



Reduce Identity Attack Surface with Device Posture Assessment

SentinelOne & StrongDM Joint Solution Brief

Market Challenges

According to the Verizon Data Breach Investigation Report (2023), 74% of all breaches include the human element, with people involved either via error, privilege misuse, use of stolen credentials, or social engineering. This becomes even more challenging with the rapid evolution of cloud resources presenting a significant challenge in implementing Zero Trust access across a wide variety of infrastructures. The complexity does not end with granting initial access; it is also about continuously assessing whether that access remains appropriate. Access needs to be continuously assessed and granted based on contextual factors, allowing organizations to make real-time access decisions that enhance security while preserving productivity.

Joint Solution

To reduce security risk, SentinelOne and StrongDM integrate to amplify device trust across organizations. The SentinelOne Singularity Platform, powered by Singularity Data Lake, continuously protects, detects, and responds to threats across endpoints, identities, and cloud workloads, gaining valuable insight into an organization's security posture. StrongDM grants dynamic access to critical infrastructure, including databases, clouds, servers, clusters, and web applications.

The integration between SentinelOne and StrongDM ensures that a user's device meets specific security standards to add context to the access decision for critical infrastructure. Access is granted only after authentication and authorization for that resource. This adds context to every access request by assessing the risk profile of the device the person is using. Trust the user, trust the device, and then grant access. With continuous risk assessment, access and active sessions can be severed at any time.

Key Use Cases

- ✔ **Zero Standing Privileges**
Eliminate standing access with just-in-time access. Admins have control over what each user can access without getting in the way of productivity. Grant or deny access based on device risk. Any access request coming from a high-risk device is blocked.
- ✔ **Secure and Auditable**
Comprehensive audit trails, with every activity and query logged. Security and Compliance teams can easily answer who did what, where, and when.
- ✔ **Identity Lifecycle Management**
As people change roles and responsibilities, automate identity-based access by managing user and group provisions directly through the organization's identity provider.



Joint Solution Highlights



Continuous Risk Assessment

Evaluate the user device regularly to ensure connections are valid. Revoke access immediately if any risk is detected.



Context-Based Access

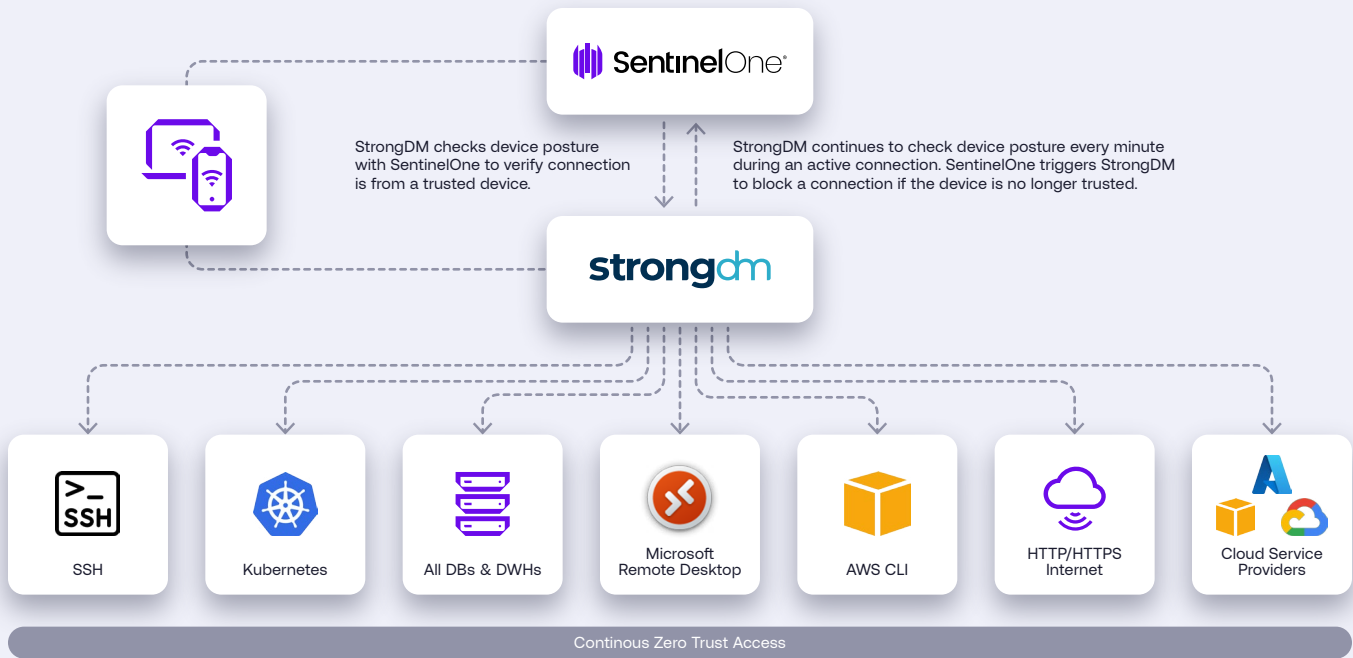
Consider user context for access, which includes device, time, location, and activity, in addition to validating the user and gaining user trust. Context narrows the aperture for access and decreases risk.



Zero Trust Access

Reach Zero Trust goals with an architecture design that is scalable, easy to deploy, and supports a modern approach to infrastructure, whether on-prem or in the cloud.

How It Works



Integration Benefits

- + **Reduce the Attack Surface**
Deny access to devices that are at high risk. Reduces the risk of unauthorized access and mitigates potential threats.
- + **Compliance Adherence**
Meet regulatory compliance by enforcing access control security policies informed by identity and device.
- + **Dynamic Security Policy**
Adjust security policies based on device posture. Implement stricter or more relaxed policies based on the specific device.

Singularity Platform

READY FOR A DEMO?

Visit the SentinelOne website for more details.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2022 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 Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FR
FedRAMP

TEVORA
PCI DSS Attestation
HIPAA Attestation

AICPA SOC

STAR LEVEL ONE

100 VIRUS
VirusTotal

SE Labs
BEST Innovator
WINNER 2021

ISACA

Trusted Cloud Provider CSA

About SentinelOne

SentinelOne (NYSE:S) is a global leader in AI-powered security. SentinelOne's Singularity™ Platform detects, prevents, and responds to cyber attacks at machine speed, empowering organizations to secure endpoints, cloud, and identities with speed, accuracy, and simplicity.

About StrongDM

StrongDM is a Dynamic Access Management platform that centralizes privileged access for all technical users to every resource in your infrastructure on-premises and in the cloud. Security teams have complete visibility into every keystroke to enhance security and compliance postures and end users enjoy fast intuitive access to the resources they need.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733