Specops Device Trust: Zero Trust Workforce Access

Allein die Identität schützen reicht nicht. Wenn der Zugriff nur von benutzerspezifischen Faktoren abhängt, kann ein einziger Session-Hijacking-Angriff eine Sicherheitslücke verursachen, selbst mit MFA. Angreifer stehlen Sitzungstoken, nutzen kompromittierte Geräte und exploitieren Schwachstellen in herkömmlichen Identitätskontrollen.

Die Lösung von Specops Device Trust: Authentifizieren und überprüfen Sie Benutzer UND Geräte an jedem Zugangspunkt kontinuierlich während jeder Sitzung.

Authentifizierung

- Identitäten an autorisierte Geräte binden
- Gestohlene Zugangsdaten können nicht von den Geräten der Angreifer verwendet werden

Verifizierung

- Gerätesicherheit während der gesamten Sitzung überprüfen
- Minimale Benutzerbelastung ohne invasives MDM

Behebung

- Schnelle Self-Service-Behebung – keine IT-Tickets erforderlich
- Ein-Klick-Behebung und Kulanzfristen für Benutzer

Implementierung & Integration

- **Betriebssysteme:** Windows, macOS, Linux, iOS, Android
- **Identitätsanbieter-Integration:** Okta, Azure AD/Microsoft Entra ID, Ping Identity
- **Implementierungsmodell:** Cloud SaaS (Verfügbarkeit > 99,99 %)
- **Leistungsimpact:** Keine Verlangsamung der Benutzergeräte
- **Rollout-Optionen:** Stufenweise Implementierung nach Benutzergruppen, Gerätetyp oder Betriebssystemplattform

Unterschiede zu MDM-Lösungen

Fähigkeit	Infinipoint	MDM -Lösungen
Echtzeit-Zugriffsentscheidungen bei der Authentifizierung, nicht nur periodische Compliance-Prüfungen	✓	✗
Kontinuierliche Überprüfung während der Sitzung, nicht nur beim Login	✓	✗
Ermöglicht Self-Service-Behebung statt Zugriffssperre	✓	✗
Funktioniert mit BYOD (“Bring Your Own Device”) ohne invasive Installation	✓	✗
Direkte Integration mit IdPs für nahtlose Authentifizierung	✓	✗

Kernfunktionen

Funktion	Nutzen
Zero Device Trust Verifikation	Überprüfung des Gerätestatus bei jeder Zugriffsanforderung und kontinuierlich während der gesamten Sitzung. Hunderte granularer Checks.
Phishing-resistente Authentifizierung	Benutzeridentitäten werden an ihre genehmigten Geräte gebunden. Die Authentifizierung erfolgt nur von autorisierter Hardware.
User-device Pinning	Genehmigte Geräte registrieren und bestimmten Benutzern zuweisen. Kontrolle über Anzahl, Gerätetyp (Desktop, Mobile) und Klassifikation (Corporate, BYOD).
Kontinuierliche Kontrollprüfungen	Sicherheitsüberprüfung bei Anmeldung und alle 10 Minuten. Erkennt aktive Bedrohungen, deaktivierte Sicherheitskontrollen und Compliance-Verstöße.
Ein-Klick-Behebung	Self-Service-Compliance-Fixes („Verschlüsselung aktivieren“, „OS aktualisieren“, „Firewall aktivieren“) mit konfigurierbaren Kulanzfristen. Reduziert den IT-Aufwand und sichert gleichzeitig die Produktivität.
Sichtbarkeit für Drittgeräte	Volle Transparenz über alle Endpoints, inklusive unverwalteter BYOD- und Fremdgeräte. Unterscheidung zwischen Unternehmensgeräten und Shadow IT.
Risikobasierte Zugriffsrichtlinien	Granulare Richtlinien nach Benutzergruppen, Gerätetypen, Betriebssystemen und Echtzeit-Compliance. Dynamische Zugriffskontrolle basierend auf Gerätesicherheit.

Specops Device Trust selbst entdecken

Sichern Sie den Zugriff Ihrer Mitarbeiter mit Zero Trust

Mehr erfahren: https://specopssoft.com/de/produkte/specops-device-trust/
Demo anfordern: https://specopssoft.com/de/kontakt/