STORMSHIELD

DATA SECURITY

STORMSHIELD
GOOGLE WORKSPACE

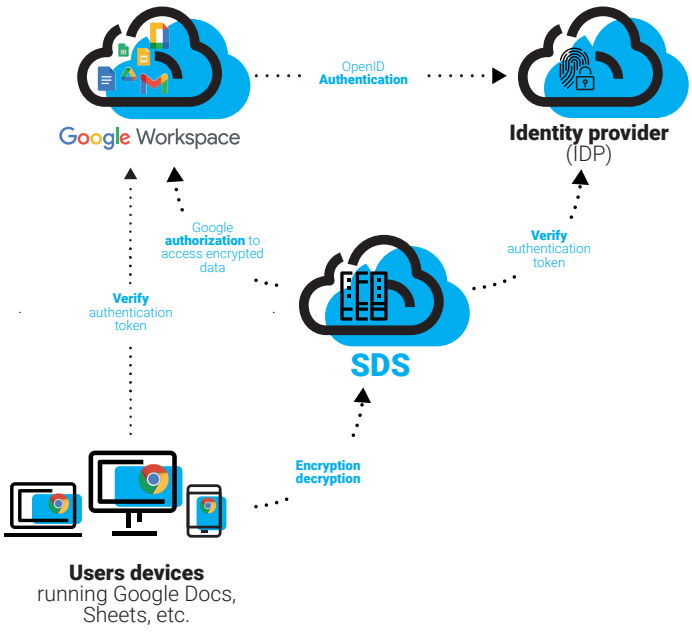
Behalten Sie die Kontrolle über den Schutz Ihrer sensiblen Daten in einer unbeaufsichtigten Cloud-Infrastruktur.

Agentenlos
FÜR EINEN SICHEREN AUSTAUSCH

Transparenz
DURCH AUTOMATISCHE VERSCHLÜSSELUNG

Einhaltung
GESETZLICHER VORSCHRIFTEN

Einfachheit
VERSCHLÜSSELUNG IM SAAS-MODUS



Datenverschlüsselung

Vor dem Hintergrund der kontinuierlichen Kommunikation und des Austauschs in der Cloud sind Daten gewissen Risiken ausgesetzt, die sich aus der Nutzung der Daten ergeben. Stormshield Data Security für Google Workspace bietet eine sichere Verschlüsselung der bei Google gespeicherten Daten.

Benutzerfreundlich

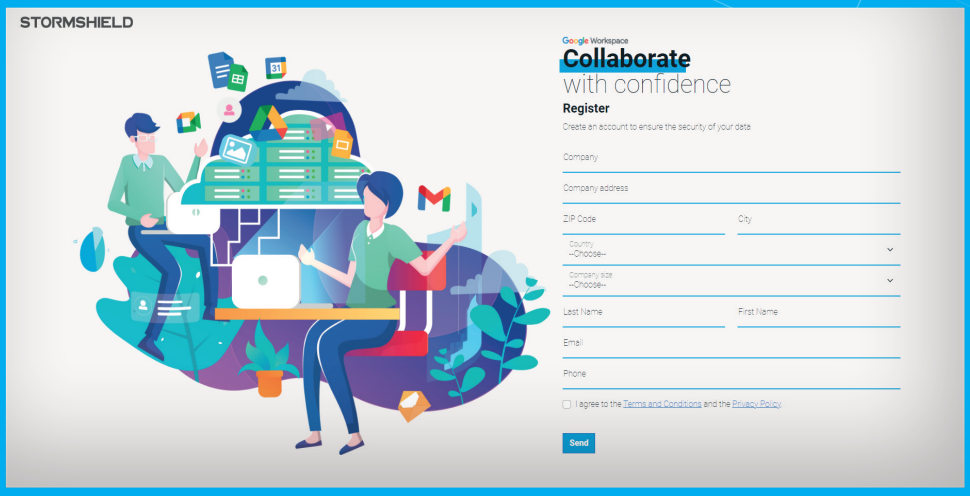
- Datenschutz im SaaS-Modus
- Wahrung des Benutzererlebnisses
- Keine Implementierung von Agenten

Integration von Google Workspace

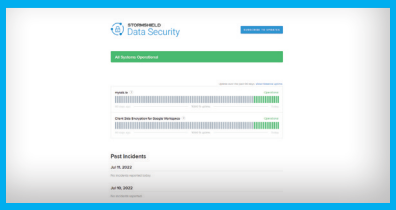
- Einsatz der Funktion Client Side Encryption von Google
- Gleiche Authentifizierung wie für Ihren Google-Bereich
- Mögliche Verwendung von IAM oder IDP

Einhaltung gesetzlicher Vorschriften

- End-to-End-Schutz sensibler Daten
- Verbesserter Schutz für personenbezogene Daten
- Sicherheitsschlüssel unter der alleinigen Kontrolle des Unternehmens



mysds.io Homepage



Statusseite

FUNKTIONEN

SDS für Google Workspace

- Unterstützung für den Client-Side-Encryption-Mechanismus
- Benutzerverifizierung mittels OpenID
- Unterstützung für Google-Anwendungen: Drive, Gmail, Meet, Calendar, Docs, Sheets und Slides
- Zusammenarbeit über Google mit jedem Gerät
- Automatische Verschlüsselung in synchronisierten und lokalen Ordnern

Agentenloser Betrieb über einen einfachen Chrome-Browser

- Wahrung der Google-Benutzererfahrung
- Angepasste Lösung für heterogene Systeme

Integrierte Schlüsselverwaltung

- Unterstützung für softwarebasierte Schlüsselgeneratoren
- Unterstützung für hardwarebasierte Schlüsselgeneratoren
- KMIP-Protokoll

Rückverfolgbare Ver- und Entschlüsselungsaktionen von Benutzern im SDS-Portal

- Überwachung der Lösungsnutzung im Unternehmen
- Vereinfachte Sicherheitsüberprüfung bei Verdacht auf Datenlecks

Trennung von Berechtigungen

- Host, Administratoren und Benutzer

Einhaltung gesetzlicher Vorschriften

- ITAR, CJIS, TISAX, IRS 1075 und EAR

Zentrale Verwaltung

- Unterstützung der OPA-Standards (Open Policy Agent) zur Definition von Sicherheitsregeln

KOMPATIBILITÄT

Server für Client Side Encryption

Datenschutz im SaaS-Modus
Vor-Ort- oder Cloud-Bereitstellung
Betriebssystem: Red Hat 8 und 9
Laufzeitumgebung: Node.js 16 und 20

Workstation

Ohne Installation von Agenten
Kompatibel mit Chrome für Desktop
ChromeOS, iOS und Android

Rückverfolgbarkeit

Lokal im System erzeugte Protokolle
Möglichkeit des Versands mittels Syslog