SentinelOne

Singularity™ Identity Posture Management

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.

Singularity Identity Posture Management, a component of the Singularity XDR platform, is an identity configuration assessment solution that identifies misconfigurations, vulnerabilities, and active threats targeting Active Directory (AD) and Azure AD. By delivering prescriptive, actionable insight into exposures in your identity attack surface, Singularity Identity Posture Management helps you reduce the risk of compromise and brings your assets in line with security best practices.

Continuously Analyze Identity Exposure

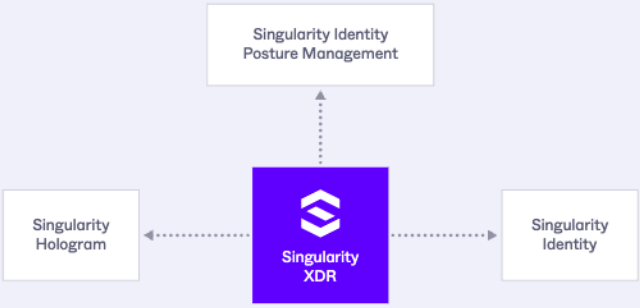
Skip the expensive and manual audits. Automatically pinpoint critical domain, device, and user-level exposures in Active Directory and Azure AD.

Reduce the AD Attack Surface

Analyze configuration changes to conform with best practices and eliminate excessive privileges using automated AD exposure remediation with rollback capability.

Detect Active AD Attack Indicators

Proactively monitor AD and Azure AD for activities that indicate potentially active attacks continuously.



Identity Components

Singularity Identity Posture Management is simple to deploy and provides fast, actionable insights into hardening Active Directory and Azure AD implementations, thereby reducing your identity attack surface.

More information at **s1.ai/ranger-ad**

84%

of organizations have experienced an identity-related breach. Singularity Identity Posture Management provides the actionable information to reduce that exposure.

Key Features and 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
- + Granular options to remediate exposures and Rollback