COHESITY | servicenow

SOLUTION BRIEF

Ransomware Protection and Recovery

Security Incident Response (SIR)

Key Benefits

- Enhance visibility of data protection alerts to eliminate blind spots.
- Automatic anomaly routing to launch incident response.
- Improve the accuracy and speed of ransomware response and recovery.

In the dynamic realm of cybersecurity risks, organizations must automate their response and recovery to counter diverse threats. This encompasses safeguarding their data security and management platform, which plays a crucial role in creating reliable backups of vital data. Maintaining a dependable platform is vital to ensure the integrity of recovery data, especially in the presence of destructive cyber incidents such as ransomware.

And the daily processing of backup data provides early warning to ransomware and other cyber threats. By monitoring how data changes, Cohesity as a unique view of whether data is changing in a way that would indicate an attack. When these anomalies happen, organizations can leverage their ServiceNow event and security incident systems to automate and speed response; every second counts in these situations and automation lowers the risk of application and data disruptions.

Threats can be quickly remedied by automating the response and investigation of potential ransomware activity. The Cohesity and ServiceNow Security Incident Response (SIR) integration will allow security teams to quickly respond to emerging threats and ensure the organization can recover with speed and confidence.

Business Challenge

Collaboration and Automation of Data Protection and Security Operations

To effectively combat the escalating wave of ransomware attacks, it is imperative for SecOps and Data Protection to integrate and collaborate on ransomware response. However, traditional security measures and outdated data protection solutions pose significant challenges for these enterprise teams. These challenges include:

1. **Complexity**: Operations professionals engaged in countering attacks often find themselves investigating incidents across multiple consoles, lacking a reliable way to estimate ransomware recovery service level agreements (SLAs). This complexity introduces additional risk to the business.

2. **Siloed Visibility**: When ransomware attacks occur, enterprises often realize that they lack unified visibility into their data. This lack of comprehensive insight increases dwell time, hampering swift response and containment.

3. **Slow Remediation**: Manual coordination becomes a necessity for teams, as they are compelled to involve multiple groups scattered across operational silos in the investigation and recovery process. This manual coordination leads to business disruptions and places an additional burden on employees, resulting in burnout.

To effectively address these challenges, it is crucial for organizations to seek modern solutions that foster collaboration, streamline processes, and provide comprehensive visibility into data.

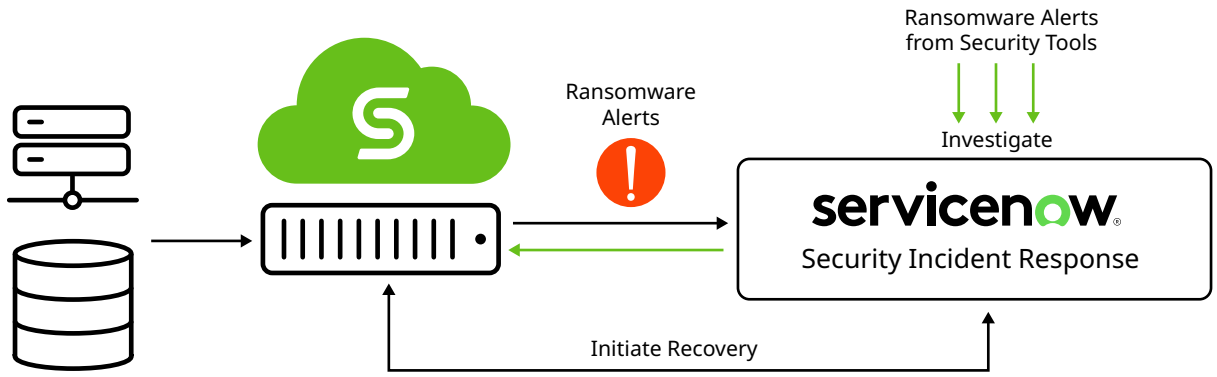

Figure 1: ServiceNow and Cohesity Architecture

Integrated Ransomware Protection and Security

The integration of Cohesity and ServiceNow brings significant improvements to ransomware defense and response by providing immediate visibility and context to anomalies detected in production data to the event and security teams. This integration enables IT administrators and Security Operations Centers (SOCs) to have simultaneous access to alerts when a ransomware attack targeting enterprise data is identified.

With Cohesity and ServiceNow Security Incident Response organizations can leverage closed-loop detection and response for ransomware attacks via SOAR integration, adding to the existing capability to create workflows through their IT service management (ITSM) solution. This allows teams to rapidly access, and address threats based on the potential impact to the business.

ServiceNow product administrators can route alerts as ServiceNow security incidents. With automated playbooks, IT teams investigate, remediate and if appropriate recovery clusters that may have been affected by the incident.

To learn more, visit the Cohesity Marketplace

COHESITY