MFA FÜR WINDOWS-LOGIN, RDP UND VPN mit SPECOPS SECURE ACCESS

Specops Secure Access fügt Windows-Anmeldungen, RDP- und VPN-Verbindungen eine zusätzliche MFA-Schutzebene hinzu und unterstützt Unternehmen dabei, hybride Umgebungen besser abzusichern sowie Compliance- und Cyberversicherungsanforderungen zu erfüllen. Mit flexiblen MFA-Optionen, einschließlich eines Offline-Modus, ermöglicht Secure Access eine sichere Authentifizierung beim Login, an der Konsole, bei der Nutzung von Remote Desktop sowie bei VPN-Verbindungen über RADIUS.

Specops Secure Access integriert sich in Ihre SIEM-, SOC- und Analytics-Plattformen und sorgt so für vollständige Transparenz über Sicherheitsereignisse. Zusätzlich unterstützt die Lösung Single Sign-On (SSO) für SaaS-Anwendungen über OIDC und SAML.

Die Einrichtung von Specops Secure Access ist einfach. Benutzer werden bei ihrem ersten Authentifizierungsversuch über den Windows-Client durch den Registrierungsprozess geführt. Zur MFA-Registrierung stehen YubiKey, Microsoft Authenticator, Google Authenticator, die Specops:ID App sowie SMS-OTP zur Verfügung. Offline-MFA wird mit Specops:ID, Microsoft Authenticator, Google Authenticator und YubiKey unterstützt. Wenn Sie Specops Secure Access in Kombination mit anderen Specops-Authentifizierungslösungen einsetzen, können Sie die Benutzerregistrierung auf sichere Passwort-Resets, Benutzerverifizierung im Service Desk sowie die Wiederherstellung von Festplattenverschlüsselungsschlüsseln erwei

FUNKTIONEN	Specops SECURE ACCESS
MFA beim Windows-Login	Ja
MFA für RDP-Verbindungen	Ja
MFA für VPN-Verbindungen (RADIUS)	Ja

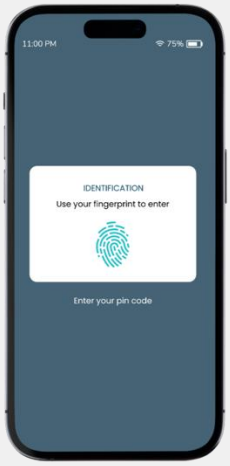
FUNKTIONEN	Specops SECURE ACCESS
SSO-Unterstützung für SaaS-Anwendungen über OIDC und SAML	Ja
Integration von Security Event APIs für SIEM-, SOC- und Analytics-Plattformen	Ja
Anpassbare „Remember Me“-Einstellungen zur Reduzierung der MFA-Abfragen bei Anmeldung/Entsperrung, VPN oder RDP	Ja
OOTB-Authentifizierung mit Yubikey	Ja
Microsoft Authenticator und Google Authenticator	Ja
Push-Benachrichtigungen ohne bestehenden Drittanbieter-Identity-Service	Ja, mit der enthaltenen Specops:ID-App
Biometrische Authentifizierung	Ja, mit der enthaltenen Specops:ID-App
Offline-Unterstützung	Ja, mit Specops:ID, Microsoft Authenticator, Google Authenticator und Yubikey
Schutz beider Login-Ebenen – Active Directory Passwort und flexible 2FA-Optionen	Ja, mit Specops Password Policy

Passwörter werden 1287 Mal pro Minute angegriffen (Microsoft)
Microsoft hat im Jahr 2022 1287 Passwortangriffe pro Minute beobachtet. Die beste Verteidigung gegen ein solches Angriffsvolumen ist ein mehrschichtiger Ansatz.

Wie sieht das in der Praxis aus?

Benutzererfahrung beim Windows-Login

Mit installiertem und konfiguriertem Specops Client für Secure Access werden Benutzer nach Eingabe ihres Windows-Benutzernamens und Passworts zur zusätzlichen Authentifizierung mit einem zweiten Faktor aufgefordert. Nach erfolgreicher Bestätigung erfolgt die Anmeldung wie gewohnt.



Unternehmen, deren Benutzer per VPN auf das Netzwerk zugreifen oder über ein Remote Desktop Gateway (RDGW) arbeiten, können ihre Zugriffe durch eine zusätzliche Authentifizierungsebene absichern.

Der VPN-Server oder das Remote Desktop Gateway kann über RADIUS so konfiguriert werden, dass Microsoft NPS (Network Policy Server) mit installiertem Specops NPS Companion angesprochen wird, wodurch Secure Access genutzt werden kann.

Zentrale Authentifizierung mit SSO

- Erweitern Sie die Specops-Authentifizierung auf SaaS-Anwendungen von Drittanbietern und reduzieren Sie die Notwendigkeit separater Identity Provider
- Die Unterstützung von OpenID Connect und SAML ermöglicht Single Sign-On über eine Vielzahl moderner Anwendungen
- Verwalten Sie Benutzerzugriffe zentral an einem Ort, vereinfachen Sie die Administration und reduzieren Sie Ihre Identitäts-Angriffsfläche

Eine Demo von Specops Secure Access anfordern

Möchten Sie sehen, wie Specops Secure Access in Ihrer Umgebung funktioniert?

Klicken Sie hier