ISEC7 THE DIGITAL WORKPLACE COMPANY | Hypergate

MOBILE ANMELDUNG MIT HYPERGATE



Komfort wie in der Cloud. Souveränität wie im eigenen Rechenzentrum.

Hypergate bringt Kerberos-Single-Sign-On auf Android und iOS, gegen das Active Directory, das bei Ihnen schon läuft. ISEC7 integriert und betreibt die Lösung.

Kerberos-SSO
für Android und iOS

Kein zusätzlicher Server
direkt gegen Ihre Domain Controller

On-Premises
Authentifizierung und Daten bleiben im eigenen Rechenzentrum

Über Ihr UEM
als verwaltete App verteilt

HERAUSFORDERUNG

Zwei Änderungen treffen dieselbe Stelle im Netz: wie sich ein Diensthandy anmeldet und wie es an die Dateiablage kommt. Microsoft schaltet NTLM schrittweise ab, und Acronis Cyber Files bekommt nach dem 31. Dezember 2026 keine Sicherheitsupdates mehr.

Die Ersatzverfahren, die Microsoft für NTLM baut, gibt es für Windows. Smartphones und Tablets, die bisher über NTLM an Intranet, interne Webanwendungen und Freigaben kamen, brauchen einen Weg über Kerberos.

CHANCE

Hypergate, ein Schweizer Anbieter aus Zug, schließt beide Lücken. Hypergate Authenticator meldet Android- und iOS-Geräte per Kerberos direkt an den vorhandenen Domain Controllern an, mit einem Benutzerzertifikat aus Ihrem UEM oder mit Benutzername und Passwort. Hypergate Files öffnet damit die bestehenden Freigaben, mit den NTFS-Rechten, die Sie schon vergeben haben.

DIE LÖSUNG & USP

- Kerberos-Single-Sign-On auf Android und iOS, ohne Passwortabfrage in jeder App
- Keine Cloud-Identität nötig: Authentifizierung und Daten bleiben im eigenen Rechenzentrum
- Kein zusätzlicher Server zwischen Gerät und Domain Controller
- Dateizugriff über SMB2 und SMB3 auf Windows-Freigaben und NetApp, in der nativen Dateien-App des Geräts
- Verteilung als verwaltete App über Microsoft Intune, Ivanti, Omnissa Workspace ONE, BlackBerry UEM, SOTI oder 42Gears
- Keine Daten auf dem Gerät: Dateien bleiben auf Ihren Servern, lokal wird nichts zwischengespeichert, und die DLP-Vorgaben Ihres UEM gelten

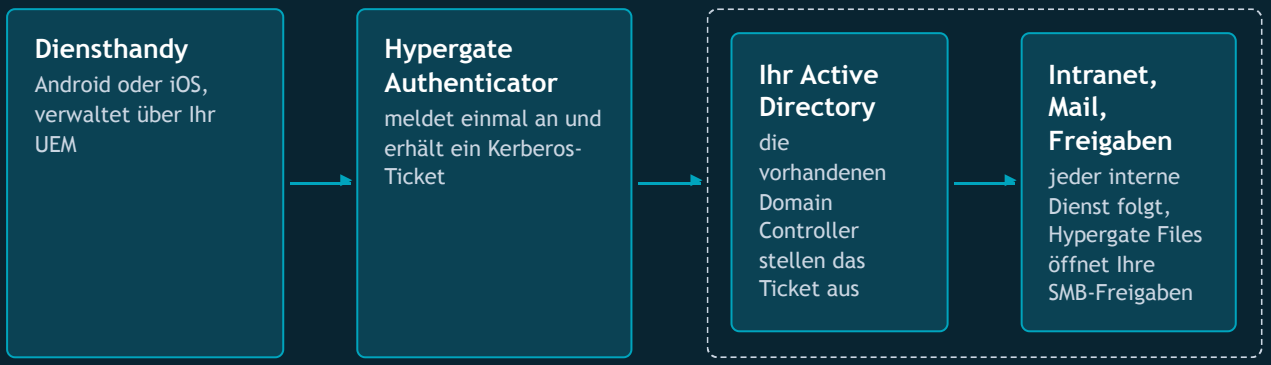
WER WAS MACHT

Hypergate stellt die Software her. ISEC7 ist Partner von Hypergate, integriert die Apps in Ihr UEM, betreibt sie und ist Ihr Ansprechpartner im Support. Ein Proof of Concept läuft rund 30 Tage, ist kostenlos und kommt ohne Änderung an Ihrer Infrastruktur aus.

Die ISEC7 Group betreibt seit 2003 Digital Workplace und Managed Mobility Services. Für Behörden, internationale Konzerne, KRITIS-Betreiber, geheimschutzbetreute Unternehmen und alle Organisationen, die hohe Compliance-Anforderungen erfüllen müssen. Über 700 Kunden weltweit, darunter Regierungen, Polizeibehörden und Streitkräfte. Der Hauptsitz von ISEC7 ist in Deutschland, weitere Standorte gibt es in den USA, Australien, Neuseeland und Polen.

ISEC7 | Hypergate

Einmal anmelden. Auf alles zugreifen.



Alles im Rahmen läuft in Ihrem eigenen Rechenzentrum.

ZIELGRUPPE

- Endpoint Manager und Administratoren mit Android- und iOS-Flotten
- CISO, für die eine Cloud-Identität als Anmeldeweg nicht in Frage kommt
- Behörden, Verteidigung, Finanzwesen, Versicherungen und Gesundheitswesen
- Organisationen, die Acronis Cyber Files ablösen müssen

ANWENDUNGSBEREICHE

- Single Sign-On für Intranet und interne Webanwendungen
- Zugriff auf Freigaben von Smartphone und Tablet
- Ausstieg aus NTLM auf Mobilgeräten
- Ablösung von Acronis Cyber Files

WOMIT SIE ANFANGEN

Zuerst klären Sie, welche Geräte und Dienste noch auf dem alten Anmeldeverfahren stehen. ISEC7 SPHERE liefert diese Bestandsaufnahme. Im Netz brauchen die Geräte Kerberos (Port 88) zu den Domain Controllern und SMB (Port 445) zu den Fileservern, über Ihr vorhandenes VPN. ISEC7 MAIL unterstützt die Anmeldung mit Hypergate.

MEHR ERFAHREN

www.isec7.com/de/hypergate-migration

ISEC7 THE DIGITAL WORKPLACE COMPANY
Schellerdamm 16, 21079 Hamburg · isec7.com · sales@isec7.com · +49 40 325076 0