SentinelOne

SOLUTION BRIEF

SentinelOne for AWS Elastic Disaster Recovery

Cloud Ransomware On The Rise

Cloud adoption continues to rise as organizations lift, shift, modernize, and refactor applications to take advantage of the scalability, cost-optimization, and resiliency of the hybrid cloud. Infrastructure-as-a-service (IaaS) spending will reach $120 billion in 2022, a 30% increase from the year prior. However, as applications move to the cloud, existing code scanning approaches aren't sufficient as nearly 75% of workloads in production contain critical vulnerabilities. These vulnerabilities can be abused by adversaries to launch ransomware campaigns which can disrupt business operations and expose confidential data. Ransomware costs are steadily increasing – in 2021 the average cost of a ransomware or destructive malware attack was $4.62 million. That cost includes notification, lost business, and response costs but more importantly doesn't include the ransom payment. Organizations subsequently are not only investing in solutions to protect themselves from cyberattacks, but are also motivated to improve their resiliency and minimize the business disruption of potential ransomware events. For the modern enterprise, the availability and integrity of cloud resources are paramount to ensuring a smooth end-user experience and the continuance of business operations.

Business Continuity and Cloud Incident Response

If a workload is infected with ransomware, the security operations and cloud operations teams need to collaborate to stem the attack before it can move laterally, encrypt, and exfiltrate data. Traditional approaches to ransomware recovery may include restoring from backups, rolling over to a disaster recovery site, or tearing down and rebuilding systems; however, this can prove complex and time-consuming to orchestrate in the midst of an incident. While setting up disaster recovery failovers for critical systems is part of good cyber hygiene, it can be costly to maintain a logically separated parallel infrastructure, especially for on-premises environments. A new approach to disaster recovery which leverages the scalability and cost-efficiency of the cloud is needed to rapidly respond to and recover from ransomware.

SentinelOne partnered with Amazon Web Services (AWS) to create **SentinelOne for AWS Elastic Disaster Recovery**, a new integration with AWS Elastic Disaster Recovery (DRS) to insulate organizations against the damaging effects of ransomware. The combination of AWS DRS and the SentinelOne Singularity™ XDR Platform accelerates incident response by making it simple to remediate and recover from ransomware, minimizing downtime and data loss with fast, reliable recovery for on-premises and cloud-based applications.

SentinelOne for Amazon Elastic Disaster Recovery (DRS)

AWS DRS uses cost-effective storage, minimal compute, and point-in-time recovery to minimize downtime and data loss. Data is replicated from the source server (on-prem or in AWS) to readily

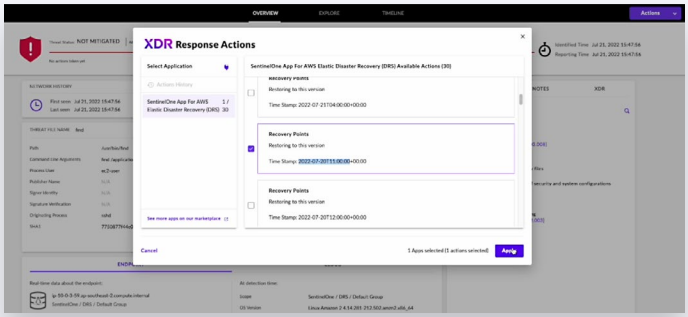
aws

KEY BENEFITS

- **Built in Static and Behavioral AI Analysis**
- **In-Depth Visibility**
- **Cloud Workload Protection**
- **Increased Resiliency**
- **Rapidly Recover from Ransomware**

accessible, low-compute disaster recovery service, enabling organizations to recover from ransomware attacks within minutes, whether they're based on-prem, hybrid, or cloud-native.

SentinelOne delivers malware protection, detection, and response for AWS workloads running in cloud compute instances, containers, and Kubernetes clusters. SentinelOne's patented Storyline™ technology provides analysts with real-time, actionable correlation and context, automatically linking, enriching, and visualizing all related events in a ransomware attack sequence. With Storyline, security teams can see the full context of the attack within seconds rather than needing to spend hours, days, or weeks correlating logs and linking events manually.



When SentinelOne detects behavior typical of ransomware, like the initial stages of encryption, it can automatically kill the related processes, quarantine the malicious file and remediate the threat. With SentinelOne for AWS Disaster Recovery, impacted organizations can initiate AWS DRS directly from the SentinelOne console, rolling back to the last-known-good state of the workload within minutes to ensure business continuity and exceed recovery time objectives. With Storyline context, SentinelOne can restore and rewind workloads from backup to before the attack occurred.

Conclusion

When combined with other SentinelOne Singularity Marketplace integrations such as ServiceNow Security Incident Response and SentinelOne integration for AWS Security Hub, organizations have a control plane for coordinating prevention, detection, response, and recovery across their enterprise cloud footprint with best-in-class tools that fit with their incident response and DevOps workflows.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY™

Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection.
- Top Analytic Coverage 3 Years Running
- 100% Real-time with Zero Delays

Gartner peerinsights™ 4.9 ★★★★★

99% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · AICPA SOC · TEVORA PCI DSS Attestation HIPAA Attestation · VB 100 VIRUS virusbtn.com · AAA · SE Labs BEST Innovator WINNER 2021

About SentinelOne

SentinelOne is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks at faster speed, greater scale and higher accuracy than human-powered technology alone. The Singularity XDR platform offers real-time visibility and intelligent AI-powered response. Achieve more capability with less complexity.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733