Specops Device Trust: Zero Trust Workforce Access

Identity alone isn't enough. If access depends solely on "who you are," then you're one session hijacking attack away from a breach (even with MFA). Attackers steal session tokens, use compromised devices, and exploit gaps in traditional identity controls.

The Specops Device Trust solution: Authenticate and verify both user AND device at every login and continuously throughout sessions.

Authentication

- Bind identities to authorized devices
- Stolen credentials can't be used from attacker's devices

Verification

- Check device posture throughout sessions
- Minimal user friction without invasive MDM

Remediation

- Rapid self-service remediation – no IT tickets
- One-click fixes and user grace periods

Deployment & Integration

- **Operating Systems**: Windows, macOS, Linux, iOS, Android
- **Identity Provider Integration**: Okta, Azure AD/Microsoft Entra ID, Ping Identity
- **Deployment Model**: Cloud SaaS (99.99%+ availability)
- **Performance Impact**: Won't slow down users' devices
- **Rollout Options**: Phased deployment by user group, device type, or OS platform

How Infinipoint differs from MDM solutions

Capability	Infinipoint	MDM Solutions
Makes real-time access decisions at authentication, not periodic compliance checks	✓	✗
Verifies continuously throughout sessions , not just at login	✓	✗
Enables user self-remediation instead of blocking access	✓	✗
Works with BYOD without invasive installation	✓	✗
Integrates directly with IdPs for seamless authentication	✓	✗

Core Features

Feature	How you'll benefit
Zero Device Trust Verification	Verify device posture at every access request and continuously throughout each session. Hundreds of granular posture checks.
Phishing-Resistant Authentication	Binds users to trusted devices. Authentication only occurs from approved, enrolled hardware, preventing credential attacks and session hijacking.
User-Device Pinning	Enroll approved devices and bind specific users to authorized hardware. Control device count, type (desktop, mobile), and classification (corporate, BYOD) per user or group.
Continuous Posture Checks	Device security verification at logon and every 10 minutes throughout active sessions. Checks for active threats, disabled security controls, and failed compliance checks.
One-Click Remediation	Self-service compliance fixes ("Enable Encryption," "Update OS," "Enable Firewall") with configurable grace periods. Automated workflows reduce IT support burden while maintaining security posture.
Third-Party Device Security	Complete endpoint visibility including unmanaged BYOD and contractor devices. Distinguishes between corporate-managed assets and shadow IT accessing network resources.
Risk-Based Access Policies	Granular policy controls based on user groups, device types, OS platforms, and real-time compliance state. Dynamic access decisions adjust to current device health.

See Specops Device Trust in action

Secure your workforce access with zero trust.

Learn more: www.specopssoft.com/product/specops-device-trust/
Request a demo: https://specopssoft.com/contact-us/