



Singularity™ Identity Detection & Response

Real-time Identity Threat Detection & Response

AD and Entra ID 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 Detection & Response, a component of the SentinelOne Singularity Platform, defends Active Directory and domain-joined endpoints, in real-time, from adversaries aiming to gain privilege and move covertly. Singularity Identity Detection & Response expands on Singularity Platform 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, and provide AD conditional access with partnered MFA solutions



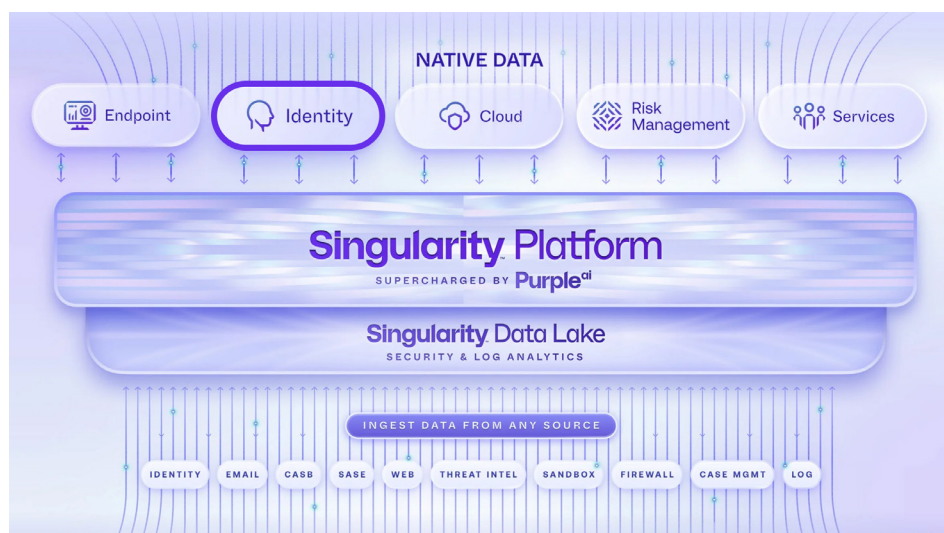
Thwart the Adversary

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



84%

of organizations have experienced an identity-related breach. Singularity Identity Detection & Response Sentinels defend identity in real time.

Key Features and Benefits

- + Real-time detection of identity-based cyber attacks, including ransomware, targeting Active Directory
- + Easy implementation with low friction results; supports on premises and cloud- hosted Active Directory Domain Controllers
- + 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

Keep Credentials Safe, See Value Quickly

Get started quickly with fast, frictionless, and flexible deployment options: Singularity Identity Detection & Response enables full coverage for on-premises AD, Entra ID, 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 Detection & Response Features

01 | Detect Attacks Targeting Domain Controllers

The Singularity Identity Detection & Response Agent senses identity-based attacks from across the domain infrastructure. Singularity Identity Detection & Response 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 Detection & Response 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 Detection & Response 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.

04 | Learn Attack Paths

Singularity Identity Detection & Response 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 Detection & Response

- + 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
- + Enables AD conditional access with MFA partners

Singularity™ Identity Detection & Response

Ready for a Demo?

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

s1.ai/identity →

Innovative. Trusted. Recognized.



A Leader in the 2024 Magic Quadrant for Endpoint Protection Platforms



Record Breaking ATT&CK Evaluation
+ 100% Protection. 100% Detection
+ Outstanding Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays



96% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity



About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

sentinelone.com

sales@sentinelone.com

+1 855 868 3733