製品・テクノロジー最新情報とロードマップ-2

Taeil Goh, CTO
October 2018

OPSWAT.

Use Case 2:
File Upload & Web Application Protection

METADEFENDER SOLUTIONS

Implementation through API or ICAP

MetaDefender API

Integrate MetaDefender with your web application using the REST API.

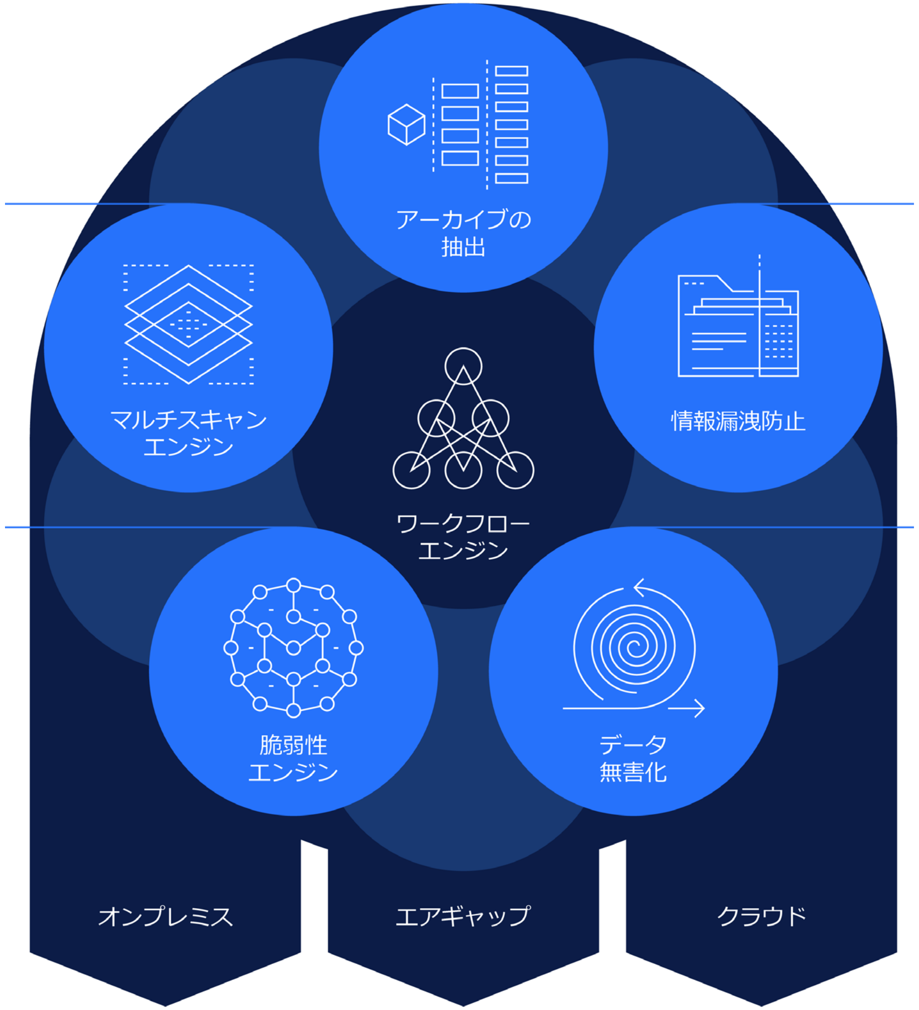
MetaDefender ICAP Server

Deploy MetaDefender with ICAP-enabled devices, such as WAF or proxy server.

MetaDefender API

Protection for File Upload, Storage and IPS

- All MetaDefender Technologies
- Deploy in your own environment or in the cloud
- RESTful API

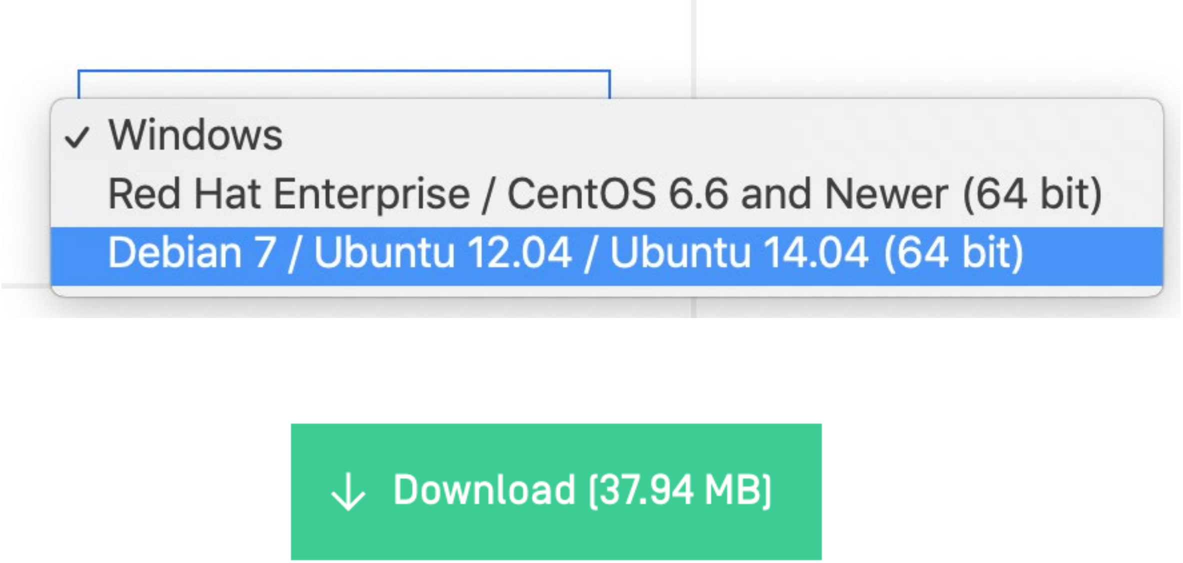


OPSWAT.

MetaDefender API

Protection for File Upload, Storage and IPS

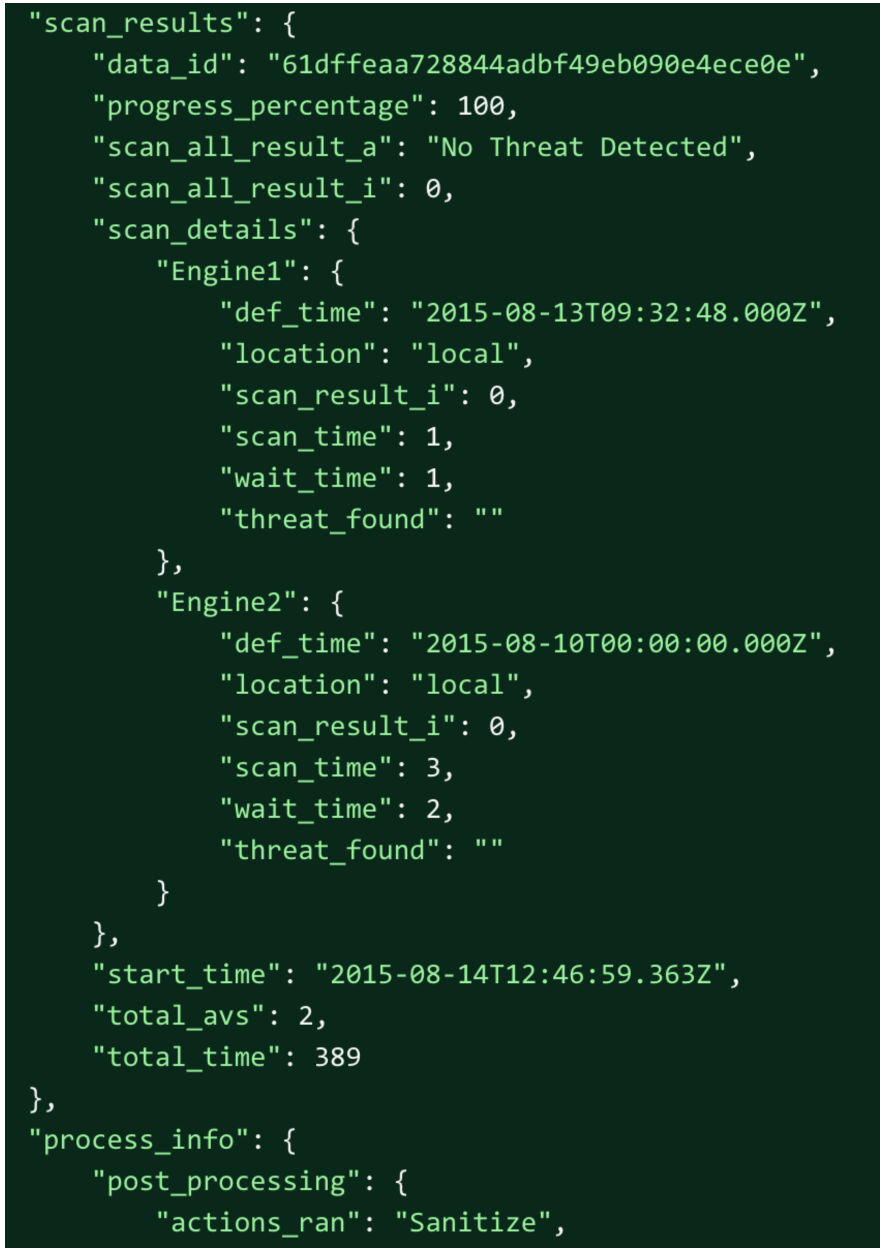
- All MetaDefender Technologies
- Deploy in your own environment or in the cloud
- RESTful API


✓ Windows
Red Hat Enterprise / CentOS 6.6 and Newer (64 bit)
Debian 7 / Ubuntu 12.04 / Ubuntu 14.04 (64 bit)
Download [37.94 MB]

MetaDefender API

Protection for File Upload, Storage and IPS

- All MetaDefender Technologies
- Deploy in your own environment or in the cloud
- RESTful API



```
"scan_results": {
    "data_id": "61dffeaa728844adbf49eb090e4ece0e",
    "progress_percentage": 100,
    "scan_all_result_a": "No Threat Detected",
    "scan_all_result_i": 0,
    "scan_details": {
        "Engine1": {
            "def_time": "2015-08-13T09:32:48.000Z",
            "location": "local",
            "scan_result_i": 0,
            "scan_time": 1,
            "wait_time": 1,
            "threat_found": ""
        },
        "Engine2": {
            "def_time": "2015-08-10T00:00:00.000Z",
            "location": "local",
            "scan_result_i": 0,
            "scan_time": 3,
            "wait_time": 2,
            "threat_found": ""
        }
    },
    "start_time": "2015-08-14T12:46:59.363Z",
    "total_avs": 2,
    "total_time": 389
},
"process_info": {
    "post_processing": {
        "actions_ran": "Sanitize",
```

MetaDefender ICAP Server

Protection for File Upload, Storage and IPS

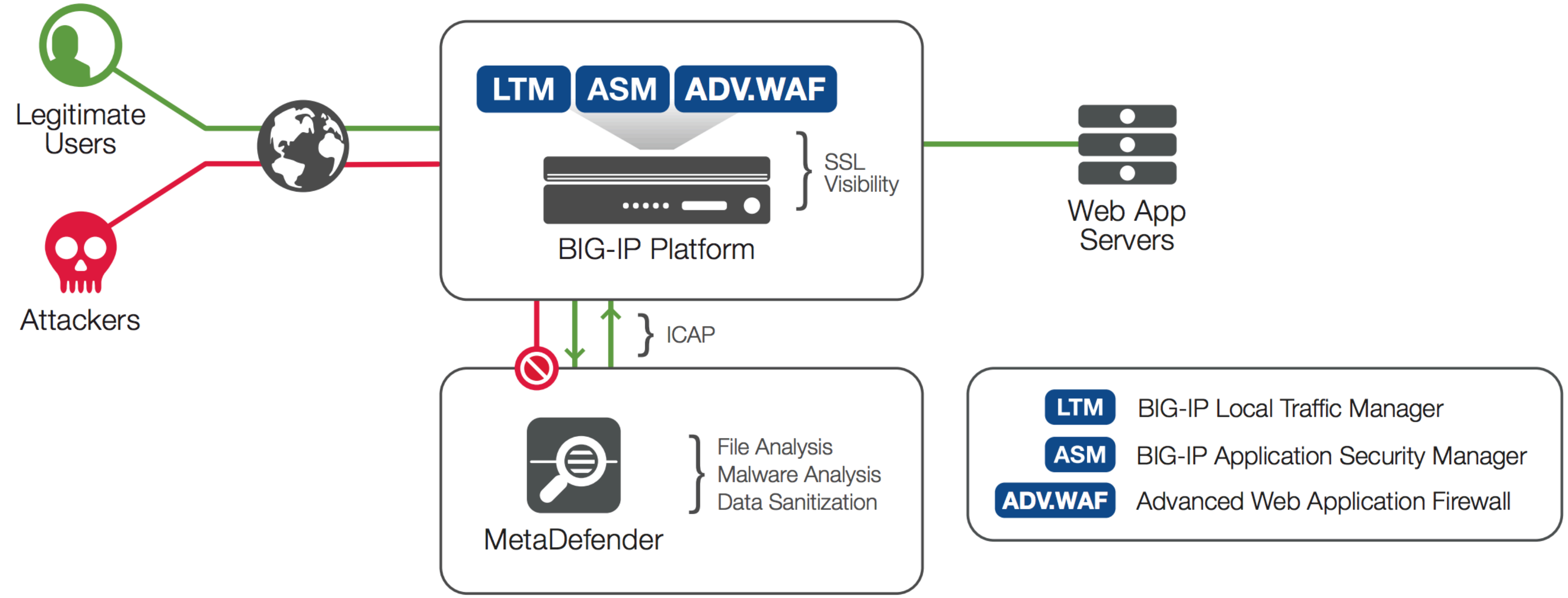
- Support Any ICAP enabled devices
- Web application protection

F5
Squid
BlueCoat ProxySG
Next-Generation Firewall
web proxy
McAfee Web Gateway
Fortinet FortiGate

MetaDefender ICAP Server

Protection for File Upload, Storage and IPS

- Support Any ICAP enabled devices
- Web application protection



Source: f5.com

OPSWAT.

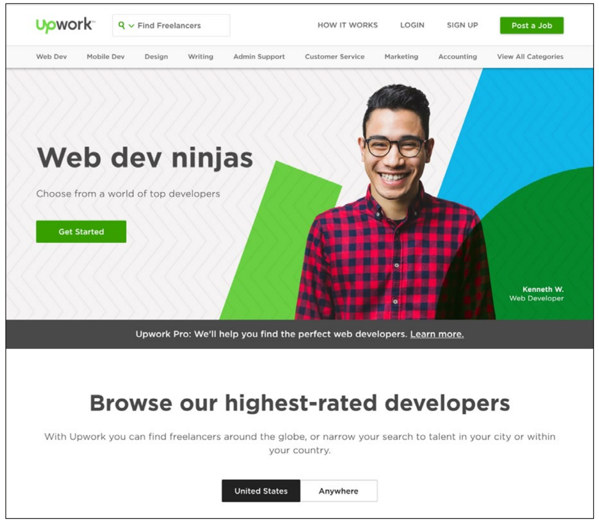
OPSWAT CDR: Securely Support Cloud Source processing millions of files a day

Upwork

Upwork is a freelancing website that connects businesses with freelance talent for highly-skilled knowledge work such as web, mobile and software development and design.

Challenges

receives millions of files a day from clients and freelancers and needs to ensure that those files are free from threats to protect both their own systems and the systems of everyone using their platform.



Web dev ninjas

Choose from a world of top developers

Upwork Pro: We'll help you find the perfect web developers. Learn more.

Browse our highest-rated developers

With Upwork you can find freelancers around the globe, or narrow your search to talent in your city or within your country.

OPSWAT CDR: Securely Support Cloud Source processing millions of files a day

upwork™

OPSWAT Solutions

Added data sanitization to an existing multi-scanning environment

Results

- Data sanitization effectively nullified the remaining attacks
- Upwork saw a 70% drop in malware attacks
- Upwork was able to prevent 100% of zero-day file attacks

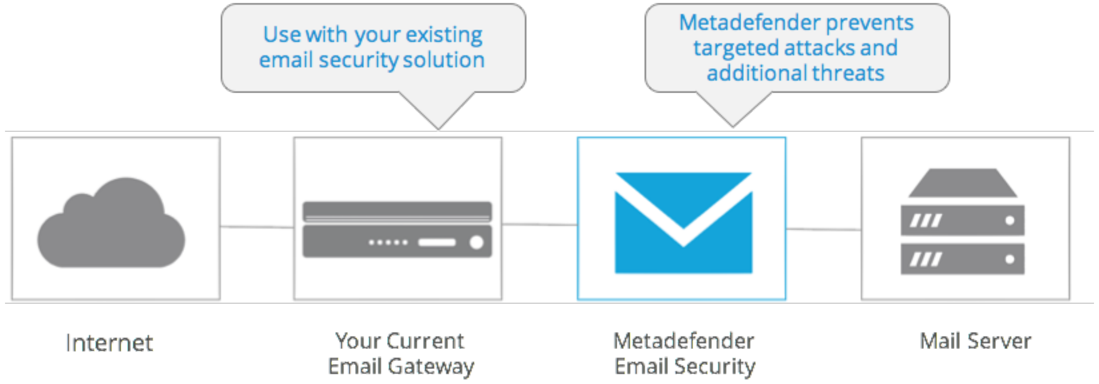
> "Upwork has always been focused on providing a secure environment for its community of millions of users, so they can safely transfer files and collaborate. Upwork and OPSWAT's mutual commitment to security reinforces our pledge to ensure all users can have the necessary protection to keep their home and business IT environments safe."
>
> Teza Mukkavilli Head of Security, Upwork

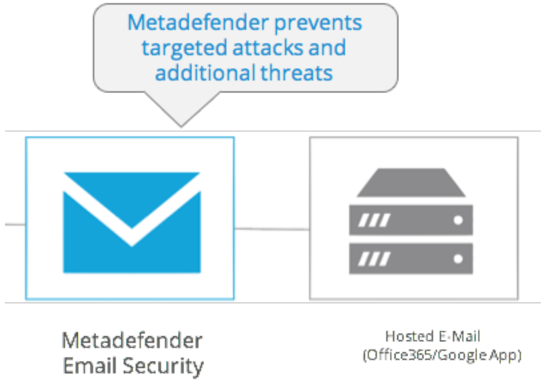
Use Case 3:
Email Security

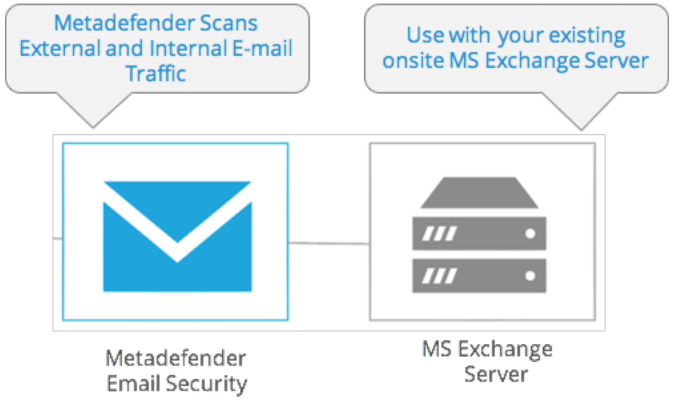
MetaDefender Email Security

Phishing is the beginning of every attack

- Flexible deployment
- Easy deployment
- Encrypted email attachment
- Bulk operations
- Integrated to MetaDefender Vault


Use with your existing email security solution
Metadefender prevents targeted attacks and additional threats
Internet
Your Current Email Gateway
Metadefender Email Security
Mail Server

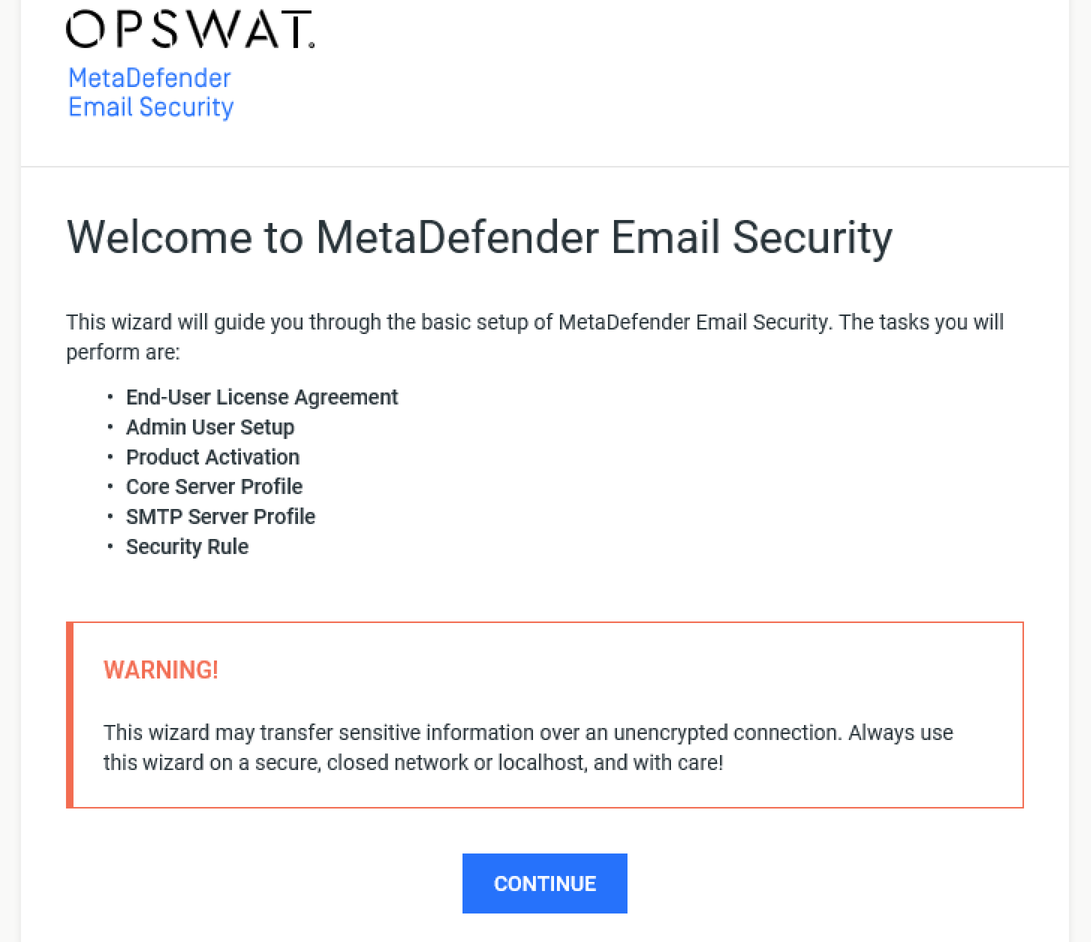

Metadefender prevents targeted attacks and additional threats
Metadefender Email Security
Hosted E-Mail (Office365/Google App)


Metadefender Scans External and Internal E-mail Traffic
Use with your existing onsite MS Exchange Server
Metadefender Email Security
MS Exchange Server

MetaDefender Email Security

Phishing is the beginning of every attack

- Flexible deployment
- Easy deployment
- Encrypted email attachment
- Bulk operations
- Integrated to MetaDefender Vault



Welcome to MetaDefender Email Security

This wizard will guide you through the basic setup of MetaDefender Email Security. The tasks you will perform are:

- End-User License Agreement
- Admin User Setup
- Product Activation
- Core Server Profile
- SMTP Server Profile
- Security Rule

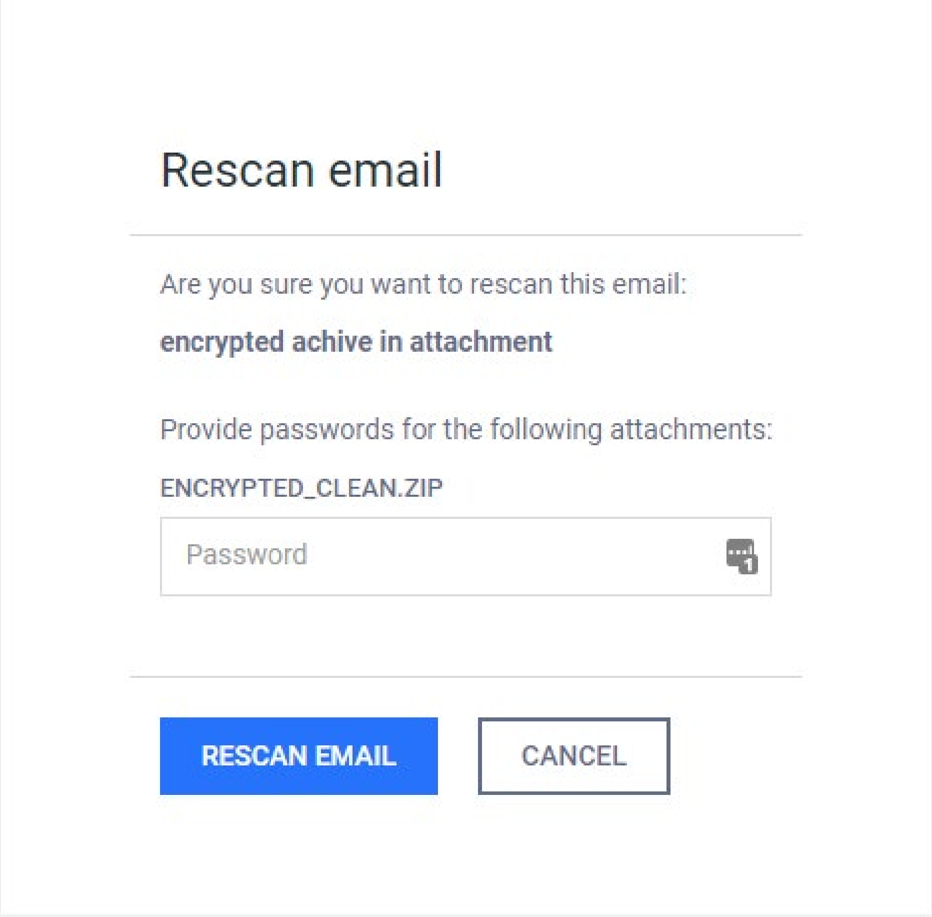
WARNING!

This wizard may transfer sensitive information over an unencrypted connection. Always use this wizard on a secure, closed network or localhost, and with care!

MetaDefender Email Security

Phishing is the beginning of every attack

- Flexible deployment
- Easy deployment
- Encrypted email attachment
- Bulk operations
- Integrated to MetaDefender Vault



Rescan email

Are you sure you want to rescan this email:

encrypted achive in attachment

Provide passwords for the following attachments:

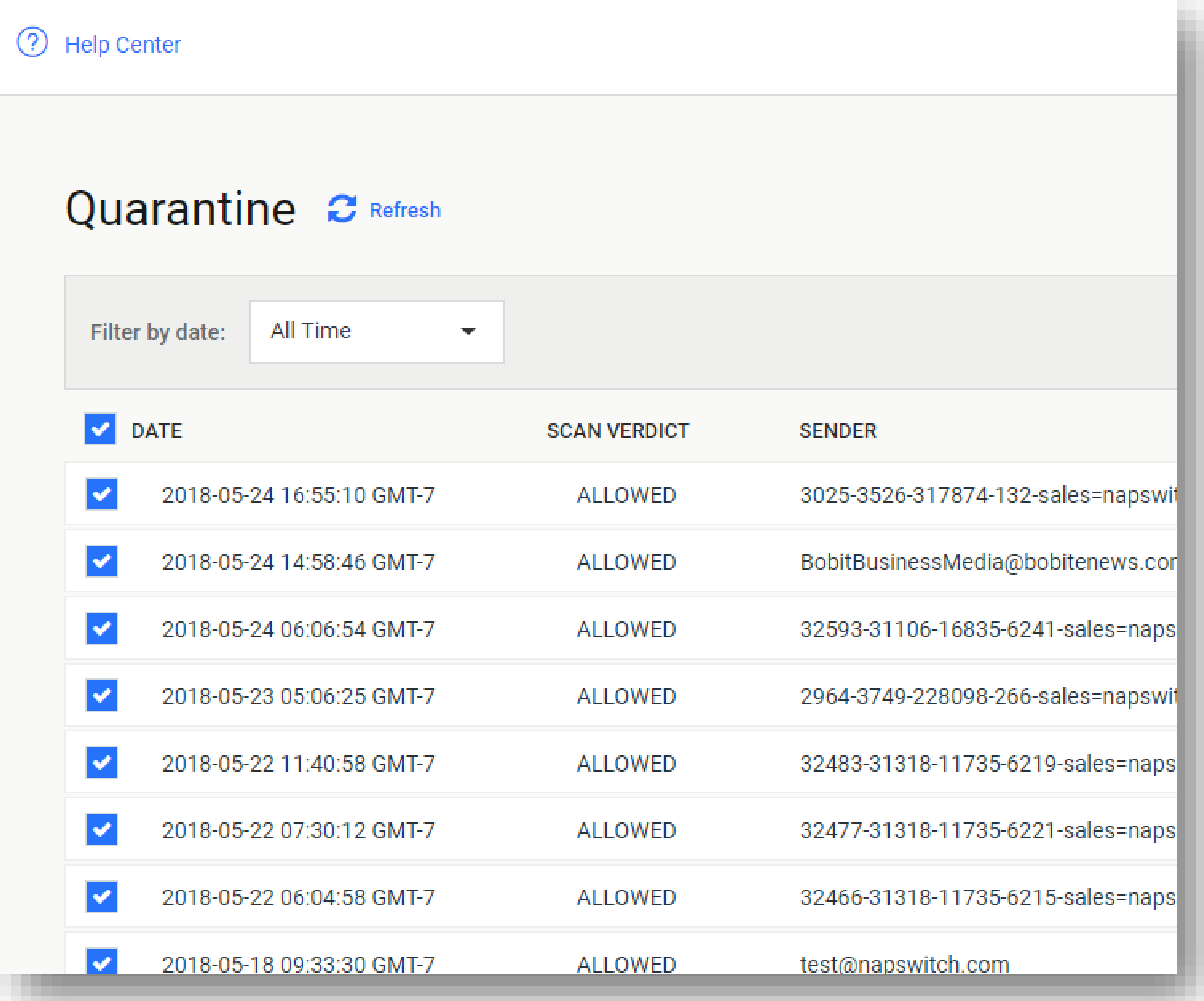
ENCRYPTED_CLEAN.ZIP

Password

MetaDefender Email Security

Phishing is the beginning of every attack

- Flexible deployment
- Easy deployment
- Encrypted email attachment
- Bulk operations
- Integrated to MetaDefender Vault



Quarantine

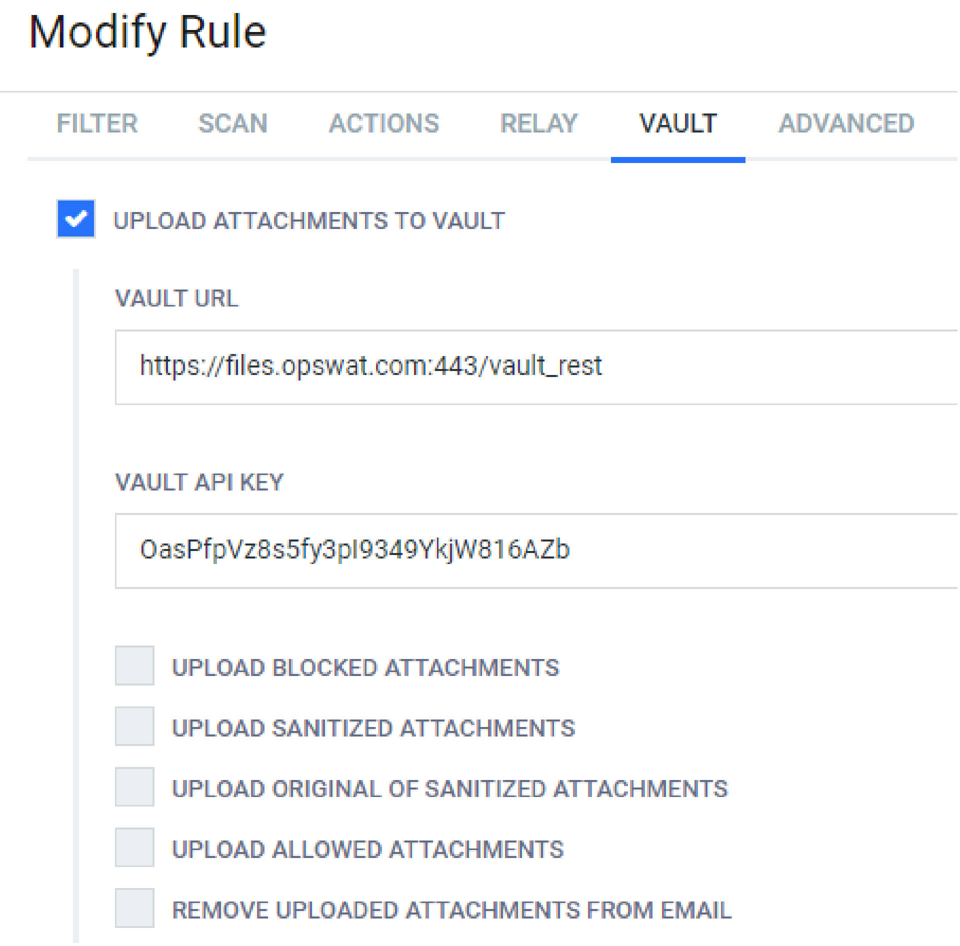
Filter by date: All Time

☑	DATE	SCAN VERDICT	SENDER
☑	2018-05-24 16:55:10 GMT-7	ALLOWED	3025-3526-317874-132-sales=napswi
☑	2018-05-24 14:58:46 GMT-7	ALLOWED	BobitBusinessMedia@bobitenews.cor
☑	2018-05-24 06:06:54 GMT-7	ALLOWED	32593-31106-16835-6241-sales=naps
☑	2018-05-23 05:06:25 GMT-7	ALLOWED	2964-3749-228098-266-sales=napswi
☑	2018-05-22 11:40:58 GMT-7	ALLOWED	32483-31318-11735-6219-sales=naps
☑	2018-05-22 07:30:12 GMT-7	ALLOWED	32477-31318-11735-6221-sales=naps
☑	2018-05-22 06:04:58 GMT-7	ALLOWED	32466-31318-11735-6215-sales=naps
☑	2018-05-18 09:33:30 GMT-7	ALLOWED	test@napswitch.com

MetaDefender Email Security

Phishing is the beginning of every attack

- Flexible deployment
- Easy deployment
- Encrypted email attachment
- Bulk operations
- Integrated to MetaDefender Vault



Modify Rule

☑ UPLOAD ATTACHMENTS TO VAULT

VAULT URL: https://files.opswat.com:443/vault_rest

VAULT API KEY: OasPfpVz8s5fy3pl9349YkjW816AZb

☐ UPLOAD BLOCKED ATTACHMENTS

☐ UPLOAD SANITIZED ATTACHMENTS

☐ UPLOAD ORIGINAL OF SANITIZED ATTACHMENTS

☐ UPLOAD ALLOWED ATTACHMENTS

☐ REMOVE UPLOADED ATTACHMENTS FROM EMAIL

Customer Testimonial

MetaDefender Email Security

“We use OPSWAT’s MetaDefender as one of the tools in our arsenal that protects our email users against advanced malware threats. We’ve been using the product for many years now. OPSWAT’s multi-engine scanning technology is fast, easy to integrate, and has been highly effective in our pursuit of offering the best security available to our customers. OPSWAT has been a great company to work with and I highly recommend them.”

Chris Cain

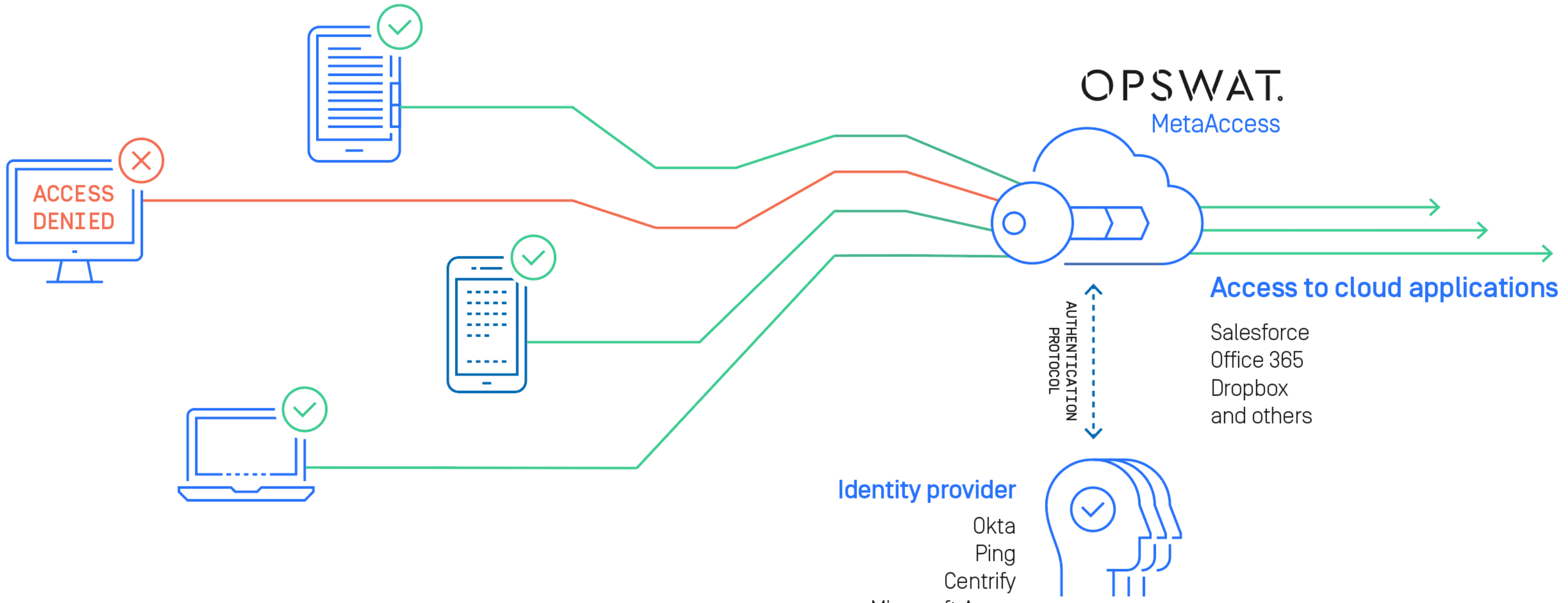
VP of New Technologies, AppRiver

appriver® Email & Web Security Experts™

Use Case 4:
Secure Access & Endpoint Compliance

Overview

What is MetaAccess?



Access to cloud applications

Salesforce
Office 365
Dropbox
and others

Identity provider

Okta
Ping
Centrify
Microsoft Azure
and others

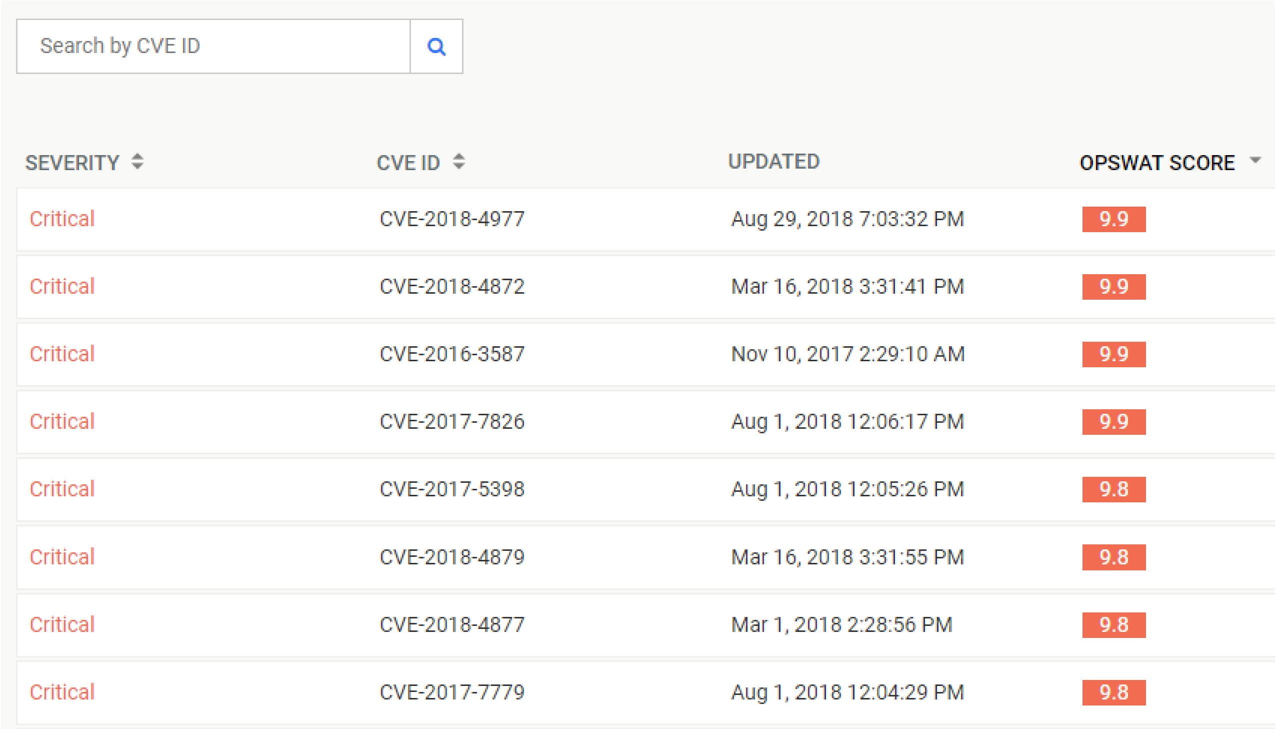
MetaAccess

How do we do it?

- Application vulnerabilities and missing patches
- Detection of over 5,000 3rd party applications
- Advanced Threat Prevention
  - Multi-antimalware scanning
  - Repeated threats detection
- Cloud security and access control
- Flexible customization and integration

What set us apart?

- Full visibility for all devices
- Criticality ranking with CVEs



Search by CVE ID

SEVERITY	CVE ID	UPDATED	OPSWAT SCORE
Critical	CVE-2018-4977	Aug 29, 2018 7:03:32 PM	9.9
Critical	CVE-2018-4872	Mar 16, 2018 3:31:41 PM	9.9
Critical	CVE-2016-3587	Nov 10, 2017 2:29:10 AM	9.9
Critical	CVE-2017-7826	Aug 1, 2018 12:06:17 PM	9.9
Critical	CVE-2017-5398	Aug 1, 2018 12:05:26 PM	9.8
Critical	CVE-2018-4879	Mar 16, 2018 3:31:55 PM	9.8
Critical	CVE-2018-4877	Mar 1, 2018 2:28:56 PM	9.8
Critical	CVE-2017-7779	Aug 1, 2018 12:04:29 PM	9.8

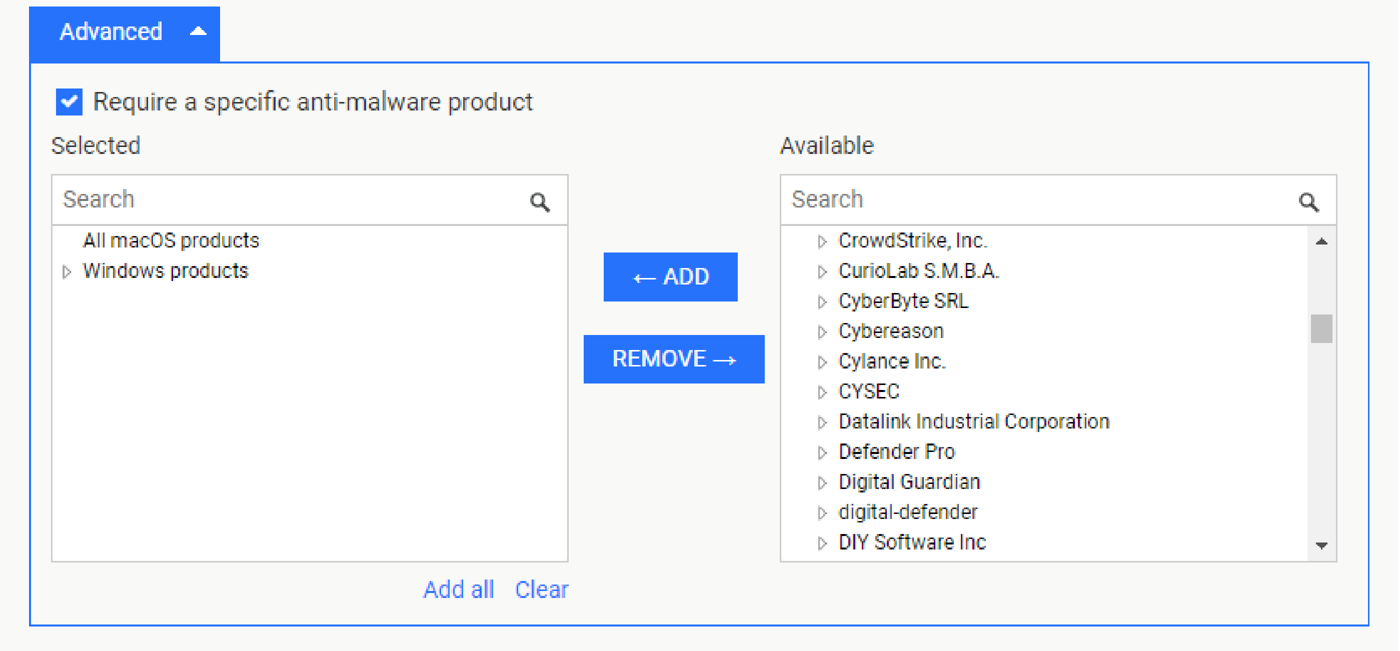
MetaAccess

How do we do it?

- Application vulnerabilities and missing patches
- Detection of over 5,000 3rd party applications
- Advanced Threat Prevention
  - Multi-antimalware scanning
  - Repeated threats detection
- Cloud security and access control
- Flexible customization and integration

What set us apart?

- Anti-Malware
- Encryption
- User Authentication
- Firewall
- Backup
- Anti-phishing



☑ Require a specific anti-malware product

Selected: All macOS products, Windows products

Available: CrowdStrike, Inc., CurioLab S.M.B.A., CyberByte SRL, Cybereason, Cylance Inc., CYSEC, Datalink Industrial Corporation, Defender Pro, Digital Guardian, digital-defender, DIY Software Inc

OPSWAT.

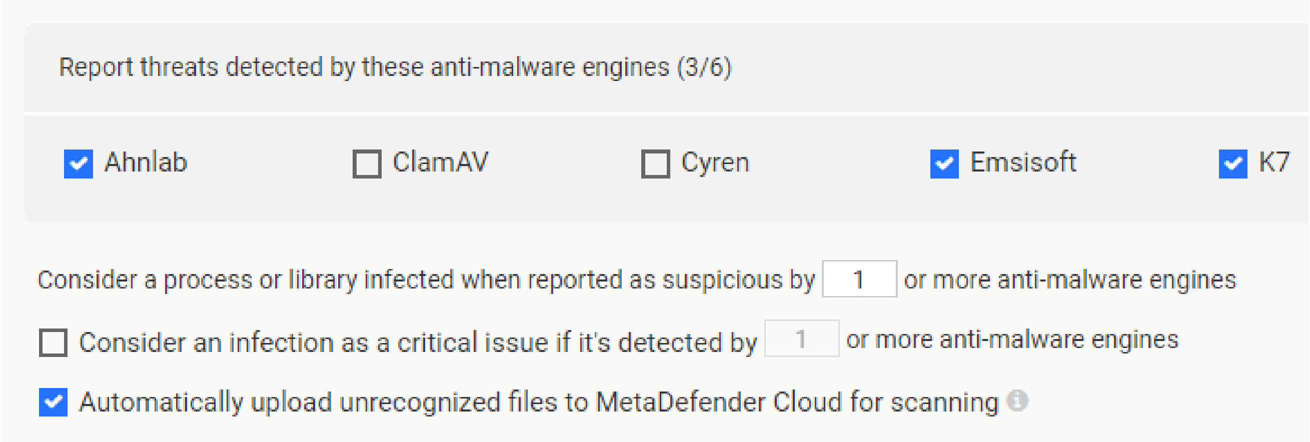
MetaAccess

How do we do it?

- Application vulnerabilities and missing patches
- Detection of over 5,000 3rd party applications
- Advanced Threat Prevention
  - Multi-antimalware scanning
  - Repeated threats detection
- Cloud security and access control
- Flexible customization and integration

What set us apart?

- Active malware detection with multiple Antimalware engines



Report threats detected by these anti-malware engines (3/6)

☑ Ahnlab ☐ ClamAV ☐ Cyren ☑ Emsisoft ☑ K7

Consider a process or library infected when reported as suspicious by 1 or more anti-malware engines

☐ Consider an infection as a critical issue if it's detected by 1 or more anti-malware engines

☑ Automatically upload unrecognized files to MetaDefender Cloud for scanning

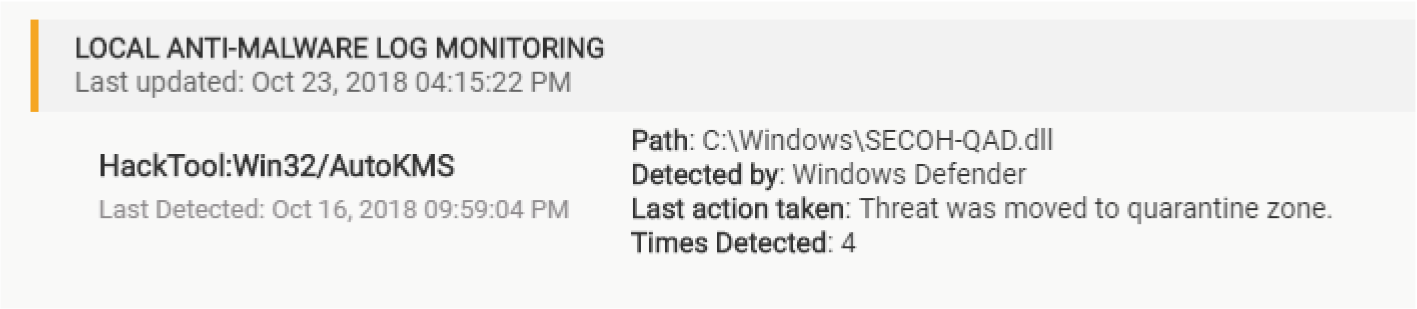
MetaAccess

How do we do it?

- Application vulnerabilities and missing patches
- Detection of over 5,000 3rd party applications
- Advanced Threat Prevention
  - Multi-antimalware scanning
  - Repeated threats detection
- Cloud security and access control
- Flexible customization and integration

What set us apart?

- Analyzing local threat activities for additional insight of repeated threats



LOCAL ANTI-MALWARE LOG MONITORING
Last updated: Oct 23, 2018 04:15:22 PM

HackTool:Win32/AutoKMS
Last Detected: Oct 16, 2018 09:59:04 PM

Path: C:\Windows\SECOH-QAD.dll
Detected by: Windows Defender
Last action taken: Threat was moved to quarantine zone.
Times Detected: 4

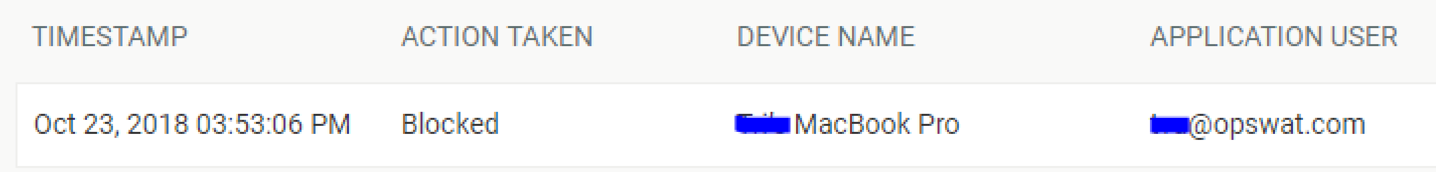
MetaAccess

How do we do it?

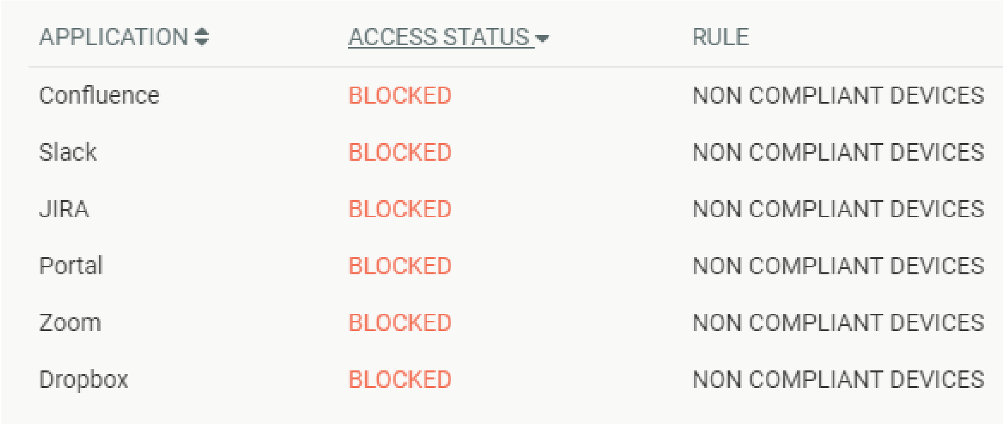
- Application vulnerabilities and missing patches
- Detection of over 5,000 3rd party applications
- Advanced Threat Prevention
  - Multi-antimalware scanning
  - Repeated threats detection
- Cloud security and access control
- Flexible customization and integration

What set us apart?

- Easy setup, up and running in minutes
- Monitor mode for least disruption in IT operation
- Full visibility from user to devices



TIMESTAMP	ACTION TAKEN	DEVICE NAME	APPLICATION USER
Oct 23, 2018 03:53:06 PM	Blocked	[redacted] MacBook Pro	[redacted]@opswat.com



APPLICATION ⬍	ACCESS STATUS ▾	RULE
Confluence	BLOCKED	NON COMPLIANT DEVICES
Slack	BLOCKED	NON COMPLIANT DEVICES
JIRA	BLOCKED	NON COMPLIANT DEVICES
Portal	BLOCKED	NON COMPLIANT DEVICES
Zoom	BLOCKED	NON COMPLIANT DEVICES
Dropbox	BLOCKED	NON COMPLIANT DEVICES

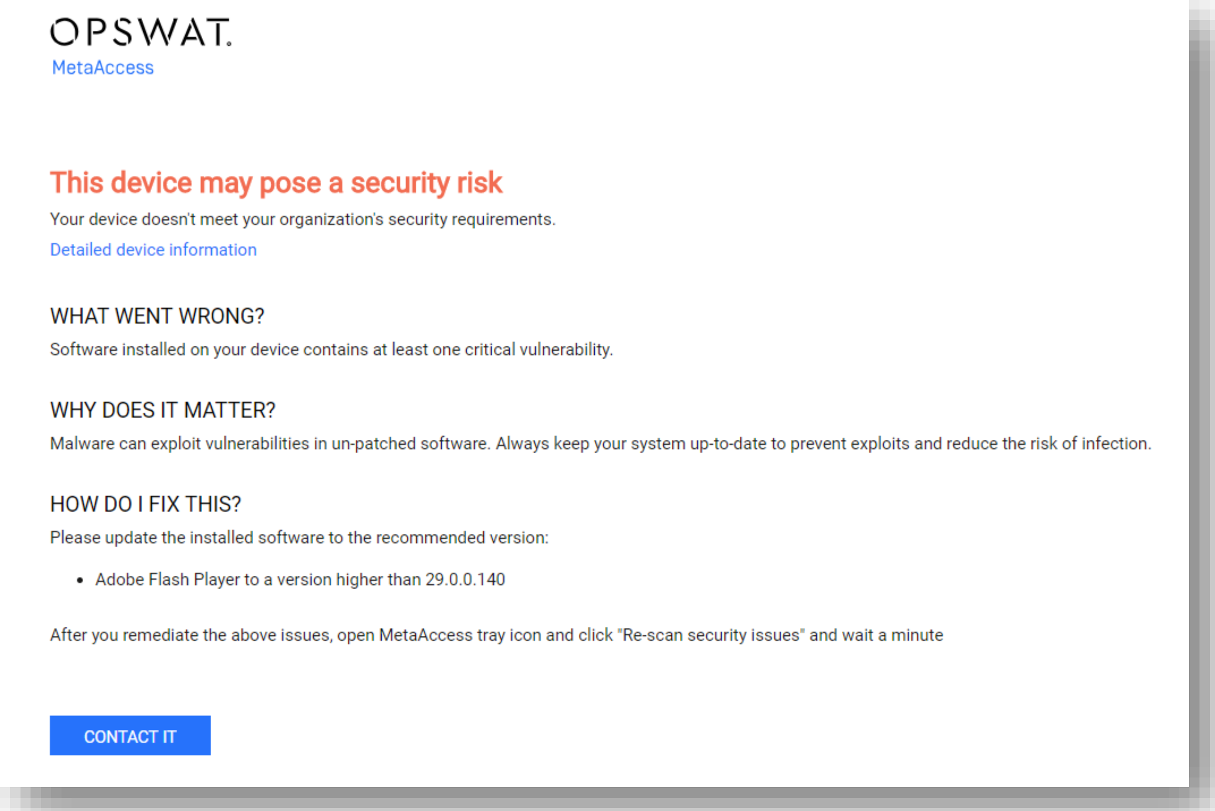
MetaAccess

How do we do it?

- Application vulnerabilities and missing patches
- Detection of over 5,000 3rd party applications
- Advanced Threat Prevention
    - Multi-antimalware scanning
    - Repeated threats detection
- Cloud security and access control
- Flexible customization and integration

What set us apart?

- Customizable remediation pages



OPSWAT.
MetaAccess

This device may pose a security risk

Your device doesn't meet your organization's security requirements.

Detailed device information

WHAT WENT WRONG?

Software installed on your device contains at least one critical vulnerability.

WHY DOES IT MATTER?

Malware can exploit vulnerabilities in un-patched software. Always keep your system up-to-date to prevent exploits and reduce the risk of infection.

HOW DO I FIX THIS?

Please update the installed software to the recommended version:

- Adobe Flash Player to a version higher than 29.0.0.140

After you remediate the above issues, open MetaAccess tray icon and click "Re-scan security issues" and wait a minute

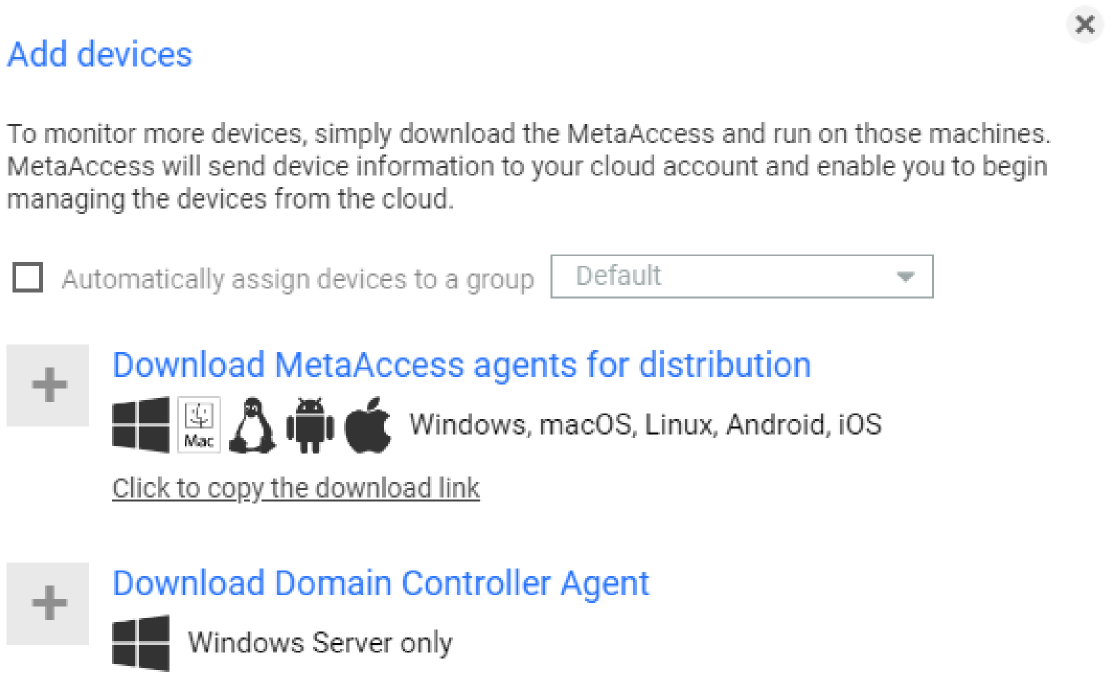
MetaAccess

How do we do it?

- Application vulnerabilities and missing patches
- Detection of over 5,000 3rd party applications
- Advanced Threat Prevention
  - Multi-antimalware scanning
  - Repeated threats detection
- Cloud security and access control
- Flexible customization and integration

What set us apart?

- Full platform support
- Easy agent onboarding



Add devices

To monitor more devices, simply download the MetaAccess and run on those machines. MetaAccess will send device information to your cloud account and enable you to begin managing the devices from the cloud.

□ Automatically assign devices to a group: Default

+ Download MetaAccess agents for distribution

Windows, macOS, Linux, Android, iOS

Click to copy the download link

+ Download Domain Controller Agent

Windows Server only

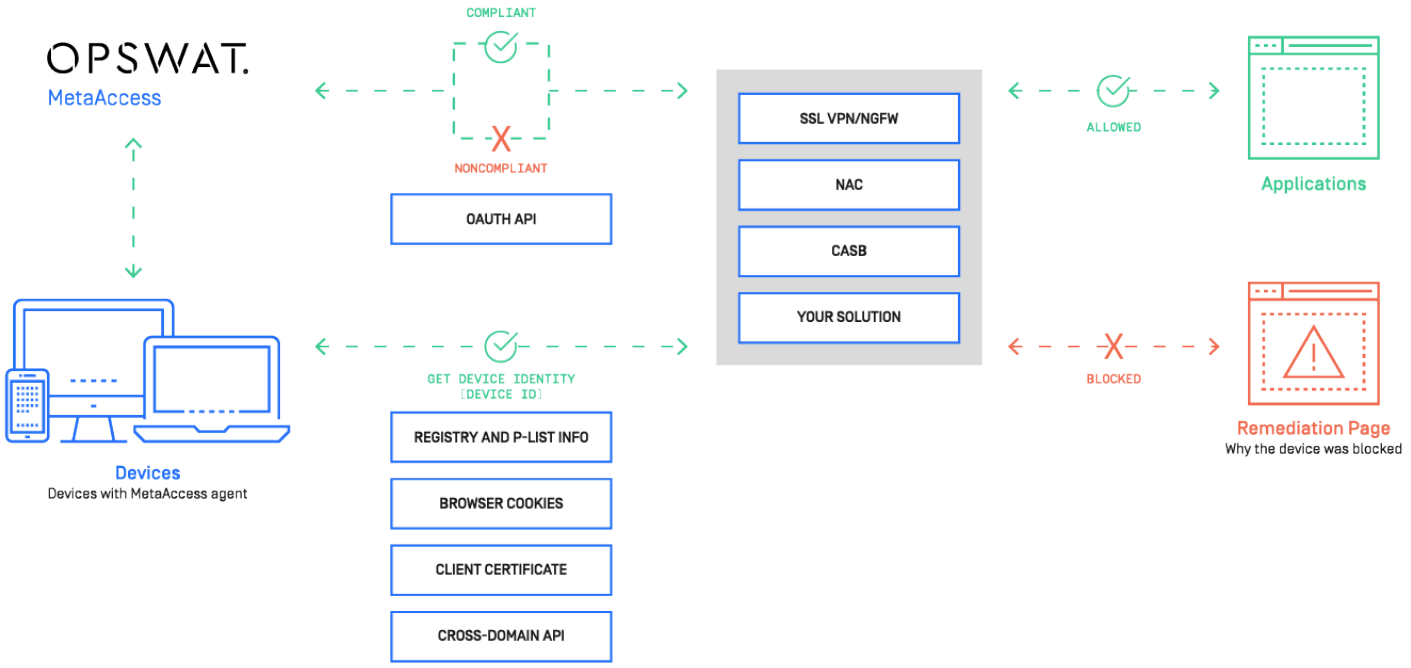
MetaAccess

How do we do it?

- Application vulnerabilities and missing patches
- Detection of over 5,000 3rd party applications
- Advanced Threat Prevention
  - Multi-antimalware scanning
  - Repeated threats detection
- Cloud security and access control
- Flexible customization and integration

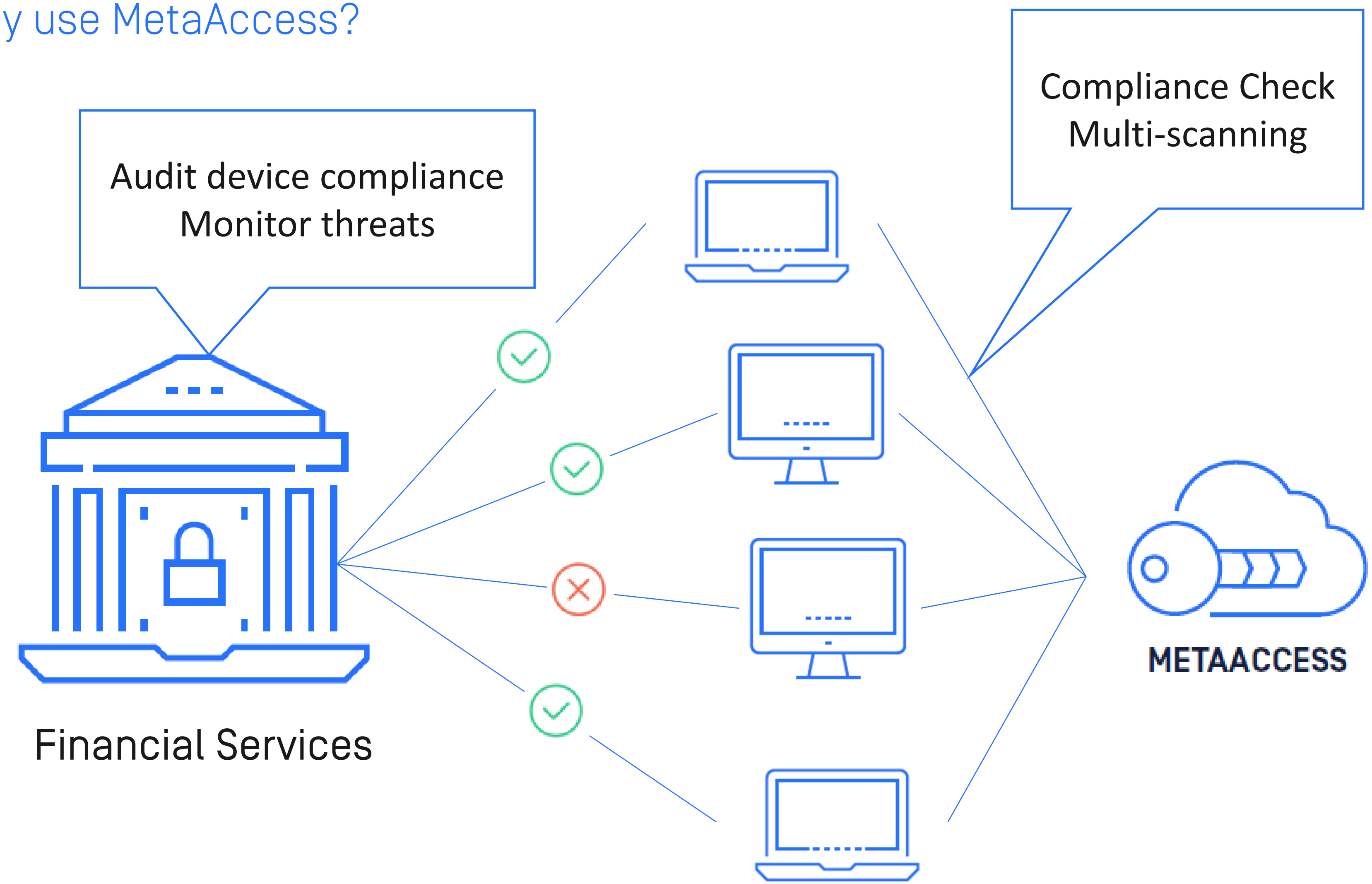
What set us apart?

- Multiple integration options
- Comprehensive Cloud APIs



Customer Case Studies

How do they use MetaAccess?

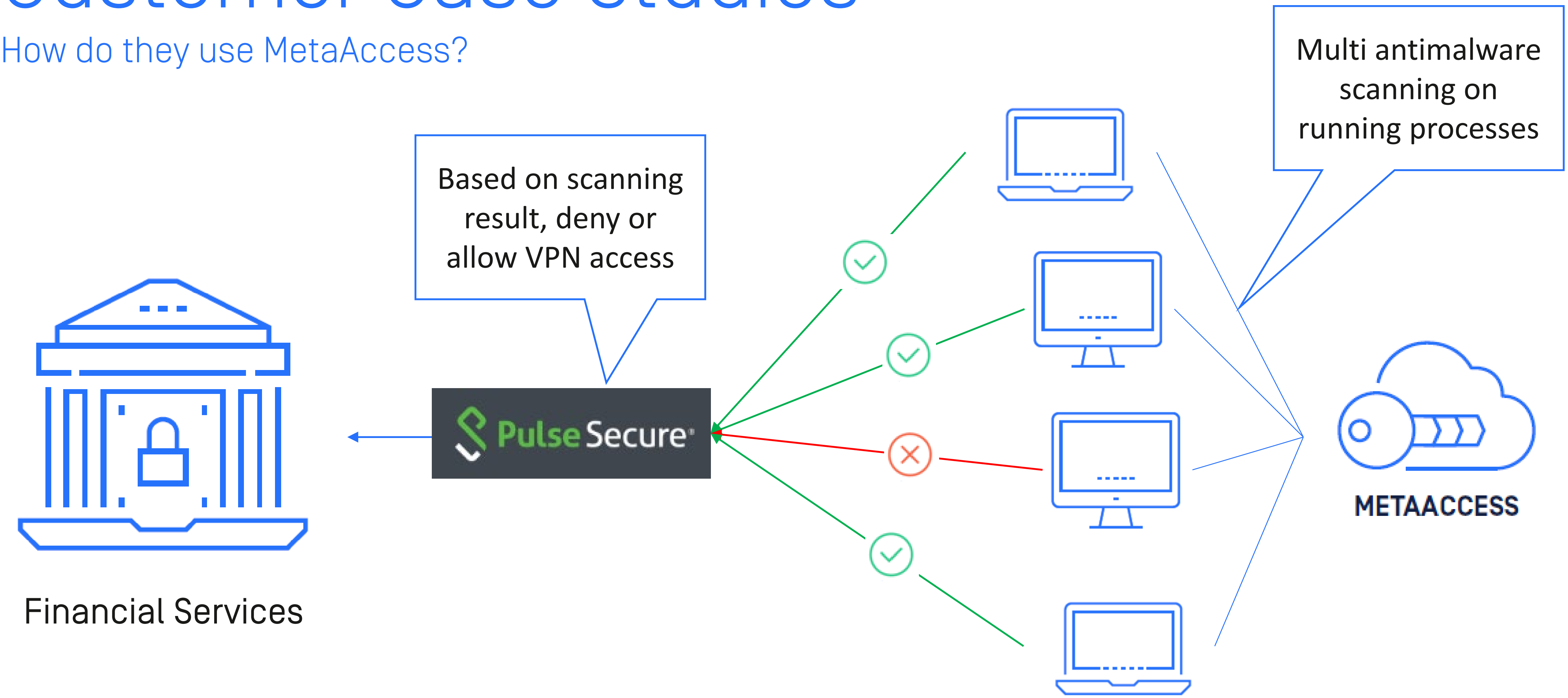


Audit device compliance
Monitor threats

Compliance Check
Multi-scanning

Customer Case Studies

How do they use MetaAccess?



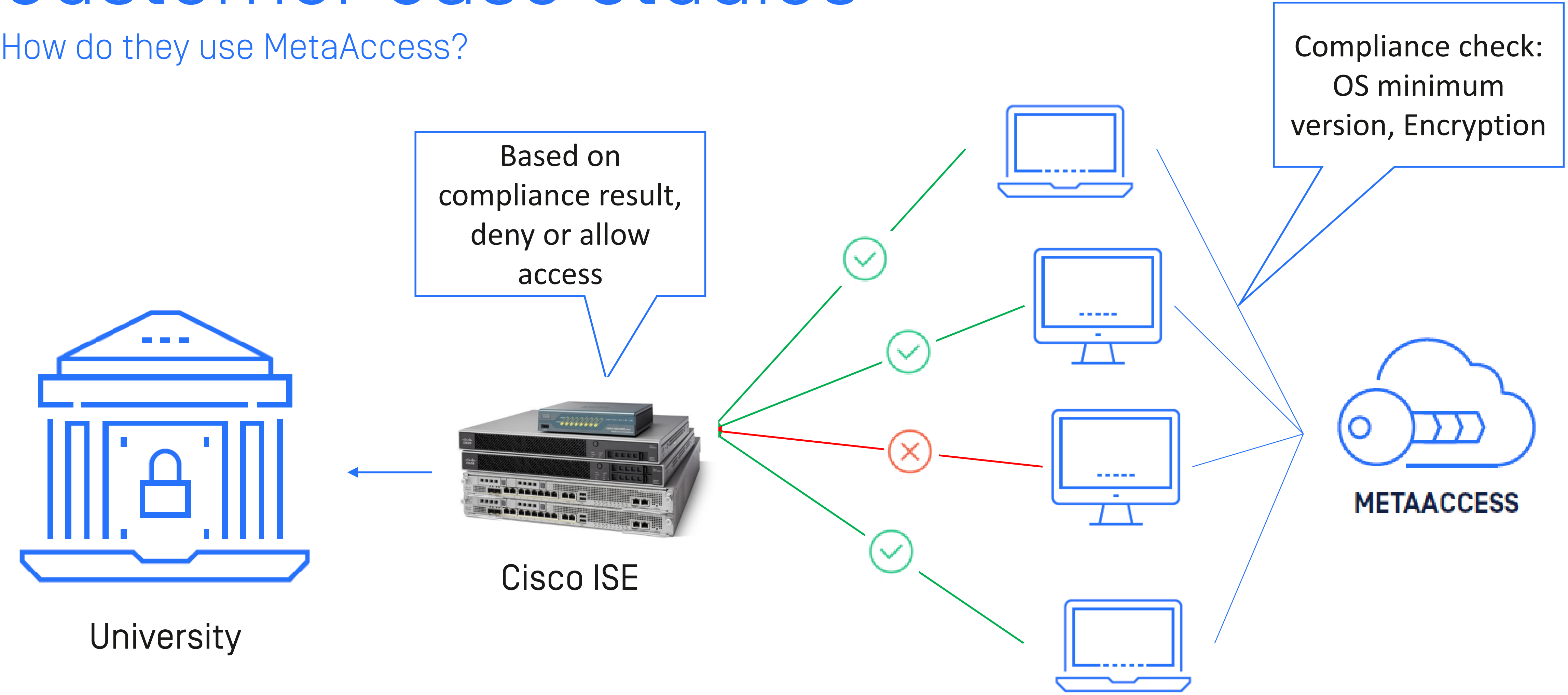
Based on scanning result, deny or allow VPN access

Multi antimalware scanning on running processes

Financial Services

Customer Case Studies

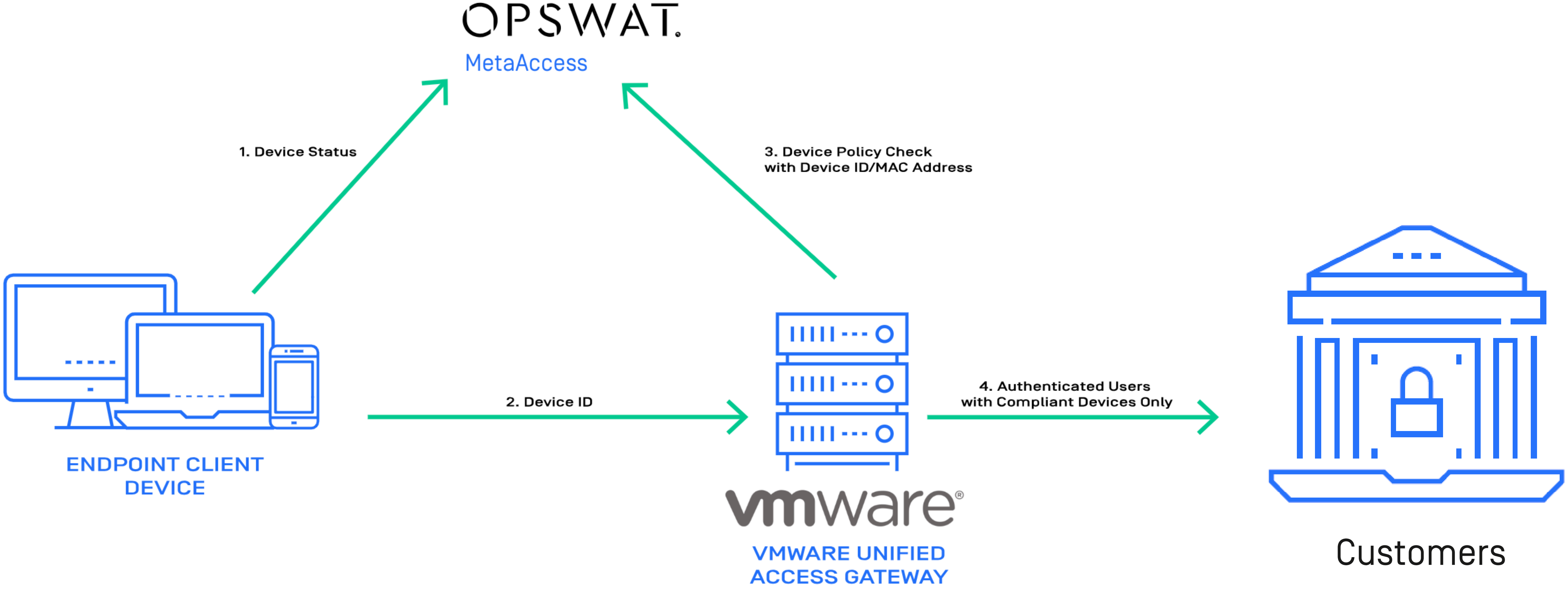
How do they use MetaAccess?



Based on compliance result, deny or allow access
Compliance check: OS minimum version, Encryption
University
Cisco ISE
METAACCESS

Customer Case Studies

How do they use MetaAccess?



OPSWAT.