

## MetaAccess®

### Sicherer Zugriff auf Cloud-Anwendungen

Durch das Notebook eines Mitarbeiters mit veralteter oder falsch konfigurierter Sicherheitssoftware kann Ihr Netzwerk mit Schwachstellen und Malware konfrontiert werden. Unternehmen mit Remote-Geräten benötigen deshalb Kontrolle und Transparenz bei der Umsetzung von IT-Security-Richtlinien.

MetaAccess sorgt vor dem Zugriff auf Cloud-Anwendungen wie beispielsweise Salesforce und Microsoft 365 für die Gewissheit, dass Ihre Geräte den Sicherheitsanforderungen entsprechen. Gleichzeitig entsteht unternehmensweite Transparenz.

#### Transparenz. Kontrolle. Compliance.

Die zunehmende Verbreitung des Konzepts "Bring Your Own Device" (BYOD) erhöht das Risiko für Unternehmen. Ist das jeweilige Endgerät passwortgeschützt? Ist eine Antiviren-Software installiert? Sind die Dateien verschlüsselt? Wurde das Gerät eventuell bereits durch Malware infiziert?

MetaAccess löst die Herausforderungen bei der Verwaltung des Gerätezugriffs auf Ihr Netzwerk und Ihre Cloud-Anwendungen. Ein übersichtliches Dashboard sorgt für unternehmensweite Transparenz. Durch flexible Kontrollmöglichkeiten können die Richtlinien innerhalb der gesamten Infrastruktur angepasst werden – bis hin zum Blockieren eines einzelnen, spezifischen Geräts. Über APIs steht eine sichere Gerätezugriffssteuerung für Cloud-Anwendungen zur Verfügung und auch eine direkte Integration in bestehende und ältere Sicherheitslösungen ist realisierbar.

**MetaAccess bietet Sicherheit, Transparenz und Kontrolle für jedes Gerät, das auf Ihr Netzwerk und Ihre Cloud-Anwendungen zugreift.**



#### Vorteile

##### Compliance-Anforderungen erfüllen

Definiert und erzwingt Sicherheitsrichtlinien, erstellt Audit-Dokumentationen und Berichte

##### Isolierte Silos reduzieren

Konsolidieren Sie unterschiedliche Lösungen für die Erkennung von Bedrohungen, die Prüfung von Schwachstellen, die Auditierung, Compliance und Incident Response in einer zentralen Oberfläche

##### Bekämpft Datenpannen und Datendiebstahl

Die Endpunkt-Zugriffskontrolle minimiert Risiken durch Malware und regulatorische Strafzahlungen

##### Geringer Wartungsaufwand

Durch die eigenständige Korrektur sind Anwender in der Lage, viele Probleme selbst zu lösen

##### Flexibler Einsatz

Skalieren Sie Ihr Unternehmen mit flexiblen Pay-as-you-grow-Lizenzen

# OPSWAT.

MetaAccess

## Merkmale

Prüfung und **Bewertung der Endpunkt-Schwachstellen** von installierten Anwendungen und fehlenden oder veralteten Betriebssystem-Patches

Erkennung von Bedrohungen und Analyse wiederholter Infektionen mit über **30 Anti-Malware-Engines**, einschließlich Zero-Day-Bedrohungen

Compliance-Prüfung von mehr als **5.000 Sicherheitsanwendungen**

Sperrung des Benutzerzugangs zu **tragbaren Speichermedien/Geräten**, bis diese gescannt wurden, darunter zum Beispiel CD, USB und Smartphones

**Die Integration von Identity-Management**-Anbietern funktioniert einfach und unkompliziert mit SSO Diensten wie zum Beispiel OKTA oder Centrify

Über einen einzigen, schlanken Agent werden alle Sicherheitsrisiken gebündelt. Das **reduziert die Lizenzkosten**, vereinfacht die Integration und sorgt für bessere Performance

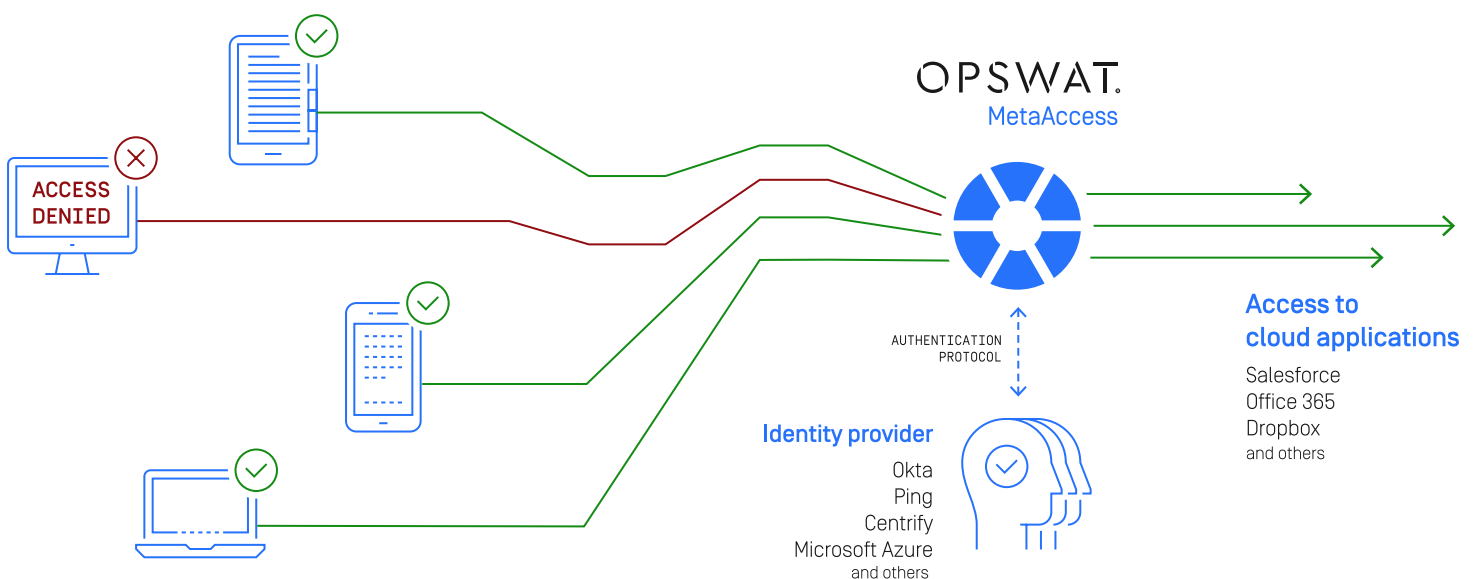
## Eigenschaften

- Granulare Gruppenrichtlinien
- Export von Event-Logs mit optionalen E-Mail-Benachrichtigungen
- Ferndiagnose
- REST API-Unterstützung für die Integration in bestehende Lösungen und benutzerdefinierte Berichte
- Wartung per Self Service

## Spezifikationen

### Unterstützte Clients [Minimum] Betriebssysteme

- Windows  
Windows 7, Windows Server 2008
- Linux
  - Debian-based Linux v4 [15.4.x]  
Ubuntu 16/Mint 18/Debian 8
  - Red Hat-based Linux v4 [15.6.x]  
CentOS 7.14/Red Hat Enterprise 7/OpenSuse 11.4/Suse Enterprise 12.x/Fedora 27
- MacOS  
OSX 10.9
- iOS  
iOS 8.3
- Android  
Android 5.1



OPSWAT.

Trust no file. Trust no device.