SecureW2 + Palo Alto Cortex® Integration Overview

Real-time Intelligence For Continuous Trust Enforcement

SecureW2 provides a dynamic and adaptive approach to secure network access by integrating seamlessly with third-party security solutions like **Palo Alto**. This integration leverages SecureW2's Dynamic PKI to ensure continuous compliance and security without slowing down network performance.

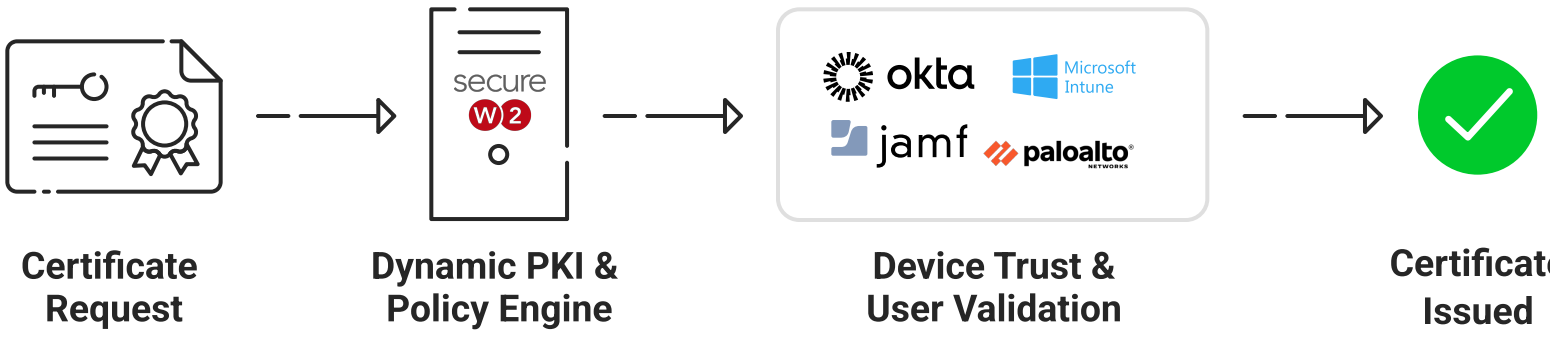
Traditional PKI relies on static, point-in-time checks (e.g. SCEP key), to determine device compliance at the moment of certificate issuance. After that, organizations have limited visibility into whether devices remain compliant.

By leveraging your Palo Alto instance with SecureW2, you gain access to dynamic security signals, ensuring access is tied to trusted devices, not outdated assumptions.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:** Palo Alto intelligence keeps certificate issuance and access retention decisions aligned with real-time security posture.

How the Palo Alto 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. Palo Alto data is streamed via API, allowing Risk Score to dynamically influence certificate issuance, or the ingested IDP/MDM data 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

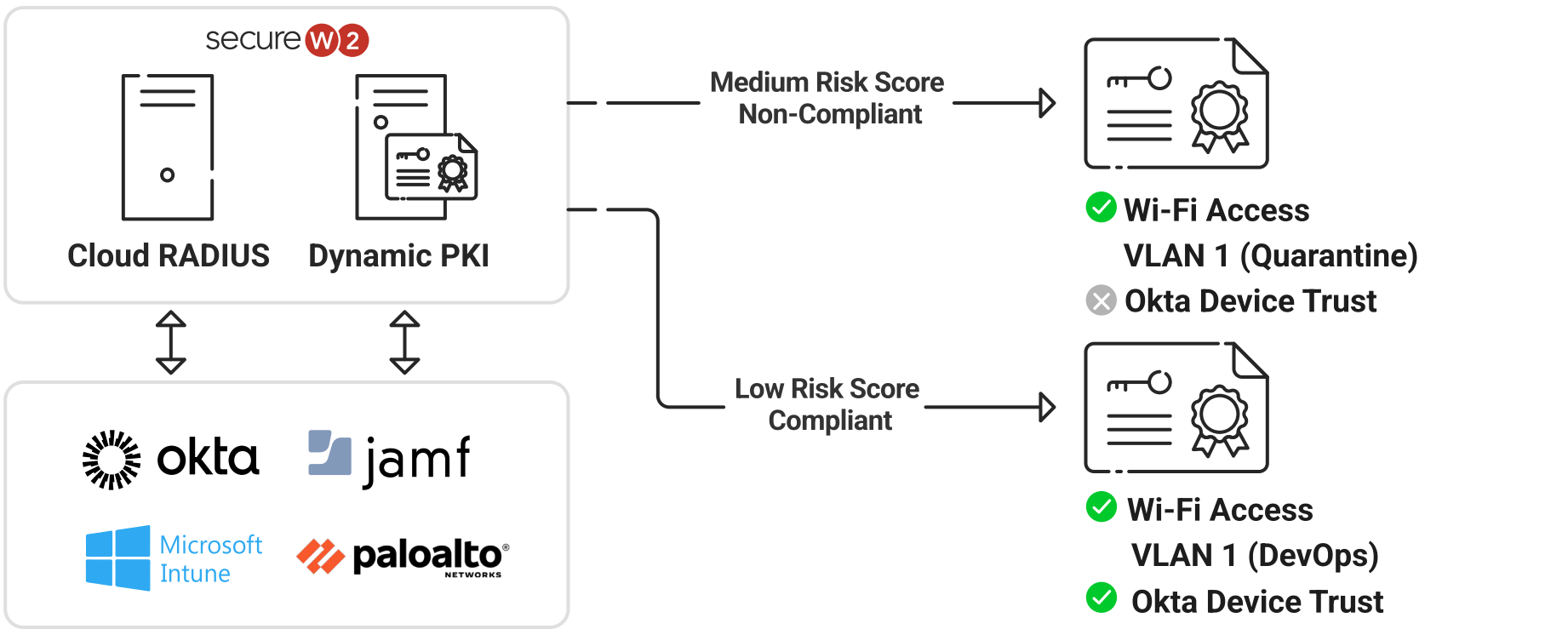
Email
sales@securew2.com

Website
www.securew2.com

Dynamically Authorize Access via Palo Alto Risk Score

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

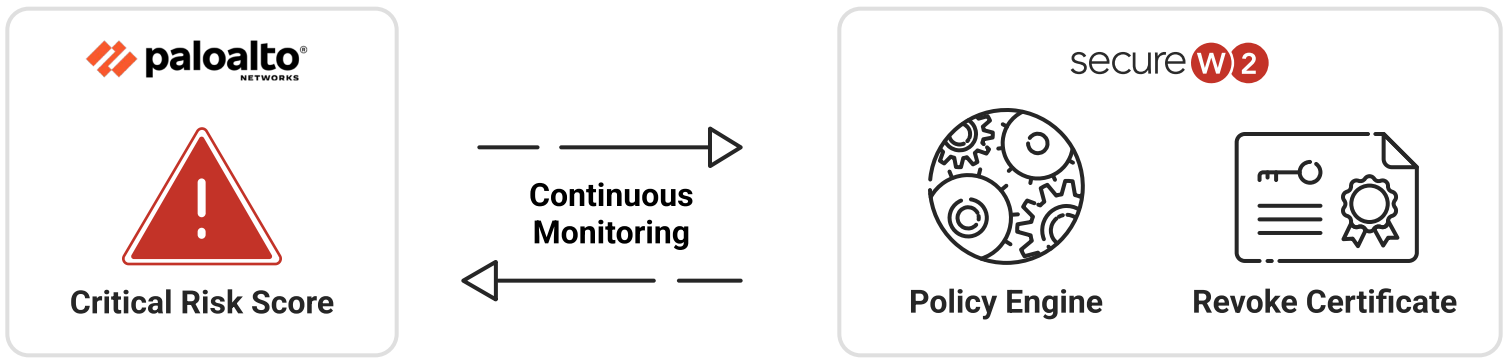
As shown below, non-compliant devices may be restricted while compliant ones maintain seamless access, ensuring security policies adapt in real time without unnecessary friction.



- **Manage Certificate Lifecycles:** During issuance, or throughout it's life cycle, SecureW2 queries Palo Alto's API to assess the device's overall Risk Score to ensure the right certificate exists.

Continuous Monitoring for Critical Events

When a device reaches a critical risk score, through continuous monitoring SecureW2 can revokes its certificate in real-time. Cutting off access before threats escalate. The workflow below shows how 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 as it's ingested with Palo Alto, 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