OPSWAT.

Trust no file. Trust no device.

Implementing Zero Trust Secure Access for Work from Home

George Chereches – Presales Engineer

Matt Boksa- Senior Presale Enginner

OPSWAT.

OPSWAT.

Protecting the World's Critical Infrastructure

2002	Founded
9	Offices
1,500+	Customers
2,000+	Certified professionals
24/7	Support

Agenda

Preparing for Work from Home

Secure Remote Device Access

Secure Remote Network Access

Details and Programs

Q&A

OPSWAT.

Implementing Work from Home (WFH)

In today's environment, work from home is a critical reality. How can you implement quickly, safely and productively?

- Make sure everyone has technology and resources required to be productive.
- Ensure sufficient bandwidth
- Enable virtual collaboration
- Be realistic about the human impact
- Implement Secure Access

OPSWAT.

WFH Secure Access Concerns:

Threat actors are taking advantage of this situation, causing more risks.

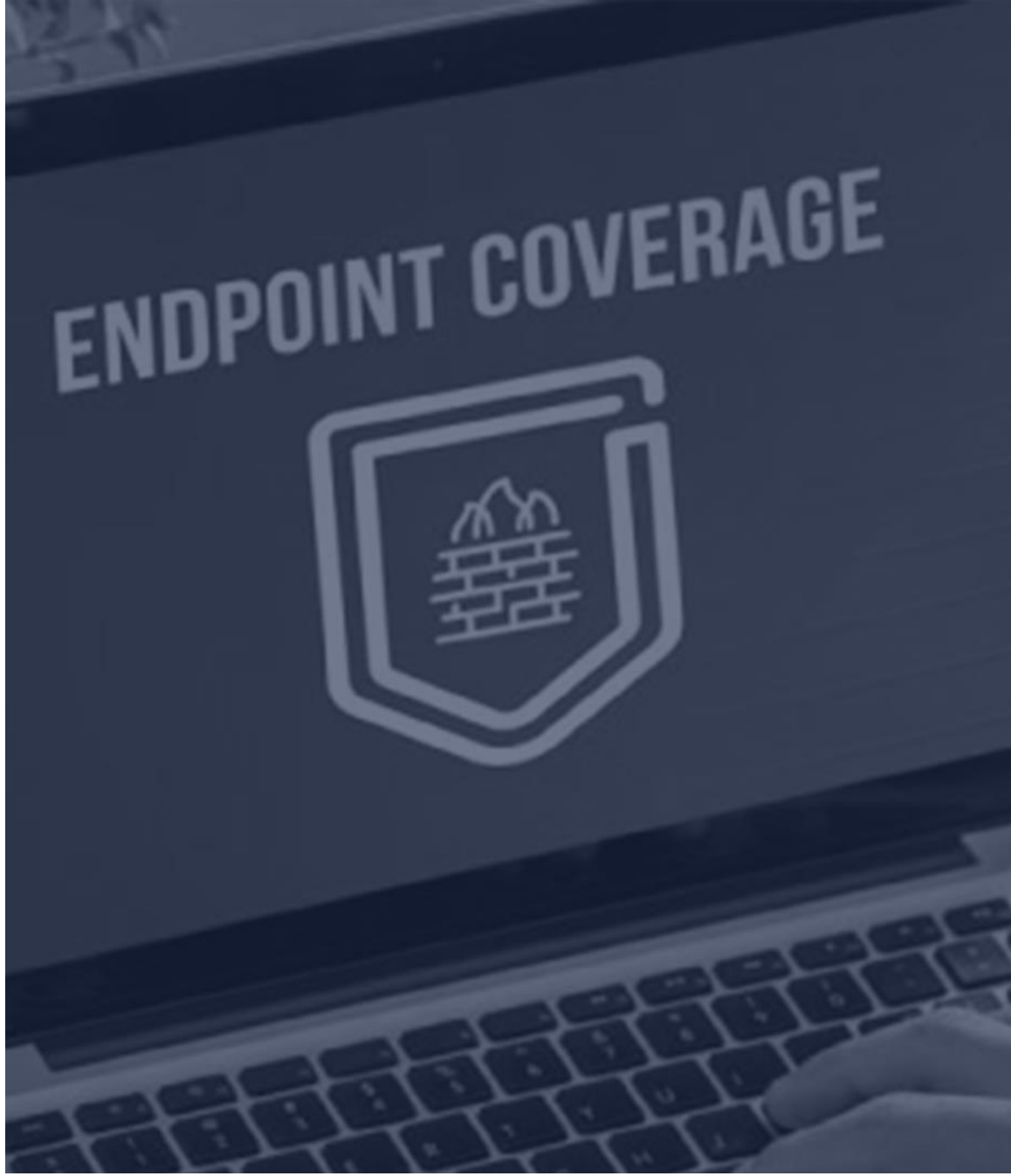
- the **Department** of Homeland Security's cyber agency issued an Alert pointing to specific cyber vulnerabilities around working from home versus the office
- CSO Online Six ways Attackers are Exploiting the CovID-19 Crisis focuses primarily on issues related to Work from Home
- What makes WFH so much more vulnerable to these attacks?

WFH Vulnerabilities Result From:

- Opening additional applications up for remote access
- Opening the network to more users via a VPN
- Having more workers using insecure home or public Wi-Fi
- Lack of visibility into application & cloud access remotely
- Permitting use of personal devices/BYOD from home
- Compliance sensitive data moved outside the perimeter
- New Approaches are required!

How OPSWAT Can Help:

- End-point security – checked before connecting
- Wi-Fi – ensuring the connection is encrypted
- Secure Virtual Desktop – keeping data on-prem
- Application exposure – limiting access and visibility
- Device Security Compliance –ensuring encryption



OPSWAT.

Agenda

Preparing for Work from Home

Secure Remote Device Access

Secure Remote Network Access

Details and Programs

Q & A

OPSWAT.

Secure WFH- MetaAccess Capabilities & Features

Compliance

- Ensure security applications are installed and configured
- Ensure devices encrypted, password protected
- Remove, updates software & components

Security

- Detect malware infection using multiple anti-malwares
- Report repeated threats
- Block and scan portable media content

Vulnerabilities

- Detect application, IoT and firmware vulnerabilities
- Report OS missing patches
- CVE prioritization

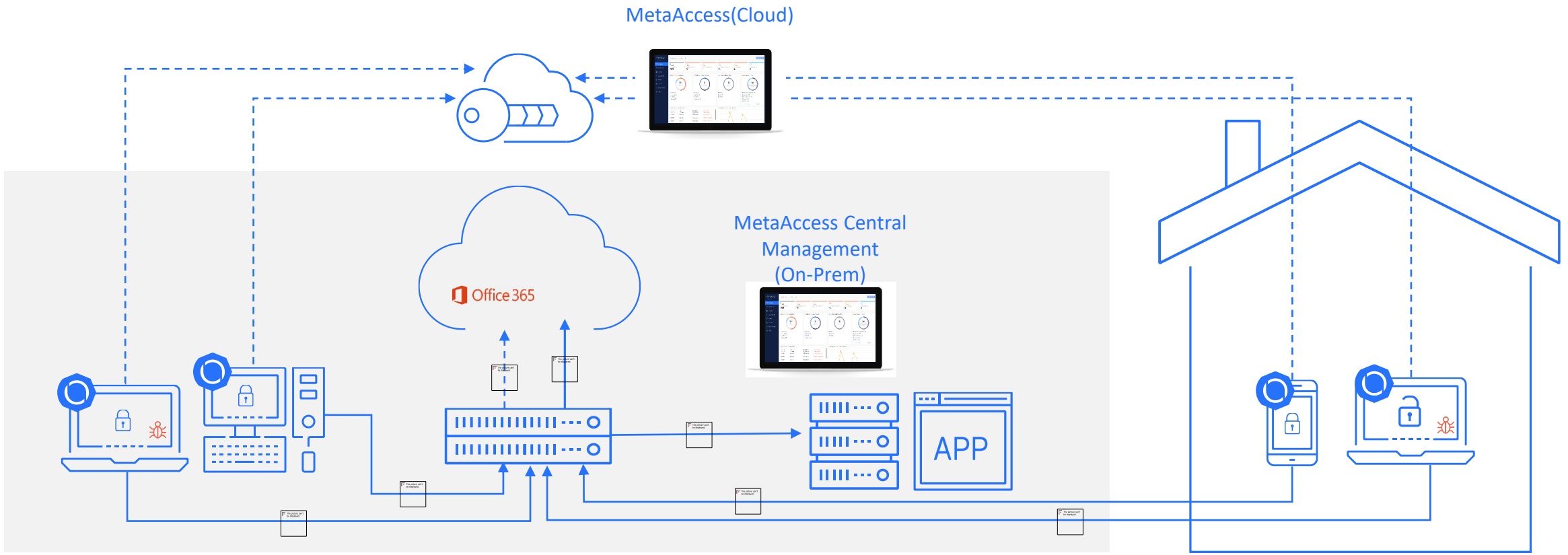
Access Control

- NAC/ VPN Integration
- VDI Integration
- SDP Integration
- Single sign-on (SAML) device access

OPSWAT.

Concept Diagram

Improve Existing NAC Deployment



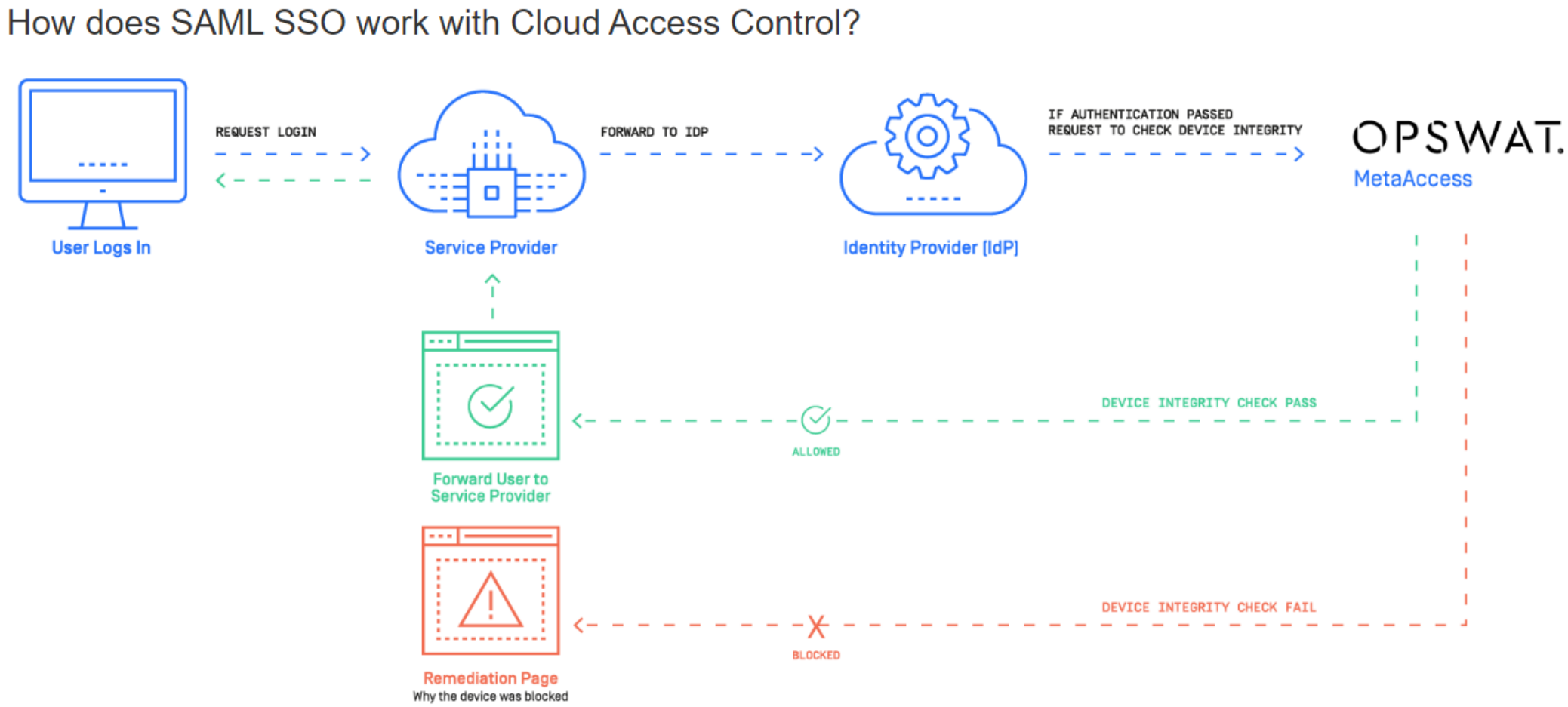
ENV 1
Corporate Office

NAC
Cisco ISE / Pulse Secure / Aruba / Etc..

Internal Resources
Server/Local Applications

ENV 2
Home Office

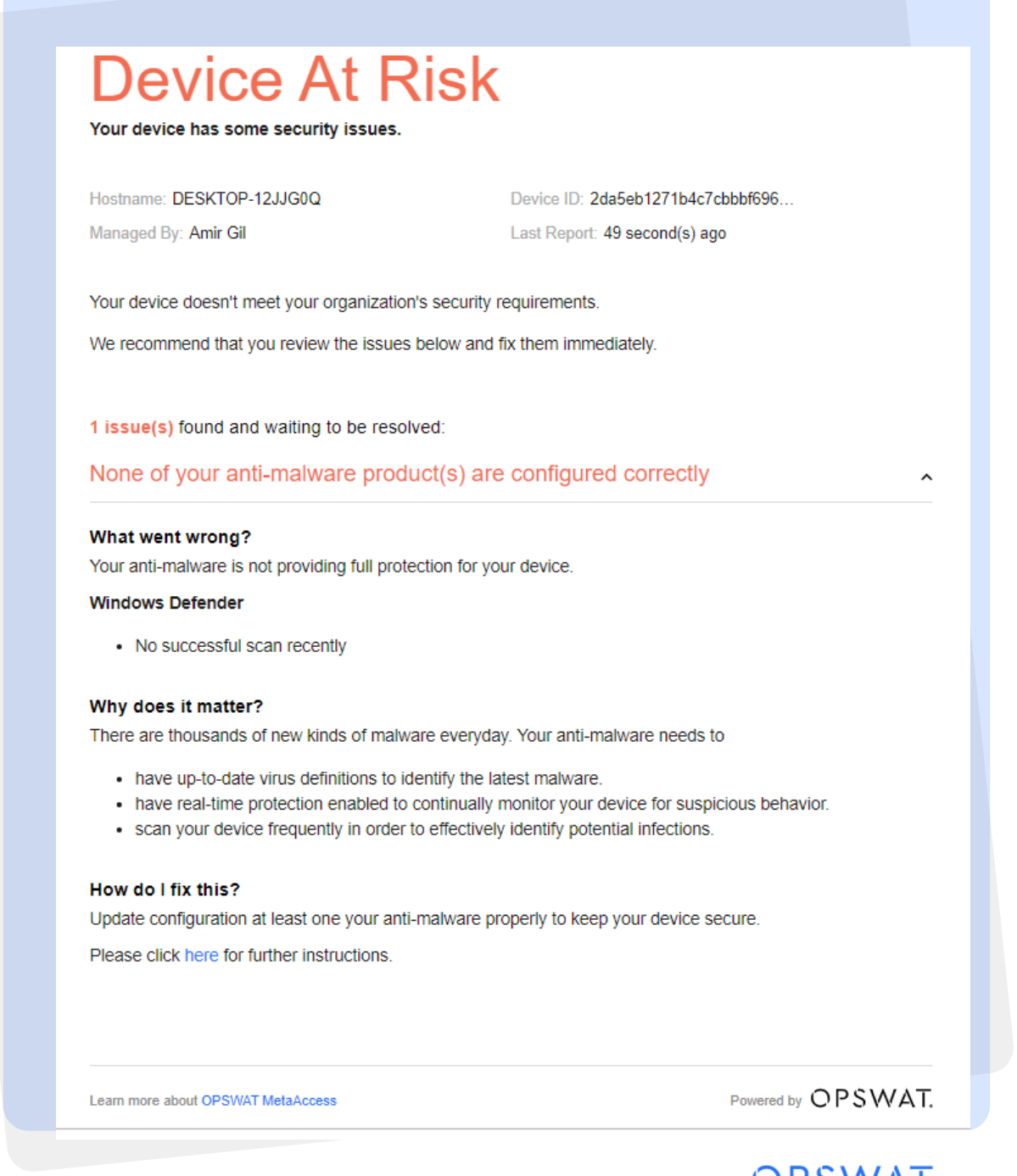
Device Zero Trust- SAML Integration



OPSWAT.

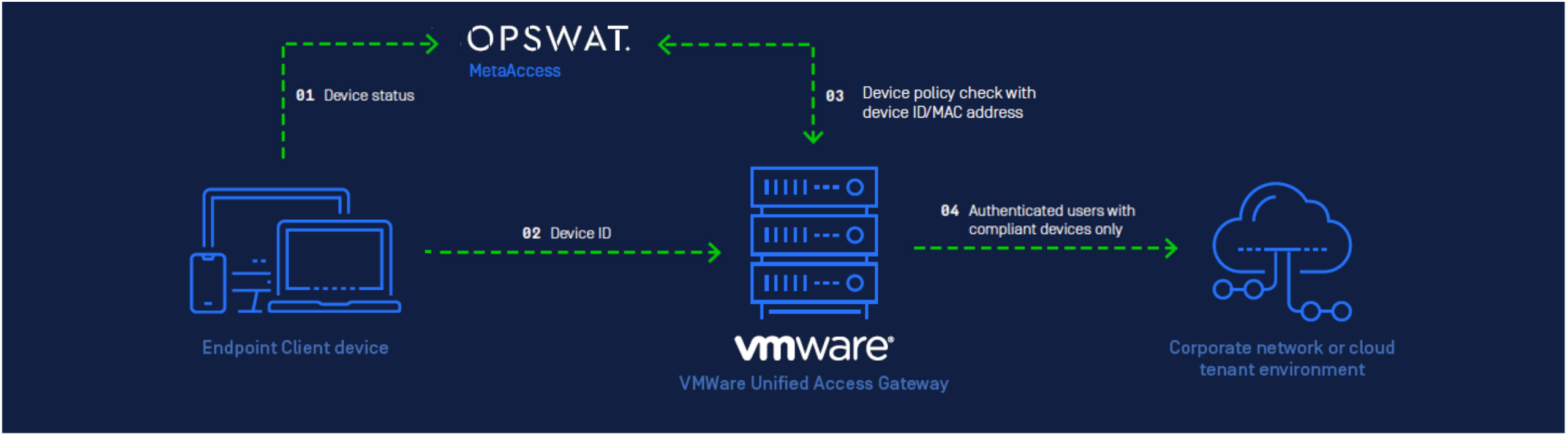
MetaAccess Remediation Page

Block and recommend (Save IT time)



OPSWAT.

Device Zero Trust- VMWare Integration



WFH- Regain Confidence for Compliance

HIPAA, PCI DSS, SOX, FINRA and Many More

Certification Assured Compliance- we know them all

- Zero-gap detection of updated software
- Advanced and in-depth checks
- Based on OPSWAT OESIS access control technology that is checking >100M devices worldwide as OEM in Cisco AnyConnect, F5, Palo Alto and many others

OPSWAT.

Agenda

Preparing for Work from Home

Secure Remote Device Access

Secure Remote Network Access

Details and Programs

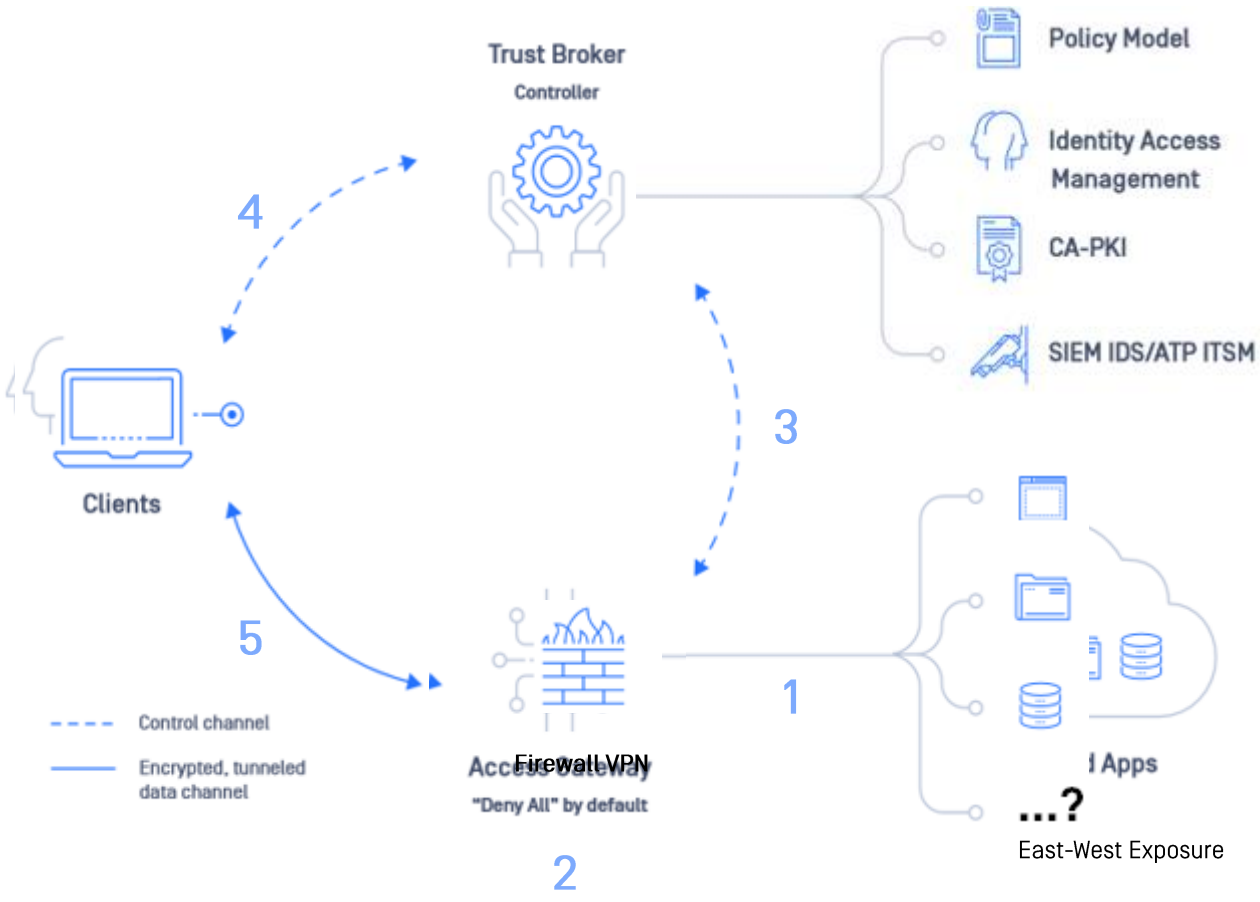
Q & A

OPSWAT.

Zero Trust Network Access

SafeConnect Software-Defined Perimeter (SDP)

- Traditionally, threat actors had a wide attack surface through a firewall VPN or LAN connection
- Zero trust is layered on through a DENY ALL, **Access Gateway** in front of applications
- A **Trust Broker** (controller) acts as an intermediary
- Before **Clients** connect to applications, trust policies are checked
- With SDP, only then can the **Clients** connect

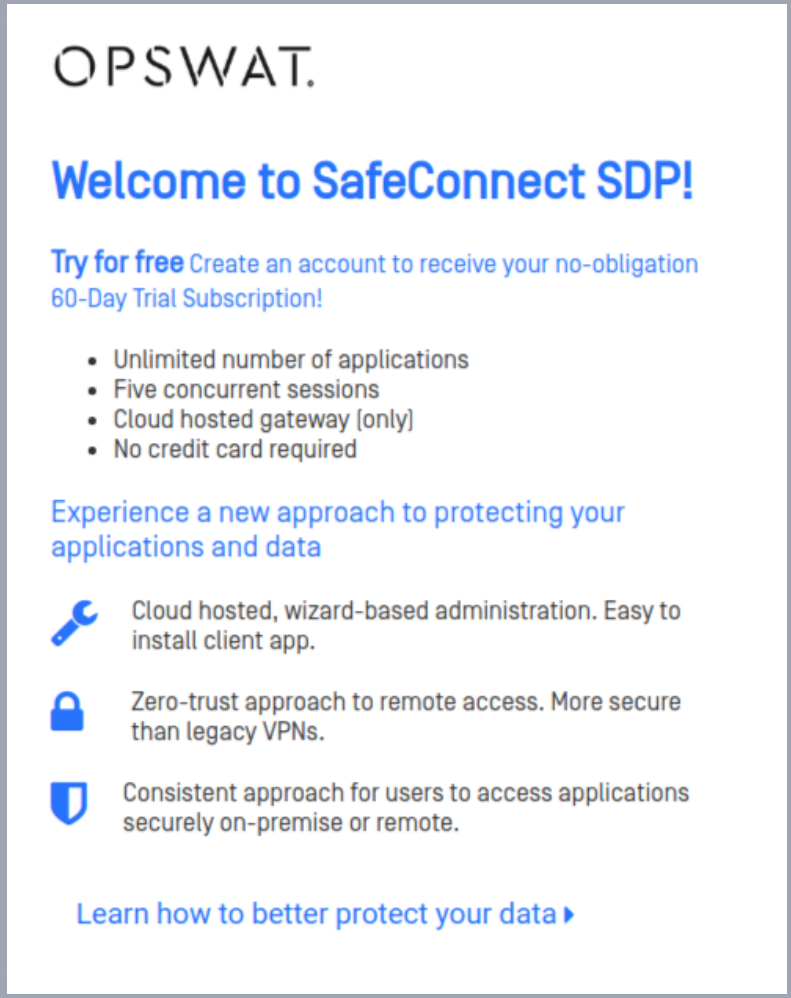


OPSWAT.

Use cases for SDP

Zero Trust Network Access

- Next-gen VPN
- Device compliance and security
- Multi cloud application security
- Unified, improved visibility
- Third party access, enabling collaboration



New Approach: Zero Trust Network Access

SafeConnect Software-Defined Perimeter (SDP)

Securely expose applications for remote use –

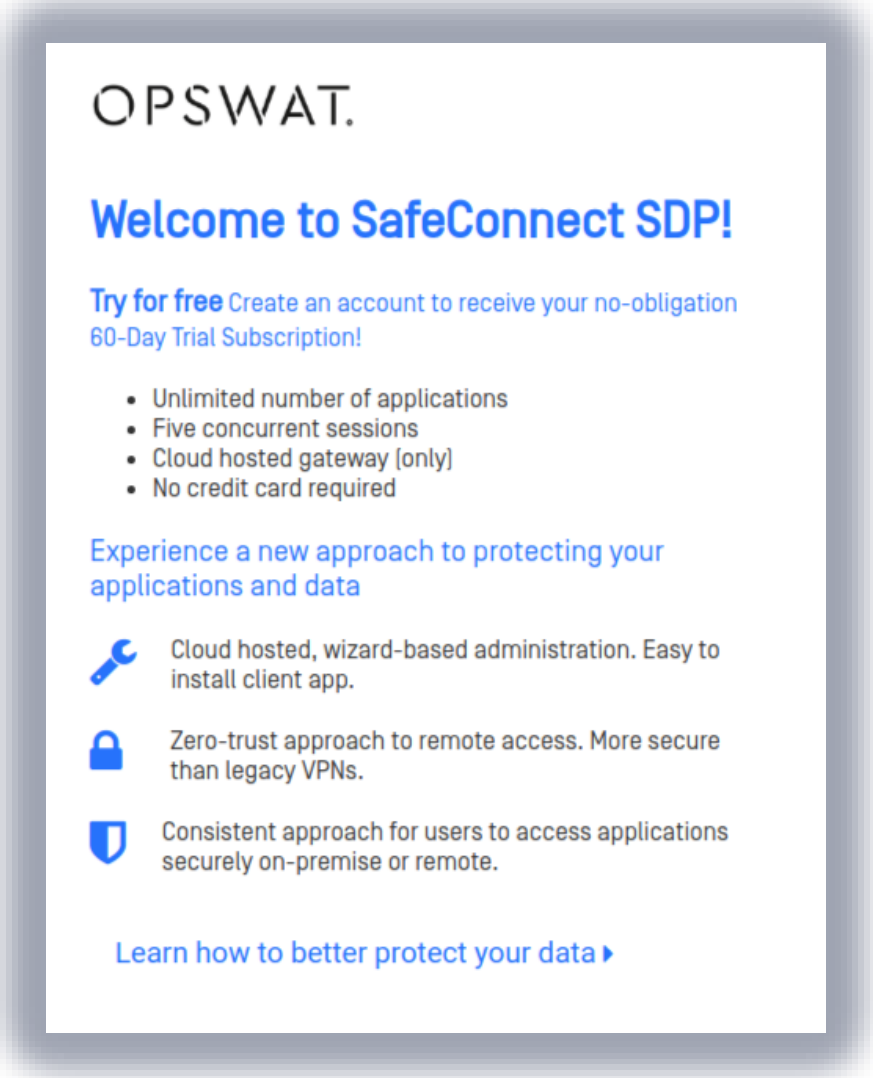
- Applications invisible — No access until authorized
- Prevents the most common attacks like DDoS
- Perimeter of one leveraging PKI, mTLS, tunnels

Visibility and Control - local or remote

- Deep end point security and compliance
- Consistent application of access policies
- Same user experience

VPN Alternative -

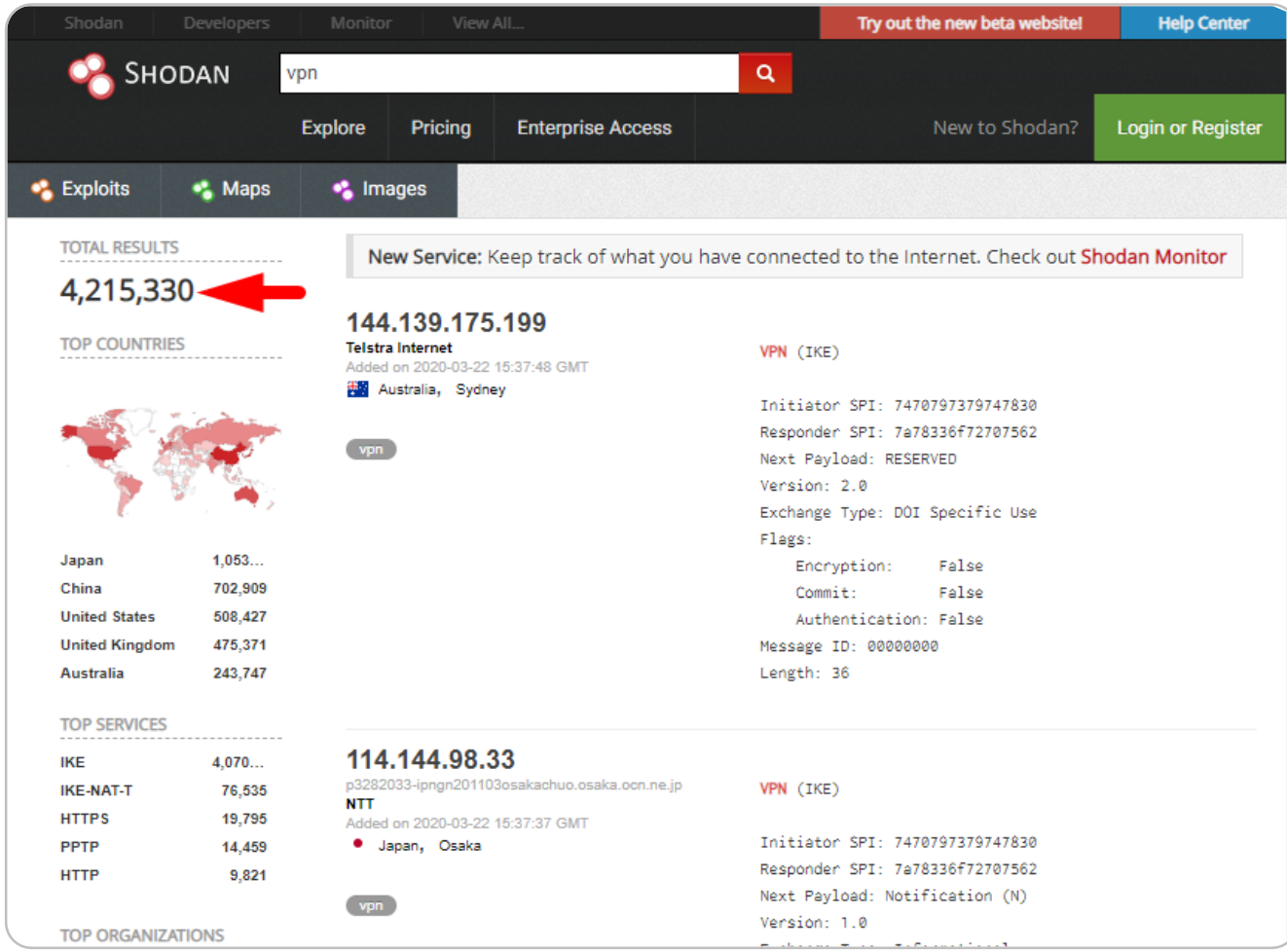
- Easier to deploy, scale
- Easer, modern management
- More secure



Zero Trust Network Access

Why Traditional VPNs are not Sufficient

- SDP not exposed for attack on the internet
- SDP automatically/easily:
  I. Mutually authenticates
  II. Controls access narrowly (allow East-West movement using phished credentials)
  III. Checks device security and authorizes user before the connection attempt



OPSWAT.

Agenda

Preparing for Work from Home

Secure Device Access

Secure Remote Access

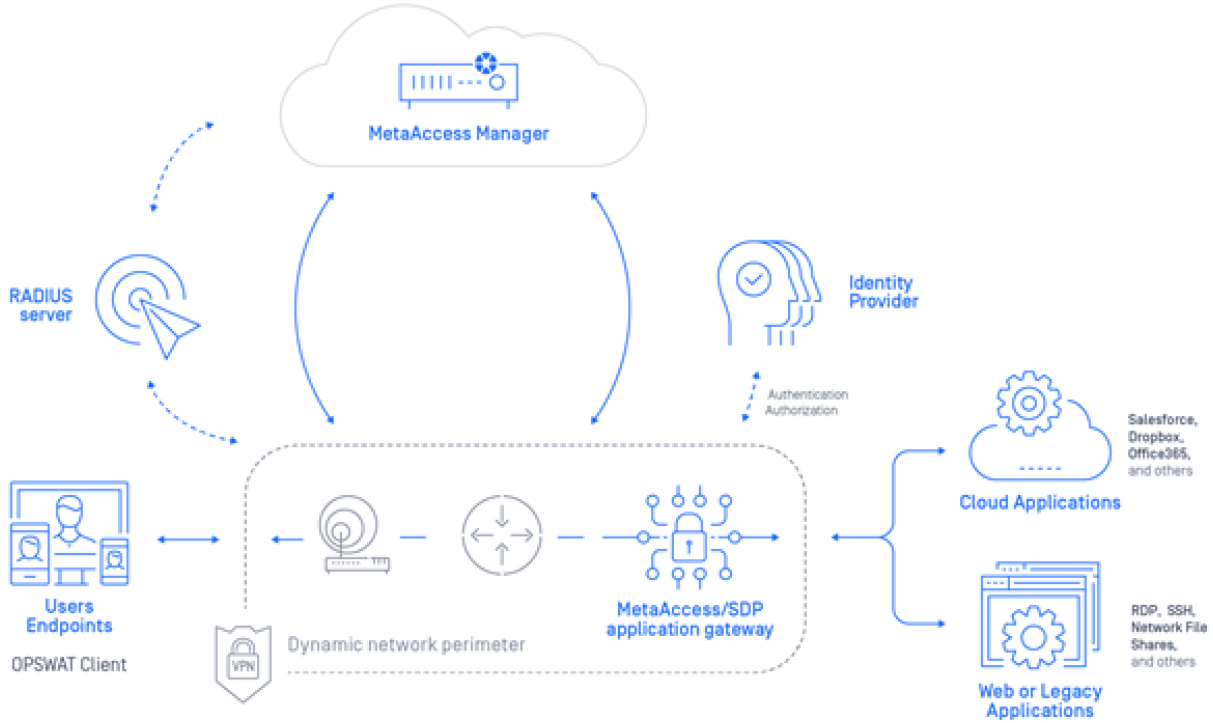
Details and Programs

Q & A

OPSWAT.

The OPSWAT Advantage: Total Device Security From Anywhere To Anywhere

- Strong network user and device identity
- Visibility and control on-prem and cloud
- Granular policy enforcement with self-remediation
- Secures Wi-fi
- Least privileged access to applications
- Compliance on end-points
- Positive, consistent user experience



OPSWAT.

Other Solutions We Offer

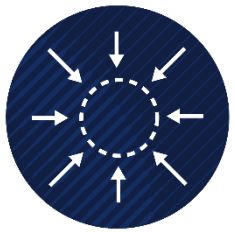
Cross-Domain Solutions

Malware Analysis

File Upload Security

Email Security

Secure Device Access



Network Access Control

OPSWAT.