OPSWAT.

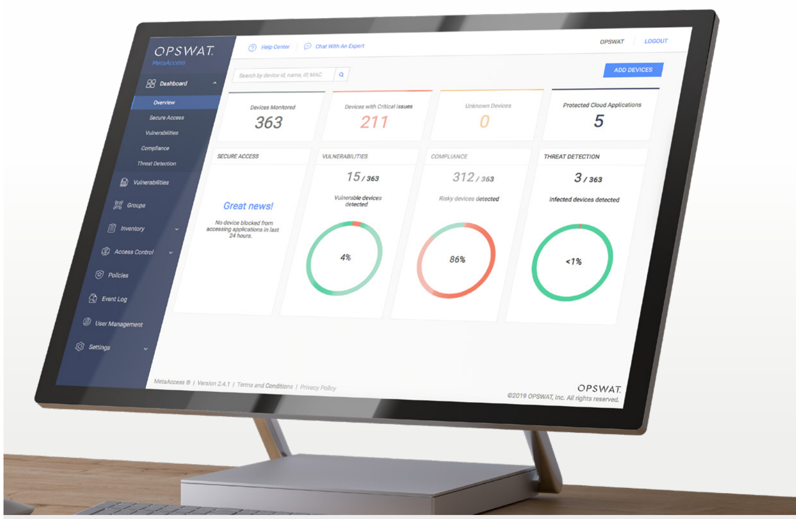
DATASHEET

MetaAccess®

Trust endpoint access to cloud applications

An employee's laptop with outdated or misconfigured security software exposes your network to vulnerabilities and malware. Enterprises with remote devices need control and visibility of security policy compliance.

MetaAccess confirms that your devices comply with security policies before accessing cloud applications, like Salesforce and Microsoft 365, while delivering cross-enterprise visibility on a single pane of glass.



Visibility. Control. Compliance.

The proliferation of Bring Your Own Device (BYOD) increases enterprises to exposure. Is the device password protected? Does it have anti-virus software? Are the files encrypted? Has the device been infected by malware?

MetaAccess solves managing device access to your network and cloud applications. A dashboard provides visibility across the entire enterprise. Flexible controls allow policy modification across the ecosystem down to blocking a single device. APIs provide secure device access control to cloud applications and can integrate directly into your existing and legacy security solutions.

MetaAccess delivers security, visibility, and control to every device accessing your network and cloud applications.

Benefits

Meet Compliance Requirements
Defines and enforces security policy, creates audit documentation and reports

Reduce Isolated Silos
Consolidate disparate solutions for threat detection, vulnerability assessment, audit, compliance, and incident response into a single point of oversight

Combats Data Breaches
Endpoint access control minimizes malware exposure and regulatory fines

Low Maintenance
Self-remediation guides users to solve issues themselves

Flexible Deployment
Scale your business with pay-as-you-grow licensing

OPSWAT

MetaAccess

Features

Endpoint **vulnerability assessment** of installed applications and missing or outdated OS patches

Threat detection, including zero-day threats, with **30+ anti-malware engines** and repeated infection analysis

Compliance check of over **5,000 security applications**

Blocks user access to **portable media** until it is scanned, including CD, USB, and mobile phones

Identity provider integration works out-of-the-box with SSO services, like OKTA and Centrify

Single lightweight agent collects all security risks, **reducing licensing costs**, simplifying integration requirements, and speeding performance

Capabilities

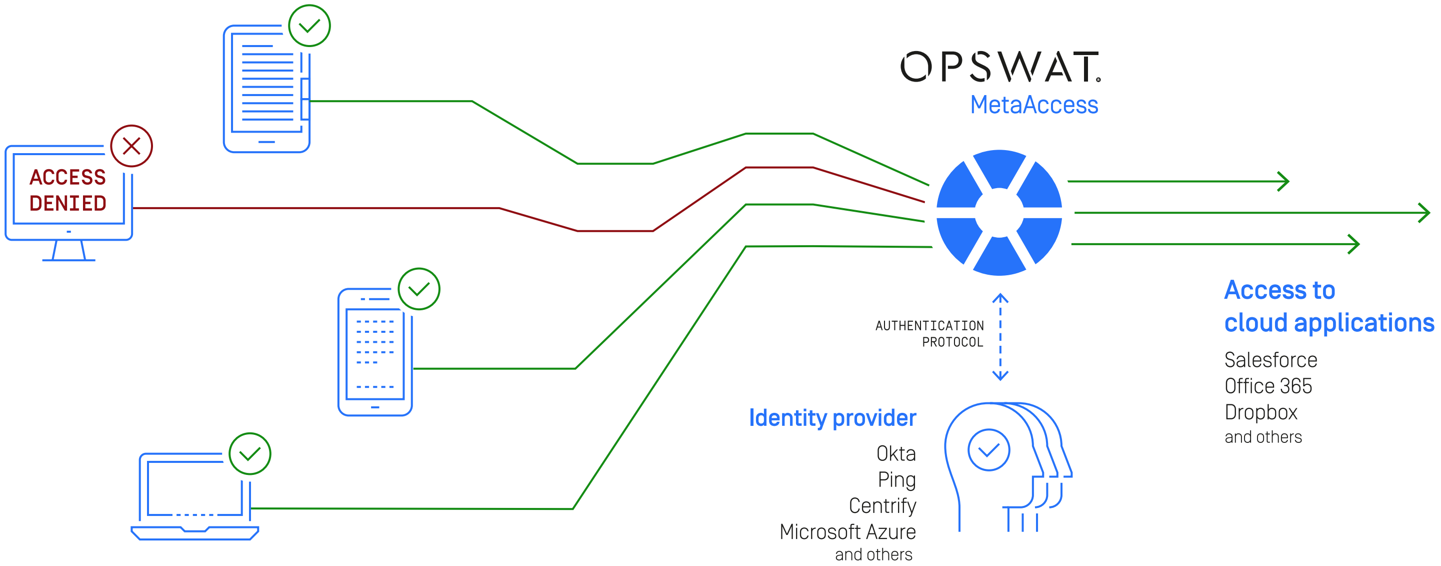
- Granular group policies
- Remote diagnostics
- Self-service maintenance

- Event log exports with optional email notifications
- REST API support for integration into existing solutions and custom reporting

Specifications

Minimum Supported Client Operating Systems

- **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.

opswat.com/contact