SentinelOne ActiveEDR

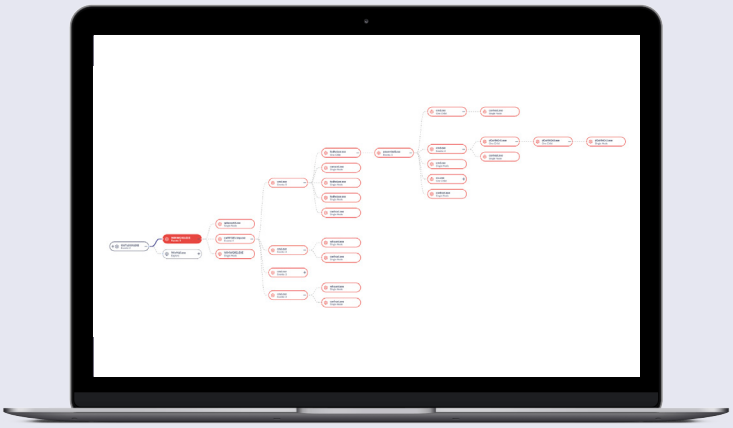
Powerful visibility, autonomous detection, automated response, and proactive hunting — Simplified

Enterprise security teams face multiple challenges when attempting to detect, investigate and remediate an advanced attack. Lack of visibility into critical control points, manual searches through large and disparate data sources that lack context and correlation, alert fatigue from poor signal to noise ratio, and difficulty containing the attack quickly disrupt business-critical processes, impact productivity and increase operating costs.

SentinelOne ActiveEDR™ is an advanced EDR and threat hunting solution that delivers real-time visibility with contextualized, correlated insights accelerating triaging and root cause analysis. The solution lightens the SOC burden with automated threat resolution, dramatically reducing the mean time to remediate (MTTR) the incident. ActiveEDR enables proactive hunting capabilities to uncover stealthy, sophisticated threats lurking in the environment.

Key capabilities

Detect high-velocity threats with patented Storyline™



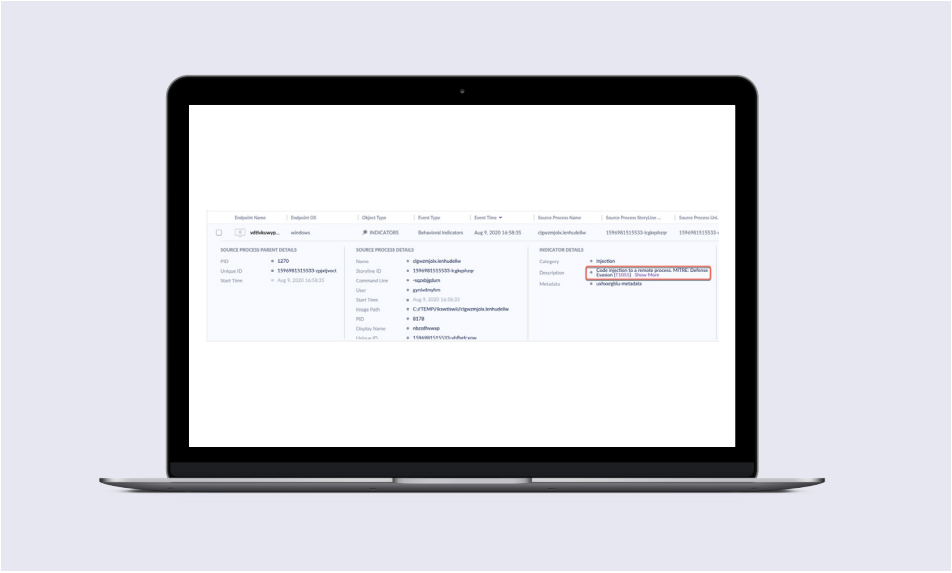
SOLUTIONS BENEFITS

+ Get high efficacy, actionable threat detection without the noise
+ Rapidly uncover and contain advanced threats to reduce incident dwell time and time to resolution
+ Get a complete understanding of the root cause to close existing gaps
+ Empower and uplevel the security team with an easy-to-use, intuitive product
+ Reduce SOC burden by automating manual tasks with automated correlation and one-click remediation
+ Single cloud-delivered platform with true multi-tenant capabilities to address the needs of global enterprises and MSSPs
+ Best-in-industry coverage across Linux, MacOS, Windows
+ Affordable EDR data retention of 365 days+ for full historical analysis

Storyline™ automatically correlates atomic events into unified context-rich stories that provide campaign level insights.

ActiveEDR, powered by SentinelOne's patented Storyline technology, provides analysts with real-time, actionable correlation and context and lets security analysts understand the full story of what happened in their environment. Storyline automatically links all related events and activities together an attack storyline with a unique identifier. This allows security teams to see the full context of what occurred within seconds rather than needing to spend hours, days, or weeks correlating logs and linking events manually. SentinelOne's behavioral engine tracks all activities on the system, including file/registry changes, service start/stop, inter-process communication, and network activity. It detects techniques and tactics that are indicators of malicious behavior to monitor stealthy behavior and effectively identify fileless attacks, lateral movement, and actively executing rootkits. SentinelOne automatically correlates related activity into unified alerts that provide campaign-level insight. This reduces the amount of manual effort needed, helps with alert fatigue, and significantly lowers the skillset barrier of responding to alerts.

Accelerate investigations with seamlessly integrated MITRE ATT&CK techniques



Correlate multiple MITRE detections to the same Storyline to reduce manual investigation times and alert fatigue for SOC.

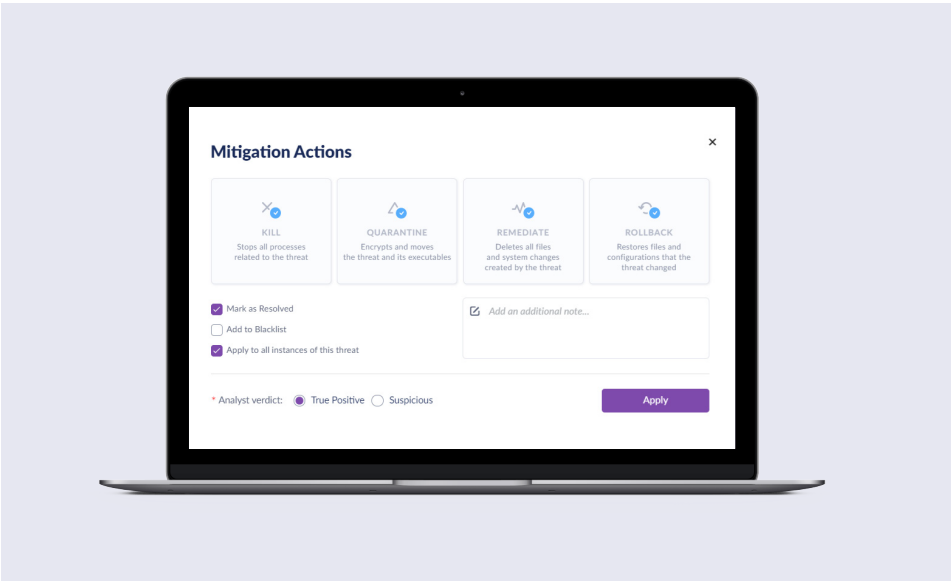
SentinelOne ActiveEDR maps attacks in real-time to the MITRE ATT&CK framework, providing analysts immediate in-product indicators and attack technique context. SentinelOne correlates multiple MITRE observations to the same Storyline, making searching for MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) fast and painless across your environment. It's as easy as entering the MITRE technique ID and using this to perform investigations, enabling the security team to understand complex detections quickly.

Remediate the entire attack with patented 1-click remediation & rollback

SentinelOne enables analysts to take all the required actions needed to respond and remediate the threat with a single click. With one click, the analyst can execute a full suite of remediation actions such as network quarantine or killing a process to remove persistence mechanisms. Rollback functionality automatically restores deleted or corrupted files caused by ransomware activity to their pre-infected state without needing to reimage the machine. SentinelOne one-click remediation simplifies response and dramatically reduces mean time to resolution. SentinelOne also offers full Remote Shell capabilities on all platforms to give your security team a quick way to investigate attacks, collect forensic data, and remediate breaches no matter

Remediate the entire attack storyline with a single click, accelerating threat resolution.

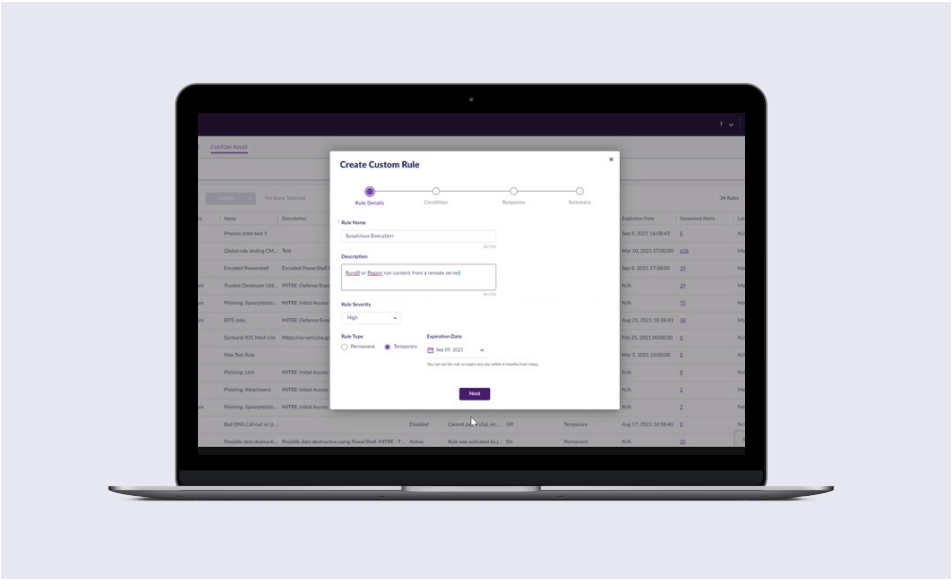
where the compromised endpoints are located. This eliminates uncertainty and significantly reducing any downtime that results from an attack.



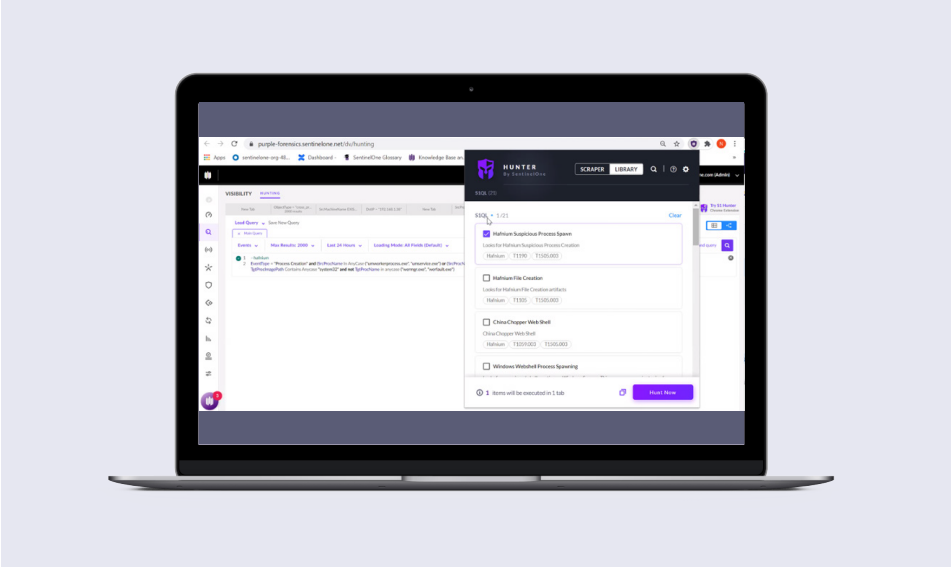
Customize EDR to your environment with STAR™

Modern adversaries are automating their techniques, tactics, and procedures to evade preventative defenses, so it makes sense that enterprise security teams can better keep up with attacks by automating their manual workloads. SentinelOne enables customers to leverage the insights Storyline delivers and create custom automated detection rules specific to their environment with Storyline Active-Response (STAR). STAR lets enterprises incorporate their business context and customize the EDR solution to their needs. With STAR custom detection rules, you can turn Deep Visibility queries into automated hunting rules that trigger alerts and responses when rules detect matches. STAR gives you the flexibility to create custom alerts specific to your environment that can enhance alerting and triaging events.

Create custom alerts specific to your environment with automated hunting rules.



Proactively hunt to uncover advanced adversaries



Empower hunting teams to easily uncover and stop advanced hidden attacks with an intuitive user interface.

SentinelOne's Deep Visibility empowers rapid threat hunting capabilities to conduct a deep investigation and enable hunting at scale. Threat hunters can quickly and easily query and pivot across the captured endpoint telemetry. SentinelOne automatically correlates all related objects (processes, files, threads, events, and more). For instance, say a process modifies another process by injecting code. When you run a query, all interactions between the source process, target process, and parent process are shown clearly in the cross-process details. This lets threat hunters quickly understand the data relationships: the root cause behind a threat with all of its context, relationships, and activities and enable them to understand the full story of what happened on an endpoint and see the complete chain of events.

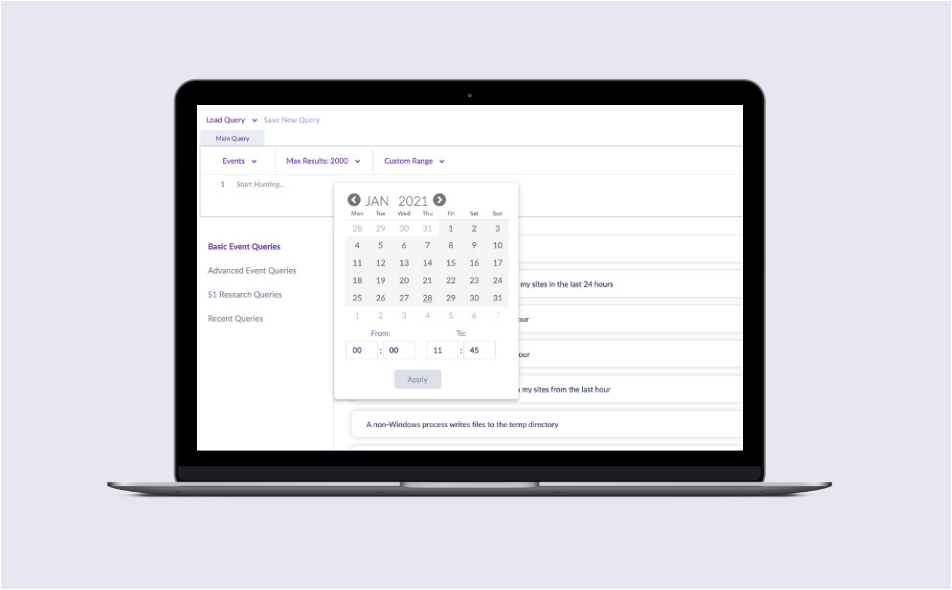
You can create powerful hunting queries with easy-to-use shortcuts. Leverage a query library of hunts curated by SentinelOne research who continually evaluate new methodologies to uncover new IOCs and TTPs. These insights are the output of hypotheses that are proven across research data and are generic. For example, the use of unmanaged, unsigned Powershell is likely abnormal in most environments; and would commonly require additional investigation. The above example is not malicious in and of itself but fits in a hunting workflow, as they are descriptive of anomalies.

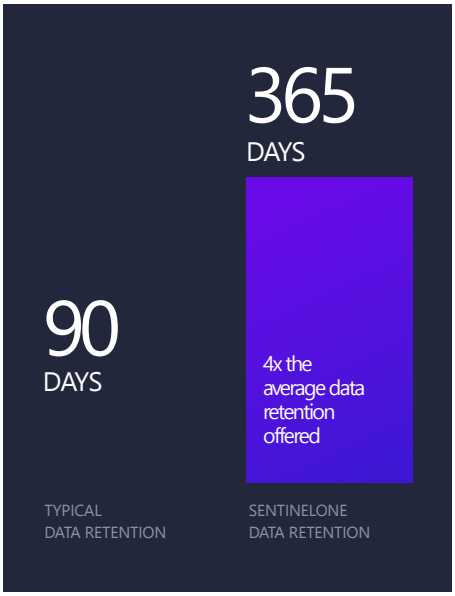
SentinelOne Hunter, a Chrome Extension, helps Security Operations and hunters save time. Hunter lets you quickly scrape data from your browser and opens a query in your SentinelOne Management Console to search for that data across your organization. Hunter captures these indicators from information open in your current browser tab: IP addresses, DNS names, and hashes (MD5, SHA-1, and SHA-256). When the indicators of interest are captured, they are redirected to your SentinelOne Management Console. The Hunter extension does not capture any personal or private data from the browser or the user.

Investigate historical data with affordable extended data retention

EDR data retention of 365 days and beyond, for full historical analysis of any attack.

The ability to look back into any point in time allows analysts to see if the threat has targeted your organization in the past and view the full stream of information on how that attack occurred, including the entire process tree, timeline, and related activities. SentinelOne provides visibility

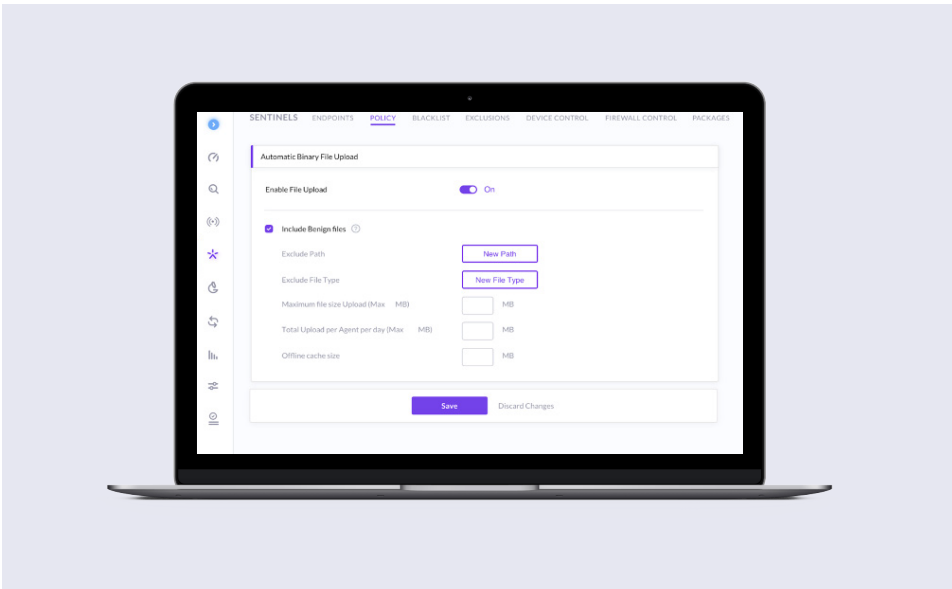




into your environment with 365 days and beyond of EDR data to let your team analyze incident activities and conduct historical analysis within the same UI.

Upload executables to the cloud for automated analysis workflows with Binary Vault

Analysts often want to be aware of new, unique executables in the environment so that they may be further scrutinized for forensic analysis. Binary Vault lets you automatically upload benign and malicious executables to the SentinelOne Cloud, where they are stored for 30 days. These samples are easily downloaded from the console or via API for local forensics analysis or additional investigation workflows. Only unique executables are uploaded. For example, any standard set of binaries will be identical across the enterprise. This function delivers one copy of each newly detected binary to the vault as it is discovered so that it may enter the SOC dynamic analysis and reverse engineering workflow. Files can be retrieved from the SentinelOne console from a threat's incident details or Deep Visibility, or downloaded via API.



Stream telemetry locally to automate SOAR workflows with Cloud Funnel

SentinelOne Cloud Funnel enables secure, near-real-time streaming of EDR telemetry from SentinelOne Deep Visibility to your data lake via a Kafka subscription. SentinelOne Deep Visibility aggregates endpoint telemetry data in the cloud from your fleet of autonomous Sentinels, where AI reveals hidden threats, correlates activity, and delivers actionable insights. A Kafka subscription securely sends your telemetry to your own data lake. Your connection to Deep Visibility is secured via TLS 1.2+, and access is governed by SCRAM (Salted Challenge Response Authentication Mechanism) supported by Kafka. When new data is available, Kafka streams to your data lake. Once there, Security teams may take any number of actions on their EDR data, such as correlation with non-SentinelOne data sources, integration with SIEM tooling, and orchestration and enrichment of security incident workflows.

Gartner peerinsights

"SentinelOne smokes the competition."

★★★★★

Sr. Director, Cybersecurity
Retail, 1B - 3B USD

Gartner peerinsights

"Easy and effective EPP and EDR."

★★★★★

Security Analyst
Manufacturing, 3B - 10B USD

Gartner peerinsights

"One of the greatest EDRs I have used to date!"

★★★★★

Security and Risk Management
Healthcare, 3B - 10B USD

SOLUTION HIGHLIGHTS

+ Real-time detection and remediation of complex threats with no need for human intervention
+ Accelerated triage and root cause analysis with incident insights and the best MITRE ATT&CK alignment on the market, with or without MDR
+ Integrated threat intelligence for detection and enrichment from leading 3rd party feeds as well as our proprietary sources
+ Patented 1-Click Remediation & Rollback
+ Intuitive user experience reduces the skills required to add threat hunting to your security operations
+ Data retention options to suit every need, from 14 to 365+ days. Hunt by MITRE ATT&CK Technique
+ Uncompromising protection across Windows, Linux, and macOS endpoints - physical, virtual, container - cloud or data center
+ Rapid deployment interoperability features ensure a fast, smooth rollout
+ RESTful APIs and pre-built integrations to various Enterprise applications and services

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

Gartner peerinsights 4.9 ★★★★★

98% of Gartner Peer Insights ™ Voice of the Customer Reviewers recommend SentinelOne

FedRAMP · SOC 2 Type II · ISO 27001 CERTIFIED by schellman · VB 100 VIRUS virusbtn.com · SOC 2 Type II · TEVORA PCI DSS Attestation HIPAA Attestation

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Their technology is designed to scale people with automation and frictionless threat resolution. Contact us to discuss if this is the solution you need.

UVSINC.COM/Technology

TechSales@uvsinccom
866-613-4747