

Singularity RemoteOps

Power Forensics, Deep Investigation, and Response at Scale

When a threat is detected within an organization, time is the most crucial factor. Security teams do not have the time or resources to manually access hundreds of infected machines, one by one, to collect all relevant information to conduct an investigation and resolve the event. Any delay in the investigation and remediation workflow leaves a company vulnerable to a myriad of security risks. Security teams need a flexible and efficient solution for visibility and remediation.

SentinelOne Singularity RemoteOps permits customers to remotely investigate threats across multiple endpoints and remotely manage their entire fleet. The ability to run scripts allows incident responders to easily collect forensic artifacts, modify incident response tools, and more, to accelerate investigation and response workflows. RemoteOps empowers security teams to efficiently protect their enterprise from time-sensitive threats.



Enable Power Forensics at Scale

Time is one of the most significant aspects of cybersecurity. With RemoteOps, incident response (IR) teams and security analysts can run multiple forensic scripts and tools across their entire fleet to collect any relevant information to an attack, such as Memory Dumps, Event logs, MFT, YARA Scans and more.



Reduce mean time to respond (MTTR)

IR teams utilize RemoteOps to reduce MTTR while deploying actions against threats in real time, such as removing files and terminating processes. Quickly operate on attacks with a simple UI, and by creating automations with RemoteOps end-to-end API support.



Simplify Vulnerability and Configuration Management

Many organizations rely on a complex security stack, with unintentional gaps that leave them open to vulnerabilities. Consolidate management activities within a single console to identify potential security compromises, perform assessments, manage configurations and patch systems and softwares with RemoteOps.

Key Benefits

Accelerate

Quickly collect forensic data at scale for remediation

Automate

Automate response workflows to MTTR to minimize business impact

Simplify

Easily identify potential vulnerabilities and misconfigurations across the entire fleet and increase security defenses

- + Execute scripts from both a built-in script library and the option to upload customer scripts
- + Execute scripts directly from the SentinelOne console or via command-line interface
- + Investigate and analyze results at scale in Singularity XDR
- + Supports Windows, macOS and Linux - via the UI and/or API