

WARUM REICHT TRADITIONELLE MFA NICHT MEHR FÜR UNTERNEHMENS-SICHERHEIT?

Phishing- und Social-Engineering-Angriffe sind im Laufe der Zeit immer raffinierter geworden. Über 60% der Unternehmen sind täglich oder wöchentlich mit Phishing-Angriffen konfrontiert. Die meisten modernen MFA-Techniken können dem Druck der Angriffe nicht mehr standhalten und müssen ersetzt werden.

Eine Phishing-resistente, passwortlose Lösung ist die Antwort auf diese Herausforderungen. **SystoLOCK** ist eine zuverlässige und einfach zu bedienende passwortlose MFA-Lösung für Ihre On-Premises- und Cloud-Identitäten.



6000+ aktive Lizenzen



Made in Germany



Patent pending



On-Premise-Lösung



Passwordless MFA-Plattform



Cloud-Kompatibel



Niedrige TCO



Einfache Verwaltung



Hohe Qualität seit 2003



Was ist SystoLOCK?



Diese passwortlose Multi-Faktor-Authentifizierungslösung (MFA) von Systola kann Ihr Unternehmen **vor Phishing und anderen identitätsbasierten Angriffen schützen**, selbst wenn diese gegen unbemannte Netzwerkknoten durchgeführt werden. Dies funktioniert für alle Anmeldungen über Active Directory und darüber hinaus.

In Deutschland hergestellt, schützt **SystoLOCK** Organisationen seit fast einem Jahrzehnt und wird ständig weiterentwickelt, um neuen und ständig wachsenden Sicherheitsanforderungen gerecht zu werden.

4-schichtiger Schutz vor identitätsbasierten Angriffen

01

Passwortlose
Authentifizierung

SystoLOCK verlässt sich nicht auf Passwörter, um Benutzer zu authentifizieren. **SystoLOCK** entfernt sogar die Passwörter aus den Benutzerkonten und macht es so unmöglich, geschützte Konten durch passwortbasierte Angriffe zu kompromittieren. Anstelle von Passwörtern verwendet **SystoLOCK** abgetrennte Anmeldeinformationen, die innerhalb von Active Directory ohne **SystoLOCK** unbrauchbar sind.

02

Multi-Faktor-
Authentifizierung

SystoLOCK-Anmeldedaten sind immer Multi-Faktor. Diese variablen Faktoren umfassen Wissen, Besitz und Inhärenz und werden immer zusammen verwendet, um sicherzustellen, dass **nur der vollständige Satz übermittelt werden kann**, um Brute-Force-Angriffe zu verhindern.

03

Phishing-
Resistenz

SystoLOCK unterstützt phishing-resistente Tokens, die die Benutzerfreundlichkeit mit der Leistungsfähigkeit kryptografischer Signaturen kombinieren. Diese Maßnahme fügt den Authentifizierungsmechanismen einen **kryptografischen Eigentumsnachweis** hinzu, während die gleiche reibungslose und äußerst ergonomische Erfahrung beibehalten wird.

04

Erweiterte
Kryptographie

SystoLOCK verwendet fortschrittliche Kryptographie, um sicherzustellen, dass die zwischen den Knoten übertragenen Informationen **immer verschlüsselt** sind und auch zu einem späteren Zeitpunkt nicht abgefangen oder entschlüsselt werden können. Wo immer möglich, werden digitale Zertifikate verwendet, um die Integritätsprüfung zu erleichtern.

Wie sich Benutzer mit SystoLOCK authentifizieren



QR-Codes und Push-
Benachrichtigungen



OTP-Generatoren
und Smartphones



NFC- und RFID-Karten
und -Transponder



FIDO-Schlüssel
alias PassKeys

Was SystoLOCK für Sie leisten kann

Verwenden Sie **SystoLOCK** für die Authentifizierungsszenarien in Ihrem Active Directory und darüber hinaus:

- **Windows-Anmeldung**
- **RDP-Anmeldung**
- **Anmeldung bei VPN**
- **Privilegienerhöhung**
- **Identitätswechsel**
- **Offline-Anmeldung**
- **Anmeldung bei Office 365**
- **Anmeldung bei externen Ressourcen**

Dieser Satz von Anmeldeszenarios deckt die meisten Ihrer Active Directory-Anmeldeanforderungen ab und bietet ein Höchstmaß an Schutz vor identitätsbasierten Bedrohungen und Angriffen.



Compliance leicht gemacht

SystoLOCK hilft, die Anforderungen von Sicherheitsstandards wie NIS2, DORA und PCI DSS zu erfüllen. Es schützt Benutzerkonten und Unternehmensressourcen vor potenziellen Bedrohungen bei der Authentifizierung. Als umfassende passwortlose MFA-Lösung gewährleistet **SystoLOCK** einen sicheren Zugang zu:

- privilegierten Assets
- kommandozeilen-Apps
- kritische Anwendungen und Servern
- täglichem Betrieb



Bereitstellung und Konfiguration

SystoLOCK ist eine einfach zu konfigurierende Plattform, die in wenigen Minuten installiert werden kann. Viele mühsame Aufgaben sind von Anfang an automatisiert. Weitere Automatisierung über PowerShell ist das Herzstück der Plattform.

- ✓ On-Premises-Lösung
- ✓ Modernste Industriestandards
- ✓ Flexible Konfiguration und Roll-out pro Benutzer
- ✓ Faire Lizenzierung
- ✓ Einfache und automatische Bereitstellung (MSI)
- ✓ Konfigurierbare Richtlinien
- ✓ Natives Windows-Look-and-Feel
- ✓ Selbstkonfiguration durch Benutzer
- ✓ Inklusive Audit und Diagnose
- ✓ Automatisch erkennbar und hochverfügbar

SystoLOCK Companion-App

SystoLOCK Companion ist eine mobile Anwendung, die entwickelt wurde, um den Anmeldeprozess für Endbenutzer zu vereinfachen. Diese einfach zu bedienende und benutzerfreundliche Anwendung ermöglicht vereinfachte und schnellere Anmeldungen und erhöht gleichzeitig die Sicherheit durch die Eliminierung gemeinsamer Geheimnisse.

Es ist außerdem kompatibel mit den meisten anderen Authentifizierungsanwendungen und kann diese ersetzen.

SystoLOCK Companion ist im AppStore und PlayMarket erhältlich.

Made in Germany von Systola GmbH



Systola bietet seit 2003 IT-Dienstleistungen für Unternehmen in Europa an und hat sich auf Microsoft Windows-Unternehmensumgebungen und IT-Sicherheit spezialisiert.

Unser Portfolio umfasst eine Vielzahl von Management-Tools und patentierten Technologien sowie Expertise in Microsoft Windows-Domänenumgebungen.

Die Lösungen von Systola sind robust, skalierbar und lassen sich leicht in Ihre Unternehmensinfrastruktur und Microsoft Active Directory integrieren.

**Lassen Sie uns gemeinsam
Ihr Unternehmen schützen!**



Roman Kuznetsov, Systolas Geschäftsführer

SYSTOLA

SystoLOCK-Plattform und ihre Komponenten



SystoLOCK Authentifizierungsserver

Ein schlanker Dienst oder eine Gruppe von redundanten Diensten, die auf Maschinen innerhalb des Netzwerks laufen und die Verbindungen von verschiedenen Typen von **SystoLOCK**-Clients bedienen, ihre Anmeldeinformationen validieren und digitale Zertifikate von der Unternehmens-CA im Namen der Benutzer anfordern. Ausgestattet mit 3 PowerShell-Modulen für die Einrichtung, Verwaltung und Diagnose.



SystoLOCK Verwaltungstools

Wird typischerweise auf den PCs der Administratoren und auf den **SystoLOCK**-Servern installiert und ist als MMC Snap-In und PowerShell Modul implementiert. Kombiniert mit einer Erweiterung für die ADUC-Konsole bietet es eine umfassende Verwaltungs- und Überwachungslösung für **SystoLOCK**.



SystoLOCK Windows-Client

Der Treiber, der für das Sammeln der **SystoLOCK**-Anmeldedaten von den Benutzern verantwortlich ist, bietet auch erweiterte Funktionen, wie z. B. Diagnose und Selbstbedienung. Kann über Softwareverteilungstools in großem Umfang eingeführt werden.



SystoLOCK VPN Client

Der **SystoLOCK** VPN-Client läuft in der Regel auf Notebooks und kann VPN-Verbindungen unter Verwendung von **SystoLOCK**-Anmeldeinformationen herstellen. Kompatibel mit Microsoft VPN und Cisco AnyConnect.



SystoLOCK Identitätsanbieter und AD FS-Adapter

Läuft auf On-Prem-Servern oder in Azure und bietet **SystoLOCK**-Kompatibilität zu einer Vielzahl von Webanwendungen und Authentifizierungsdiensten, die SAML2 nutzen, wie z.B. Office 365, Sales Force, etc.



SystoLOCK Remote Desktop-Gateway-Plugin

Ein Plugin, das eine Cookie-basierte Authentifizierung für Remote Desktop Gateway für Internet-zugewandte Server von Remote Desktop Session Host Farmen bietet. Entwickelt für die Zusammenarbeit mit dem **SystoLOCK** Web Portal Plugin.



SystoLOCK Companion

Ein moderner mobiler Authentifikator, der in der Lage ist, eine automatische Benutzerauthentifizierung mit **SystoLOCK**-Servern durchzuführen und auch OATH-kompatible Einmalpasswörter für den allgemeinen Gebrauch zu generieren.



SystoLOCK RADIUS-Plugin

Läuft als Plugin für Microsoft Network Policy Server, um VPN-Anmeldungen über nahezu jedes VPN-Gateway zu ermöglichen.



SystoLOCK Remote Desktop Web Portal-Plugin

Ein IIS-Modul, das Authentifizierungs-Cookies in RDP-Dateien einfügt und Kompatibilität zur **SystoLOCK**-Authentifizierung über einen AD FS Proxy bietet.



SystoLOCK Companion-Proxy und Rendezvous-Agent

Ein Dienst, der eingehende Konnektivität zu Authentifizierungsservern für die Companion-App bereitstellt, ohne dass Perimeter-Ports geöffnet werden müssen.



+49 40 730 91 572



info@systola.de



systola.de