SecureW2 + CrowdStrike® Integration Overview

Real-time Intelligence For Continuous Trust Enforcement

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 **CrowdStrike**, it ensures certificates are issued only to verified devices, and stay only with those that remain compliant.

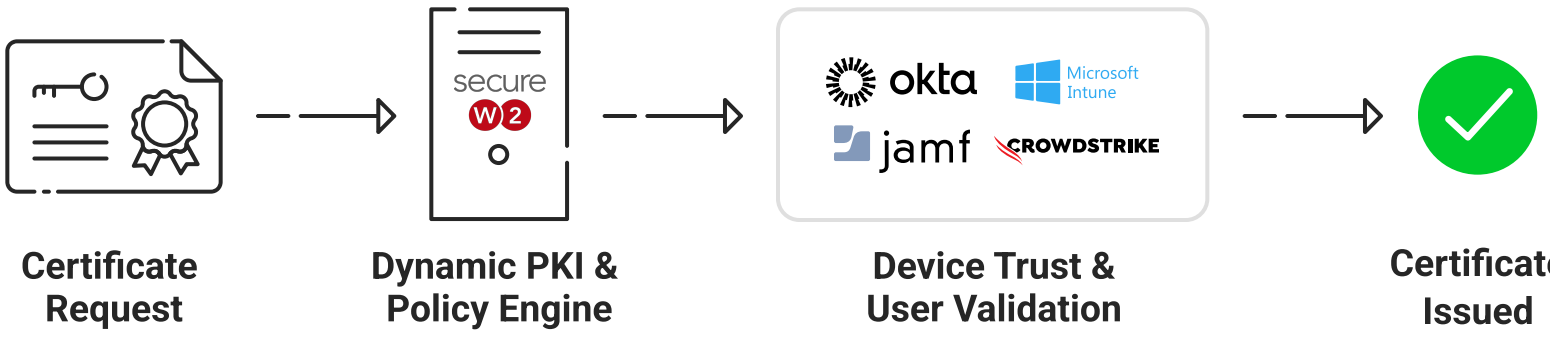
Traditional PKI relies on static, point-in-time checks (e.g. SCEP key), to determine device compliance at the moment of certificate issuance. After that, organizations have limited visibility into whether devices remain compliant.

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instance with SecureW2, you gain access to dynamic security signals, ensuring access is tied to trusted devices, not outdated assumptions.

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

How the CrowdStrike 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. CrowdStrike data is streamed via API, allowing Risk Score to dynamically influence certificate issuance, or ingested via Webhooks to instantly revoke them in response to critical security events.



- **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 Score.

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

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

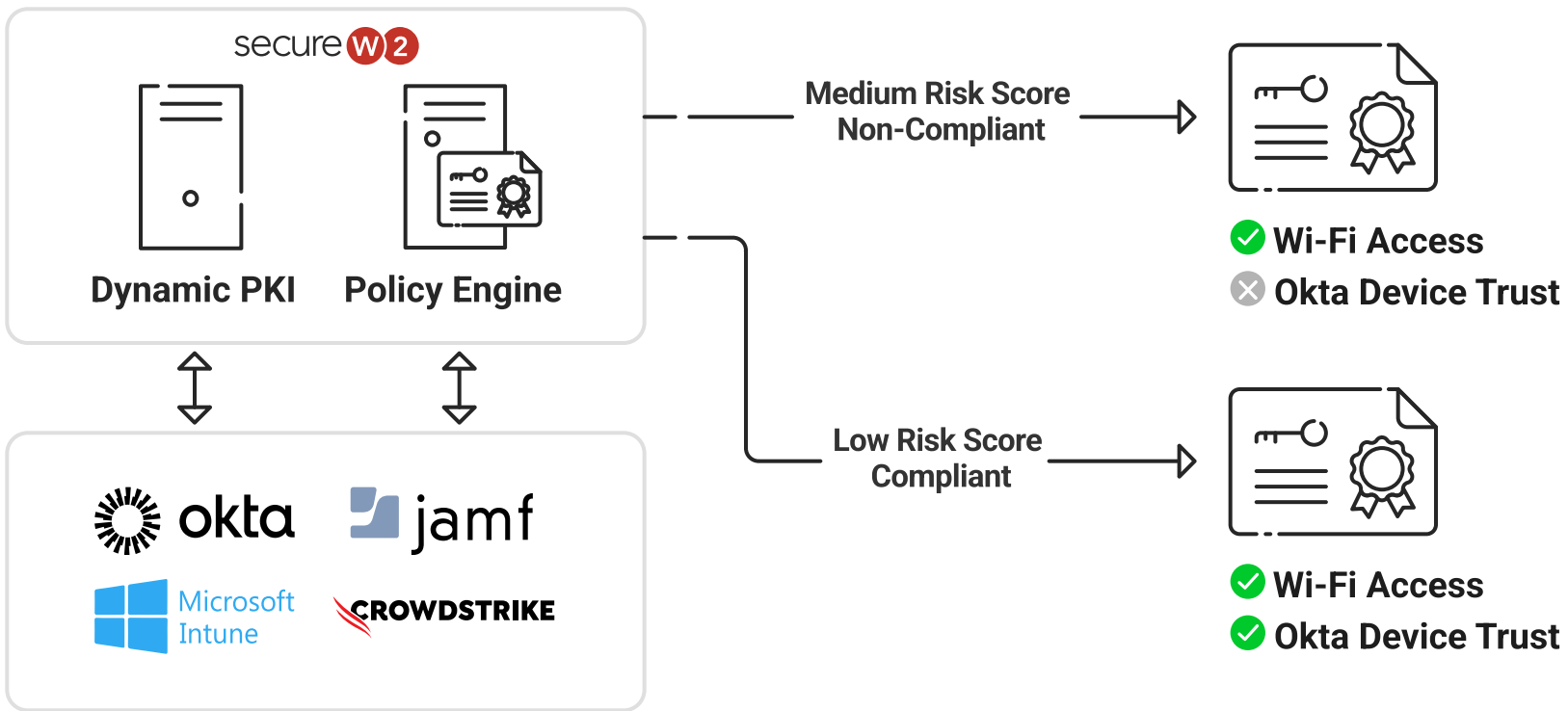
Email
sales@securew2.com

Website
www.securew2.com

Dynamically Authorize Access via CrowdStrike Risk Score

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

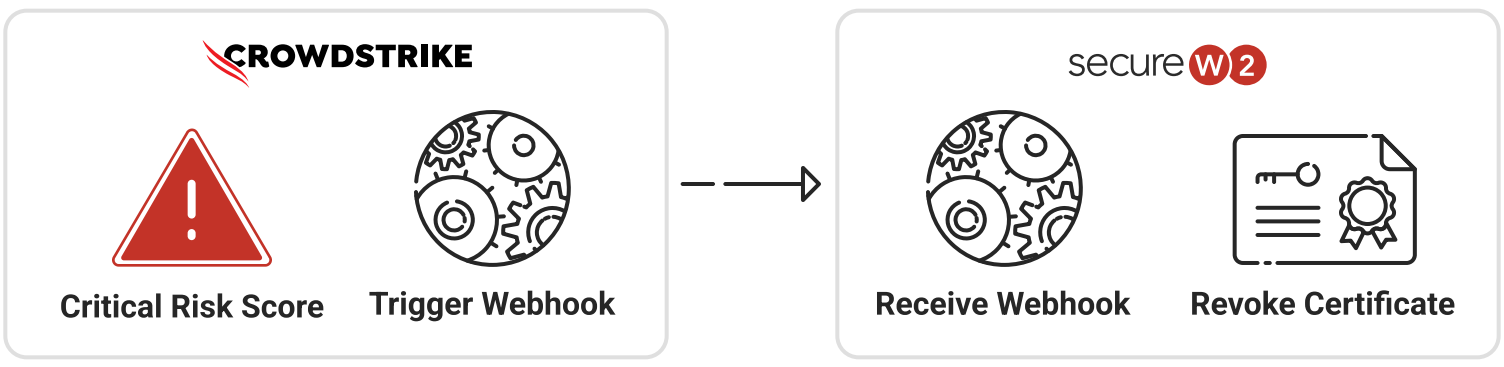
As shown below, non-compliant devices may be restricted while compliant ones maintain seamless access, ensuring security policies adapt in real time without unnecessary friction.



Manage Certificate Lifecycles: During issuance, or throughout it's lifecycle, SecureW2 queries CrowdStrike's API to assess the device's overall Risk Score to ensure the right certificate exists.

React Instantly to Critical Events

When a device reaches a critical risk score, SecureW2 immediately revokes its certificate, cutting off access before threats escalate. The workflow below shows how **CrowdStrike WebHooks** trigger real-time enforcement, ensuring only trusted devices retain access and security policies stay in sync with the latest threat intelligence.



Real-Time Threat Response: Receive information from Crowdstrike as it happens with Webhooks, and SecureW2 will immediately revoke the affected certificate.

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