SOLUTION BRIEF

Self-Healing Endpoint Security

Maintain and Prove Protection against Evolving Threats

Security teams know they are in a constant race against evolving cyber threats, where even advanced endpoint protection can degrade over time. New attack techniques, environmental changes and control misconfigurations continuously introduce gaps that attackers can exploit.

Modern endpoint security platforms combine behavioral and signature-based prevention with detection and response to deliver broad coverage across MITRE ATT&CK tactics. Maintaining this protection requires continuous validation and adaptation. To stay resilient, security teams must:

- Adapt to emerging threats as they evolve
- Identify and address security drift
- Continuously validate and optimize controls

Continuous Validation and Optimization

Cymulate and SentinelOne deliver self-healing endpoint security by combining advanced protection with continuous validation. SentinelOne Singularity Endpoint provides prevention, detection and response, while Cymulate validates its effectiveness against real-world attack techniques.

With Cymulate Auto Mitigation, organizations move beyond identifying gaps to automatically closing them. Cymulate continuously tests SentinelOne controls and, when gaps are identified, generates and deploys mitigations directly to the platform.

This includes:

- Automated updates of indicators of compromise (IoCs) for immediate prevention
- Automated generation and direct deployment of SentinelOne detection rules
- Continuous validation and re-testing to confirm mitigation effectiveness
- Detection of security drift caused by configuration or environmental changes

Together, Cymulate and SentinelOne create a closed-loop system that strengthens endpoint protection, reduces manual effort and keeps defenses aligned with evolving threats.

Production-Safe, Automated Security Validation

Cymulate delivers production-safe validation using SaaS-based threat emulation and a lightweight test point to simulate real-world attacks across endpoints. This approach validates SentinelOne's ability to prevent and detect threats, including IoCs, exploits and advanced TTPs (tactics, techniques and procedures). Through integration with the SentinelOne API, Cymulate confirms detection effectiveness by validating alerts and attacker activity logs.

Solution Benefits

Continuous validation

Automated continuous testing proves security effectiveness.

Maintain prevention

Automated updates to block the latest threats.

Optimize detection

Configure, test and tune detection rules to minimize false positives and optimize threat coverage.

Identify drift

Detect changes to threat coverage from control or infrastructure updates.

Optimize Threat Prevention

With a daily update of the latest threats, Cymulate continuously tests and proves the effectiveness of Singularity Endpoint to block advanced cyber attacks. When threats are not prevented, Cymulate Auto Mitigation automatically generates the relevant IoCs and deploys them directly to SentinelOne for immediate protection.

IoCs can be deployed in multiple ways: individually, in bulk, or automatically based on predefined policies. This flexible deployment model ensures rapid and continuous threat prevention without manual effort.

Optimize Threat Detection and Response

For threats requiring detection, Cymulate validates SentinelOne Singularity Endpoint's ability to detect and log advanced TTPs. When gaps are identified, Cymulate Auto Mitigation generates vendor-specific EDR detection rules based on observed attack behavior and deploys them directly to SentinelOne. Each rule includes a quality ranking to help balance detection coverage and operational risk; higher-ranked rules provide more precise detection, while broader rules may require tuning in complex environments.

After deployment, Cymulate re-runs the simulation to confirm detection effectiveness and validate that the mitigation is working as intended. Once validated, security teams can promote detection rules to prevention within SentinelOne to further strengthen protection.

Baseline Security Posture and Identify Security Drift

By continuously validating Singularity Endpoint against new threats, exploits and the latest techniques, Cymulate provides security teams and leaders with evidence-based metrics for threat prevention and detection with trending and baselining of those results over time. Dashboards and reports make this trending data easily accessible for security leaders to present in executive meetings, create board reports and share with auditors.

Because updates to control configurations and changes in IT infrastructure can impact security posture, security teams rely on Cymulate to identify security drift. With continuous validation and correlation of previous results, Cymulate highlights any decreases in threat coverage while providing the mitigation path in the form of new IoCs or detection rules.

Why Choose Cymulate for Validating and Optimizing SentinelOne?

Automated Validation

Over 490 test scenarios using thousands of known malicious file samples and behaviors to simulate real-world attacks.

Production safe

The full suite of test cases is completely production-safe and will not harm endpoint environments.

Adapt to New Threats

Actionable and automated findings to maximize threat prevention and optimize detection for the most effective threat coverage.

About Cymulate

Cymulate is the leader in proactive, AI-powered security that continuously proves, prioritizes and adapts against real attacker behavior – before incidents occur. More than 1,000 enterprise security teams rely on Cymulate for autonomous threat validation and cyber defense engineering. Founded and led by experienced red teamers who know that testing alone does not deliver better security, Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.