INTEGRATION OVERVIEW

secure W2 + SentinelOne

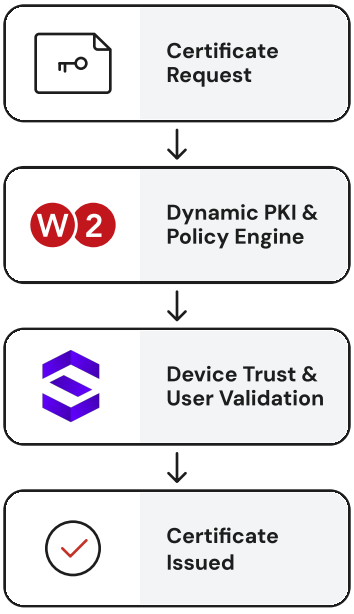
Adaptive Access Management for Continuous Trust

SecureW2's Dynamic PKI delivers a modern, adaptive approach to securing network and application access. By continuously ingesting real-time security signals from sources like **SentinelOne**, it ensures certificates are issued only to verified devices, and stay only with those that remain compliant.

Traditional PKI relies on static, point-in-time checks (e.g. SCEP key), to determine device compliance at the moment of certificate issuance. After that, organizations have limited visibility into whether devices remain compliant.

By leveraging your **SentinelOne** instance with SecureW2, you gain access to dynamic security signals, ensuring access is tied to trusted devices, not outdated assumptions.

How the Integration Works



SecureW2 continuously ingests signals from your identity, device management, and security infrastructure to validate whether a user or device should be issued — and retain – a certificate.

Signals from SentinelOne are streamed via API, to dynamically influence certificate issuance and network policies.

Security events directly control access to resources, auto remediating risky behavior.

BENEFITS

Modern, Flexible Enrollment

Use Dynamic SCEP, ACME, OAuth, JSON, self-enroll via dissolvable clients, and more.

High-Assurance Policy Engine

Build adaptive workflows that validate identity through limitless integrations.

Continuous Trust Enforcement

SentinelOne intelligence keeps certificate issuance and access retention decisions aligned with real-time security posture.

Instantly React to Threats

Revoke certificates immediately after critical threats surface.

Continuously Monitor Risk

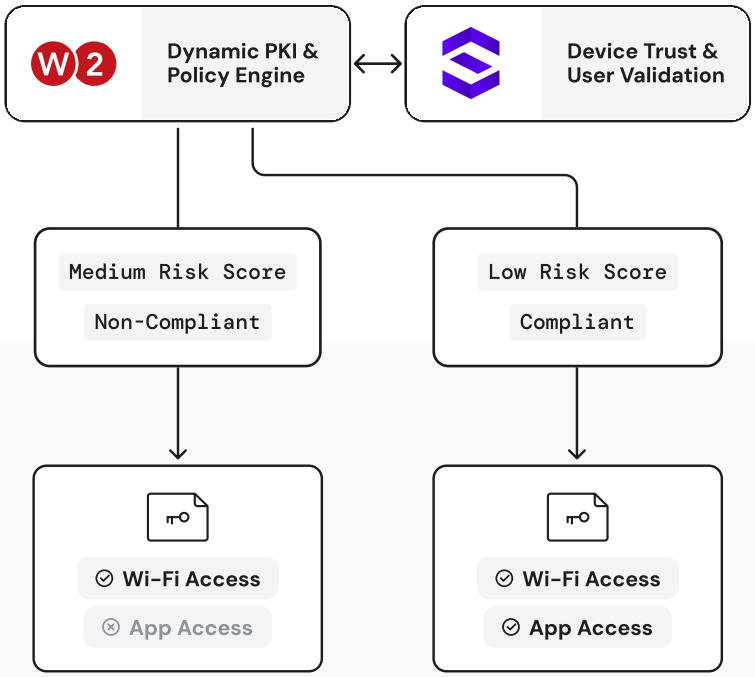
De-risk system access by dynamically issuing certificates for different levels of authentication, based on current risk exposure.

Adaptive Access Policies via SentinelOne Risk Score

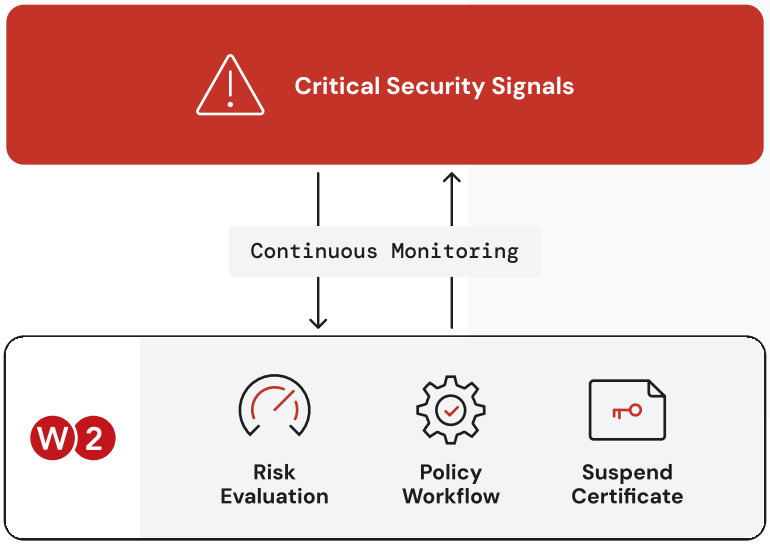
Access decisions should be as dynamic as the risks they protect against. SecureW2 continuously ingests security signals from SentinelOne, issuing certificates with access levels that adjust based on a device's Risk Exposure levels.

Higher-risk devices may be quarantined, while lower-risk ones maintain seamless access, ensuring authentication policies adapt in real time without creating unnecessary friction.

Manage Certificate Lifecycles: Throughout the certificate lifecycle, SecureW2 uses SentinelOne's API to assess the device's Risk Exposure level to ensure trusted and verified access.



Mitigate Risks Instantly via Continuous Monitoring



Through continuous monitoring, SecureW2 automatically takes predefined remediation actions before threats can escalate. The workflow below shows how SecureW2 triggers real-time enforcement as a reaction to a critical event reported by **SentinelOne**, ensuring only trusted devices retain access and security policies stay in sync with the latest threat intelligence.

Critical Threat Response: SecureW2 immediately suspends or revokes the affected certificate as information from SentinelOne or other sources is received.