COHESITY

SOLUTION BRIEF

Automated Response and Recovery from Ransomware

Service Orchestration, Automation, and Response

Key Benefits

- Lower ransomware risk
- Improve recovery/cyber resilience
- Reuse of existing controls and processes

With today's challenging cyber threats, organizations need to pay special attention to data anomalies that could indicate ransomware attacks or other malicious activity. They need to monitor all mission critical data with a modern data security and management platform like Cohesity that monitors ingested recovery data for anomalous changes. These anomalies can indicate an emerging attack that requires immediate investigation and response from security teams.

Ransomware attacks and other attacks create changes in data sets, anomalies that can be detected with analytics driven by machine learning. When anomalies do occur, security teams need to quickly investigate the anomaly and determine if an attack is underway. And they need to determine if production data has been compromised and should be restored to its last known good point.

Business Challenge

Improve Cyber Resilience

Cyber resilience depends on not only preventing incidents with traditional cybersecurity, but on effective recovery; recovery that enables organizations to confidently recover their business processes and data in hours vs days. Organizations need to quickly identify ransomware attacks and remediate any impacts as rapidly as possible.

Along with traditional cyber security controls, data anomalies provide early warning of ransomware attacks. Without anomaly detection integrated to existing incident response process,ransomware attacks may evade detection.

Automate the Response and Recovery to Data Anomalies with Cohesity and Palo Alto Networks CORTEX XSOAR

Cohesity and Palo Alto Networks XSOAR (XSOAR) helps organizations quickly identify emerging ransomware and leverage their security operations' investigation and response processes to thwart attacks. Powered by XSOAR you can reduce risk with investigation and response controls that improve ransomware detection and recovery.

Confident, Reliable Ransomware Remediation and Recovery

Ransomware targets production data with encryption that renders data unusable. Cohesity anomaly detection can spot changes in data and enrich SOC visibility into active ransomware threats with insights. With XSOAR and Cohesity, organizations can correlate, triage, investigate, and respond to ransomware incidents in one location. This enables organizations to rapidly identify, investigate, and remediate ransomware attacks and automatically recover impacted data.

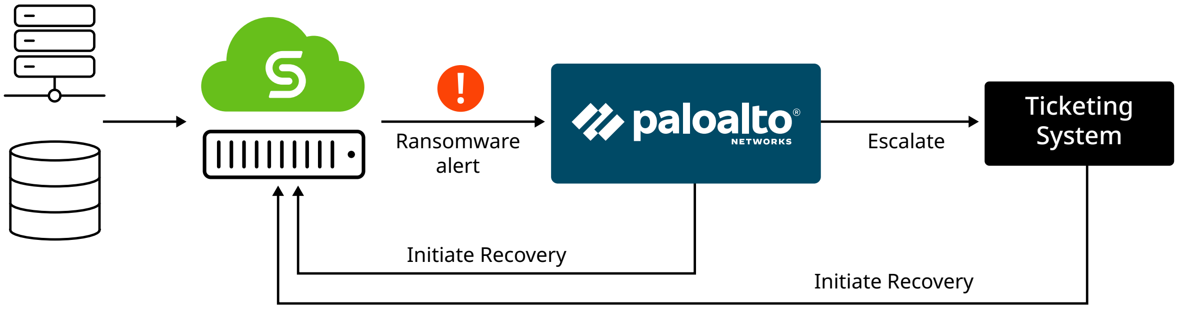

Figure 1: Palo Alto Networks CORTEX XSOAR and Cohesity Integration Architecture

To learn more, visit Cohesity Marketplace.