WHITE PAPER

Zero Trust Identitätssicherheit für Unternehmen

Passwortlose Authentifizierung mit PKI, mTLS und Federated SSO

Wie Soliton OneGate und NetAttest EPS passwortbasierte Risiken eliminieren. Von der Netzwerksicherheit (IEEE 802.1X) bis zum Cloud-SSO (SAML/OIDC). Mit automatisiertem Zertifikats-Lifecycle, SASE-Integration und nachweisbarer Compliance für NIS2, DSGVO und ISO 27001.

SecureComply GmbH | April 2026

SecureComply
Secure by Design. Compliant by Default.

SecureComply

Secure by Design. Compliant by Default.

Soliton OneGate & NetAttest EPS

Zero Trust Identitätssicherheit von der Netzwerkschicht bis in die Cloud

Für Verwaltungsräte, Geschäftsleitungen und IT-Entscheider

Kompromittierte Zugangsdaten sind heute das grösste Einfallstor für Cyberangriffe und damit ein direktes Geschäftsrisiko. Täglich werden weltweit zwischen 3,4 und 6 Milliarden Phishing-E-Mails verschickt. 60 bis 80 % aller Datenpannen lassen sich auf gestohlene oder schwache Passwörter zurückführen. Die finanziellen und reputativen Folgen eines solchen Vorfalls treffen nicht nur die IT-Abteilung, sondern das gesamte Unternehmen und letztlich die Organe, die für das Risikomanagement verantwortlich sind.

Dieses White Paper zeigt, wie sich mit Soliton OneGate und NetAttest EPS eine passwortlose Zero-Trust-Infrastruktur aufbauen lässt, die vom Netzwerkzugang bis zur Cloud-Anwendung greift. Der Fokus liegt dabei nicht auf technischen Details, sondern auf der strategischen Frage:

Wie schützen wir unsere Organisation wirksam und wie weisen wir diese Sorgfalt gegenüber Regulatoren und Stakeholdern nach?

Inhaltsverzeichnis

01 Executive Summary

Passwörter sind heute das schwächste Glied jeder Sicherheitsarchitektur. Täglich werden zwischen 3,4 Milliarden und 6 Milliarden Phishing-E-Mails verschickt. Rund 31% aller Datenpannen beginnen mit kompromittierten Zugangsdaten (Verizon DBIR 2024).

Die Lösungen von Soliton bieten messbare geschäftskritische Vorteile.

Risikominimierung und Compliance:

- Signifikante Reduktion des Haftungsrisikos durch Minimierung passwortbasierter Schwachstellen
- Erfüllung regulatorischer Anforderungen (DSGVO, NIS2, ISO 27001) durch nachweisbare Zero Trust Architektur
- Schutz vor Reputationsschäden und schwerwiegenden Datenpannen

Operative Effizienz:

- Signifikante Kosteneinsparungen durch Reduktion von Password-Reset-Anfragen
- Produktivitätssteigerung durch nahtlosen, passwortlosen Zugriff für Mitarbeitende
- Minimierung von Ausfallzeiten durch proaktive Sicherheitsarchitektur

Wettbewerbsvorteil:

- Vertrauensbildung bei Kunden und Partnern durch höchste Sicherheitsstandards
- Attraktivität als Arbeitgeber durch moderne, benutzerfreundliche IT-Infrastruktur
- Zukunftssichere Investition in skalierbare Enterprise-Technologie

Dieses White Paper zeigt, wie Soliton OneGate und NetAttest EPS gemeinsam eine vollständige Zero Trust Infrastruktur bilden. Von der Netzwerkschicht bis zur Cloud-Anwendung, von der Gerätezertifizierung bis zum passwortlosen Single Sign-On und damit einen ROI liefern, der weit über reine IT-Sicherheit hinausgeht.

02 Einleitung

Unternehmen investieren erheblich in IT-Sicherheit und werden dennoch täglich mit erfolgreichen Angriffen auf Identitäten und Zugangsdaten konfrontiert. Der Grund ist strukturell. Die meisten Sicherheitsarchitekturen vertrauen jedem Gerät, das gültige Credentials vorweist. Echte Zero Trust Sicherheit erfordert mehr als ein Passwort.

Soliton OneGate und NetAttest EPS bilden zusammen eine vollständige Zero Trust Identity-Infrastruktur, die von der Netzwerkschicht bis zur Cloud-Anwendung reicht. X.509-Gerätezertifikate bilden das Fundament. Sie ergänzen die Anmeldung durch einen kryptographisch starken, gerätegebundenen Faktor, der beim gegenseitigen TLS-Handshake (mTLS) in beide Richtungen zur Absicherung dient. Das Ergebnis ist eine Authentifizierung, die gegen Phishing, Credential Stuffing und MFA-Fatigue-Angriffe strukturell resistent ist.

80%+	**28'000**	**1,5 Mon.**	**3,4 Mrd.**
aller Datenpannen beginnen mit kompromittierten Zugangsdaten (Verizon DBIR)	installierte NetAttest EPS, die meistverkaufte RADIUS-Appliance in Japan	durchschnittliche Implementierungszeit bis zur Produktivität	Phishing-E-Mails täglich weltweit (Verizon / Check Point 2025)

Das Wichtigste in Kürze:

- OneGate ergänzt die Sicherheit durch X.509-Gerätezertifikate und FIDO2 als starken zweiten Faktor, phishing-resistant und gerätegebunden durch den mTLS-Mutual-Handshake
- NetAttest EPS sichert den Netzwerkzugang (LAN, WLAN, VPN) auf Schicht 2 mit IEEE 802.1X, bevor ein Login überhaupt erfolgt
- OneGate CA dient häufig als Root-CA, die EPS-CA wird von ihr signiert; beide Systeme bilden eine integrierte PKI-Infrastruktur
- Vollständige SASE-Integration: OneGate fungiert als starker Identity Provider für Cloudflare, Zscaler, Palo Alto und weitere Plattformen
- Password Manager bringt SSO auch zu Legacy-Systemen ohne SAML oder WebAuthn, ohne Austausch bestehender Anwendungen
- Soliton KeyManager (Windows, macOS, iOS/iPadOS, Android) ermöglicht Self-Service-Zertifikatsinstallation in drei Schritten, ohne IT-Eingriff

03 Warum klassische Authentifizierung versagt

Die Angriffsfläche moderner Unternehmen hat sich grundlegend verändert. Mitarbeitende arbeiten hybrid, nutzen private und verwaltete Geräte und greifen auf Dutzende Cloud-Dienste zu. Angreifer haben ihre Methoden entsprechend angepasst. Klassische Passwortauthentifizierung bietet kaum noch wirksamen Schutz.

Die häufigsten Angriffsvektoren

01 **Credential Stuffing**
Gestohlene Passwortlisten aus Datenpannen werden automatisiert auf Tausende von Diensten angewendet. Aktuell kursieren über 15 Milliarden kompromittierte Zugangsdaten im Dark Web (Digital Shadows 2024).

02 **Phishing & Adversary-in-the-Middle (AiTM)**
Moderne AiTM-Angriffe hebeln sogar Push-MFA aus, indem Authentifizierungstokens in Echtzeit abgefangen und missbraucht werden. Gestohlene Zugangsdaten sind einer der häufigsten initialen Angriffsvektoren (Verizon DBIR 2024).

03 **MFA Fatigue**
Nutzer werden mit Authentifizierungsanfragen überhäuft, bis sie aus Bequemlichkeit oder Erschöpfung bestätigen. Klassische Push-MFA ist kein zuverlässiger Schutz mehr gegen entschlossene Angreifer.

04 **Gerätekompromittierung & Wi-Fi-Angriffe**
Unkontrollierte Geräte wie BYOD, externe Partner und Lieferanten erhalten Netzwerkzugang allein durch gültige Credentials. Pre-Shared-Key-basierte WLANs sind anfällig für Man-in-the-Middle- und Sniffing-Angriffe.

Was Unternehmen wirklich brauchen ist eine robuste Zero Trust Architektur, welche vier Fragen gleichzeitig beantworten muss:

?	**Identität**	Wer ist der Nutzer? Wirklich, nicht nur laut Passwort?
?	**Gerät**	Von welchem verifizierten Gerät kommt die Anfrage?
?	**Netzwerk**	Hat dieses Gerät das Recht, überhaupt am Netzwerk teilzunehmen?
?	**Kontext**	Darf dieser Nutzer von diesem Gerät jetzt auf diese Ressource zugreifen?

Soliton OneGate & NetAttest EPS beantworten alle vier Fragen gleichzeitig

NetAttest EPS verifiziert auf Schicht 2, ob das Gerät ein gültiges Zertifikat besitzt und darf dieses Gerät überhaupt am Netzwerk teilnehmen. OneGate verifiziert Nutzeridentität und Gerät über mTLS und stellt bei Erfolg einen SAML-Token aus. Die SASE-Plattform prüft diesen Token und wendet Zugriffsrichtlinien an. Zero Trust ist kein einzelnes Produkt, sondern das Zusammenspiel der Komponenten.

04 Standard-Passkeys: Fortschritt mit Grenzen

Passkeys (FIDO2/WebAuthn) sind ein wichtiger Schritt in Richtung passwortloser Authentifizierung. Der private Schlüssel verlässt das Gerät nie, die Authentifizierung erfolgt biometrisch oder per PIN. Phishing-Angriffe auf Passwörter werden erheblich erschwert. Für den unternehmensweiten Einsatz stossen Standard-Passkeys jedoch an klare Grenzen.

Stärken von Standard-Passkeys

- Phishing-resistant: Schlüssel kryptografisch an Domain gebunden
- Kein Passwort, das gestohlen oder geraten werden kann
- Einfache Nutzererfahrung (Biometrie, PIN)
- Plattformübergreifend via FIDO2/WebAuthn-Standard
- Cloud-Synchronisierung (Apple, Google, Microsoft)

Grenzen für den Enterprise-Einsatz

- Schützt nur App-/Web-Login, nicht den Netzwerkzugang
- Kein Device Trust: jedes Gerät mit Passkey kann sich anmelden
- Synchronisierte Passkeys verlassen das Gerät (Cloud-Sync)
- Abhängigkeit vom Ökosystem des Plattformanbieters
- Keine eigene Certificate Authority möglich
- Kein gegenseitiges TLS (mTLS) zwischen Client und Server
- Kein Schutz für Legacy-Systeme ohne WebAuthn-Unterstützung

Der Soliton-Ansatz

Soliton OneGate nutzt FIDO2/Passkeys als optionalen zweiten Faktor. Das Fundament bilden jedoch X.509-Zertifikate mit mTLS, was ein strukturell höheres Sicherheitsniveau ergibt, da sowohl Netzwerkzugang als auch Anwendungszugang abgesichert werden.

05 Soliton OneGate: PKI-basierte Identity-Plattform

Soliton OneGate ist eine Cloud-basierte IDaaS-Plattform (Identity-as-a-Service), die Authentifizierung, Zertifikatsmanagement und Single Sign-On in einer einheitlichen Lösung vereint. Das Fundament ist kein Passwort und kein einfacher Passkey, sondern ein X.509-Gerätezertifikat oder Benutzer-Zertifikat, ausgestellt von der organisationseigenen Certificate Authority. OneGate dient dabei häufig als Root-CA. Die CA von NetAttest EPS wird von ihr signiert und ist damit in der gesamten PKI-Infrastruktur vertrauenswürdig.

Die vier Kernfunktionen

① **Starke MFA mit mTLS**
X.509-Zertifikate als Kern, ergänzt durch FIDO2, IC-Karte, Smartphone-App und OTP. Der mTLS-Mutual-Handshake authentifiziert sowohl den Client als auch den Server gegenseitig, was die Lösung phishing- und AiTM-resistant macht. Auch die Anmeldung am Windows-Client selbst wird durch den OneGate Windows Logon Provider abgesichert.

② **Single Sign-On (SSO): Cloud und Legacy**
SAML 2.0 SSO für Microsoft 365, Google Workspace, Salesforce und viele weitere Dienste. Über den PasswordManager auch für Legacy-Systeme ohne SAML (ERP, RDP, klassische Windows-Anwendungen, Branchenanwendungen). Nutzer kennen ihre Passwörter für diese Systeme nicht mehr; OneGate verwaltet sie vollständig im Hintergrund.

③ **Netzwerkzugang & Zero Trust**
Zertifikatsbasiertes EAP-TLS für LAN, WLAN und VPN. Nur Geräte mit gültigem Zertifikat erhalten Netzwerkzugang, nahtlos integriert mit NetAttest EPS-edge.

④ **ID-Management & Provisioning**
Automatische Synchronisation mit Active Directory und Entra ID. Automatisches Provisioning und De-Provisioning in SaaS-Diensten. Das Management von Personalwechseln wird zur einfachen Standardprozedur.

Unterstützte Authentifizierungsfaktoren

Digitales Zertifikat (X.509)	Stärkster Faktor, geräte- oder benutzergebunden, privater Schlüssel verlässt das Gerät nie. Gegenseitiger mTLS-Handshake in beide Richtungen.
FIDO2 / Sicherheitsschlüssel	Hardware-Token wie YubiKey und Windows Hello, als ergänzender zweiter Faktor zur Zertifikatsauthentifizierung.
Soliton KeyManager App	Eigene App für Windows, macOS, iOS/iPadOS und Android. Self-Service-Zertifikatsinstallation in drei Schritten ohne IT-Eingriff.
Soliton Authenticator App	Smartphone-App für Push-Authentifizierung und Zertifikatsverwaltung.
IC-Karte / FeliCa	Mitarbeiterausweis-basierte Authentifizierung für Umgebungen mit gemeinsam genutzten Geräten.
OTP / Passwort	Weiterhin unterstützt für Legacy-Systeme und Übergangsszenarien.
PasswordManager	SSO auch für Legacy-Systeme. Ein entscheidender Vorteil gegenüber reinen FIDO2-Lösungen: Der PasswordManager ermöglicht passwortloses SSO auch für Systeme, die kein SAML oder WebAuthn unterstützen – darunter klassische Windows-Anwendungen, ERP-Systeme, RDP und Branchenanwendungen. Nutzer kennen ihre Passwörter für diese Systeme nicht mehr – OneGate verwaltet sie vollständig im Hintergrund.

Erklärung zum OneGate Windows Logon Provider

Der OneGate Windows Logon Provider ist eine Komponente von Soliton OneGate, die die Windows-Anmeldung absichert.

Was er macht: Er ersetzt oder ergänzt den normalen Windows-Login-Mechanismus, sodass sich ein Nutzer beim Hochfahren des PCs nicht nur mit Passwort oder PIN anmeldet, sondern via X.509-Zertifikat und mTLS.

Warum das wichtig ist: Standard-Windows-Anmeldung ist passwortbasiert und anfällig für Phishing oder Credential Stuffing. Mit dem OneGate Windows Logon Provider wird bereits der Desktop-Login durch starke, gerätegebundene Zertifikatsauthentifizierung geschützt, bevor überhaupt eine Anwendung geöffnet wird.

Praktisches Beispiel: Ein Mitarbeitender öffnet seinen Laptop. Statt Passwort einzugeben, authentifiziert sich das Gerät automatisch via Zertifikat gegenüber OneGate. OneGate gibt grünes Licht, Windows öffnet sich. Kein Passwort, das gestohlen oder erraten werden kann.

Risikoadaptive Authentifizierung

Im Standard-Plan passt OneGate die Stärke der Authentifizierung dynamisch an den Risikokontext an. Ungewöhnliche Quell-IP-Adressen, abweichendes Zugriffsverhalten oder der Zugriff auf besonders sensible Ressourcen lösen automatisch eine verstärkte Verifizierung aus, ohne manuellen Eingriff durch Administratoren.

06 NetAttest EPS: Netzwerksicherheit auf Geräteebene

NetAttest EPS (EAP Policy Server) ist eine der führenden RADIUS-Appliance in Japan mit über 28'000 installierten Einheiten weltweit. Sie sichert den Netzwerkzugang auf Schicht 2 (IEEE 802.1X) für LAN, WLAN und VPN gleichermassen, lange bevor ein Nutzer sich an einer Anwendung anmeldet. Nur Geräte mit einem gültigen Zertifikat erhalten Netzwerkzugang. Alle anderen werden still abgewiesen.

Kernfunktionen

- IEEE 802.1X EAP-Authentifizierung für LAN, WLAN und VPN (EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-FAST)
- Integrierte Certificate Authority mit eigener privater CA für Geräte- und Benutzer-Zertifikate, häufig signiert durch die OneGate CA
- Dynamische VLAN-Zuweisung für automatische Netzwerksegmentierung nach Nutzer- und Geräteprofil
- SCEP-Server für automatisierte Zertifikatsverteilung über MDM-Systeme wie Microsoft Intune und Jamf
- RADIUS-Proxy für die Weiterleitung von Authentifizierungsanfragen an externe RADIUS-Server in hybriden Umgebungen
- Active Directory / LDAP-Integration mit direkter Nutzervalidierung gegen bestehende Verzeichnisdienste

Deployment-Modelle

NetAttest EPS ist sowohl als physische Appliance in drei Grössen, als auch als virtuelle Appliance verfügbar:

Modell	EPS-SX (Klein)	EPS-ST (Mittel)	EPS-DX (Gross)
Zielgrösse	Dutzende bis hunderte Clients	Hunderte bis tausende Clients	Tausende bis 100k Clients
Formfaktor	Desktop	19" Rack (1U)	19" Rack (1U), Hot-Swap
Redundanz	–	Active-Standby	Active-Standby
Virtuell	VMware / Hyper-V	VMware / Hyper-V	VMware / Hyper-V

Alle Modelle sind auch als virtuelle Appliance für VMware ESXi 7.0/8.0 und Hyper-V (Windows Server 2016/2019/2022) verfügbar – ideal für Unternehmen, die keine zusätzliche Hardware betreiben möchten.

07 Das Zusammenspiel: OneGate + NetAttest EPS + SASE

Die grösste Stärke liegt im Zusammenspiel der Komponenten. OneGate und NetAttest EPS bilden zusammen eine vollständige Zero Trust Infrastruktur, die sich nahtlos in bestehende SASE-Architekturen integriert. Eine SASE-Plattform übernimmt Traffic-Inspektion, Web-Filterung, CASB und ZTNA, aber keine starke, gerätegebundene Identitätsverifizierung auf PKI-Basis. Genau das liefert Soliton.

Mit Standard-IDPs (Entra ID, Okta) ist der erste Faktor oft noch ein Passwort. OneGate hebt diesen Standard erheblich an. Die SASE Lösung sieht somit nur zertifizierte Geräte von verifizierten Nutzern. Die Architektur ist ein Fünf-Schichten-Konzept.

1 ↓

Nutzer + Gerät

Gerät besitzt ein gültiges X.509-Zertifikat, ausgestellt von der OneGate Root-CA oder der davon signierten NetAttest EPS-CA.

2 ↓

Netzwerkzugang (NetAttest EPS)

IEEE 802.1X EAP-TLS: Nur zertifizierte Geräte erhalten Netzwerkzugang. Dynamische VLAN-Zuweisung erfolgt automatisch. Nicht-autorisierte Geräte werden abgewiesen, bevor ein Login-Dialog erscheint.

3 ↓

Identity Verification (Soliton OneGate)

mTLS-gegenseitige Authentifizierung: Client und Server verifizieren sich gegenseitig. Optionaler zweiter Faktor (FIDO2, Authenticator App, IC-Karte). SAML-Token wird ausgestellt, auch über den Windows Logon Provider für Desktop-Anmeldungen.

4 ↓

SASE-Plattform / Anwendung

Cloudflare One, Zscaler, Palo Alto Prisma Access oder vergleichbare SASE-Plattformen prüfen den SAML-Token und wenden Zugriffsrichtlinien an. Vollständiges Audit-Log über alle Zugriffe.

5 ↓

Zugang gewährt – kontextbasiert, auditiert

Cloud-App, On-Prem-System oder Netzwerkressource – mit vollständigem Audit-Log.

Zertifikatsverteilung: Automatisch für alle Geräte

- Microsoft Intune / MDM: Automatische Zertifikatsverteilung via SCEP an alle verwalteten Geräte, kein Nutzereingriff nötig
- Soliton KeyManager App (Windows, macOS, iOS/iPadOS, Android): Self-Service-Installation in drei Schritten für BYOD und externe Partner
- Einladungscode / QR-Code: Für externe Partner und Lieferanten: Zertifikat in einem Schritt selbst installieren
- Bis zu 10 Zertifikate pro Nutzer, für alle Geräte, die ein Mitarbeitender verwendet

08 Praxisbeispiele aus der Industrie

Die folgenden Einsatzszenarien zeigen, wie Unternehmen aus verschiedenen Branchen die Soliton-Plattform einsetzen. Der Einstieg erfolgt vielfach mit einem konkreten Problem, die Skalierung auf die gesamte Organisation folgt dann innerhalb von 12 bis 24 Monaten.

Fertigung & Industrie

Grossunternehmen Automobilzulieferung - Fertigungsindustrie

Herausforderung
MFA für über 160 Lieferanten bei der Migration eines Auftragsmanagement-Systems in die Cloud. Externe Partner durften keinen komplexen Setup-Aufwand haben.

Ergebnis
Zertifikats-MFA via Einladungscode für alle Lieferanten eingeführt. Starke Authentifizierung ohne IT-Aufwand auf Lieferantenseite. Supply-Chain-Sicherheit signifikant verbessert.

Grossunternehmen Konsumgüter - Fertigungsindustrie

Herausforderung
Absicherung von WLAN für über 1'000 Nutzer: PCs, iPhones, iPads. MAC-Address-Authentifizierung war zu fehleranfällig und administrativ aufwendig.

Ergebnis
Automatische Zertifikatsverteilung via EPS-edge und KeyManager. WLAN-Authentifizierung deutlich gestärkt, Aufwand bei Personalfluktuation massiv reduziert.

Baugewerbe & Infrastruktur

Shimizu Corporation (Grossbauprojekte) - Baugewerbe

Herausforderung
27'000 Nutzer-IDs, mehrere Standorte, MAC-Address-Authentifizierung mit hohem Betriebsaufwand und Sicherheitsrisiken, Redundanzanforderungen.

Ergebnis
OneGate + NetAttest EPS mit MDM-Integration (Intune). Einheitliche Zero Trust Umgebung, reduzierter MAC-Management-Aufwand, vollständige Redundanz.

Mittelgrosses Bauunternehmen - Baugewerbe

Herausforderung
Mehrere IDs und Passwörter pro Mitarbeitenden, Passwort-Leakage-Risiko, fehlende Sicherheit für Lieferantenportale.

Ergebnis
Zertifikats-MFA + PasswordManager für alle Business-Systeme (SAML und Non-SAML). SSO über die gesamte Systemlandschaft, keine Passwortrotation mehr nötig.

Öffentliche Hand & Bildung

Kommunalverwaltung - Öffentliche Verwaltung

Herausforderung
WLAN-Sicherheit im Büro, Schutz vor unbefugtem Zugang, flexible Geräteverwaltung bei häufigem Personalwechsel.

Ergebnis
Wi-Fi-Authentifizierung via EPS-edge, Zertifikatsverteilung auf bestehende Geräte. Erhöhte Sicherheit, freie Gerätebeweglichkeit, papierloser Betrieb ermöglicht.

Bildungsbehörde (Landesebene) - Bildung & Öffentliche Verwaltung

Herausforderung
Separate Absicherung von Lern- und Verwaltungsnetzwerk, nahtlose WLAN-Anmeldung für Lehrkräfte ohne ID-Eingabe gewünscht.

Ergebnis
Automatische Zertifikatsverteilung via Intune. Nahtloses WLAN-Onboarding, standortunabhängige Digitalisierung sicher umgesetzt.

Der wichtigste Quick Win

Die Abschaffung der MAC-Address-Authentifizierung zugunsten von Zertifikaten.

Der zweite starke Treiber

Externe Partnerzugriffe von Supply Chain, Lieferanten und Subunternehmern sicher und compliant zu gestalten.

Gemeinsames Muster aus Enterprise-Deployments mit Soliton

09 Lizenzmodell & Einstieg

Soliton OneGate ist als monatliches SaaS-Modell erhältlich, ohne Vorabinvestitionen in Infrastruktur, einfache Skalierung mit dem Unternehmenswachstum. Drei Pläne decken von PKI-Management bis zur vollständigen Zero Trust Plattform alle Anforderungen ab.

	PKI Plan	Basic Plan	Standard Plan
Private CA + Zertifikate	✓	✓	✓
MFA (Cert, FIDO2, Smartphone)	✓	✓	✓
SAML SSO (Cloud-Dienste)	–	✓	✓
PasswordManager (Non-SAML SSO)	Option	Option	Option
Risikoadaptive Authentifizierung	–	Option	✓
ID-Provisioning (SaaS)	–	✓	✓
SecureBrowser (Datenschutz)	–	Option	✓

Alle Pläne beinhalten

Private CA, Zertifikatsmanagement (bis zu 10 Zertifikate pro Nutzer), AD/Entra ID Sync, vollständiges Logging und einen kostenfreien Trial-Tenant. Für einen kombinierten NAC- und IDaaS-Test empfehlen wir eine Trial-Dauer von 60 Tagen, da Integrationen mit Diensten wie HubSpot (Enterprise-Lizenz) oder Atlassian (erweiterte Admin-Rechte) zusätzliche Vorbereitung erfordern können.

So starten Sie

1	Trial-Antrag: Tenant wird innerhalb von 5 Werktagen bereitgestellt. Eine direkte Migration in Produktion ist möglich.
2	Kickoff mit SecureComply & Soliton: Analyse Ihrer bestehenden Infrastruktur, Empfehlung des optimalen Plans und Deployment-Modells.
3	Pilotdeployment: Typischerweise abteilungsweise Einführung innerhalb von 4 bis 6 Wochen.
4	Unternehmensweiter Rollout: Schrittweise Erweiterung auf alle Nutzer und Systeme. Investitionsschutz: Bestehende Active Directory / Entra ID Umgebungen, MDM-Systeme (Intune, Jamf) und SASE-Plattformen bleiben vollständig erhalten und werden integriert.

10 Mehrwert auf einen Blick

Dimension	Konkreter Nutzen
Sicherheit	Gerätegebundene X.509-Zertifikate + mTLS verhindern Zugriff mit gestohlenen Credentials und sind resistent gegen Phishing, AiTM und MFA-Fatigue.
Zero Trust	Netzwerkzugang und Anwendungszugang werden separat und kombiniert abgesichert - kein Gerät erhält Zugang ohne explizite Verifikation.
Compliance	Erfüllt Anforderungen aus ISO 27001, BSI IT-Grundschutz, NIS2 und branchenspezifischen Regulatoriken. Vollständige Auditierbarkeit aller Zugriffe.
Betriebseffizienz	Self-Service-Zertifikate, automatische Erneuerung und ID-Provisioning reduzieren Helpdesk-Anfragen messbar. Keine manuelle Passwortrotation.
Nutzererfahrung	Passwortlose Anmeldung per Biometrie oder Zertifikat – schneller und einfacher als jedes bisherige MFA-Verfahren.
Legacy-Integration	PasswordManager bringt SSO auch zu Systemen ohne SAML/WebAuthn - kein Austausch bestehender Anwendungen notwendig.
Datensouveränität	Organisationseigene CA, On-Premises-Optionen und keine Abhängigkeit von US-Hyperscaler-Identitätsprovidern.
Investitionsschutz	Integration in bestehende AD, MDM und SASE Infrastruktur – kein Greenfield. Schrittweise Erweiterung möglich.

11 Fazit & nächste Schritte

Zero Trust ist kein Produkt, sondern eine Architekturphilosophie. Soliton OneGate und NetAttest EPS liefern die technischen Bausteine, um diese Philosophie konsequent umzusetzen. Von der Netzwerkschicht bis in die Cloud, von der Gerätezertifizierung bis zum passwortlosen Single Sign-On ist Alles aus einer Hand.

Mit über 28'000 installierten NetAttest-Einheiten und zahlreichen Enterprise-Deployments in Fertigung, Infrastruktur und öffentlicher Verwaltung ist die Plattform praxiserprobt. Die ISMAP-Registrierung (Information system Security Management and Assessment Program) ist Japans staatliches Sicherheitszertifizierungsprogramm für Cloud-Dienste, vergleichbar mit dem europäischen C5-Testat oder SOC 2. Dies macht die Plattform auch für regulierte Umgebungen und öffentliche Ausschreibungen qualifiziert.

Typische Herausforderungen bei der Einführung

Wie bei jeder grundlegenden Architekturumstellung gibt es auch beim Übergang zu einer zertifikatsbasierten Zero-Trust-Infrastruktur Herausforderungen, die Organisationen realistisch einplanen sollten:

- **PKI-Komplexität:**
  - Der Aufbau und Betrieb einer Public-Key-Infrastruktur erfordert spezifisches Know-how. OneGate vereinfacht dies durch eine vollständig verwaltete Cloud-CA mit automatisiertem Zertifikats-Lifecycle – dennoch sollte die initiale Planung der Zertifikatsrichtlinien und Vertrauensketten sorgfältig erfolgen.
- **Change Management:**
  - Mitarbeitende sind an Passwort-Workflows gewöhnt. Die Umstellung auf zertifikatsbasierte Anmeldung ist zwar einfacher für den Endnutzer, erfordert aber gezielte Kommunikation und Schulung, insbesondere in den ersten Wochen nach der Einführung.
- **Migrationsaufwand bei Legacy-Systemen:**
  - Nicht alle bestehenden Systeme unterstützen SAML, OIDC oder zertifikatsbasierte Authentifizierung nativ. Der PasswordManager von OneGate schliesst diese Lücke, doch die Anbindung älterer Branchenanwendungen kann individuelle Konfiguration erfordern.
- **Schrittweise Einführung empfohlen:**
  - Ein Big-Bang-Rollout ist selten ratsam. Die erfolgreichsten Deployments beginnen mit einer Pilotabteilung und erweitern schrittweise – typischerweise über 4 bis 6 Monate bis zur unternehmensweiten Abdeckung. SecureComply begleitet diesen Prozess von der Architekturplanung bis zum Rollout.

Diese Herausforderungen sind lösbar und gehören zum normalen Einführungsprozess einer PKI-basierten Sicherheitsarchitektur. Entscheidend ist eine realistische Planung und die richtige Begleitung – beides bietet SecureComply gemeinsam mit Soliton.

Drei strategische Kernargumente für Ihre Entscheidung

- Höhere Sicherheit als Standard-Passkeys: X.509 + mTLS + IEEE 802.1X decken Netzwerk und Anwendung ab – nicht nur den Login-Dialog
- SASE-Kompatibilität mit PKI-Fundament: OneGate als zertifikatsbasierter IdP ergänzt Ihre SASE-Plattform um Device Trust auf Zertifikatsebene und dies unabhängig vom Plattformanbieter
- Bewährt und skalierbar: Von 40 bis 27'000+ Nutzern in einem einzelnen Deployment. Am Besten mit einem schrittweisen Einstieg, der sich Ihrem Tempo anpasst

SecureComply
Secure by Design. Compliant by Default.

Jetzt Beratungsgespräch vereinbaren

Wir analysieren Ihre bestehende Infrastruktur und zeigen Ihnen, wie Soliton OneGate und NetAttest EPS konkret bei Ihnen greifen.

info@securecomply.ch | www.securecomply.ch

Antwort innerhalb von 24 Stunden – 90 Tage kostenloser Trial-Tenant auf Anfrage