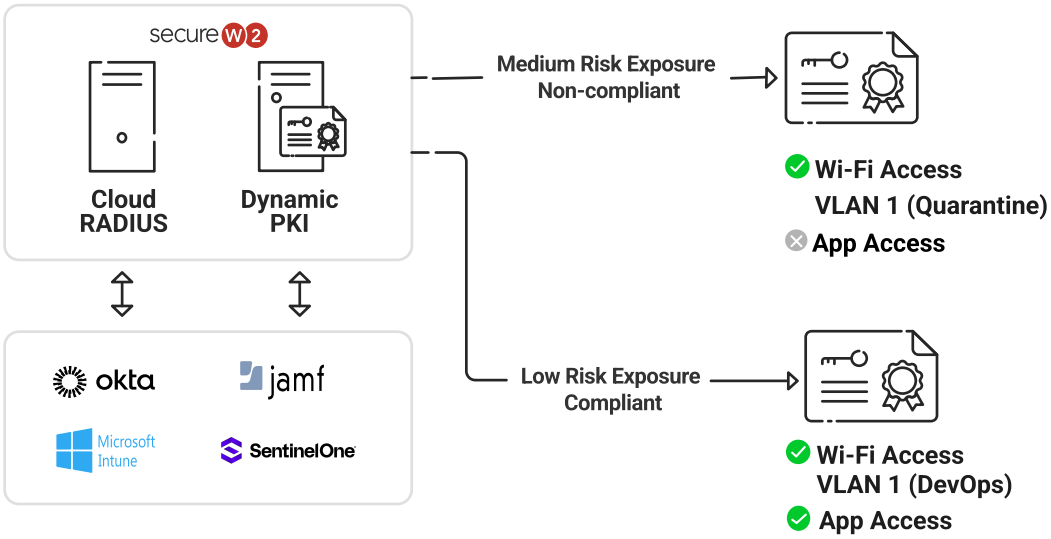
Adaptive Access Policies via ServiceNow Risk Score

Access decisions should dynamically match the risks they protect against. SecureW2 continuously ingests security signals from **ServiceNow**, issuing certificates with access levels adjusting based on the device's Risk Exposure levels.

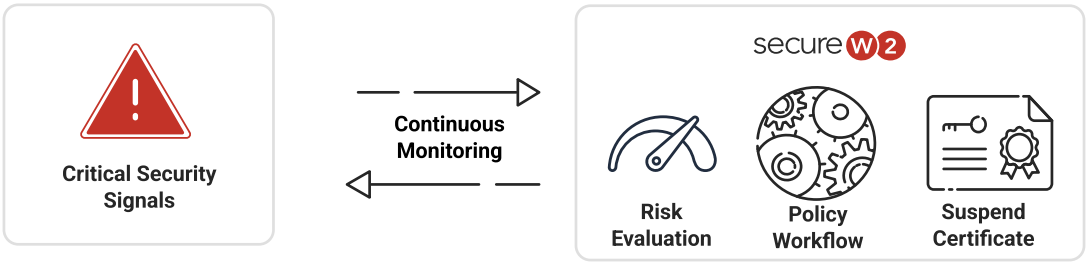
Higher-risk devices might face quarantine, whereas lower-risk ones continue seamless access, ensuring authentication policies adapt in real time.



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

Mitigate Risks Instantly via Continuous Monitoring

SecureW2 implements predefined remediation actions via continuous monitoring before threats can escalate. The workflow below demonstrates SecureW2's real-time enforcements as a reaction to critical threat events from **ServiceNow**, maintaining sync between security policies and threat intelligence.



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

North America Sales
(888) 363-3824
(512) 900-5515

UK, Europe and Middle East Sales
+44 20 3912 9916

Email
sales@securew2.com

Website
www.securew2.com

INTEGRATION OVERVIEW

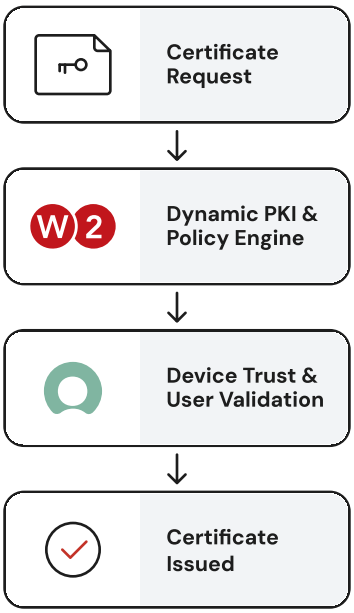
secure W2 + servicenow

Automating Network Access with Dynamic 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 ServiceNow, it ensures certificates are issued only to verified devices, and stay only with those that remain compliant.

By leveraging your ServiceNow 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 ServiceNow 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

ServiceNow 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.