Elastio Achieves Veeam Ready Security Incident API Status to Advance Data Integrity Control for Ransomware

Elastio's integration with Veeam enables proactive validation of data integrity, detecting ransomware encryption and ensuring clean, reliable recovery at scale.

RESTON, VA, UNITED STATES, March 23, 2026 /EINPresswire.com/ -- Elastio, the market leader in ransomware recovery assurance, today announced it has achieved Veeam® Ready Security Incident API status as part of the Veeam Ready Program. This program validates partner solutions for seamless integration with Veeam Data Platform capabilities. As the Data and AI Trust Company, Veeam Software recognizes Elastio's compatibility with its platform, highlighting the increasing importance of Data Integrity Control in today's backup architectures.

> "
> Veeam is foundational to our data protection strategy, and integrating Elastio adds the critical layer of data integrity validation that modern ransomware demands."
>
> *Boris Voltchenko, Chief Information Security Officer*

Modern ransomware no longer relies on detectable malware artifacts. Today's attackers deploy fileless techniques, living-off-the-land methods, and polymorphic encryption that evade traditional endpoint and signature-based tools. These tactics silently compromise production data and propagate into backups, turning recovery infrastructure into an unseen liability.

Elastio removes this uncertainty by deploying a dedicated Data Integrity Control that inspects backup data independently of the backup process. Through deep file inspection and AI-driven encryption analysis, Elastio detects ransomware impact, including stealthy and zero-day variants, before it's too late.

"Ransomware has shifted from a perimeter security problem to a recovery integrity problem," said Najaf Husain, CEO of Elastio. "Immutability and vaulting protect storage. They do not validate the integrity of the data itself. Achieving Veeam Ready Security Incident API status reinforces that encryption scanning and data integrity validation are now critical security controls for any organization running Veeam solutions."

Strengthening the Last Line of Defense

The Veeam Ready Security Incident API qualification confirms Elastio's interoperability with Veeam Data Platform security capabilities, enabling customers to integrate continuous backup integrity validation into their existing Veeam environments.

By adding Data Integrity Control to Veeam deployments, organizations gain:
 Recovery Confidence: Ensures backup data is clean, uncompromised, and safe to restore.
 Encryption Detection at Scale: Identifies ransomware-driven encryption and hidden corruption that traditional tools can miss.
 Faster Recovery Decisions: Automatically identifies the last known clean recovery point, reducing downtime during an incident.
 Compliance Readiness: Produces audit-ready proof of recoverability to support regulations and standards such as NYDFS, DORA, and NIST.

A New Security Baseline for Veeam Customers

As ransomware increasingly targets recovery paths, the ability to prove data integrity is becoming a board-level requirement. Backup without validation leaves organizations exposed to catastrophic downtime, ransom payments, and reputational damage.

With Veeam Ready Security Incident API status, Elastio formalizes its role as the integrity layer within Veeam-based architectures. Together, Elastio and Veeam enable organizations to move beyond backup storage protection toward verified recovery assurance.

"At Reynolds Consumer Products, we deliberately partner with best-of-breed technology leaders who bring deep expertise and innovation to their domain," said Boris Voltchenko, Chief Information Security Officer at Reynolds Consumer Products. "Veeam is foundational to our data protection strategy, and integrating Elastio adds the critical layer of data integrity validation that modern ransomware demands. The seamless alignment between the two platforms strengthens collaboration between our security and infrastructure teams and gives us greater confidence in our ability to recover and keep the business running."

Availability
Elastio is available for Veeam environments immediately. Organizations can assess their recovery risk posture at www.elastio.com.

About Elastio
Elastio delivers Active Cyber Resilience, a security philosophy built on one principle: recovery must be continuously proven and not periodically tested or assumed. The Elastio Hunt Engine performs Deep File Inspection across live data, replicated data, and backups to detect ransomware and malware that has evaded prevention and detection tools. Recovery you can prove.

Cecily Polonsky
Elastio
+1 609-613-7155
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/900965492