for fast and reliable recovery. Further, backup storage for the most critical applications typically operates on legacy or outdated technology, creating a bottleneck that hinders the rapid provisioning of data for recovery processes. And before the attack occurs, many security analytics tools, such as security information and event management (SIEM) and user and entity behavior analytics (UEBA), lack insights from mission-critical storage and struggle to analyze the massive volume of log data generated by the network, endpoints, storage, and servers.

At Everpure™, we recognize that storage can no longer be passive. Native security and recovery capabilities must augment existing cybersecurity and data protection architectures, **transforming storage into an active and foundational layer of your cyber defense and cyber recovery.** Built on a foundation of data intelligence—to resist malicious access, detect threats faster, and recover with unprecedented confidence—the Everpure Platform is ready to meet this challenge head-on.

Built-in security, connected threat detection, dynamic response and recovery, and a data intelligence foundation

Everpure empowers you to withstand cyberattacks and accelerate both cyber and disaster recovery. **Built-in security, connected threat detection, and dynamic response and recovery** are the pillars for effective cyber-resilient storage. The Everpure Platform protects data from ransomware and cyber threats through high-performance, automated layered resilience and recovery, native threat detection, robust data security and immutability, and seamless cybersecurity and data protection integrations, ensuring you can recover at optimal speed and that your data remains available and secure. Data and application intelligence underpin Everpure cyber resilience capabilities by providing the contextual insight, operational visibility, and adaptive control needed to strengthen these pillars.

Cyber-ready storage

Storage is the primary recovery mechanism, secured, replicated, integrated, and automated to strengthen cyber resilience and accelerate recovery.

Accelerated security analytics

Everpure provides visibility into threats targeting critical workloads and accelerates threat detection for on-premises SIEM.

Supercharged data protection

Everpure reduces backup windows and recovery time with performance and SafeMode™ Snapshots integration.

Solution overview

Built-in security provides native prevention and a secure-by-default design, protecting both the platform and data through indelible and immutable storage, Zero Trust principles, and deep integrations with leading data security solutions.

- Everpure indelible and immutable snapshots ensure your critical data cannot be altered, deleted, or encrypted by ransomware or malicious actors. These snapshots are automatically versioned and protected at the storage layer, providing a secure, tamper-proof copy of your data for rapid recovery. By combining instant accessibility with built-in indelibility, organizations can confidently meet compliance requirements, accelerate recovery, and maintain business continuity, even during sophisticated cyberattacks.
- Everpure applies Zero Trust principles to secure every layer of the data infrastructure, ensuring that every access request is verified, every action is authenticated, and every component is trusted. Built on a secure-by-default architecture, Everpure enforces role-based access control (RBAC), multifactor authentication (MFA), and end-to-end encryption to protect both management and data planes. Hardware-based security features like trusted platform module and UEFI secure boot safeguard system integrity from the moment of startup, while bring-your-own-key capabilities give customers complete control over their encryption keys. Together, these controls establish a hardened, verifiable foundation aligned with Zero Trust frameworks, ensuring data confidentiality, integrity, and resilience across the enterprise.
- Everpure IAM 2.0 delivers advanced, enterprise-grade identity and access control to strengthen data security across environments. Built on Zero Trust principles, IAM 2.0 introduces granular RBAC, federated identity integration, and MFA to ensure only verified users and services can access critical data and management functions. With centralized policy management and audit-ready visibility, IAM 2.0 simplifies administration while enhancing protection, compliance, and operational efficiency across the Everpure ecosystem.
- The Everpure Evergreen® model extends this secure-by-default architecture with ongoing nondisruptive upgrades, firmware validation, and continuous innovation. This ensures your environment remains available, compliant, hardened, and optimized over time.

Everpure delivers **connected threat detection** with built-in and integrated capabilities to identify and resolve threats, combining native threat detection and remediation, continuous security and ransomware assessments, and seamless integrations with leading cybersecurity platforms.

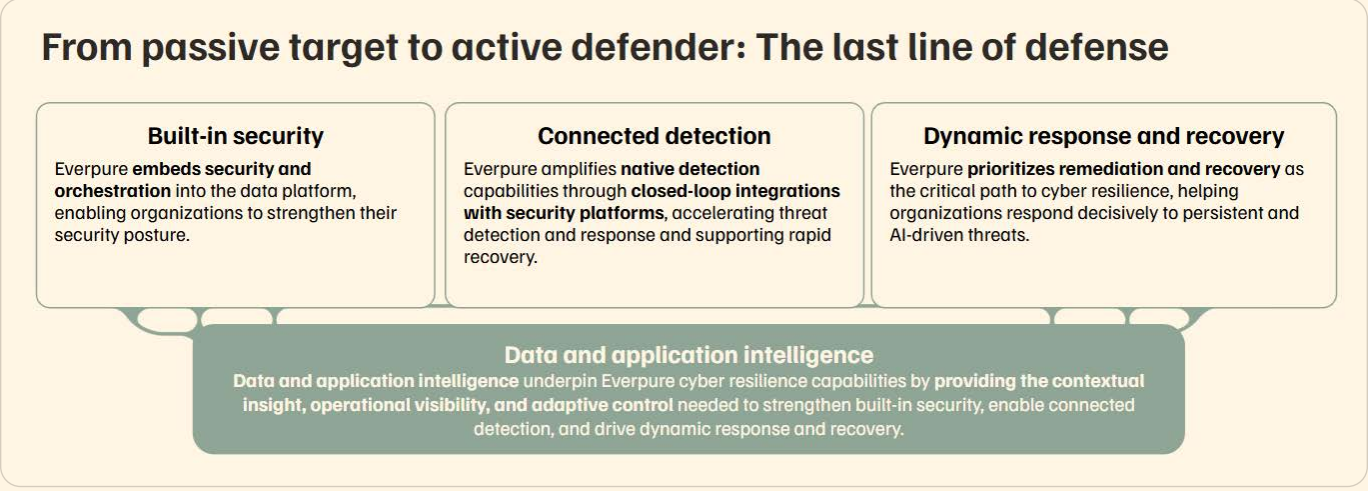
- Everpure delivers native threat detection that brings real-time visibility and actionable intelligence to the data layer. Organizations can detect anomalies, unauthorized access, and suspicious data activity using advanced behavioral and heuristic analysis. The platform proactively identifies early indicators of compromise and provides context-rich insights that enable swift, confident response with minimal operational overhead.
- Everpure Security Assessment 2.0, powered by the Everpure AI Copilot, provides deep visibility into your security posture, quickly identifying risks, vulnerabilities, and anomalies including common vulnerabilities and exposures. Built-in agents enable automated detection and remediation, allowing teams to take proactive action and resolve threats rapidly to strengthen cyber resilience with minimal operational overhead.
- Everpure integrates seamlessly with SIEM, UEBA, and extended detection and response (XDR) solutions to provide real-time visibility into storage-level threats, enabling faster detection and response. When used as the dedicated storage tier for security analytics, Everpure delivers enhanced performance and scalability, ensuring that even large-scale security workloads can run efficiently while maintaining comprehensive threat monitoring and data protection.

Dynamic response and recovery is delivered with industry-leading capabilities and integrations to rapidly respond and restore workloads, featuring automated layered resilience, on-demand recovery zones, and seamless data protection integrations.

- Automated layered resilience from Everpure, featuring Everpure Resilience service automation and provisioning capabilities, leverages a combination of immutable and indelible data snapshots, data replication, streaming data protection, and disaster recovery as a service. This ensures data availability against evolving cyber threats, giving you the power and performance to recover from simple outages to complex and destructive cyberattacks.
- Everpure recovery zones enable the automatic provisioning of complete IREs, ensuring clean, secure spaces for recovery after a cyber event. Each IRE includes compute, networking, and storage resources that are fully configured and ready for use on demand. Through automated provisioning and scripted workflows, recovery zones ensure accurate setup, speed deployment, and eliminate the risk of manual errors. This automation simplifies recovery operations, enhances resilience, and helps organizations restore critical workloads rapidly and confidently.
- Everpure delivers industry-leading performance and scalability for top data protection solutions, enabling faster backups and rapid recovery of critical workloads. Seamlessly integrated with leading vendors such as Rubrik, Commvault, and Veeam, Everpure ensures end-to-end data resilience, empowering organizations to protect, manage, and recover their data efficiently while minimizing operational impact.

The data intelligence foundation is delivered with the industry-leading Everpure Data Intelligence (formerly 1touch) solution, which provides the contextual intelligence for how to secure data, target detection, and prioritize remediation and recovery.

- **For built-in security**: Classifies sensitive data, extends secure-by-design protection beyond infrastructure, and surfaces critical data to strengthen compliance and reduce risk
- **For connected detection**: Leverages data intelligence for detection policies; enriches SIEM and security orchestration, automation, and response (SOAR) with actionable context; and combines telemetry with data intelligence for prioritized response
- **For dynamic response and recovery**: Prioritizes recovery using data and application context and informs policies and workflows



Solution components

Everpure market-leading capabilities and integrations help organizations quickly recover from cyberattacks and disasters and support the detection of and response to threats.

Everpure Data Intelligence

- **Automated discovery of data, sources, and flows** across the organization's networks
- **Accurate, contextual classification of data sensitivity** with actionable intelligence powered by continuously improving AI/ML
- **Unified, extensible data intelligence** that creates a single contextual record for compliance and reporting across integrated data sources

Everpure Resilience service

- **IREs on demand**: Automatically provision IREs that include compute, networking, and storage resources ready for rapid recovery when needed.
- **Automated provisioning**: Scripted workflows orchestrate failovers and ensure accurate, consistent setup across environments, reducing manual effort and errors.
- **Automated layered resilience**: Everpure Resilience service streamlines the provisioning and management of Everpure layered resilience, orchestrating snapshots, replication, and recovery workflows automatically to ensure consistent, reliable protection with minimal manual intervention.

Pure1®

- **Proactive threat mitigation**: Pure1 strengthens your security posture by providing actionable assessments, predicting vulnerabilities, and recommending best-practice storage configurations—including snapshots and SafeMode™ settings—to reduce risk before attacks occur.
- **Intelligent detection and response**: AI-driven anomaly detection monitors storage behavior for suspicious activity and integrates with SIEM, SOAR, and XDR platforms to trigger automated protective actions, such as creating immutable snapshots and quarantining potential threats.
- **Simplified, safe recovery**: Pure1 accelerates recovery by identifying last-known clean snapshots and correlating threat intelligence, enabling rapid and reliable restoration while minimizing business disruption and preventing reinfection.

The Everpure Platform, featuring Purity, FlashArray™, and FlashBlade® systems

- Consolidate block and file workloads, eliminating data silos by dynamically provisioning recovery workloads.
- Gain ultra-low-latency performance (150µs to 1ms) for rapid data access with best-in-class data reduction and high availability (99.9999%).
- Enable application-level recovery with real-time awareness of applications and workloads across the entire fleet.

The Evergreen subscription model

Evergreen enhances cyber resilience by continuously evolving your environment to stay secure, compliant, and optimized—without disruption.

- **Evergreen replacement service**: If hardware is compromised or damaged during a cyber event, Evergreen enables rapid, nondisruptive hardware replacement, restoring a trusted, secure foundation for recovery and continued operations.
- **Continuous hardening and compliance**: Evergreen ensures your storage environment stays secure by default with ongoing firmware validation, proactive patching, and compliance with evolving security standards—without downtime or disruption.
- **Nondisruptive upgrades**: Seamlessly apply hardware and software updates to strengthen your resilience posture while maintaining performance, availability, and protection of critical data.

Cybersecurity integrations

- Integrated with SIEM, UEBA, and XDR solutions to provide real-time visibility for storage threats
- Enhanced performance and scalability when used as the SIEM, UEBA, and XDR storage tier

Data protection integrations

- Provide performance and scalability for leading data protection solutions, ensuring faster backups and rapid recovery.
- Leverage tight integration with the latest solutions from top data protection vendors like Rubrik, Commvault, and Veeam to deliver end-to-end data resilience.

Everpure

Additional resources

- Learn more about Everpure Technology Alliance Partners.
- Learn how organizations are defending against evolving ransomware threats.
- Read the Everpure cyber resilience buyer's guide.

Explore Everpure Cyber Resilience

Visit Our Website | **800.379.PURE**

ID26677-01-en-06/26