SentinelOne & Cloudflare Joint Solution Brief

Empowering Zero Trust Conditional Access

Securing Access Beyond The Perimeter

When applications and users left the walls of the enterprise perimeter, security teams had to make compromises on how to keep data safe. Relying on yesterday's network-based controls (like VPNs and IP location restriction) for application access can increase attack surface, limit visibility, and frustrate end users. To evolve, many enterprises are turning to Zero Trust security frameworks. Where network-based controls facilitate a castle and moat model that enables risky lateral movement, Zero Trust policies require real-time identity and posture-driven checks each time users attempt to access protected resources. These policies keep sensitive data safe by ensuring it can only be accessed by verified users on trusted devices.

Joint Solution

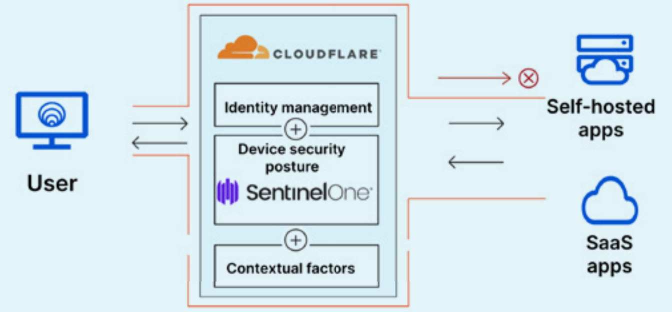
SentinelOne and Cloudflare work together to ensure that adopting Zero Trust Network Access is easy. Organizations integrate endpoint protection platforms like SentinelOne, add corporate identity providers and connect their applications (SaaS, cloud, or onpremises) to Cloudflare's global edge network in minutes. With just a few clicks in the Cloudflare dashboard, administrators can apply default-deny, Zero Trust rules that restrict user access to sensitive applications based on device posture signals from SentinelOne Singularity XDR.

Joint Solution Highlights

- **+ Enforce device-aware access policies**
- **+ Prevent lateral movement**
- **+ Decisions at machine speed**
- **+ Simple configuration**

How it Works

SentinelOne provides AI-powered protection, detection and response on the endpoint and provides valuable context to Cloudflare to be used in conditional access decisions. Instead of a VPN, users connect to corporate resources through a client or a web browser. As requests are routed and accelerated through Cloudflare's edge, they are evaluated against Zero Trust rules incorporating signals from SentinelOne, your identity providers, and other context. Where RDP software, SMB file viewers, and other thick client programs used to require a VPN for private network connectivity, teams can now privately route any TCP traffic through Cloudflare's network where it's accelerated, verified, and filtered in a single pass, facilitating improved performance and security.



Step 1

User requests access to an application.

Step 2

Cloudflare directs user to an authentication page where SentinelOne evaluates device posture for policy adherence. Additionally, user's identity and context such as geolocation and certificate are also assessed.

Step 3

If user's request adheres to policy, access is granted.

SentinelOne

CLOUDFLARE
PARTNER NETWORK

Use Cases

Prevent Malware Propagation

Stop malware from spreading laterally through a corporate network. SentinelOne provides ongoing monitoring against malware and other device-based threats. Cloudflare verifies that SentinelOne is actively running and protecting a machine before allowing access to an application. Device posture checks contain malware to the endpoint and prevents it from moving laterally to cloud resources.

Protect Production Environments

Protect remote SSH access in a production environment. Developers can render SSH clients within a Zero Trust browser running on Cloudflare's edge, and access production environments without a VPN, clunky client software, or long-lived certificates. A device posture policy that requires SentinelOne is enforced at login and throughout the session, ensuring that no infected devices can access the production environment. A secure context-driven access policy provides a more streamlined and intuitive workflow for developers.

Reduce Impact of Credential Compromise

Mitigate the impact of credential theft. An attacker uses an employee's stolen credentials to attempt to access a protected staging site. The attacker would still be blocked even with valid credentials because they do not have SentinelOne running on their device. This approach reduces reliance on passwords alone as a security signal and provides enriched detection and policy enforcement.

Conclusion

The combination of SentinelOne and Cloudflare makes it easier for organizations to adopt Zero Trust and reduce the potential impact of security incidents.

Key Features

Enforce device-aware access policies

Ensure that only protected devices connect to your resources.

Prevent lateral movement

Prevent infected or vulnerable devices from accessing sensitive data.

Decisions at machine speed

Cloudflare's lightning-fast network brings enforcement decisions within 100ms of 99% of the world's Internetconnected population.

Simple configuration

Add device posture signal from SentinelOne into application access policies with a few clicks.

Innovative. Trusted. Recognized.

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne

TEVORA
PCI DSS Attestation
HIPAA Attestation

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

About Cloudflare

Cloudflare is the security, performance, and reliability company on a mission to help build a better Internet. Today it runs one of the world's largest networks that powers approximately 25 million Internet properties, with approximately 17% of the Fortune 1000 companies using at least one Cloudflare product.

cloudflare.com | spx-partnerships@cloudflare.com | + 1 888 99 FLARE