SecurePIM
by Materna Virtual Solution

SecurePIM Gateway

Jederzeit und überall sicher verbunden – ganz ohne VPN und MDM

Die SecurePIM App macht es Anwender:innen aus Unternehmen und Behörden leicht, unterwegs sicher zu arbeiten. Doch wie gewährleistet die IT-Administration das eigentlich? Mit dem SecurePIM Gateway, das die Verbindung der App zur IT-Infrastruktur absichert. Administrator:innen können es zügig installieren, einfach verwalten und so Betriebsaufwände senken. Das Beste: Dank Authentifizierung durch Zertifikate sind weder VPN noch Mobile Device Management nötig.

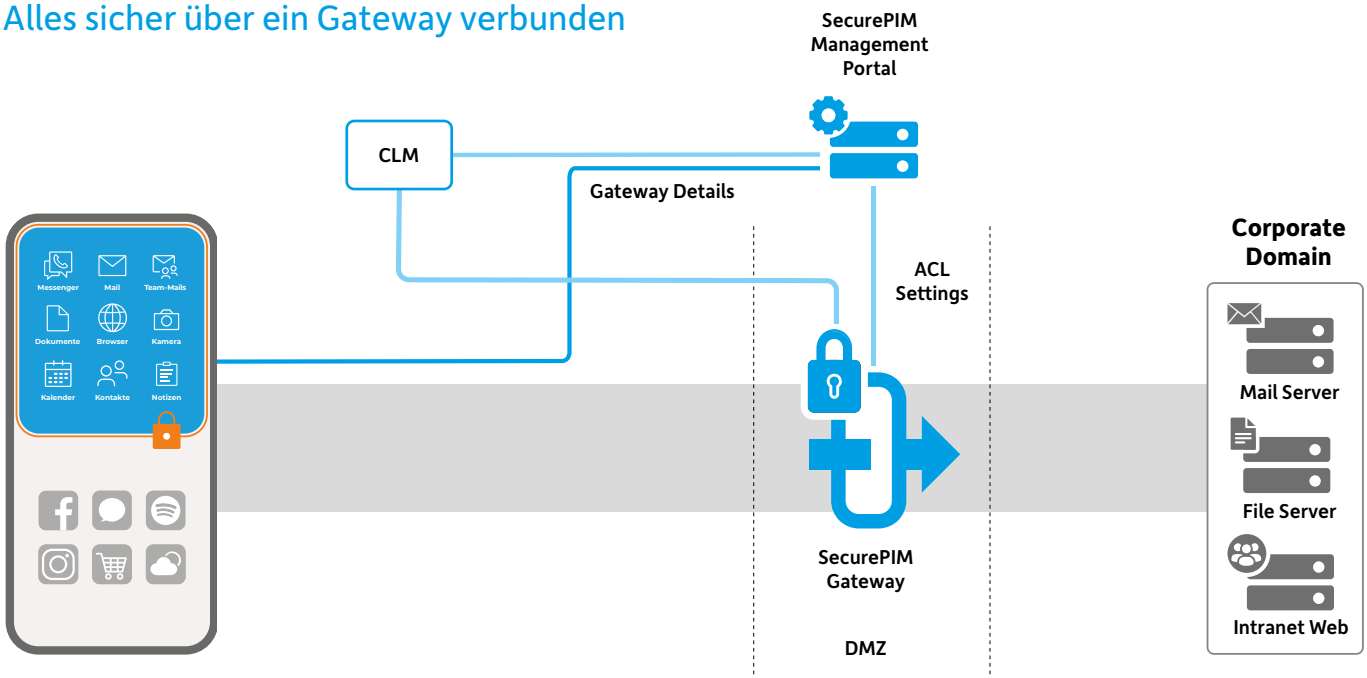
Keine Chance für Hacker: Sicherheit mit dem SecurePIM Gateway

Eine sichere Verbindung in alle Netzwerke herzustellen, ist die Grundfunktion des SecurePIM Gateways. Es ist als Anwendung in der demilitarisierten Zone auf dem Server Ihrer Organisation installiert. Das Gateway prüft die Identitäten der Nutzenden und erlaubt über die abgesicherte SecurePIM App ausschließlich vorab verifizierte Zugriffe. Hacker-Angriffe lassen sich auf diese Art vermeiden, da z. B. Exchange Server nicht mehr direkt mit dem Internet verbunden sind.

Wenig Aufwand für Admins: Zentrale Verwaltung via SecurePIM Management Portal

Wie legen Administrator:innen Zugriffsrechte für das SecurePIM Gateway und die internen Server auf Account-, Gruppen- oder Unternehmensebene fest? Dafür steht ihnen das webbasierte SecurePIM Management Portal zur Verfügung. Beim Einsatz von privaten (BYOD) und dienstlichen Geräten (COPE) sind Installation und Verwaltung des Gateways identisch und somit weniger aufwendig. Der Rollout ist einfach: Nutzer:innen installieren die SecurePIM App aus dem Apple App Store bzw. Google Play, schalten sie per Registrierungscode frei und können alle Funktionen sofort nutzen.

Alles sicher über ein Gateway verbunden



SecurePIM
by Materna Virtual Solution

Bequeme Nutzung: Schnell und konfigurationsfrei aufs Netzwerk zugreifen

Nutzer:innen der SecurePIM App haben einen sicheren und hochperformanten Zugriff auf E-Mail- und Kalenderserver, Filesharing sowie Web-Apps. Und das ganz bequem, denn dank Gateway müssen sie SecurePIM nicht selbst konfigurieren. Der gehärtete Browser von SecurePIM sichert den mobilen Zugang zu webbasierten Anwendungen wie Wissens- und Kollaborationstools, Support- und Ticketsystemen und CRM ab. Um Zugriffe zu erleichtern, können Administrator:innen Lesezeichen definieren sowie Block- und Allow-Listen für Webseiten definieren.

Die wichtigsten Fragen & Antworten zum SecurePIM Gateway

Wie erhält eine SecurePIM-Installation die Konfiguration für das SecurePIM Gateway?

Anwender:innen registrieren sich beim Start von SecurePIM mit den Zugangsdaten, die sie vorab erhalten haben. Dabei erzeugt SecurePIM einen Key-Pair, einen privaten und öffentlichen Schlüssel. Anschließend registriert sich SecurePIM mit dem öffentlichen Schlüssel beim SecurePIM Management Portal. Während der Registrierung schickt es Konfigurationsdaten an SecurePIM. Diese Daten enthalten unter anderem die Konfiguration für das SecurePIM Gateway.

Wie funktioniert die Zugriffskontrolle?

Die Verwaltung der Zugriffsrechte erfolgt im SecurePIM Management Portal. Die einzelnen SecurePIM-Anwender:innen können spezifische Zugriffsrechte auf Server im Unternehmensnetzwerk erhalten. Um die Konfiguration zu vereinfachen, lassen sich auch Gruppen von SecurePIM-Installationen mit spezifischen Zugriffsrechten erstellen. Ist eine erhöhte Sicherheit gewünscht, lässt sich das Zugriffsrecht auf spezifische TCP-Ports, z. B. 443 für einen Webserver einschränken. Das verringert die Einfallstore für Cyber-Angriffe signifikant.

Wie behalten Admins den Überblick über die Zugriffsrechte?

Das SecurePIM Gateway fordert das SecurePIM Management Portal in regelmäßigen Abständen auf, ihm eine Zugriffskontrollliste zuzusenden. Sie enthält die öffentlichen Schlüssel der berechtigten SecurePIM-Installationen und deren Zugriffsrechte. Ändern sich diese, sendet das SecurePIM Management Portal einen sogenannten Trigger-Request an das SecurePIM Gateway, um die aktuelle Zugriffskontrollliste anzufordern.

Die Vorteile des SecurePIM Gateways

Entlastend für Ihre IT-Abteilung

+ Schnellere Absicherung durch unkomplizierte Installation
+ Einfache, zentrale Verwaltung von Nutzenden und Rechten
+ Weniger Betriebs- und Supportaufwand ohne VPN- bzw. MDM-Einsatz
+ Hochflexibel: BYOD- und COPE-Modelle im Mischbetrieb möglich

Beruhigend für Ihre Compliance-Beauftragten

+ Aktive Risikominimierung: Exchange-Server & Co. ohne direkte Internetverbindung
+ Zertifikatsbasierter Zugriff auf interne Systeme
+ Zentrale Verwaltung, die für mehr Kontrolle sorgt

Komfortabel für Ihre Anwender:innen

+ Bequemer und schneller Start ohne Geräte-Konfiguration
+ Sicherer Zugriff von überall auf Firmendaten und interne Webanwendungen
+ Hochperformantes mobiles Arbeiten ohne VPN-Anmeldung

SecurePIM
by Materna Virtual Solution

Wie ermöglicht das SecurePIM Gateway einen hochperformanten und effizienten Verbindungsaufbau?

Das SecurePIM Gateway ist auf maximale Leistung optimiert: Innerhalb der TLS-Verbindung zwischen SecurePIM und Gateway lassen sich beliebig viele Verbindungen zu Ziel-Servern im Unternehmensnetzwerk aufbauen. Dabei teilen sich die Verbindungen den Kanal zwischen SecurePIM und dem Gateway in einem sog. Zeitmultiplexverfahren. Eine einmal aufgebaute Multiplexverbindung zwischen beiden bleibt so lange bestehen, bis für eine konfigurierbare Zeitspanne (Time-out) kein Datenverkehr mehr stattfindet. Damit ist nicht für jeden Zugriff auf einen Netzwerk-Server eine neue TLS-Verbindung nötig, was die Leistung entsprechend optimiert.

>500 Behörden & Unternehmen

>120 Behörden & sicherheitsbetreute Industrie

>45 Bundesbehörden

>330.000 Nutzer:innen auf iOS und Android

>92% erweitern & erneuern ihre Lizenzen

Wenn auch Sie sichere mobile Zugriffe auf Ihr Unternehmensnetzwerk ermöglichen möchten, sprechen Sie mit uns über SecurePIM Gateway.

MATERNA
Virtual Solution

Materna Virtual Solution GmbH
Blutenburgstraße 18 · 80636 München · T +49 89 30 90 57-0
kontakt@virtual-solution.com · www.materna-virtual-solution.com

VS-NfD
FÜR iOS UND ANDROID
SICHERHEIT MADE IN GERMANY

NATO RESTRICTED
FÜR iOS
SICHERHEIT MADE IN GERMANY

P-23.0038_SPIM_Faktenübersicht_Gateway_de/de_v5_02/23