SentinelOne

DATA SHEET

Singularity RangerAD Protect

Assess, Detect, and Remediate Threats to Your Active Directory

AD and Azure AD are common targets of identity-based cyber attacks. Their compromise can give attackers the foothold to expand access, establish persistence, escalate privileges, identify more targets, and move laterally.

Ranger® AD Protect, composed of Ranger AD and Singularity Identity-Domain Controller edition, is an identity configuration assessment and threat detection bundle. It identifies misconfigurations, vulnerabilities, and attack indicators within Active Directory (AD) and Azure AD and detects active attacks aimed at on-premises AD controllers. By delivering prescriptive, actionable insight into exposures in your identity attack surface and detecting attacks targeting AD, Ranger AD Protect helps reduce the risk of compromise and aligns your assets with security best practices.

Continuously Analyze Identity Exposure

Skip the expensive and manual audits. Automatically pinpoint critical domain, device, and user-level exposures in Active Directory and Azure AD.

Reduce the AD Attack Surface

Analyze configuration changes to conform with best practices and eliminate excessive privileges with actionable recommendations for quick remediation.

Detect Active AD Attack Indicators

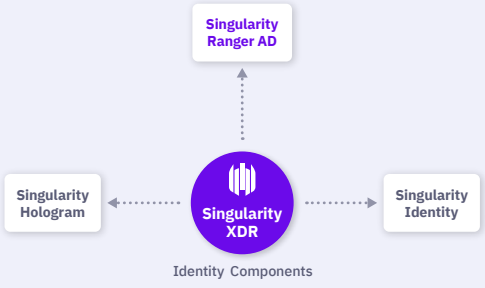
Proactively monitor AD and Azure AD for activities that indicate potentially active attacks, both continuously and on-demand.

Protect AD Controllers from Attack

Detect attacks targeting on-premises AD controllers from any device on the network to stop threat actors early.

Provide Conditional Access

Forces partner MFA reauthentication when detecting unusual activity targeting AD controllers. Note that this capability is also available with the Singularity XDR platform.



Ranger AD is simple to deploy and provides fast, actionable insights into hardening Active Directory and Azure AD implementations, thereby reducing your identity attack surface. Singularity Identity-DC installs quickly on AD controllers and detects attacks from any device on the network.

84% of organizations have experienced an identity-related breach. Ranger AD Protect provides actionable information and threat detection to reduce that exposure.

KEY FEATURES & BENEFITS

+ Proactively address identity-based risk
+ Compare AD & Azure AD configurations to best practices
+ Understand AD & Azure AD security misconfigurations
+ Reveal domain, device, and user-level exposures
+ Stay informed of suspicious AD change events
+ Reduce the MTTR to identity-based attacks
+ Gain visibility and flexibility from continuous & on-demand monitoring for active AD attacks
+ Detect attacks actively targeting on-premises AD controllers from any networked device.
+ Triggers MFA reauthentication when detecting suspicious activity on AD controllers

Reduce Your AD Attack Surface & Detect Identity-Based Attacks

By analyzing your AD configuration for conformance to best practices and guiding you towards quick remediation for any excessive privilege across the organization, Ranger AD helps tangibly reduce your attack surface. Detecting attacks targeting your AD controllers early in the attack cycle can stop attacks by triggering MFA before threat actors cause significant damage.

Hundreds of Real-Time Checks

Domain Level

+ Weak policies
+ Credential harvesting
+ Kerberos vulnerabilities

Device Level

+ Rogue domain controllers
+ OS issues
+ AD vulnerabilities

User Level

+ Credentials analysis
+ Privileged accounts
+ Stale accounts
+ Shared credentials

Singularity Identity-DC Detections

- Golden Ticket Attacks
- Silver Ticket Attacks
- Skeleton Key Attacks
- Pass-the-ticket Attacks
- Pass-the-hash Attacks
- Overpass-the-hash Attacks
- Forged PAC Attack
- DCSync Attack
- DCShadow Attack
- AS-REP Roasting Attack
- Recon of Privileged and Service Accounts across LDAP, SAMR, and LSAR protocols

FAST TIME-TO-VALUE

+ Flexible deployment: on-prem and SaaS
+ Flexible coverage: on-prem AD, Azure AD, and multi-cloud
+ Low friction implementation with fast, actionable results for Ranger AD, requiring just one endpoint and no privileged credentials
+ Achieve complete coverage for on-premises Active Directory, Azure AD, and multi-cloud environments
+ Singularity Identity-DC detects attacks from any device on the network with a single agent installed on each AD controller.
+ Singularity Identity-DC provides conditional access protections to AD controllers with partner MFA provides.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection.
- Top Analytic Coverage 3 Years Running
- 100% Real-time with Zero Delays

Gartner peerinsights 4.9

99% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · AICPA SOC · TEVORA PCI DSS Attestation HIPAA Attestation · VB 100 VIRUS · AAA · SE Labs BEST Innovator WINNER 2021

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733

© SentinelOne 2022