Elastio Makes Cyber Recovery Compliance Simple with Audit Dashboards

Elastio's next-gen dashboards deliver real-time recovery insights aligned with global standards to simplify compliance, reduce risk, and ease audits.

DORA Customer Dashboard for Elastio

BOSTON, MA, UNITED STATES, October 7, 2025 /EINPresswire.com/ -- Elastio today announced the release of its Compliance-ready recovery capabilities via global security dashboards, designed to help organizations strengthen operational resilience and meet rising regulatory demands across multiple cybersecurity frameworks.

As ransomware and malicious encryption become certainties rather than mere threats, regulators are placing greater emphasis on backup and data integrity, recovery testing, and incident response planning. Elastio addresses these challenges directly by detecting ransomware and data corruption, well before the recovery process begins.

> Compliance isn't just checkboxes—it protects businesses from ransomware's real costs. Regulators expect proof of resilience."
>
> *Ron Green, Cyber Resiliency Board member for Elastio*

"Compliance requirements aren't abstract checkboxes. They're designed to protect businesses from the very real and costly impacts of ransomware," said Ron Green, Cyber Resiliency Board member for Elastio and cybersecurity expert. "For customers, the stakes are high and regulators expect proof of resilience and data integrity."

Alignment With Leading Security Standards

Elastio's capabilities are designed to support key controls in NYDFS 500.16, DORA, NIST CSF, ISO/IEC 27001:2022, and PCI DSS v4.0, among others:

- NYDFS 500.16 – Validates backup integrity, continuously tests recovery readiness, and provides immutable scan logs to support incident response and audit requirements.
- PCI DSS v4.0 – Delivers malware detection in backup data, change monitoring, and verified

recovery paths to support incident response and data integrity mandates.
- DORA (Digital Operational Resilience Act) – Strengthens ICT risk management, recovery testing, and reporting obligations, including third-party oversight.
- NIST Cybersecurity Framework (CSF) – Extends coverage across Detect, Respond, and Recover functions through continuous monitoring, automated tagging, and validated clean restores.
- ISO/IEC 27001:2022 – Provides end-to-end evidence collection, forensic readiness, and malware protection aligned to Annex A controls.

NIST Customer Dashboard for Elastio

NYDFS Customer Dashboard for Elastio

Why This Matters
In today's threat landscape, resilience is no longer optional; it's survival. Traditional approaches can't keep up. Elastio's next-generation dashboards give customers the visibility and assurance they need to:
1. Ensure recoverability – Detecting ransomware in backups before recovery ensures that clean data is always available.
2. Reduce audit pain – Built-in logs, reporting, and validation directly map to regulatory controls, saving time and cost during audits.
3. Strengthen resilience – Continuous backup verification and automated recovery testing assure that systems can be restored quickly and safely.
4. Protect investments across platforms – Operating independently of the backup source, Elastio validates data integrity across multiple systems and cloud providers.

Elastio turns regulatory obligations into operational advantages. Customers not only stay compliant with frameworks like NYDFS 500.16, DORA, NIST CSF, and ISO/IEC 27001:2022, but also gain real-world confidence in their ability to withstand and recover from attacks.

Reducing Risk and Audit Burden
Elastio's independent, source-agnostic approach enables organizations to scan and validate

backups across disparate systems without impacting production.

The solution provides:
- Continuous ransomware and malware detection in backups
- Automated validation of recovery paths to ensure data cleanliness
- Immutable audit logs for compliance verification and forensics
- Integration with security operations for incident response support

By fitting seamlessly into compliance workflows, Elastio helps financial services firms and other regulated industries reduce both operational risk and audit complexity.

About Elastio
Elastio is the leading provider of provable recovery and the control point for cyber resiliency. By continuously validating the data integrity of backups, detecting ransomware, and ensuring day-zero detection, Elastio eliminates the risk of encrypted data blocking recovery. Trusted by AWS, Deloitte, IBM, NetApp, Azure, and more.

Danielle Goode
Elastio
email us here
Visit us on social media:
LinkedIn
