PARTNER BRIEF

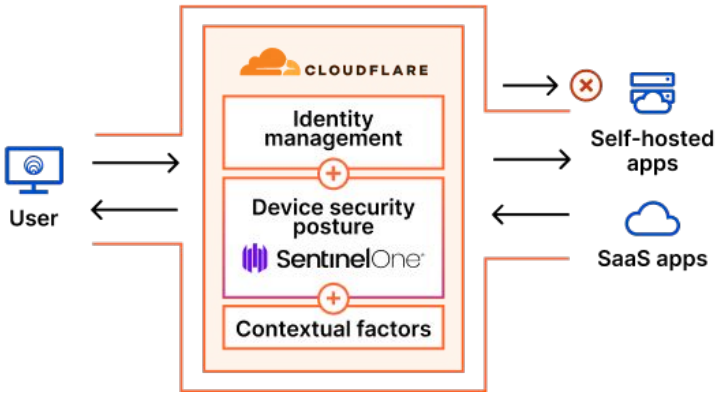
SentinelOne and Cloudflare

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.



- **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.

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 Internet Connected population.