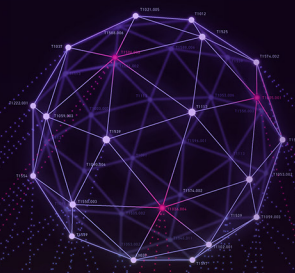
SentinelOne

SOLUTION BRIEF



SentinelOne Storyline Active Response (STAR)™

Customize EDR to adapt to your environment.

Modern adversaries are continually automating their techniques, tactics, and procedures (TTPs) to evade defenses. Hence, it makes sense that enterprise security teams should also stop the latest threats and identify ongoing campaigns in their environment. Machine-learning and rules-based detections capture unusual behaviors and common threats. However, they often require new agent logic, and updating your entire fleet to the latest agent to stop a new threat may not always be possible. Similarly, with EDR data producing millions or even billions of events a day, security teams need a way to look for the interesting behavioral and static indicators of compromise (IOCs) that might indicate a zero-day attack. While robust EDR data helps investigations, it may prove too noisy for useful alerting or discovering unusual behaviors.

Singularity ActiveEDR® provides advanced detection capabilities, best in class visibility, and allows the end-user to write custom detection rules that address new threats or targeted threats specific to their industry or organization with Storyline Active Response (STAR)™. STAR, lets enterprises incorporate custom detection logic and immediately push it out to their entire fleet, or a subset, to either kill any matching process or alert on it for further investigation. STAR can alleviate SOC burden as it can be used as a powerful policy enforcement tool, automatically mitigating threats and quarantining endpoints. STAR can also add a new layer between threats and EDR data that can alert on a subset of interesting events instead of the entire dataset. This data can be easily consumed into a SIEM, bringing down the cost of using EDR data in a SIEM while making sure that no interesting events slip by.

How STAR Works

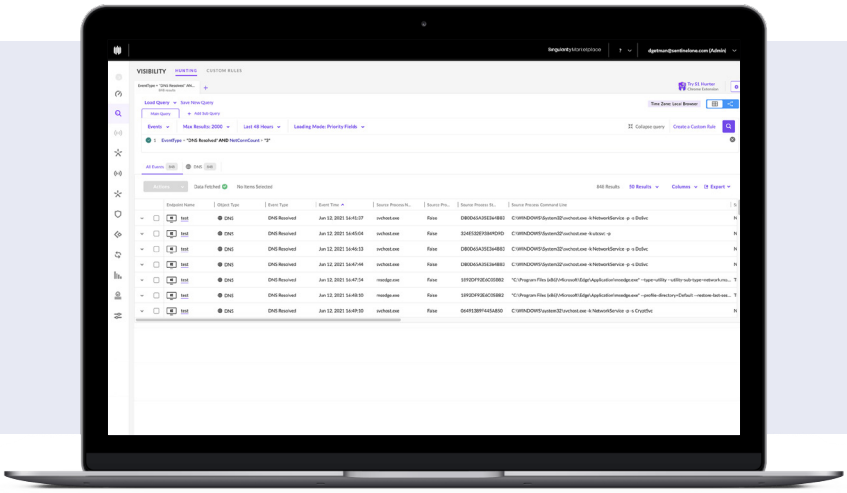
ActiveEDR comes with a default set of behavioral detection rules created by high-level research teams and provides endpoint protection from day one. SentinelOne enables customers to leverage these insights with STAR. With STAR custom detection rules, SOC teams can turn Deep Visibility queries into automated hunting rules that trigger alerts and responses when rules detect matches. STAR also allows users an automated way to look at every endpoint event collected across their entire fleet and evaluate each of those events against a list of rules.

STAR BENEFITS

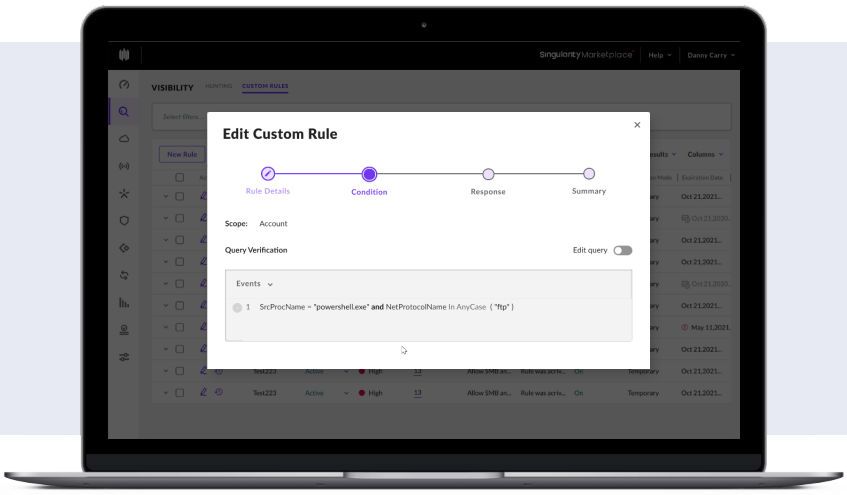
+ Stay ahead of adversaries by customizing and automating detection rules that fit your business and environment.
+ Proactively monitor and respond by turning queries into automated hunting rules.
+ Easy to use, powerful, flexible Deep Visibility query language with regular expression support for complex queries.
+ Enable alerts in Syslog for quick triage and SIEM integration.
+ Automate flexible response capabilities based on your environment: Chose to get alerts or define custom response actions such as network quarantine.
+ Get superior protection compared to watchlists with granular response actions.

Creating a STAR rule is as simple as four steps.

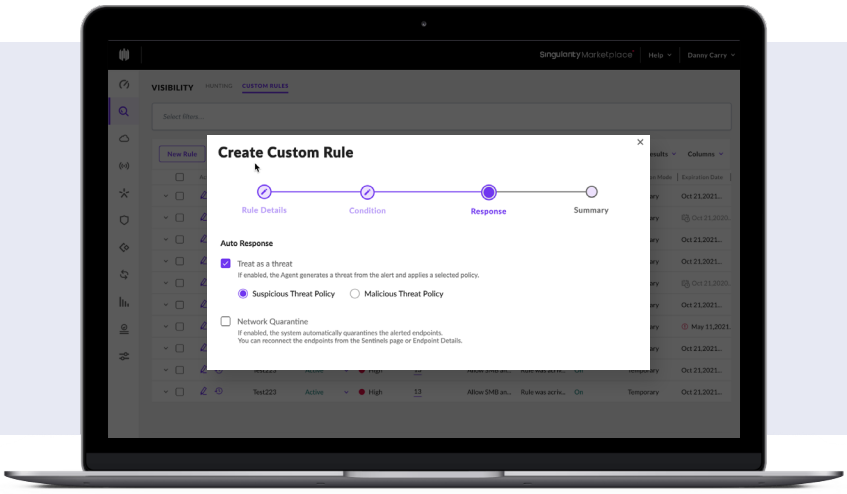
01 | Write a query in Deep Visibility or create a new custom rule



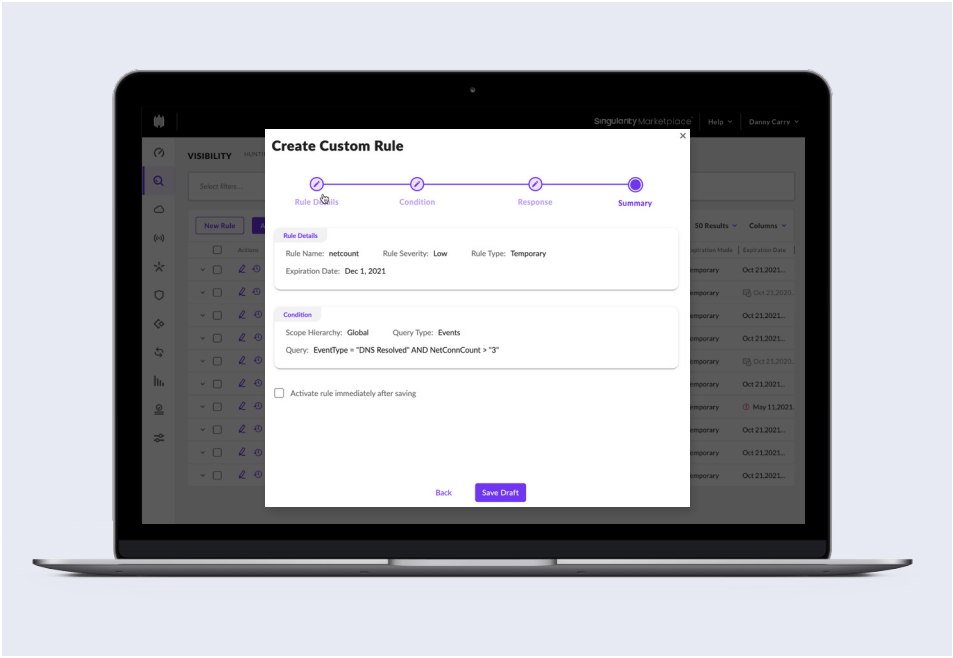
02 | Add event condition



03 | Designate response actions



04 | Save the rule



Gartner peerinsights™

"Great technical solution, excellent support and service, continuous evolution."

★★★★★

GLOBAL CISO
Media, 1B - 3B USD

Gartner peerinsights™

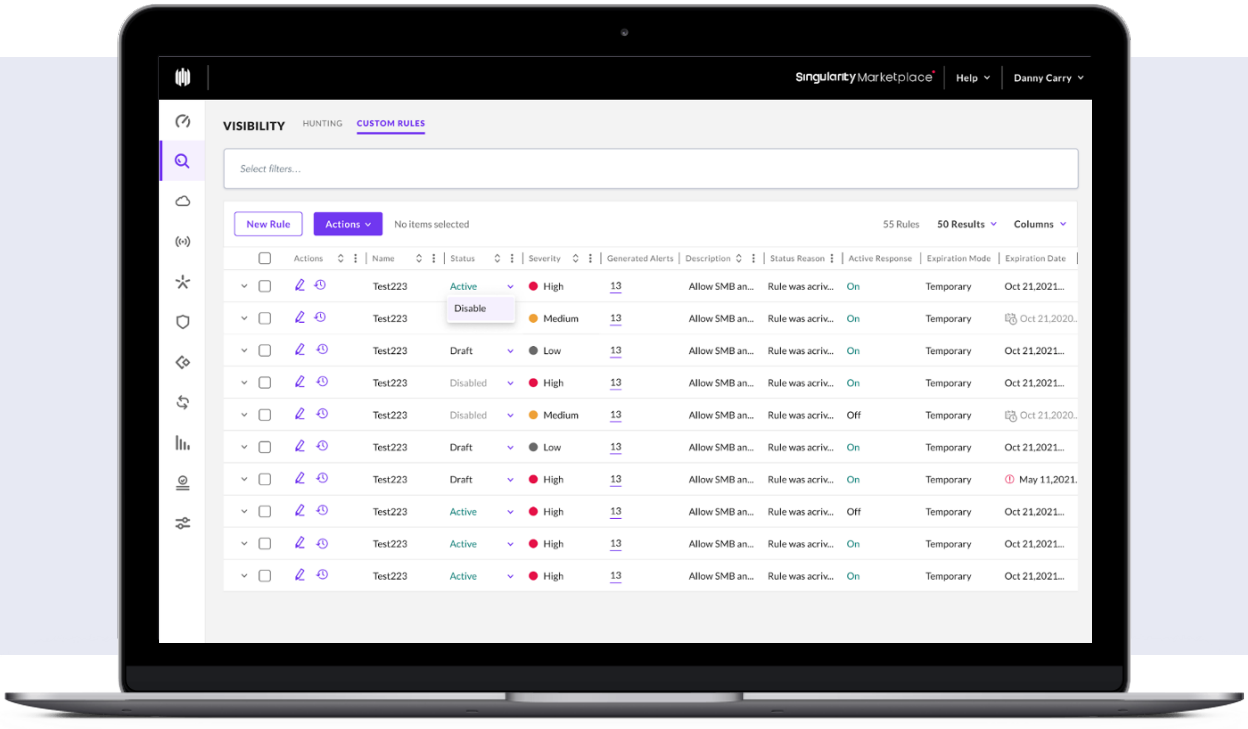
"Great product focused on automation and efficiency!

The API-first interface makes it simple to write custom automation... to build forms for policy creation/modification.

★★★★★

LEAD SYSTEM ENGINEER
Media, 3B - 10B USD

STAR allows users an automated way to look at every endpoint event collected across the organization in real-time and evaluate each of those events against a list of rules. STAR evaluates every endpoint event collected against every STAR rule. For large enterprises, STAR evaluates each event, in a stream of a billion daily events, against up to 1,000 STAR rules. It does this by working with Deep Visibility, SentinelOne's EDR data collection and querying mechanism. Deep Visibility collects billions of events a day, so many that it detected every step of the 176-step attack in the latest MITRE test. STAR leverages that industry-leading technology and query language to write criteria that determine, in near real-time, if a collected event is part of a threat or is suspicious.



What makes STAR invaluable is the set of response tools it puts in the users' hands when an event matches its criteria. The engine not only integrates with Deep Visibility but also with the agent. By checking a box when creating a rule, the analyst can enable STAR to kill any process that matches a STAR rule. By checking a different box, the user can enable STAR to automatically quarantine any device that sees a matching event. Rules can also be written to detect suspicious events and alert on them, allowing the users to then consume those alerts in the UI or via Syslog for further analysis in a SIEM.

Gartner peerinsights™

"SentinelOne believes in their product and that is clear in the delivery in the solution.

★★★★★

HEAD OF SECURITY OPERATIONS
Manufacturing, 30B+ USD

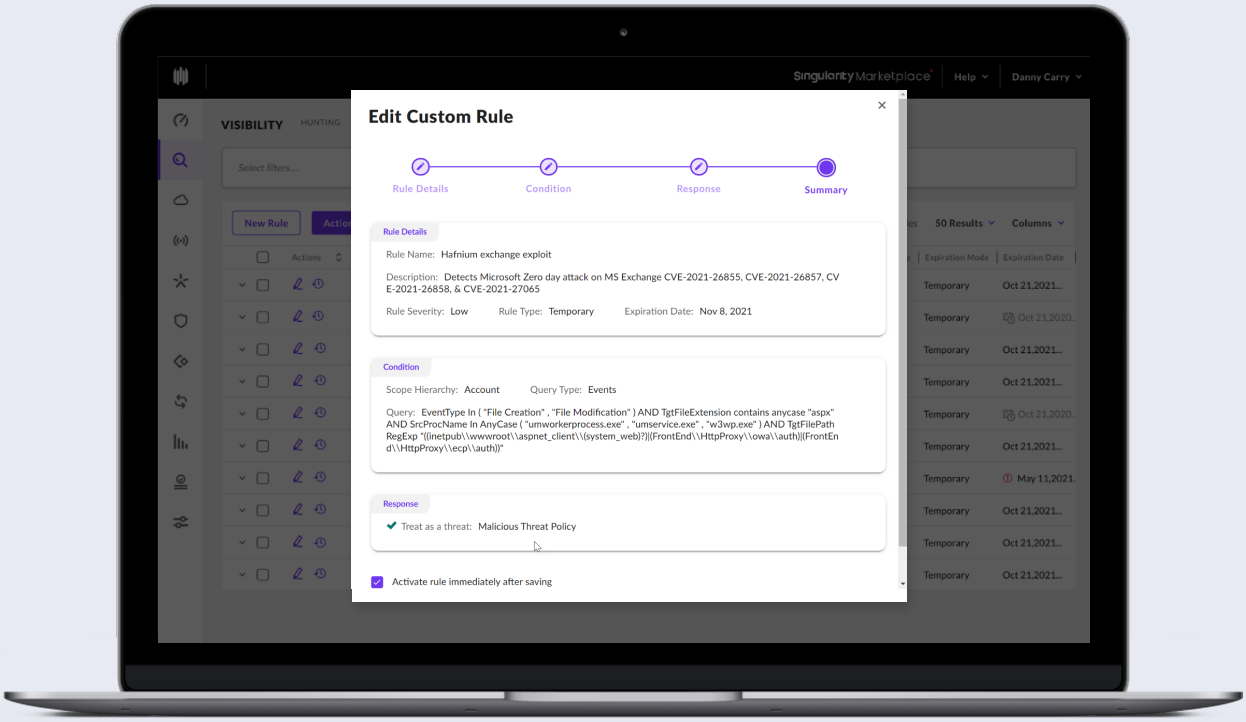
Key STAR Use Cases:

STAR has two main functions within a SOC, and most customers find value in both.

01 | Mitigate new and emerging zero-day threats

No SOC Analyst wants to depend entirely on a vendor to protect from bleeding-edge attacks or novel threats emerging in niche locations or industries. As soon as they see a new threat emerge, analysts want the ability to write a rule that will detect and prevent that threat. Teams deeply value having the power to write their policy when they need to. STAR allows users to write rules that look for highly specific threats to their environment and automatically kill those threats.

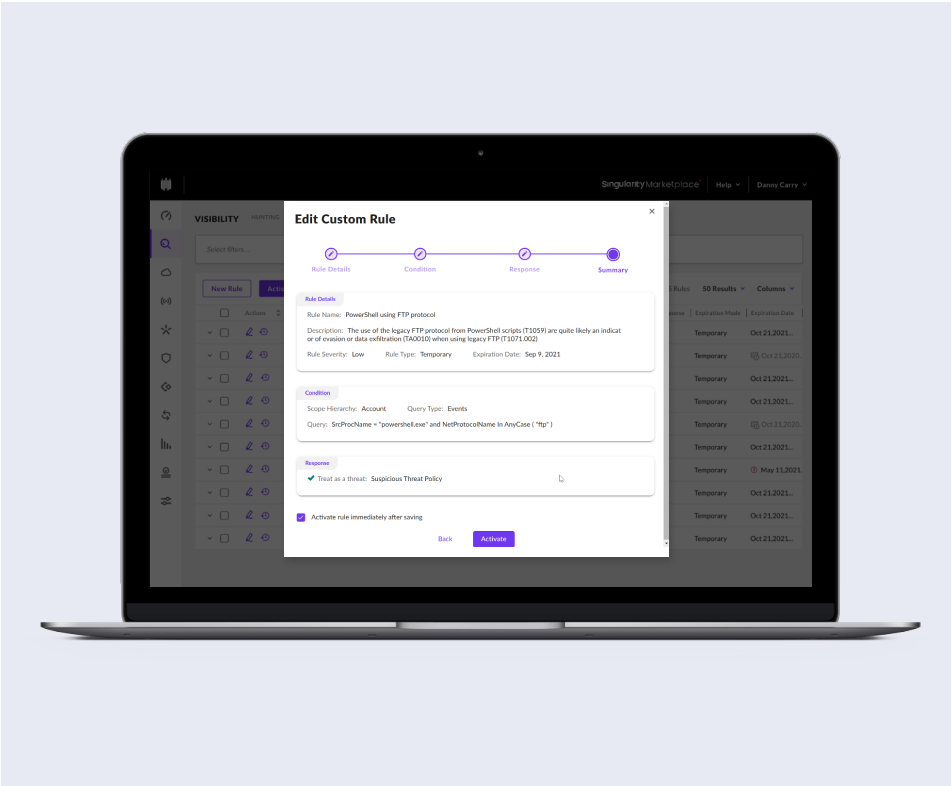
The below screenshot shows an example of a STAR rule to detect Hafnium Exchange zero-day threat.



02 | Augment SIEM data with low volume, high-value telemetry

STAR allows users to generate new data points, highlighting suspicious behavior in their environment for automated cross-correlation in a SIEM or manual investigation. Security teams also find data to be invaluable. SentinelOne has quickly become known for its industry-leading EDR visibility and longer default retention. STAR builds on that story with the ability to generate alerts on almost anything. Customers leverage that data via UI, API, and Syslog to stitch together complicated attacks and shut them down.

The below screenshot shows an example of a STAR rule to find a compromised computer using FTP to exfiltrate data.



STAR USE CASES

+ Mitigate new and emerging zero-day threats with custom detection rules.
+ Augment SIEM and Data lake data with low volume, high-value telemetry.
+ Trigger automated workflows.
+ Replace watchlists.
+ Automate hunting queries.

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 · ISO 27001 CERTIFIED by schellman · VB 100 VIRUS virusbtn.com · 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. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

sentinelone.com

sales@sentinelone.com

+ 1 855 868 3733