Advanced cybersecurity protection with SentinelOne

next generation endpoint and sever security

Dealing with today's cyber threats requires a fundamentally different approach, SentinelOne does just that

Key Benefits

- 24x7 security operations center monitoring alerts
- Immediate risk identification
- Effective response, quick remediation
- Ransomware rollback
- High-fidelity, data-driven escalations reduce false positives and provide context to critical in

Antivirus only solutions don't cut it. **Today's advanced malware, exploits, and other cyberattacks will blow right by AV-based solutions in a fraction of the time it takes to get updated with the latest threat signatures. Prevention should never be your last line of defense, no matter how sophisticated your static analysis claims to be.**

Vulnerability exists in the gap between detection and response. **Even when an attack is detected, that attack can still proliferate to other areas of your infrastructure. The key to effective endpoint security lies in the ability to intelligently uncover and behaviorally detect advanced threats, and respond at machine speed.**

SentinelOne unifies prevention, detection, incident response and remediation in a single platform driven by sophisticated machine learning and intelligent automation, and is backed by a security operations center.

With coverage from multivariant ransomware attacks to the latest cryptomining infiltrations, advanced endpoint threat management from Microtel coupled with SOC monitoring and remediation services stops active threats and minimizes harm.

Protect endpoints across *every* threat vector

Deep system-level monitoring
Deployed on each endpoint, SentinelOne's lightweight autonomous agent monitors all activity in both kernel and user space (including files, processes, memory, registry, network, etc.). The agent is virtually silent and will never degrade user productivity.

Intelligent, signature-less static prevention
As a first line of defense, SentinelOne's Deep File Inspection (DFI) engine expertly uncovers and blocks known and unknown file-based malware, leveraging advanced machine learning algorithms instead of signatures.

Behavioral detection of advanced attacks
SentinelOne broadens protection against advanced threats through cutting-edge behavior-based detection. SentinelOne's Dynamic Behavior Tracking (DBT) Engine detects any type of malicious activity—from polymorphic malware to sophisticated exploits to stealthy insider attacks—against a full context of normal system activity.

Respond automatically

Zero-touch mitigation and containment
SentinelOne's fully integrated, policy-driven mitigation covers all endpoints—local and remote — allowing for decisive incident response that makes dwell time a thing of the past.

Upon detection, SentinelOne i mmediately stops lateral threat spread cold by swiftly killing malicious processes, quarantining infected files, or disconnecting the infected endpoint device from the network while still maintaining the agent's connection to the man-agement console.

Full remediation
Easily reverse malware-driven modifications to registry and system settings.

Single-click rollback
Instantly restore any compromised files back to their previous trusted states

Auto-immunization
Each time SentinelOne finds a new, never-before- seen malicious binary, it instantly flags it and notifies all agents on the network, rendering other endpoint devices immune to the attack.

Microtel Systems
804 254-2057
microtelsystems.com