



OPSWAT.

Trust no file. Trust no device.

# Implementing Zero Trust Secure Access for Work from Home

George Chereches – Presales Engineer

Matt Boksa- Senior Presale Engineer

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



# 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



# 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

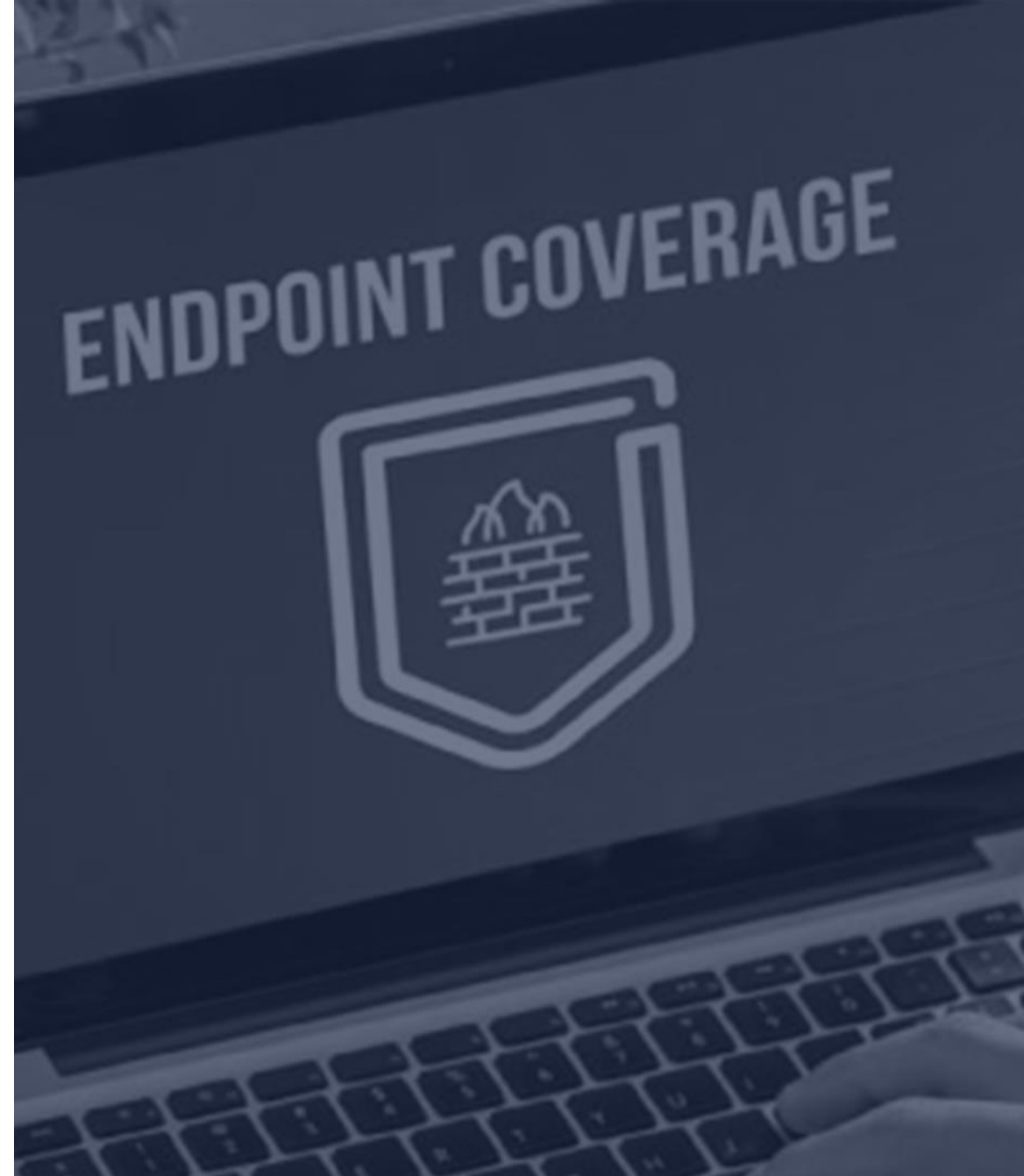
## Result From:

- 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





# Agenda

Preparing for Work from Home

Secure Remote Device Access

Secure Remote Network Access

Details and Programs

Q & A

# 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

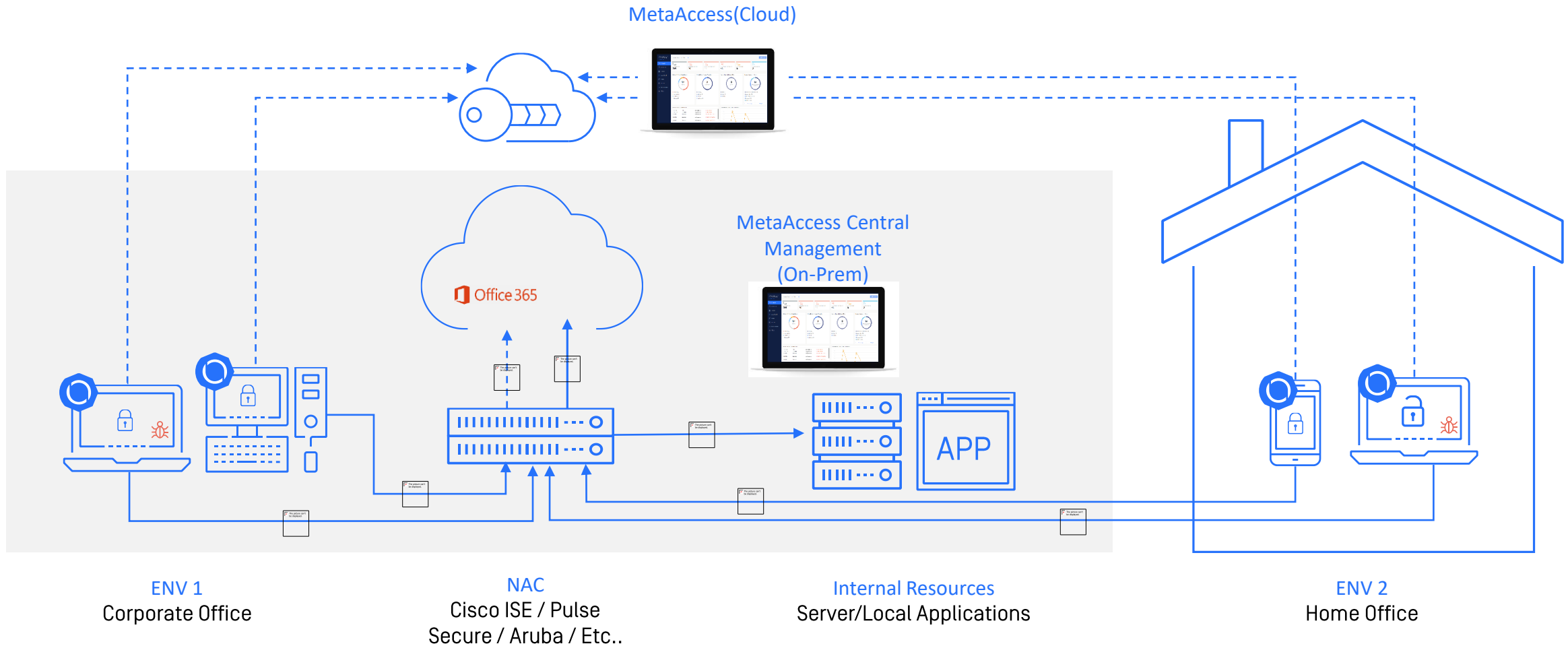
- Detect application, IoT and firmware vulnerabilities
- Report OS missing patches
- CVE prioritization

## Access Control

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

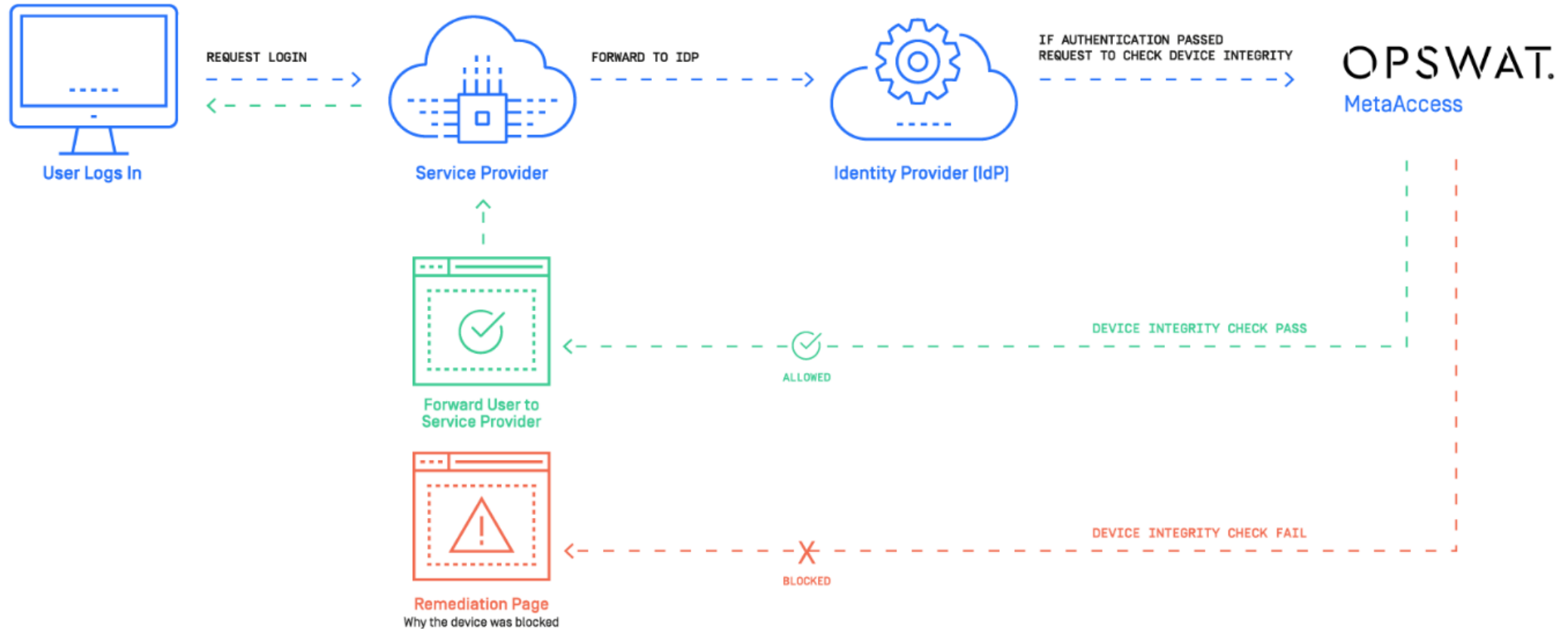
# Concept Diagram

## Improve Existing NAC Deployment



# Device Zero Trust- SAML Integration

How does SAML SSO work with Cloud Access Control?



# MetaAccess Remediation Page

Block and recommend (Save IT time)

## Device At Risk

Your device has some security issues.

Hostname: DESKTOP-12JJG0Q

Device ID: 2da5eb1271b4c7cbbb696...

Managed By: Amir Gil

Last Report: 49 second(s) ago

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

We recommend that you review the issues below and fix them immediately.

**1 issue(s)** found and waiting to be resolved:

**None of your anti-malware product(s) are configured correctly** ^

### What went wrong?

Your anti-malware is not providing full protection for your device.

#### Windows Defender

- No successful scan recently

### Why does it matter?

There are thousands of new kinds of malware everyday. Your anti-malware needs to

- have up-to-date virus definitions to identify the latest malware.
- have real-time protection enabled to continually monitor your device for suspicious behavior.
- scan your device frequently in order to effectively identify potential infections.

### How do I fix this?

Update configuration at least one your anti-malware properly to keep your device secure.

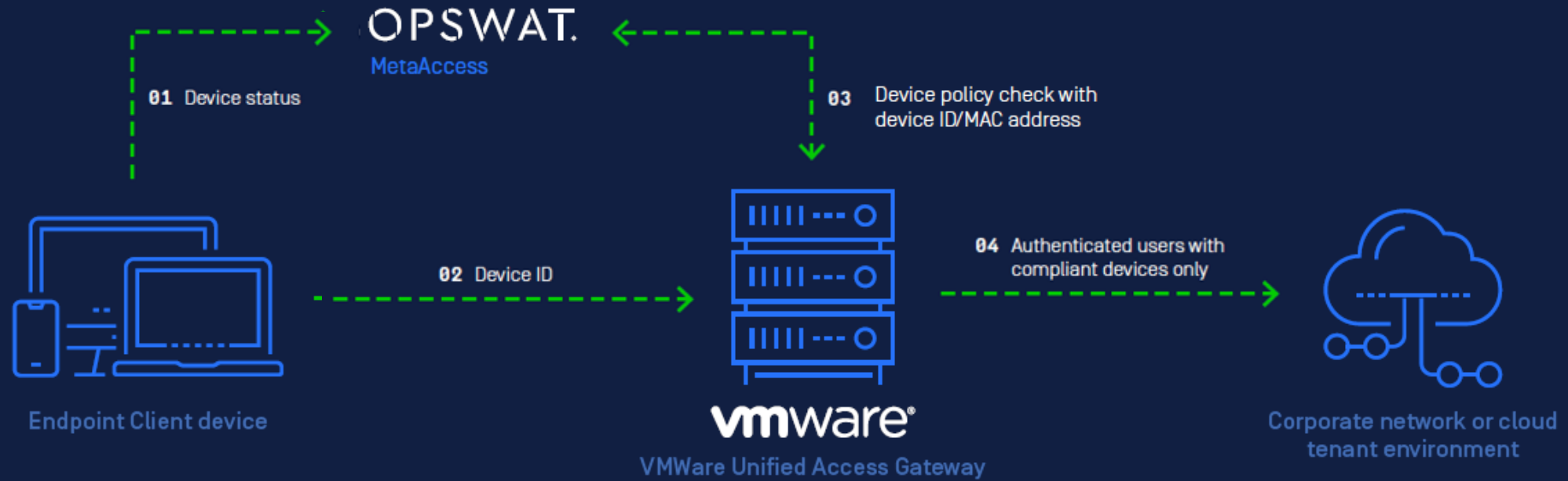
Please click [here](#) for further instructions.

Learn more about [OPSWAT MetaAccess](#)

Powered by 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



# Agenda

Preparing for Work from Home

Secure Remote Device Access

Secure Remote Network Access

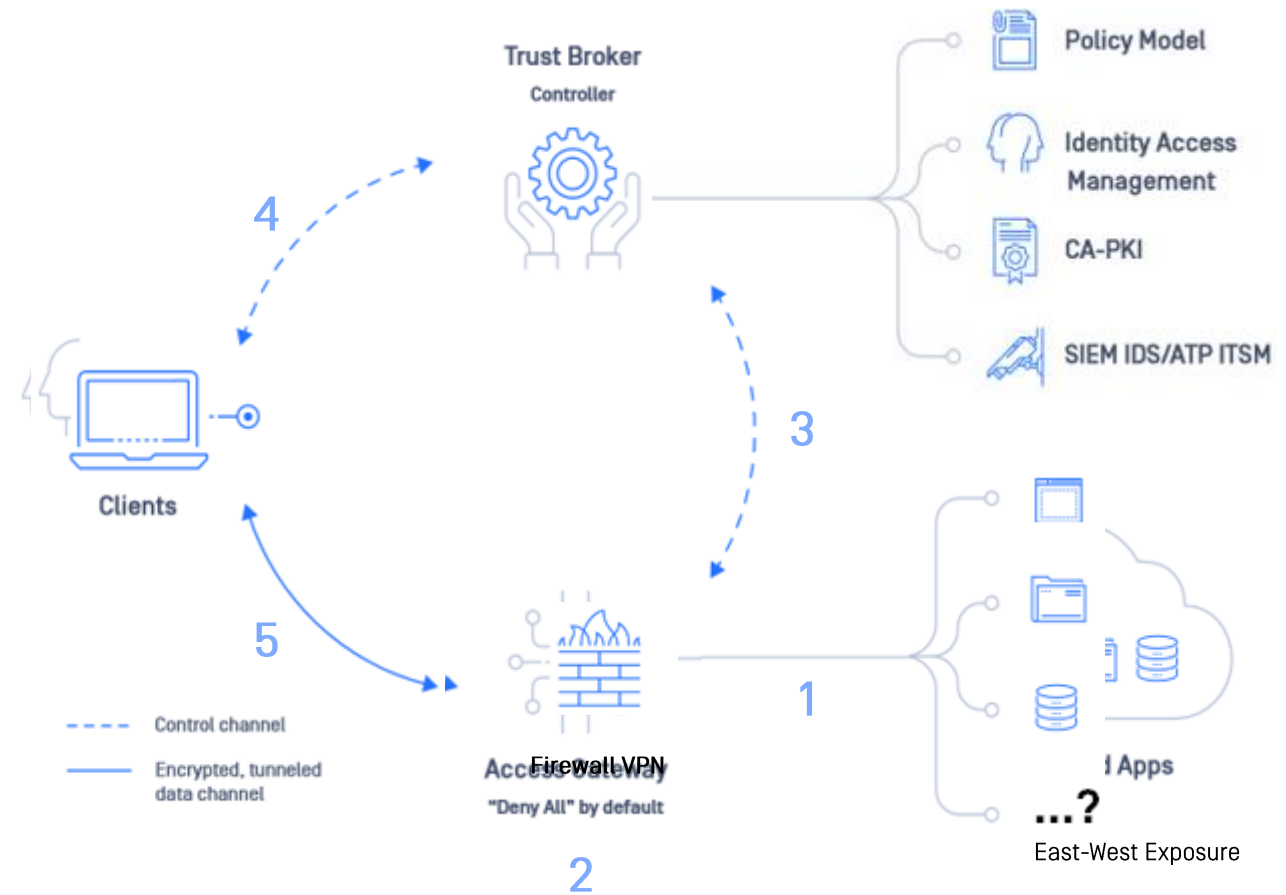
Details and Programs

Q & A

# 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



# 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

OPSWAT.

## Welcome to SafeConnect SDP!

**Try for free** Create an account to receive your no-obligation 60-Day Trial Subscription!

- Unlimited number of applications
- Five concurrent sessions
- Cloud hosted gateway (only)
- No credit card required

Experience a new approach to protecting your applications and data



Cloud hosted, wizard-based administration. Easy to install client app.



Zero-trust approach to remote access. More secure than legacy VPNs.



Consistent approach for users to access applications securely on-premise or remote.

[Learn how to better protect your data ▶](#)



# 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
- Easier, modern management
- More secure

OPSWAT.

## Welcome to SafeConnect SDP!

**Try for free** Create an account to receive your no-obligation 60-Day Trial Subscription!

- Unlimited number of applications
- Five concurrent sessions
- Cloud hosted gateway (only)
- No credit card required

Experience a new approach to protecting your applications and data



Cloud hosted, wizard-based administration. Easy to install client app.



Zero-trust approach to remote access. More secure than legacy VPNs.



Consistent approach for users to access applications securely on-premise or remote.

[Learn how to better protect your data ▶](#)

# 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

Shodan Developers Monitor View All... Try out the new beta website! Help Center

SHODAN vpn

Explore Pricing Enterprise Access New to Shodan? Login or Register

Exploits Maps Images

TOTAL RESULTS  
4,215,330

TOP COUNTRIES

Japan	1,053...
China	702,909
United States	508,427
United Kingdom	475,371
Australia	243,747

TOP SERVICES

IKE	4,070...
IKE-NAT-T	76,535
HTTPS	19,795
PPTP	14,459
HTTP	9,821

TOP ORGANIZATIONS

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

**144.139.175.199**  
Telstra Internet  
Added on 2020-03-22 15:37:48 GMT  
Australia, Sydney

vpn

VPN (IKE)  
Initiator SPI: 7470797379747830  
Responder SPI: 7a78336f72707562  
Next Payload: RESERVED  
Version: 2.0  
Exchange Type: DOI Specific Use  
Flags:  
Encryption: False  
Commit: False  
Authentication: False  
Message ID: 00000000  
Length: 36

**114.144.98.33**  
p3282033-ipngn201103osakachuo.osaka.ocn.ne.jp  
NTT  
Added on 2020-03-22 15:37:37 GMT  
Japan, Osaka

vpn

VPN (IKE)  
Initiator SPI: 7470797379747830  
Responder SPI: 7a78336f72707562  
Next Payload: Notification (N)  
Version: 1.0

# Agenda

Preparing for Work from Home

Secure Device Access

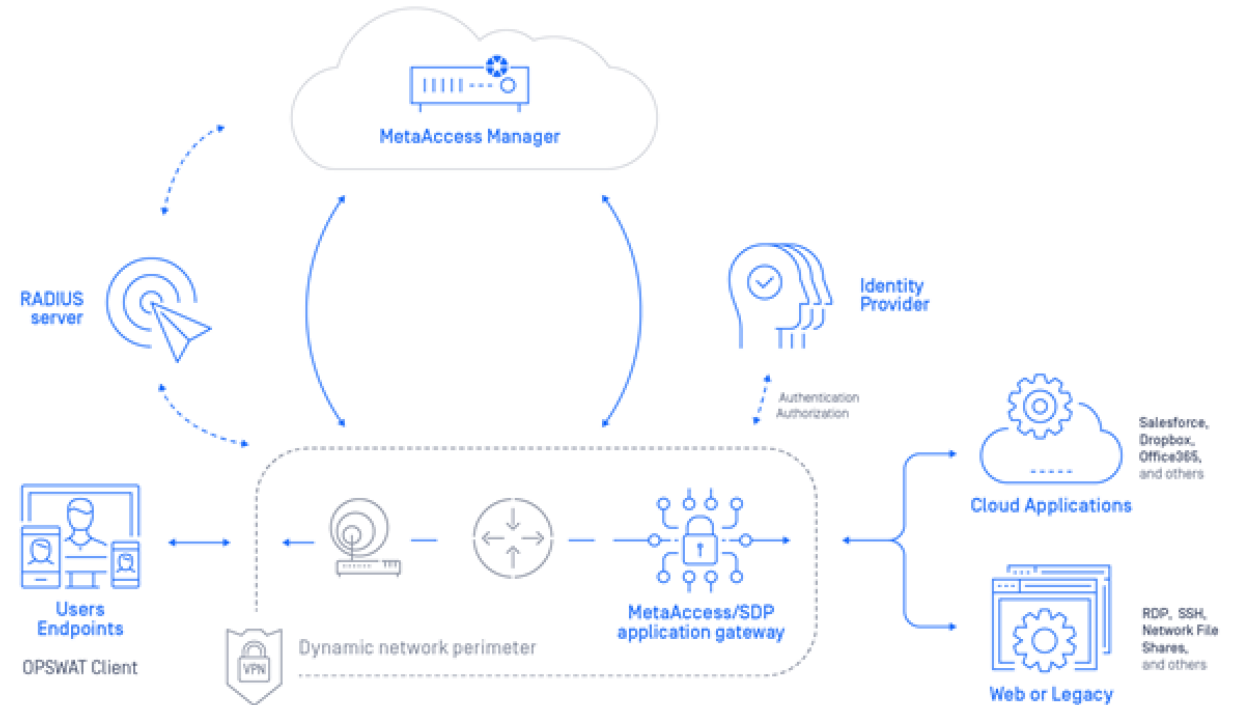
Secure Remote Access

Details and Programs

Q & A

# 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



# Other Solutions We Offer



Cross-Domain Solutions



Malware Analysis



File Upload Security



Email Security



Secure Device Access



Network Access Control