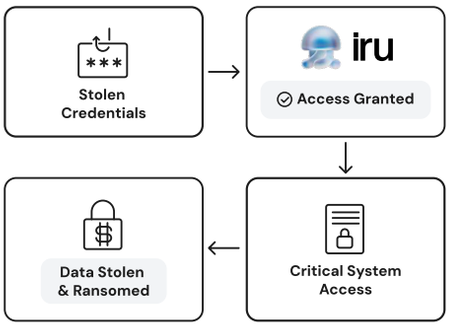
# SecureW2 + Iru®

# Better Together for Device Trust

## Credentials and MFA Alone Can't Secure Critical System Access




Organizations managing Apple device fleets with Iru rely on certificate-based authentication for Wi-Fi, VPN, and application access. However, legacy SCEP enrollment undermines security at the source: every device in the fleet shares a single static challenge secret. If that secret is exposed, any machine can obtain a valid certificate, whether or not it is enrolled in Iru.

Consider an employee offboarding scenario. A MacBook is unenrolled from Iru, but the certificate issued via static SCEP remains valid. The device continues authenticating to corporate Wi-Fi and VPN until the certificate naturally expires, potentially months later. No administrator action, no revocation, no access cutoff.

**What could have prevented it?**

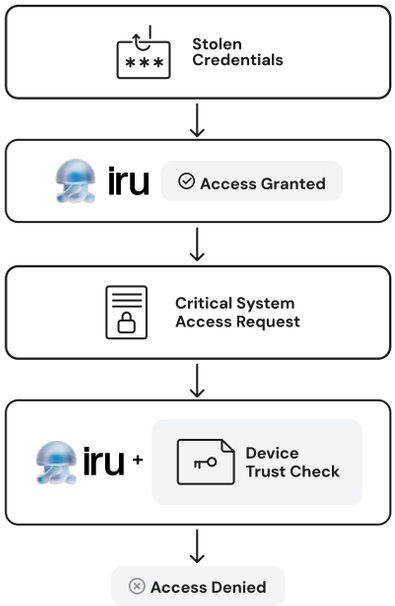
The SecureW2 platform blocks this exploit by utilizing **Apple Managed Device Attestation (MDA) and an ACME payload** to bind automated certificate profiles directly to an endpoint's hardware-bound Secure Enclave.

## Enforcing Device Trust in Iru for Systems Access

Iru manages Apple device fleets and distributes enrollment profiles via Blueprints, automating certificate delivery to all managed devices. However, legacy certificate enrollment methods fall short of modern device trust requirements.

- **Hardware-bound issuance**
- **Compliance-driven revocation**
- **Comprehensive lifecycle management**

**It's like issuing building badges without verifying the hardware that holds them or even knowing when they should be revoked.**




## Customers that Trust SecureW2 and Iru

BOMBAS color Gigamon® monday.com

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

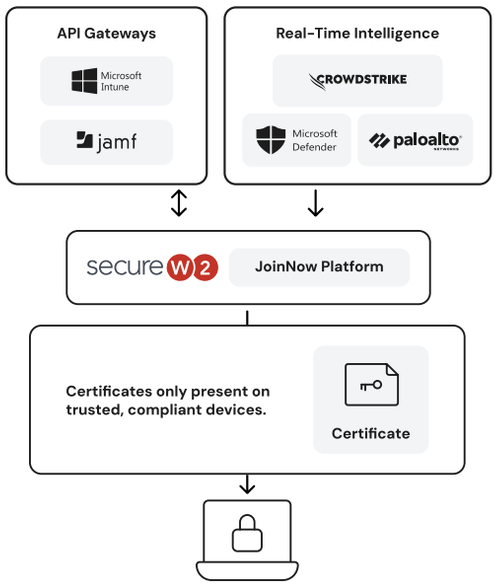
**UK, Europe and Middle East Sales**
+44 20 3912 9916

**Email**
sales@securew2.com

**Website**
securew2.com

# SecureW2 + Iru® Better Together for Device Trust

## SecureW2's platform transforms how organizations enroll, manage, and enforce certificates across Iru managed Apple fleets.

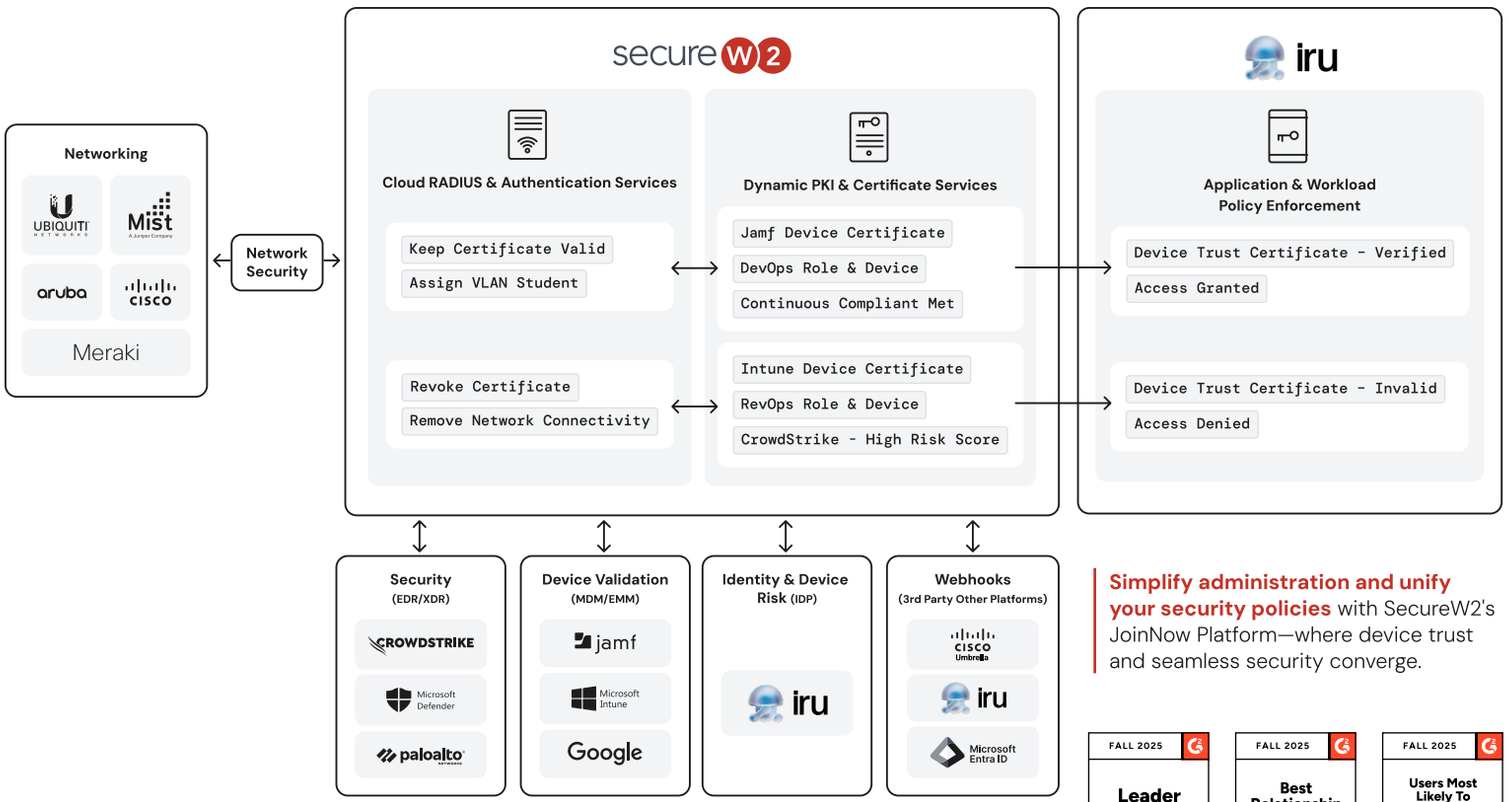



Our Advanced Certificate Services ensure:

- **Secure Delivery:** Using advanced protocols like ACME, OAuth, OpenID Connect, and SCEP APIs to eliminate vulnerabilities in legacy SCEP.
- **Policy Automation:** Our policy engine seamlessly enforces certificate issuance and lifecycle controls.
- **Native Integrations:** Easily integrate with tools like Okta, Intune, Jamf, Google, CrowdStrike, and more for advanced validation and security orchestration.

## The SecureW2 JoinNow Platform: Real-Time Device Trust for Apple Fleets

JoinNow ensures certificates represent genuinely trustworthy, Iru-managed Apple devices by integrating across identity, endpoint, and network layers.




**Simplify administration and unify your security policies** with SecureW2's JoinNow Platform—where device trust and seamless security converge.



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

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

**Email**
sales@securew2.com

**Website**
securew2.com