

SPECOPS SECURE SERVICE DESK

Datenblatt

ÜBER SPECOPS Specops Software ist der führende Anbieter von Lösungen zur Passwortverwaltung und Authentifizierung. Specops schützt Ihre Geschäftsdaten, indem es schwache Passwörter blockiert und die Benutzer-Authentifizierung absichert. Täglich nutzen Tausende von Unternehmen Specops Software, um ihre Geschäftsdaten zu schützen. Für weitere Informationen besuchen Sie bitte specopssoft.com

SPECOPS SECURE SERVICE DESK

Das Zurücksetzen von Mitarbeiterkennwörtern ist weiterhin die Ursache einer großen Anzahl von Servicedesk-Tickets. Sie stellen nicht nur eine Belastung für die IT-Ressourcen, sondern auch eine Sicherheitslücke für Ihr Unternehmen dar. Kann Ihr Servicedesk feststellen, ob ein Benutzer wirklich der ist, für den er sich ausgibt, bevor er einem Angreifer, der sich als einer Ihrer Benutzer ausgibt, ein neues Passwort übergibt?

Die Servicedesk-Überprüfung von Benutzern basiert häufig auf wissensbasierten Fragen unter Verwendung statischer Identitätsinformationen aus Active Directory oder Entra ID und ist daher anfällig für gezielte Angriffe, wie z. B. die Ausnutzung der Mitarbeiter-ID.

Specops Secure Service Desk erhöht die Sicherheit durch stärkere Authentifizierungsmethoden, die das Risiko einer Benutzernachahmung minimieren. Die Optionen zur Identitätsüberprüfung reichen von mobilen oder E-Mail-Überprüfungs_codes bis hin zu kommerziellen Authentifizierungsanbietern wie Duo Security, Okta, Symantec VIP, PingID und YubiKey. Diese Authentifizierungsoptionen sind mit einer technischen Durchsetzung der ID-Verifizierung gepaart, die Agenten daran hindert, die Anfrage des Anrufers weiter zu bearbeiten, bis die Authentifizierung über die Plattform abgeschlossen ist.

48 % der Unternehmen erzwingen keine Benutzerverifizierung für Anrufe beim Servicedesk

Quelle: The Weak Password Report

Funktionshighlights

FUNKTIONEN	ANDERE LÖSUNGEN	SPECOPS SECURE SERVICE DESK
OOTB-Identifikationsdienste von Drittanbietern, z. B. Duo Security, Okta, Symantec VIP, PingID	Einiges an Unterstützung aber mangelhaft	Ja, plus mehrere andere ID-Optionen zur Unterstützung nicht mobiler Benutzer
Servicedesk-Schnittstelle zur Benutzerüberprüfung	Ja	Ja (plus sichere Anmeldungen für Servicedesk-Agenten)
Vom Servicedesk unterstützte Passwortzurücksetzungen	Nein	Ja (und kann Benutzer zwingen, bei der nächsten Anmeldung ihr Passwort zu ändern)



FUNKTIONEN	ANDERE LÖSUNGEN	SPECOPS SECURE SERVICE DESK
Durchsetzung der Benutzerüberprüfung (Agent kann ohne vorherige Überprüfung nicht fortfahren)	Nein (Agent muss die Identität nicht authentifizieren, bevor er dem Anrufer hilft)	Ja
Benutzerüberprüfungsverfolgung	Ja (aber es fehlen Details)	Ja (Details dazu, wer überprüft wurde, für welchen Anwendungsfall und von wem)
API zur Benutzerüberprüfung	Manche	Ja (ermöglicht die Benutzerüberprüfung mit Systemen von Drittanbietern mit einem der über 15 registrierten ID-Dienste)

Der MGM-Ransomware-Angriff im Jahr 2023, der das Unternehmen über 100 Millionen US-Dollar kostete, war auf eine fehlende ID-Verifizierung am Servicedesk zurückzuführen.

[Lesen Sie mehr über diesen Angriff.](#)

Wie funktioniert das?

Specops Secure Service Desk ist nativ in Active Directory und Entra ID integriert. Die Konfiguration des Systems erfolgt über Group oder Cloud Policy, ohne die Komplexität Ihrer Umgebung zu erhöhen. Der Datenschutz ist gewährleistet, da die Registrierung Ihrer Benutzer verschlüsselt und nicht als Ganzes an einem einzigen Ort gespeichert wird. Dadurch wird das Sicherheitsrisiko minimiert und gleichzeitig eine Bereitstellung in Echtzeit sichergestellt.



1. Der Benutzer vergisst sein Passwort und ruft den Service Desk an, um ein neues Passwort zu erhalten.



2. Bevor der Service Desk-Agent das Passwort zurücksetzen kann, muss er die Identität des Benutzers mithilfe von Secure Service Desk überprüfen.



3. Der Service Desk-Agent sendet einen geheimen Einmalcode an das mobile Gerät, das mit dem Active Directory- oder Entra ID-Konto des Benutzers verknüpft ist. Nur der Benutzer kann den geheimen Einmalcode sehen.



4. Der Benutzer erhält den Code und leitet ihn an den Service Desk-Agenten weiter.



5. Der Service Desk-Agent gibt den Einmalcode in Secure Service Desk ein und kann nun das Passwort des Benutzers zurücksetzen.



Wie sieht dieser Ansatz aus?

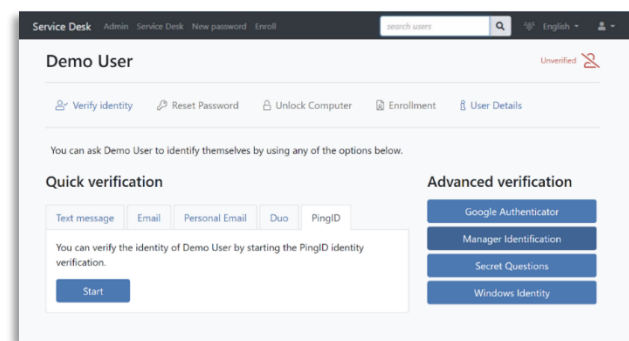
Über die Lösungsschnittstelle können Servicedesk-Agenten Benutzerdetails anzeigen und die folgenden Aktionen ausführen:

1. Verwalten von Benutzerregistrierungen
2. Active Directory-/Entra-ID-Passwörter zurücksetzen
3. Wiederherstellungsverschlüsselungsschlüssel für Sperren, die durch BitLocker oder Symantec Endpoint Encryption ausgelöst wurden (nicht verfügbar für Secure Service Desk for Cloud)

Servicedesk-Agentenansicht

Die oben genannten Aktionen können durch die Aktivierung der Durchsetzung der Benutzerüberprüfung gesichert werden.

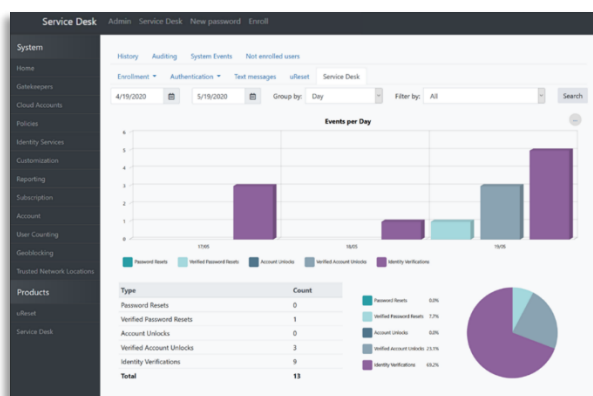
Wenn diese Funktion aktiviert ist, muss der Agent die Identität des Benutzers erfolgreich überprüfen, bevor er eine dieser risikoreichen Aktionen ausführen kann.



Admin-Berichtsansicht

Die Benutzerüberprüfung kann innerhalb der Lösung über detaillierte Prüfprotokolle verfolgt werden.

Category	Action	Result	Time	User
UserManagement	ResetPassword	Success	5/18/2020, 10:44:40 PM	1508d355-a057-4b40-a25b-454603742463
TargetWorld: 5a2b3c17-21c4-4a47-91a3-147d406c4839				
ServiceDeskUserVerificationTokenIdentifier: 0b1a1f9e-6d3e-4715-bd07-296c338b6ec				
TargetType: demoUser@specopsdemo2.com				
UserMail: 1508d355-a057-4b40-a25b-454603742463				
UserManagement	VerifyIdentity	Success	5/18/2020, 10:44:31 PM	1508d355-a057-4b40-a25b-454603742463
UserManagement	VerifyIdentity	Success	5/18/2020, 10:28:13 PM	1508d355-a057-4b40-a25b-454603742463
UserManagement	UnlockAccount	Success	5/18/2020, 10:02:20 PM	1508d355-a057-4b40-a25b-454603742463
UserManagement	UnlockAccount	Success	5/18/2020, 10:01:21 PM	1508d355-a057-4b40-a25b-454603742463
UserManagement	UnlockAccount	Success	5/18/2020, 10:00:28 PM	1508d355-a057-4b40-a25b-454603742463
UserManagement	VerifyIdentity	Success	5/18/2020, 9:41:42 PM	1508d355-a057-4b40-a25b-454603742463
UserManagement	VerifyIdentity	Success	5/18/2020, 9:38:37 PM	1508d355-a057-4b40-a25b-454603742463
UserManagement	VerifyIdentity	Success	5/18/2020, 9:09:45 PM	1508d355-a057-4b40-a25b-454603742463
UserManagement	VerifyIdentity	Success	5/18/2020, 4:09:32 PM	1508d355-a057-4b40-a25b-454603742463



Die Lösung bietet außerdem ein Berichts-Dashboard, das Überprüfungsdaten aus mehreren Anwendungsfällen widerspiegelt. Diese Daten können zur weiteren Verarbeitung auch nach JSON oder XSLX exportiert werden.



Was unsere Nutzer sagen

Hält, was es verspricht

„Specops Secure Service Desk hält, was es verspricht. Es hilft Organisationen, eine sichere Benutzerüberprüfung durch stärkere Authentifizierungsmethoden durchzusetzen.“

- [Techgenix-Bewertung](#) von Nuno Mota, Microsoft Exchange, MVP



Exponentiell schwieriger für einen Angreifer

„Es bietet Servicedesk-Technikern die Möglichkeit, die Identität eines vermeintlichen Endbenutzers, der eine Kennwortzurücksetzung anfordert, effektiv zu überprüfen. Dies sollte es einem Angreifer, der Social Engineering oder eine andere Art von Angriff durchführen möchte, exponentiell schwerer machen, Anmeldeinformationen zu stehlen.“

- [4sysops-Bewertung](#) von Brandon Lee, Senior Editor bei Virtualizationhowto.com



Sehen Sie sich eine Demo von Specops Secure Service Desk an

Sind Sie daran interessiert, zu erfahren, wie Specops Secure Service Desk für Ihr Unternehmen funktionieren kann?

[Klicken Sie hier](#), um noch heute eine Demo oder Testversion einzurichten.

Unsere Technologiepartner

Unsere Technologiepartnerschaften sorgen dafür, dass Unternehmen den Wert ihrer bestehenden Investitionen und Systeme sicher steigern können, um die Passwortsicherheit zu optimieren - sei es durch die Erweiterung bestehender Investitionen in die Multi-Faktor-Authentifizierung oder durch die Erweiterung der Microsoft Active Directory-Funktionalität. [Mehr lesen.](#)

