SOLUTION BRIEF

Singularity XDR Platform + Endpoint Detection Net (EDN) Suite

THE PROBLEM

Attackers compromise endpoints when infiltrating organizations, increasingly using credential theft and exploitation of Active Directory for privilege escalation to conduct their attacks. Current Antivirus, EPP, and EDR solutions can provide a powerful defense for detecting malware; however, they are not designed to address these forms of targeted attacks. For comprehensive endpoint protection, organizations will need to use a combination of technologies that can work synergistically and cover all attack vectors.

60%+

of all attacks use stolen credentials. These attacks are difficult to detect as they appear as authorized use by employees.

85%+

of breaches that were investigated in the last 2 years leveraged Active Directory.

Consistent feedback across tier 1 incident response firms

THE JOINT SOLUTION

SentinelOne is a leader in Endpoint Protection (EPP), Endpoint Detection & Response (EDR), IoT security, and cloud security with its Singularity XDR platform. Leveraging patented behavioral AI, SentinelOne brings prevention, detection, and response to real-time with autonomous technology. SentinelOne is the only platform that brings together comprehensive prevention and detection coupled with automatic remediation to ensure perpetual device health. Attivo Networks is the leader in detecting lateral movement by protecting credentials on endpoints and preventing attackers from leveraging Active Directory (AD) to execute their campaigns, two key targets for modern cyberattacks within the enterprise. The Attivo Networks Endpoint Detection Net (EDN) solution provides SentinelOne customers with effective ways to reduce the risk associated with credential theft, attacks against Active Directory, and privilege escalation while reducing the attack surface by removing exposed credentials.

Credential Protection Coverage

- PC, Mac, Linux Credentials and Artifacts
- Employee and Admin Credentials
- Cloud Credentials
- SaaS Credentials
- Wire Transfer Credential

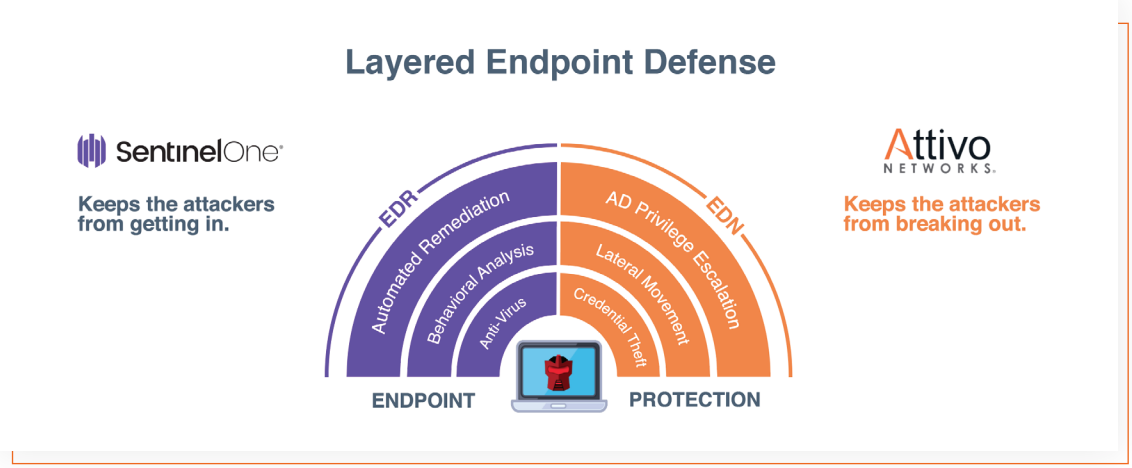
Active Directory Protection for

- Privileged Credentials
- Service Accounts
- Shadow Admin Accounts
- Domain Controllers
- Critical Users and Computers

KEY FEATURES

Deploying the Attivo EDN solution in conjunction with the SentinelOne XDR platform significantly hardens endpoint defense. It prevents attackers from discovering critical assets and accounts, stealing credentials, escalating privileges, moving laterally, and collecting data with novel capabilities that conceal and protect Active Directory and other critical assets from unauthorized access. As a SentinelOne Technology partner, Attivo Networks provides free trials to SentinelOne Customers. Learn more at attivonetworks.com.

JOINT SOLUTION BENEFITS



The SentinelOne Endpoint Protection Platform provides a purpose-built agent powered by machine learning and automation to prevent and detect of attacks across all major vectors. It rapidly eliminates threats with fully automated, policy-driven response capabilities, and gives complete visibility into the endpoint environment with full-context, real-time forensics.

The Attivo EDN suite complements the SentinelOne Singularity XDR platform by adding the ability to map how adversaries execute their attacks, deny them access to the data they seek, detect their activity quickly, and derail them with misinformation along each step of the attack. Core capabilities include restricting unauthorized access to Active Directory information or local administration accounts, placing deceptive credentials on the endpoints, gaining visibility to exposed credentials, and automating their remediation to reduce the attack surface, amongst other features that disrupt an attacker's ability to move laterally.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory, and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership. To learn more, please visit our website at www.attivonetworks.com

ABOUT SENTINEL ONE

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.