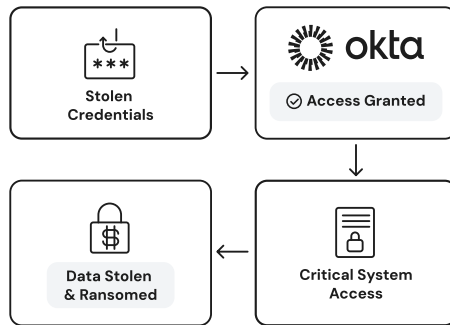


SecureW2 + Okta®

Better Together for Device Trust



Credentials and MFA Alone Can't Secure Critical System Access



Despite adopting MFA, organizations continue to face rising security threats. In fact, **57% of organizations report phishing attempts daily or weekly**, with attackers increasingly bypassing MFA methods like SMS, email codes, or authenticator apps.

Take the **2023 MGM breach** for example. As represented above, a hacker impersonated an employee to the IT helpdesk, convincing them to reset credentials and 2FA. This granted the hacker access to critical systems, escalating their attack.

What could have prevented it?

A **Device Trust** solution. By requiring devices to prove their identity and trustworthiness through digital certificates, attacks like these become virtually impossible.

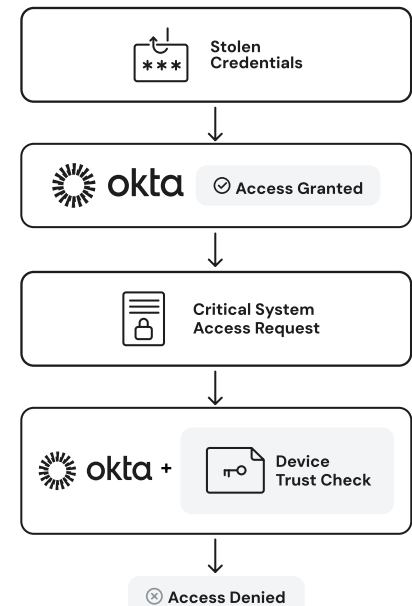
Enforcing Device Trust in Okta for Systems Access

Platforms like Okta and Entra ID support Device Trust, restricting access to only devices that prove compliance through x.509 digital certificates, as represented below. Certificates are the gold standard for enforcing trust, as they may be bound to device hardware.

However, legacy certificate solutions and “PKI-lite” options fall short. They lack:

- ❌ Robust certificate tracking and revocation
- ❌ Security-first issuance protocols
- ❌ Comprehensive lifecycle management

It's like handing out house keys without knowing who holds them, who distributed them, or how to retrieve them when necessary.



Customers that Trust
SecureW2 and Okta



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

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

Email
sales@securew2.com

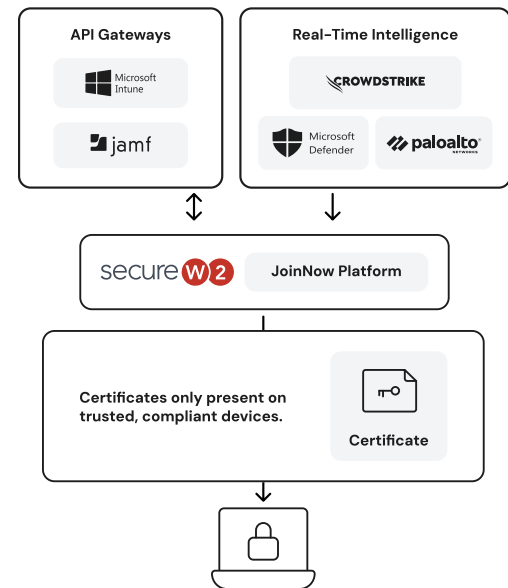
Website
securew2.com



SecureW2's platform transforms how organizations distribute, manage, and enforce certificates.

Our Advanced Certificate Services ensure:

- ✓ **Secure Delivery:** Using advanced protocols like ACME, OAuth, OpenID Connect, and Dynamic 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 Validation

JoinNow ensures **certificates represent genuinely trustworthy devices** by seamlessly integrating with leading identity and endpoint solutions.

