March 2026

A framework for securing device identities at scale

The dissolution of the traditional network perimeter has established identity as the definitive control plane for the modern enterprise. In an ecosystem driven by cloud infrastructure, a distributed workforce, and a surge in non-human identities, device identity often remains an underdeveloped aspect of an organization's security posture.

In a Zero Trust environment, device identities are not static attributes; they are non-human identities that must be verified and serve as vital context for access decisions. The device through which a user accesses corporate resources is a critical point for security enforcement. Every request to access sensitive data must be explicitly verified based on the user's identity, the device’s identity, the device's posture, and the resource's criticality.

While tactical tool deployment may offer temporary solutions, long-term security requires a more strategic approach that elevates device identity from a series of disparate challenges into a central pillar of enterprise defense.

Essential ingredients for securing device identities

To secure a diverse array of corporate-owned, managed, and unmanaged (BYOD) devices commonly found in the modern enterprise, organizations require an identity security fabric — an integrated approach to managing and monitoring all identities, human and non-human. It does not necessarily replace existing tools; instead, it weaves them together into a coherent structure that provides a unified layer of visibility and governance, enabling everything from faster threat detection to greater compliance with security mandates.

This checklist outlines the essential features of a unified identity security strategy that progresses from a state in which device identity is a siloed attribute to one in which it is an integrated component of the broader enterprise architecture and security program.

March 2026

Checklist: Securing devices as first-class identities

1. Device onboarding & account creation

- □ **Zero-touch provisioning:** Streamline device deployment by shipping corporate devices directly to employees, where the devices automatically configure themselves upon their first connection to the network. These devices can be pre-registered in the organization's management portal (e.g., Apple Business Manager) and linked to an MDM/UEM solution, which can apply initial configurations, such as device access and other identity security policies.

- □ **Management attestation:** Provide administrators with extensive control over device settings and application distribution with a dedicated cloud device management solution, rather than relying on traditional on-premises tools such as Active Directory or Group Policy Objects for Windows. Modern MDM/UEM solutions establish a consistent baseline for device health and management, leaving the identity provider (IdP) to secure the device identity itself and apply access policies based on the device's managed state.

- □ **BYOD privacy and verification:** Balance security with user privacy by creating cryptographically separate work profiles on Android and iOS devices. Organizations manage only the corporate data and applications within the work profile, while the user's personal data remains private and unmanaged. For BYOD, leverage IdP-supported browser extensions and light-weight applications to verify basic device health (e.g., checking for jailbreaking or rooting) without requiring full MDM enrollment.

- □ **Just-in-time account creation:** Enable trusted users to create new device accounts on managed desktops and laptops using IdP credentials and policy-driven permission assignment, either during device onboarding or when logging into shared workstations. Automated account management can reduce the burden on IT and security teams.

- □ **Centralized device visibility:** Support robust device profiles by registering both managed and unmanaged devices in an IdP directory, treating devices as first-class identities and making it easy to locate device details, security posture, user ownership, and more.

2. Access control

- □ **Desktop MFA:** Strengthen device access by requiring a secondary verification step, such as biometrics or a security key, at the device login touchpoint. Desktops often hold active sessions and access to critical systems, so MFA helps prevent lateral movement and privilege escalation after an initial compromise. It also strengthens compliance and auditability by enforcing consistent, verifiable access controls.

- □ **Passwordless desktop login:** Support a passwordless device login experience to enhance security by removing the use of stolen, phished, or weak passwords, while also improving the user experience by reducing login friction.

- □ **Hardware-protected application access:** Leverage device-bound credentials and sessions to sign in to applications. These technologies leverage a device's Trusted Platform Module (TPM) or Secure Enclave to provide cryptographically secure access to protected resources, making it highly resistant to credential theft and replay attacks.

3. Continuous, adaptive identity threat protection

- □ **Posture and compliance enforcement:** Assess device posture in real time for every application access decision. Device context should be incorporated into a dynamic, risk-based authentication system where policies act as a continuous gatekeeper, automatically blocking devices that fall out of compliance—due to a disabled firewall, an outdated OS, or missing encryption—from accessing resources. For BYOD, leverage IdP-supported browser extensions and light-weight applications to gain visibility and enforce compliance.
- □ **Integration with EDR tools:** Integrate endpoint detection and response (EDR) platforms with the IdP to gain deeper visibility into device-level threats. This telemetry, when shared with the IdP, can be used to dynamically adjust access based on the device's current risk level.
- □ **Device-bound single sign-on:** Enable hardware-protected, cryptographically secured SSO sessions that start from device login. This ties application access to trusted user and device identities to help eliminate session replay, while providing users access to applications with fewer authentication prompts.
- □ **Automated device logout:** Detect suspicious activity on a device mid-session, and automatically trigger actions such as a device logout, session revocation, or step-up authentication. By establishing a baseline of normal behavior through continuous monitoring, policies can deny access when anomalies are detected that may signal a compromise.

The ROI of secure device identities

The transformation to secure device identities as first-class entities is not merely a technical endeavor but a fundamental business transition that delivers measurable ROI in security, efficiency, and compliance. Organizations can realize benefits that contribute to their bottom line.

- **Reduced risk profile:** Secure device access and continuous posture assessment help reduce the likelihood and impact of credential theft, session replay, and account takeover. This directly supports breach prevention, limits lateral movement, and protects brand trust and revenue continuity.
- **Workforce productivity:** Taking steps to streamline device onboarding and reduce login friction helps eliminate repetitive work and disruption to the user's workday, freeing end users and security and IT teams to focus on higher-value tasks.
- **Compliance readiness:** Meeting internal and external security requirements becomes much easier with a mature approach to device identity and can help demonstrate to regulators that the organization has implemented a high standard of cybersecurity.

As a whole, device identities constitute a strategic control plane for access, risk reduction, and compliance. They enable scalable protection of sensitive resources while supporting a distributed workforce.

Ready to secure your device identities? Click here to contact our team.

Disclaimers: These materials are for general informational purposes only and do not constitute legal, privacy, security, compliance, or business advice. The content may not reflect the most current security, legal and/or privacy developments. You are solely responsible for obtaining advice from your own legal and/or professional advisor and should not rely on these materials. Okta makes no representations or warranties regarding this content and is not liable for any loss or damages resulting from your implementation of these recommendations. Information on Okta's contractual assurances to its customers may be found at okta.com/agreements.