SentinelOne™

Attivo NETWORKS®

# ATTIVO NETWORKS® THREATDEFEND® PLATFORM INTEGRATION WITH THE SENTINELONE SINGULARITY XDR PLATFORM

Attivo Networks has partnered with SentinelOne to give organizations early and accurate in-network threat detection, better protection at the endpoint, and automated incident response to block and quarantine attackers before they spread. The joint solution improves security through the rapid detection of and response to an attacker's attempts to move laterally across the network. The partnership provides company-centric threat intelligence to improve defenses and elevate the organization's security posture, reducing the time and resources required to detect threats, analyze attacks, and remediate infected endpoints.

## HIGHLIGHTS

- Early and Accurate Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine and Blocking
- Faster Incident Response

## THE CHALLENGE

Attackers have demonstrated their ability to bypass perimeter defenses and infiltrate networks through many tactics, such as reusing stolen credentials, exploiting zero-day vulnerabilities, using ransomware, or starting as an insider. Once attackers have established a beachhead, they will move laterally throughout the network, expanding their footprint until they can find the data they are looking for and complete their mission.

Detecting threats that are already inside the network is challenging. Once they have broken in, identifying these attackers requires a different approach that does not rely on recognizing known signatures or analyzing patterns of behavior. This detection method denies attackers from discovering sensitive or critical accounts and assets,

detects their credential theft and privilege escalation activities and derails their lateral movement and data collection attempts. This early and accurate detection allows organizations to respond to incidents quickly, deny attackers the ability to remain inside the network undetected, and develop company-specific threat intelligence on their activities to improve the security posture and strengthen defenses.

## THE ATTIVO THREATDEFEND PLATFORM AND SENTINELONE JOINT SOLUTION

The partnership between Attivo Networks and SentinelOne gives organizations an integrated defensive strategy that takes advantage of both the ThreatDefend platform and the Singularity XDR platform. The joint solution provides early, and accurate threat detection coupled with the ability to quarantine a compromised endpoint instantly. Whether it is an automated attack or a human attacker, the joint solution can reduce the risk of a breach through rapid detection, triage, and response. Additionally, the Attivo Endpoint Detection Net (EDN) solution complements the SentinelOne Singularity XDR platform to improve detection rates. It adds the ability to map how adversaries execute their attacks, denies them access to the data they seek, detects their activity quickly, and derails them with misinformation along each step of the attack.
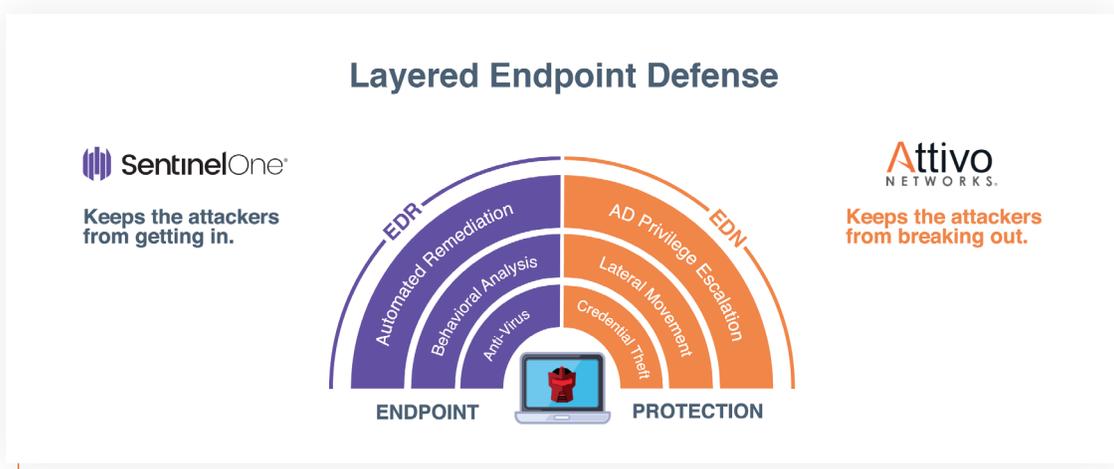
# ATTIVO NETWORKS THREATDEFEND PLATFORM

The Attivo Networks ThreatDefend® Platform provides early and accurate detection of in-network threats, regardless of attack method or surface, using deception and concealment technologies. It provides a comprehensive fabric that blankets the network with deceptive decoys, credentials, shares, bait, and other misdirection's that derail adversaries early in the attack life cycle. Automated intelligence collection, attack analysis, and third-party integrations accelerate incident response. The platform creates a threat-informed defense against attackers using its many modular components, including the BOTsink deception server, the Endpoint Detection Net Suite, and ADSecure for Active Directory protection.

# SUMMARY

The Attivo ThreatDefend Platform and the SentinelOne Singularity platform empower organizations with a robust defensive strategy that combines quick and accurate detection with rapid threat containment. Together, the joint solution allows organizations to shorten triage time with actionable alerts, reduce response delays with automated quarantines, and improves defenses with company-centric threat intelligence.

By implementing these solutions jointly, organizations can confidently detect in-network threats early and automatically block and quarantine those threats to mitigate the risk of large-scale breaches.

## Layered Endpoint Defense

**SentinelOne®**
Keeps the attackers from getting in.

EDR
- Automated Remediation
- Behavioral Analysis
- Anti-Virus

**Attivo NETWORKS®**
Keeps the attackers from breaking out.

EDN
- AD Privilege Escalation
- Lateral Movement
- Credential Theft

ENDPOINT    PROTECTION

# ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for countering threat activity. The Attivo ThreatDefend® Platform provides a customer-proven scalable solution for denying, detecting, and derailing attackers while reducing the attack surface across user networks, data centers, cloud, remote sites, and specialized attack surfaces. The portfolio provides new defenses at the most critical points of attack, including endpoints, Active Directory, and throughout the network with patented ground-breaking innovations by preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations help streamline and significantly speed incident response. The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.

# ABOUT SENTINELONE

SentinelOne is a pioneer in delivering autonomous security for the endpoint, data center, and cloud environments to help organizations secure their assets with speed and simplicity. SentinelOne unifies prevention, detection, response, remediation, and forensics in a single platform powered by artificial intelligence. With SentinelOne, organizations can rapidly detect malicious behavior across multiple vectors, rapidly eliminate threats with fully- automated integrated response, and adapt their defenses against the most advanced cyberattacks. SentinelOne has offices in Mountain View, Tel Aviv, and Tokyo. The company is recognized by Gartner as a Visionary for Endpoint Protection and has enterprise customers in North America, Europe, and Japan. To learn more, please visit our website at www.sentinelone.com