SentinelOne

SOLUTION BRIEF

# Protect Against Active Directory Attacks on Endpoints

SentinelOne & Attivo Joint Solution Brief

Attivo NETWORKS

## Market Challenges

Attackers compromise endpoints when infiltrating organizations, increasingly using Active Directory credential theft and exploitation to escalate privileges and conduct their attacks. Current Antivirus, Endpoint Protection (EPP), and Endpoint Detection and Response (EDR) solutions can provide a robust defense for protecting endpoints however, they do not address these forms of targeted credential-based attacks. For comprehensive defenses against credential-based attacks, organizations will need to use technologies that work synergistically to cover all attack vectors.

## Joint Solution

The SentinelOne Singularity Platform provides a purpose-built agent powered by machine learning and automation to prevent and detect 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 platform by mapping how adversaries execute their attacks, denying them access to the data they seek, detecting their activity quickly, and derailing 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. Furthermore, the solution activates SentinelOne's endpoint quarantine, amongst other features that disrupt an attacker's ability to move laterally.

## How It Works

Deploying the Attivo Endpoint Detection Net (EDN) solution in conjunction with the SentinelOne Singularity platform hardens endpoint defenses. It prevents attackers from discovering critical assets and accounts, stealing credentials, escalating privileges, moving laterally, and collecting data with capabilities that conceal and protect Active Directory and other critical assets from unauthorized access. The Attivo integration on the Singularity Marketplace triggers automated quarantine for affected systems to reduce response times and derail attacks before they progress.

> 85%

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

> 60%

of all attacks use stolen credentials

### JOINT SOLUTION HIGHLIGHTS

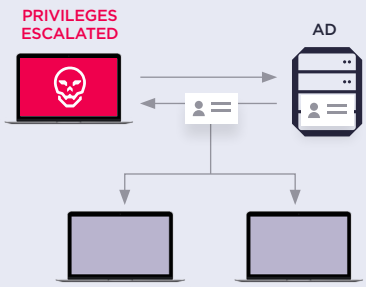
+ Expose lateral movement paths and prevent lateral propagation activity
+ Protection and detection for Active Directory attacks and post-exploit behaviors
+ Automatically quarantine targeted endpoints

### INTEGRATION BENEFITS

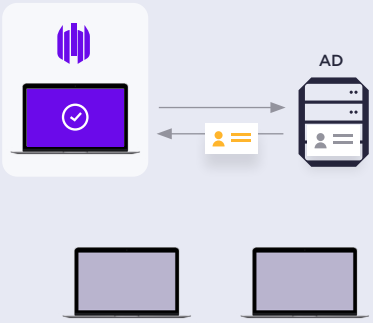
- **Lateral Movement Protection**
- **Layered Defenses for Active Directory (AD)**
- **Reduce Mean Time to Respond (MTTR)**

# Solution Use Case

Detect Attacks Targeting Active Directory.




Without Attivo and SentinelOne, advanced attackers can compromise AD, escalate privileges, remain hidden and gain privileged access to the domain.




With Attivo and SentinelOne, EDN detects the attack, returns decoy objects, and activates the Singularity XDR integration to quarantine the endpoint.

> “Attivo Endpoint Detection Net (EDN) is a critical line of defense for credential theft, attacks against Active Directory, and privilege escalation. Our integration with SentinelOne Singularity Marketplace enables joint customers to reduce their attack surface by removing exposed credentials and hardening endpoint defenses.
>
> **Venu Vissamsetty**
> VP OF SECURITY RESEARCH, ATTIVO NETWORKS

# Conclusion

Deploying the Attivo EDN solution in conjunction with the SentinelOne Singularity 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.

## READY FOR A DEMO?

Visit the SentinelOne website for more details.

## SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.

Gartner peerinsights customers' choice

**97%** Of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend SentinelOne

**97%** Customer Satisfaction (CSAT)

FedRAMP · ISO 27001 CERTIFIED by schellman · EU GDPR COMPLIANT · AAA · TEVORA PCI DSS Attestation HIPAA Attestation · Gartner peerinsights 4.9 ★★★★★

### 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?

### About Attivo

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, delivers a superior defense for countering threat activity. Through deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Attivo has won over 130 awards for its technology innovation and leadership. To learn more, please visit our website at www.attivonetworks.com.

**sentinelone.com**
sales@sentinelone.com
+ 1 855 868 3733