SentinelOne

TUCANA CYBER SECURITY SOLUTIONS

DATA SHEET

Singularity™ IDENTITY

Real-time Identity Threat Detection & Response

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

Singularity Identity™ threat detection & response (ITDR), a component of the SentinelOne Singularity XDR platform, defends, in real time, Active Directory & Azure AD domain controllers and domain-joined endpoints from adversaries aiming to gain privilege and move covertly. Singularity Identity expands on Singularity XDR protection capabilities with Sentinel agents that safeguard Microsoft AD domain controllers and end-user endpoints.

Defend Your Domain

Detect Active Directory attacks from any device type or OS—including IoT & OT

Thwart the Adversary

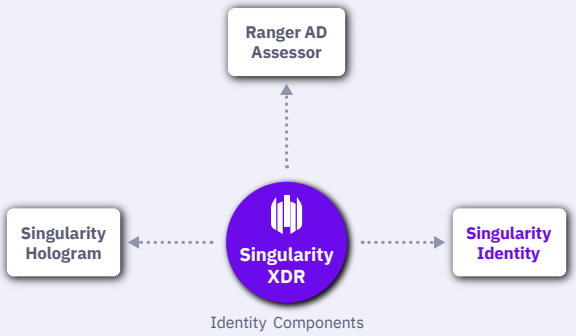
Steer attackers away from AD crown jewels with misdirection down dead-end alleys

Cloak, Deflect, Protect

Hide credentials and production data while making lateral movement difficult

Expand & Collect

Integrate with Singularity Hologram™ network deception decoys to further slow down in-network adversaries and insider threats



Identity Components

Singularity Identity Sentinels prevent attackers from gaining access to Active Directory and Azure AD crown jewels—whether on-prem or in the cloud

More information at **s1.ai/identity**

94% of organizations have experienced an identity-related breach. Singularity Identity Sentinels defend identity in real time.

KEY FEATURES & BENEFITS

+ Real-time detection of Active Directory & Azure AD-based identity cyber attacks, including ransomware
+ Easy implementation with low friction results; supports on-premises Active Directory, Azure AD, and multi-cloud environments
+ Identity attack coverage and peace of mind for all managed or unmanaged assets across all OSes; includes IoT and OT devices
+ Cloaking technology to mislead attackers and protect high-value credentials
+ Actionable insight into gaps in your identity attack surface, including misconfigurations, access controls, policy violations, and more
+ Integrates with Singularity Hologram Deception technology for network decoy engagement and threat intelligence collection

Keep Credentials Safe, See Value Quickly

Get started quickly with fast, frictionless, and flexible deployment options: Singularity Identity enables full coverage for on-premises AD, Azure AD, and multi-cloud environments. Make immediate strides towards better defenses by protecting and limiting access to local application credential stores, identifying identity exposures, and implementing controls that thwart attackers.

Singularity Identity Features

01 | Defend Identity at the Domain Controller

The Singularity Identity Sentinel agent for AD and Azure AD senses identity-based attacks from across the domain infrastructure. Singularity Identity provides actionable, high-fidelity insight as attacks emerge from managed and unmanaged devices, including ubiquitous IoT and OT, that may be compromised, regardless of their operating system or location.

02 | Defend Identity at the Endpoint

The Singularity Identity Sentinel agent for Endpoint senses identity misuse and reconnaissance activity happening within endpoint processes that are targeting critical domain servers, service accounts, local credentials, local data, network data, and cloud data. On-agent cloaking and deception techniques slow the adversary down while providing situational awareness.

03 | Halt Lateral Movement

Stop adversarial advances—including ransomware attacks—in their tracks with traps set around every corner: Singularity Identity enables you to prevent privileged credential theft, including high-value user, service, and system accounts. Unauthorized network reconnaissance and fingerprinting becomes virtually useless to attackers as legitimate data is replaced with decoy data. By integrating with Singularity Hologram, you can also redirect lateral movement attempts to network decoys.

04 | Learn Attack Paths

Singularity Identity helps you uncover and understand hidden factors that leave your environment susceptible to identity-based attacks, such as exposed surfaces, orphaned credentials, and policy violations. Supplemented by visual topographic maps, Singularity Identity shows how attackers could move across systems to reach the critical assets. Armed with this insight, your security & IT teams can preemptively block paths to critical assets and bolster your defenses using deception technology.

ENABLING AND ENFORCING ZERO TRUST WITH SINGULARITY IDENTITY

+ Limit implicit trust to applications and data resources
+ Identify identity exposures on endpoints, AD, and the cloud
+ Detect identity attacks on endpoints & domain controllers
+ Limit access to only trusted or validated applications

Singularity Identity integrates with Singularity Hologram™ for a complete Identity + Deception solution.

MORE INFORMATION

Visit us at **s1.ai/identity**

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?

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733