What Organizations are Missing for Cyber Resilience (And How Storage Can Change That)

With threats growing in sophistication and impact, cyber resilience has become more important than ever. The numbers from our report, "The State of Cyber Resilience" (produced with Ponemon Institute) tell a stark story: Organizations experience an average of one attack against data in storage every month, adding up to tens of millions of dollars per year in regular predictable losses. Cyberattacks are growing not only in frequency and sophistication, but also in impact, capable of crippling large enterprises and erasing household names virtually overnight.

For far too long, organizations have relied on disconnected cybersecurity tools to block attacks and on slow, legacy backup systems for resilience. Attacks are breaking through, and recovery is hindered by sluggish performance and manual processes. "The State of Cyber Resilience" report confirms this gap is real and costly: Less than half of IT and security practitioners rate their organization's cyber resilience as high, and just 41% say they have a strong ability to manage data consistently across all environments.

"Resiliency is the security lens. It's not about checking the right boxes. It's about whether we can take our data, operate somewhere else, and how quickly we can do it." –Rick Orloff, VP and CISO, Everpure, *The Data Wire*

True resilience has often been an afterthought, with add-on solutions that cannot keep up with the massive volume of modern threats and do not work in real time. This leads to poor threat detection, error-prone restorations, and a dangerously long time to resolution. Consider that it takes organizations an average of 12 days to recover mission-critical applications after a data security incident—an eternity when operations hang in the balance. Storage plays a major role in that recovery time and can be the difference between days versus minutes or hours.

At Everpure, we recognize that storage can no longer be passive. Native security and recovery capabilities must augment existing architectures, transforming storage into an active and foundational layer of your cyber defense and cyber recovery. The Ponemon Institute study reinforces this urgency: 63% of respondents say securing data in storage is very or extremely important compared to other security initiatives, and 66% identify automation as the key to achieving a high level of cyber resilience in data storage. Built to resist malicious access, detect

threats faster, and recover with unprecedented confidence, the Everpure Platform is ready to meet this challenge head-on.

We empower customers not only to help prevent threats but proactively detect them and recover rapidly, meeting the challenges of today's threat landscape and the need for organizations to bounce back quickly.

We're excited to build on our proven track record in cyber resilience with a new suite of innovations that take this vision even further.

1. Dynamic response and recovery

When a cyberattack hits, every second counts. The Ponemon Institute research found that recovering up-to-date backups of critical data represents the single largest cost category following an attack, accounting for 31% of the average $5 million incident cost. And with only 49% of organizations rating their backup systems as highly effective for rapid recovery, the gap between expectation and reality is painfully clear.

"Cyber recovery is not disaster recovery. If you're planning for a tornado, you're not prepared for an attack. The way these events unfold is completely different, and most teams just aren't ready to recover in a cyber context." –Andrew Stone, CTO for the Americas, Everpure, *The Data Wire*

Our new capabilities are designed to turn hours or days of manual recovery into a near-instantaneous process. We have several key features that make this possible:

- **Everpure™ Protect Service recovery zones:** This groundbreaking feature automatically provisions isolated recovery environments (IREs) so you can quickly restore workloads in a clean, secure space.
- **Layered resilience with integrated ActiveCluster™ and ActiveDR™ replication:** Automated multi-site replication for cyber recovery helps ensure your data is protected and available across multiple locations.
- **Built-in cyber resilience:** As AI moves from sandbox to enterprise production, organizations need a security-first storage infrastructure backed by native threat detection. We've partnered with leading cybersecurity companies to maintain governance, compliance, and cyber resilience at scale.
- **Application-level recovery:** Get fast, intelligent, and consistent recovery for your most mission-critical workloads, so your business-essential applications are back online in minutes. With 36% of stored data classified

as mission critical, getting these systems back online is a business survival imperative.
- **Everpure Resilience Community Edition:** Get started with powerful, free entry-level capabilities that improve your cyber recovery performance and reliability.

2. Seamless integration

Storage must be seamlessly integrated to existing security operations, controls and safeguards. Everpure offers integrated detection capabilities that give you complete visibility across your environment.

- **CrowdStrike real-time Threat Graph integration:** Enact threat intelligence and automatically detect and remediate malicious activity and attacks as they happen.
- **Threat detection:** Everpure AI Copilot helps identify risks early and enables proactive action to reduce business impact before threats can cause damage. Our report found that 53% of practitioners believe AI simplifies data security storage by automating tasks faster and at lower cost than human-only approaches.
- **Threat hunting in Log Center:** Use Log Center to investigate insider threats and anomalous user access, giving you the power to find threats that traditional tools miss. This matters more than most realize: Malicious insiders were cited as a root cause of data loss by 58% of respondents, and an average of more than 5,400 employees and third parties have access to sensitive data in storage at any given organization.
- **Real-time malware scanning with ICAP:** Enable next-gen anti-virus for file workloads to detect malware as it attempts to infect your systems.
- **Superna Data Security and CrowdStrike next-gen SIEM integrations:** Our new integrations with Superna and CrowdStrike help you accelerate remediation tactics and combat malicious activity at the data layer. Integration with SecOps tools like SIEM, XDR, and SOAR was rated the most important data storage security control by 67% of Ponemon Institute respondents—validation that connected detection isn't optional; it's foundational.

3. Built-in security

Security should not be an add-on; it must be a core principle. But our research

reveals how far most organizations still have to go: 36% of stored data is considered “dark” or unclassified, meaning organizations don’t even know what they’re protecting. And with an average of more than 5,400 people having access to an organization’s sensitive storage data, the attack surface from within is enormous. The Everpure Platform is designed with security natively built in and secure by default to protect your data from the ground up.

- **Security Assessment 2.0 with the AI Copilot:** Gain full visibility into your security posture, identify common vulnerabilities and exposures (CVEs), and take proactive action with the guidance of our AI.
- **TPM and UEFI secure boot:** Everpure helps prevent malicious tampering of cryptographic and boot functions with zero-trust capabilities, ensuring the integrity of your systems from the moment they boot.
- **Enterprise-grade identity and access management:** Secure and centralize the management of user identities, roles, and access permissions with granular control over settings. Ponemon Institute found that multi-factor authentication (71%) and role-based access control (63%) are the most widely adopted access controls for protecting data in storage, but adoption alone isn’t enough without a platform that enforces them natively at the storage layer.
- **Bring your own key:** Maintain full control over your data with the ability to provide your own encryption keys for secure multi-tenancy.

The Bottom Line

Cyberattacks are outpacing traditional defenses, exposing the limits of fragmented tools and slow, legacy recovery systems. “The State of Cyber Resilience” report puts hard numbers behind what security teams already feel: Organizations face roughly a dozen storage attacks per year on average, mission-critical recovery can drag on for nearly two weeks, and less than half of practitioners feel genuinely resilient. Delayed detection, guesswork in finding clean restore points, and lengthy recovery times put organizations at risk of prolonged outages and business disruption.

Everpure is changing that. By unifying real-time detection, automating remediation, and enabling rapid, validated recovery, we give customers true cyber resilience. The 66% of practitioners who say automation is the key to achieving resilience aren’t wrong; they just need a platform built from the ground up to deliver it. Move beyond reactive defenses to confidently protect and recover your

most critical data to ensure business continuity today and readiness for the threats of tomorrow.