Solution Brief

Prove You Can Recover from Ransomware

Know Your VCF Recovery Data Is Uncorrupted

Key Capabilities

- **Automated Scanning of Veeam Recovery Points**
  Elastio continuously inspects Veeam backups stored on IBM FlashSystem or object storage for signs of ransomware and corruption, without requiring full restores.
- **Ransomware Fingerprint Detection & AI Analysis**
  Behavioral ML engines identify malicious encryption and data corruption with 99.999% accuracy. Custom policies enable precision control.
- **Immutable Backup & Isolated Validation**
- IBM storage ensures data immutability while Elastio validates recoverability in a secure, isolated enclave, ensuring no disruption to production environments.
- **Evidence for Compliance and Cyber Insurance**
- Audit-grade reports prove you have viable, clean recovery points, supporting regulatory frameworks like DORA, NYDFS, and NIST.
- **Confidence in Recoverability**
- Elastio makes recovery provable, enabling your organization to act with speed and certainty when time and trust are on the line.

The Challenge

Can you prove you can recover from ransomware before the next attack?

Modern enterprises are doubling down on hybrid cloud infrastructure and VMware Cloud Foundation (VCF) to standardize virtualization, automation, and workload mobility across their organizations. But ransomware actors are evolving too, targeting not just production data, but backup systems and metadata. Many organizations assume their backups are safe, only to discover too late that their recovery points are corrupted or encrypted.
Relying on untested backups is no longer enough.

The Solution

The Data Protection Trinity: IBM + Veeam + Elastio

IBM and Veeam deliver robust backup and replication for VCF-based workloads. But the missing piece has been proof—a way to validate that recovery points are free of ransomware and corruption before disaster strikes.

That's where Elastio comes in.

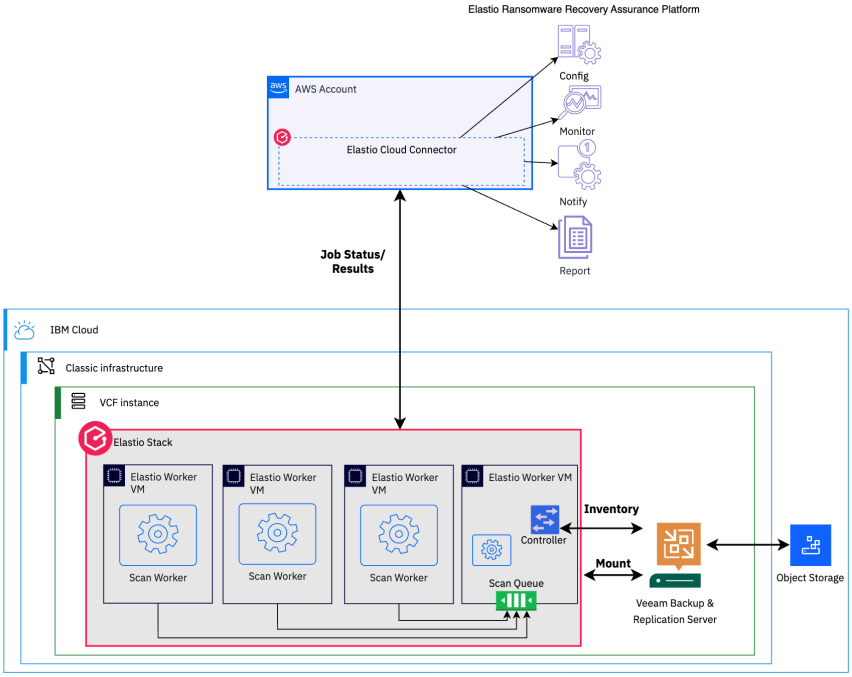
Elastio integrates seamlessly with Veeam and VCF environments to automatically:

- Scan backup data for ransomware indicators and encryption
- Validate recoverability of workloads—proving backups are clean and bootable.
- Securely isolate and test restore points with zero impact to production.
- Provide detailed audit logs to support compliance and cyber insurance.

Together, IBM, Veeam, and Elastio enable proactive ransomware recovery assurance, ensuring that your last line of defense is resilient, clean, and provable. Thorough data inspection is essential to detect and recover from ransomware attacks effectively. This process helps identify subtle indicators of pending or active attacks and determines whether data is safe before recovery.

Cyber Resilience with Elastio Overview

Here is a high-level architecture diagram:



How it Works

1. **Backup to IBM FlashSystem or Object Storage using Veeam**
   Fast, immutable, enterprise-grade backups for VCF workloads
2. **Integrate Elastio to Scan & Validate Recovery Points**
   Ransomware and integrity validation on all backups, continuous or on-demand
3. **Isolated Restore Testing and Compliance Reporting**
   Clean recoverability is proven and documented before disaster strikes

Proven Together

IBM, Veeam, and Elastio are collaborating to simplify ransomware recovery assurance for VCF-based environments. This integrated approach reduces risk, improves resilience, and ensures that when ransomware strikes, you're not relying on hope—you're relying on proof.

Ready to Prove Recovery?

Don't wait for an attack to discover your backups are compromised.

With IBM, Veeam, and Elastio, you can take a proactive, provable stance on cyber recovery.

Prove Recovery. Stop Ransomware.

Learn more:
elastio.com | IBM Blog

About Elastio

Elastio specializes in ransomware mitigation and recovery, providing businesses with advanced tools to validate their data. By bridging the gap between traditional security measures and immutable backups, the Elastio Platform ensures clean recovery from zero-day ransomware attacks, giving organizations the confidence to restore operations quickly and securely. For more information, visit www.elastio.com.