elastio Ransomware Recovery Assurance aws

Case Study

Avoiding an Extinction Event: How a SaaS Company Recovered After a Stealthy Ransomware Attack with JetSweep & Elastio

Key Capabilities

Industry: SaaS
Headquarters: United States
Cloud Environment: Jetsweep,AWS
Use Case: Ransomware Recovery Assurance, Data Cost Optimization
Data Types Protected: EHR platform data, patient records, backups, infrastructure state

Challenge:

- A SaaS company suffered a devastating ransomware attack, which encrypted critical business data and halted company operations.
- Traditional endpoint protection failed to detect the attack, and backups were compromised, making recovery uncertain.

Solution:

- JetSweep brought in Elastio, which enables rapid, automated backup scanning for ransomware.
- Elastio identified a clean recovery point in minutes and restored operations with minimal data loss. backups

Challenge

On a Saturday morning, JetSweep, an AWS consulting partner, received an urgent call from AWS. A SaaS company had fallen victim to a ransomware group, leaving its operations at a standstill.

Investigation revealed that the attackers had gained access through an unpatched firewall, which JetSweep immediately patched to prevent further access. But the real challenge emerged when the company tried to restore from backups.

The attackers had used a sophisticated tactic: fileless ransomware which encrypted data without detection by hiding the decryption key in memory. The company had been operating normally, unaware that ransomware was already stealthily encrypting the data over time. Even with a leading endpoint protection platform in place, the attack had gone undetected. The corrupted data had been replicated into backups, leaving the company without a clear recovery path.

With no confidence in their backups, the company faced prolonged downtime—or even total business failure.

Solution

JetSweep immediately took action, securing the environment and preventing further infiltration. However, the true challenge remained—finding a clean recovery point.
To eliminate the manual, time-consuming “hunt and peck” method of verifying backups, JetSweep leveraged the Elastio Ransomware Recovery Assurance Platform (Elastio Platform), which:

- **Scanned all backups for hidden ransomware threats**, pinpointing the last known clean recovery point.
- **Detected dormant malware and encryption activity** that had evaded traditional endpoint protection solutions.
- **Enabled fast, confident recovery** by identifying a known-good backup within hours of deployment instead of weeks.

Key Benefits

- **Significant Time Savings:** Elastio Platform automated scanning identified a clean backup in hours, preventing weeks of manual effort.
- **Minimized Data Loss:** Elastio Platform identified that the most recent clean backup was 10 days old—had the attackers been in the system longer, recovery might not have been possible.
- **Risk Reduction:** Elastio Platform's off-host scanning ensured no reinfection after restoration.
- **Enhanced Detection & Prevention:** Elastio Platform's ongoing backup monitoring will enable early threat detection, stopping ransomware before it spreads.

"For a SaaS company, long-term downtime is the kiss of death. If you can't meet your SLAs, it can be an extinction-level event."

— Jeff Fudge, Director of Cloud Solutions, JetSweep

Impact

Thanks to Elastio Platform, the SaaS company quickly restored services, avoiding **customer churn, SLA penalties, and reputational damage**. More importantly, they **implemented proactive backup scanning**, ensuring they could detect future threats before they could disrupt business operations.

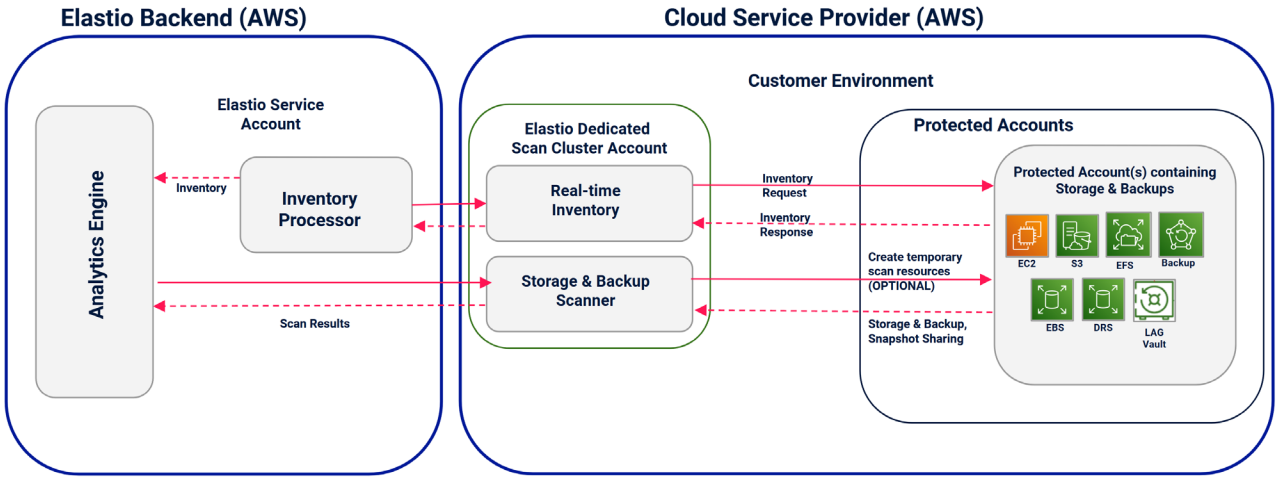
Instead of reacting to a breach after damage is done, Elastio Platform provides **early detection and faster recovery,** keeping businesses secure, even against advanced cyber threats.

Disclaimer

Details have been anonymized to protect the privacy and security of the affected organization. However, the core facts and recovery strategy remain unchanged to preserve the integrity of the lessons learned.

Elastio SaaS Deployment Architecture

Elastio Managed Scan Cluster Account



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.