Cloudflare and SentinelOne

Strengthen Zero Trust security with integrated risk data

Legacy security faces an expanding attack surface

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 the attack surface, limit visibility, and frustrate end users.

In an era of distributed work and bring your own device (BYOD) policies, users may attempt access critical data and applications from unmanaged, insecure devices, putting applications and data at risk.

Adopting Zero Trust to manage risk

Zero Trust frameworks enforce identity and posture checks each time users access resources. Device context is an important part of making access decisions. Infected or vulnerable devices should be prevented from accessing the network or applications. Determining device posture requires collaboration between solutions that power Zero Trust access and endpoint security.

The partnership between Cloudflare and SentinelOne enables better conditional access decisions. Enforce Zero Trust policies by evaluating device posture in addition to user risk and allowing only secure and trusted devices to access the network.

Enforce device-aware access policies

Prevent infected, vulnerable, or unmanaged devices from accessing sensitive data or applications.

Block unauthorized access

Make access decisions more accurate by basing them on both device posture and user behavior to align with Zero Trust principles.

Make decisions at machine speed

Bring enforcement decisions within 50 ms of 95% of the world's Internet users with Cloudflare's lightning-fast network.

Simplify Zero Trust security

Add device posture data with just a few clicks in the Cloudflare dashboard by connecting to SentinelOne APIs.

 | 1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

Cloudflare and SentinelOne

Strengthen Zero Trust security with integrated risk data

Unify how you manage risk with Cloudflare and SentinelOne

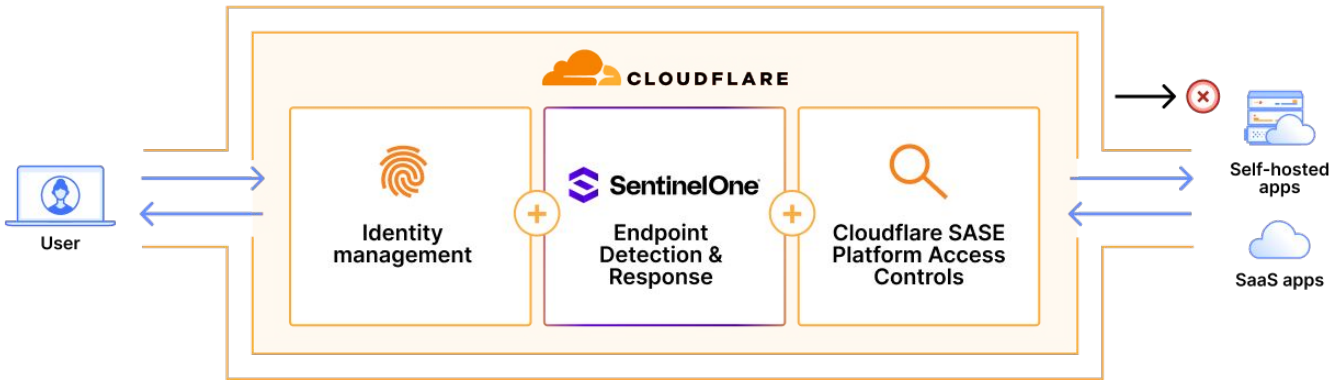
Integration with SentinelOne provides device posture and user behavior information to Cloudflare Zero Trust to determine whether a user or device should be allowed to access the network or applications.

When Cloudflare receives an access request, it verifies the device posture with SentinelOne Singularity XDR and the user's identity with the chosen identity provider. Device posture data is gathered from SentinelOne APIs and includes whether the device is infected, has active threats, or doesn't have the SentinelOne agent running.

The integration also enables Cloudflare to use SentinelOne endpoint detection and response signals to calculate a user risk score. Cloudflare's Zero Trust platform assigns a low, medium, or high risk score based on the users' activity and device posture. This risk score can be shared with identity providers.

If a device or user has been deemed a risk, Cloudflare can block access to some or all applications or move the user to a restricted group. This approach strengthens data protection and reduces the risk of breaches.

How it works



Step 1 - User requests access to an application.

Step 2 - At the Cloudflare authentication page, the user's device is automatically checked with SentinelOne Singularity XDR.

Step 3 - If user's device is deemed safe, Cloudflare grants the user access to the network.