



McAfee Unified Cloud Edge

Device-to-Cloud Data and Threat Protection

Manong Antawn
Senior Support Engineer @ McAfee
Solution Architect
University Lecturer/Researcher

[Inquire Now](#)



Content

Introduction

McAfee Unified Cloud Edge

Architecture

Use Cases

Summary

Introduction

CyberSecurity Importance

- Protecting personal and sensitive information
- It enables people to carry out their jobs, education and research
- Supporting critical business processes

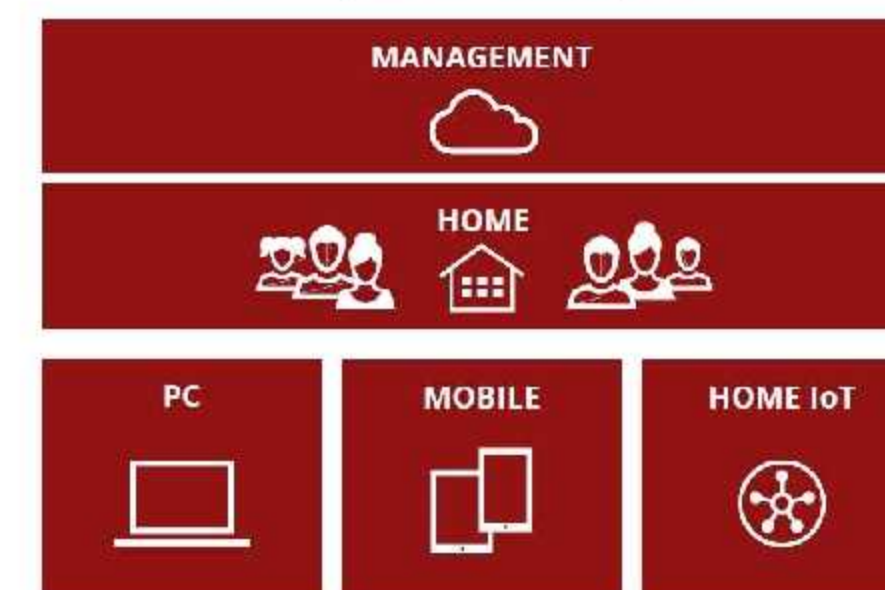
McAfee Portfolio Strategy

An integrated, open system protects from the device to the cloud



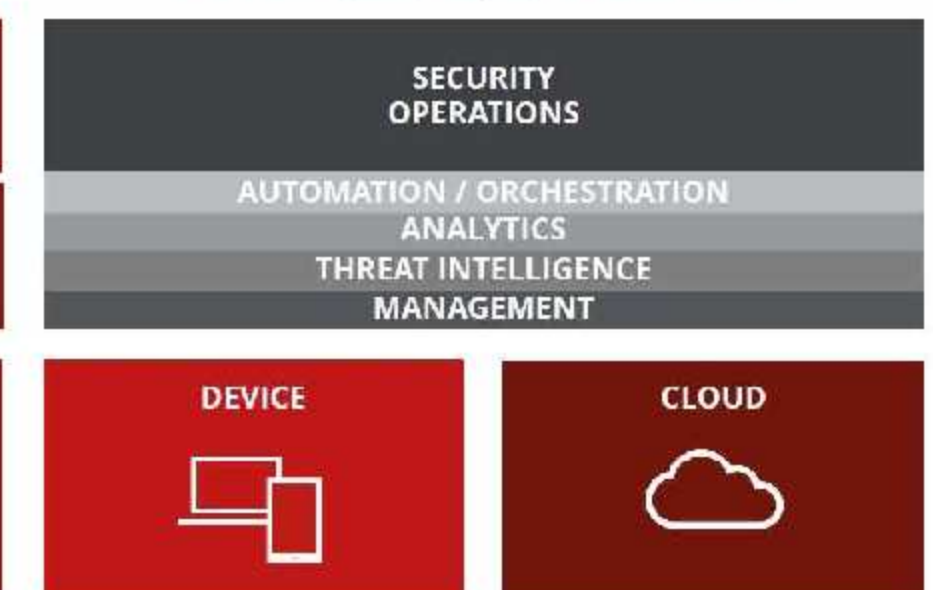
Consumer

Protecting the consumer's digital life from any cybersecurity threat across all devices (PC, mobile, and home IoT) via a simple, common, and unified user experience



Corporate

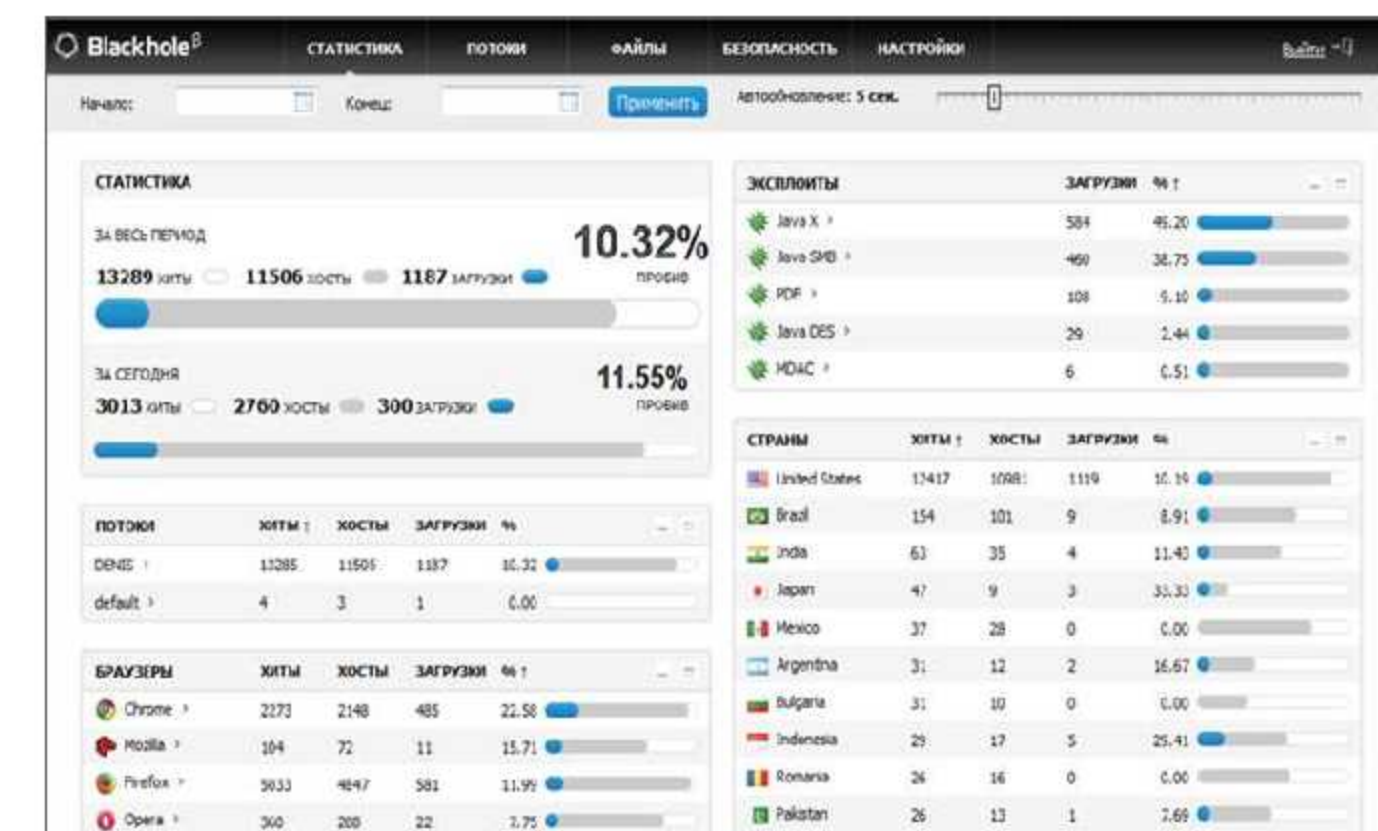
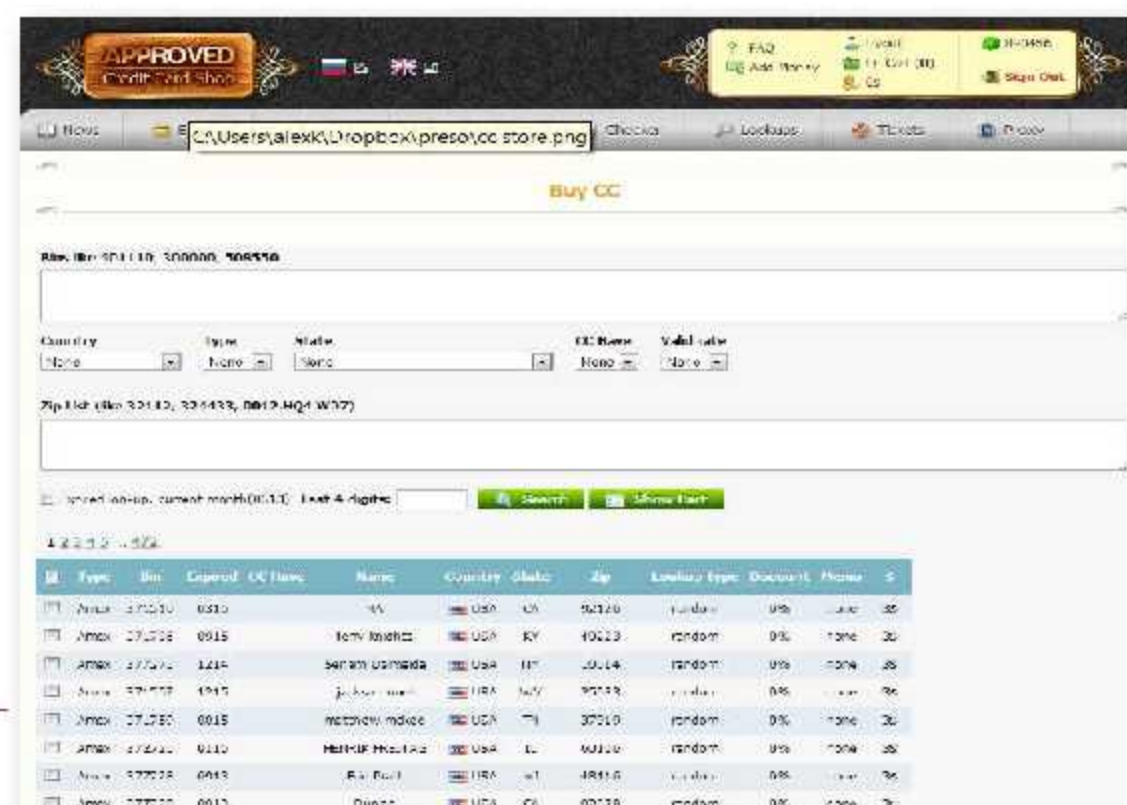
Delivering an integrated and open security system focused on devices (endpoint, mobile, and IoT) and cloud security control points, unified in security operations through management, threat intelligence, analytics, and orchestration



Motivations of the Attack

- Financial / Monetary Gain
- Revenge/ Curiosity or Intellectual Challenge
- Social Or Political Point
- Espionage or Activism
- National Security

MR. ROBOT



Top Customer Sectors

Targeted COVID-19 Related Threats



← → ↻ ⓘ coronaygwcbcgpd6.onion ... ☆

Coronaygwcbcgpd6.onion The Coronavirus Epidemic

MASK SHOP
Cornona protection masks

We are selling **Aura 3M & Farstar medial N95** face Masks to **protect** you against the Cornona VIRUS. We are a wholesaler and official supplier for Hospitals. We want to provide normal people like you with these Masks. These Masks **arent** stolen ! They are **brandnew** and **original** ! We want to help you ! Everybody need a chance to g only medical employees ! We are selling these MASK here about onlon to protect our Identities because some of our clients shouldnt know that These Masks will come in new closed packets and are usable till end of 2024.
One Packet contain 10 Masks !

← Tweet



Christiaan Beek ✓ @ChristiaanBeek · Mar 30
Seriously I hope this is a hoax/scam #Darknet



Coronavirus – COVID-19

\$1,000.00

I was infected with Coronavirus – COVID-19!!!

I sell my infected blood and saliva.

I do this to provide for my family financially.

Indicate how you prefer to get after purchase-Order notes (optional).

4

5

10



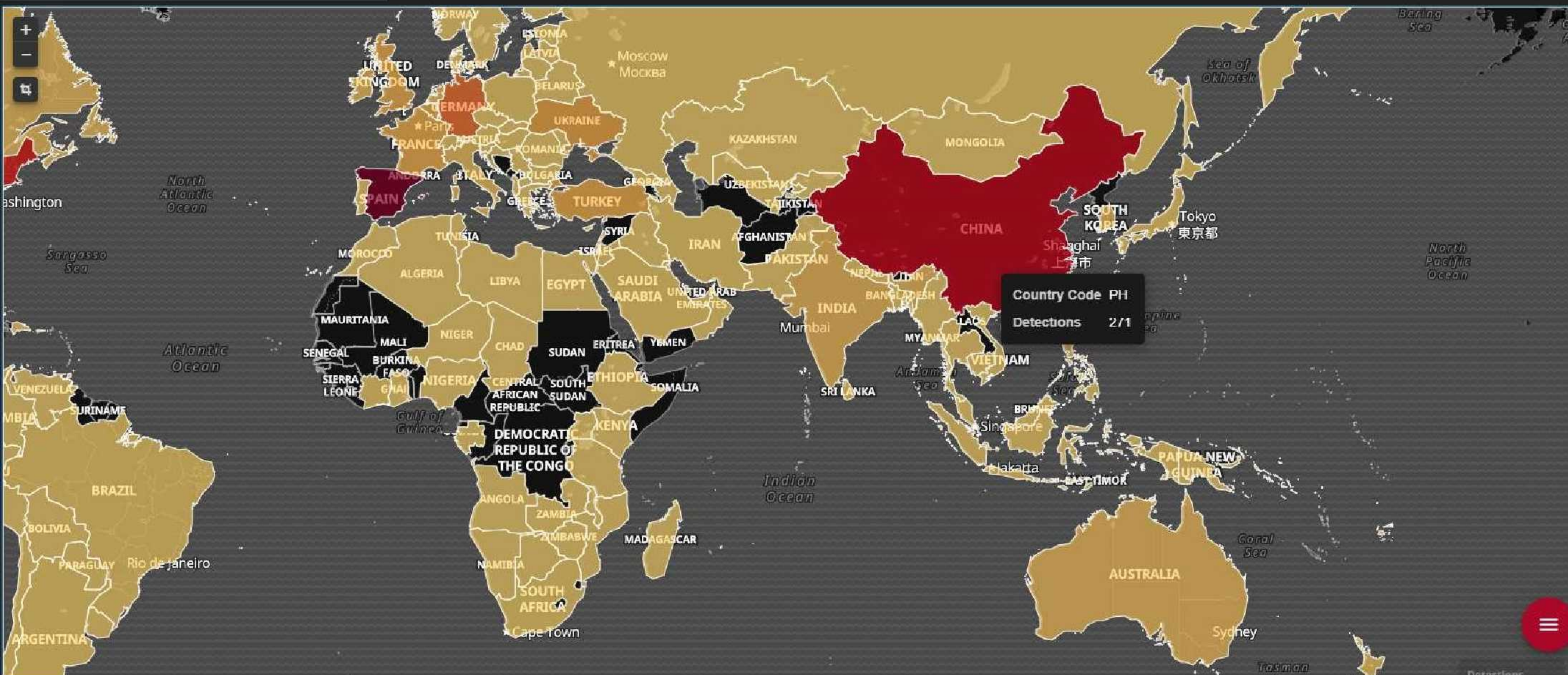
Transportation & Shi...



Corona Safety Mask - 1.0
com.coronasafetymask.app

Covid-19

Global Malicious File Detections



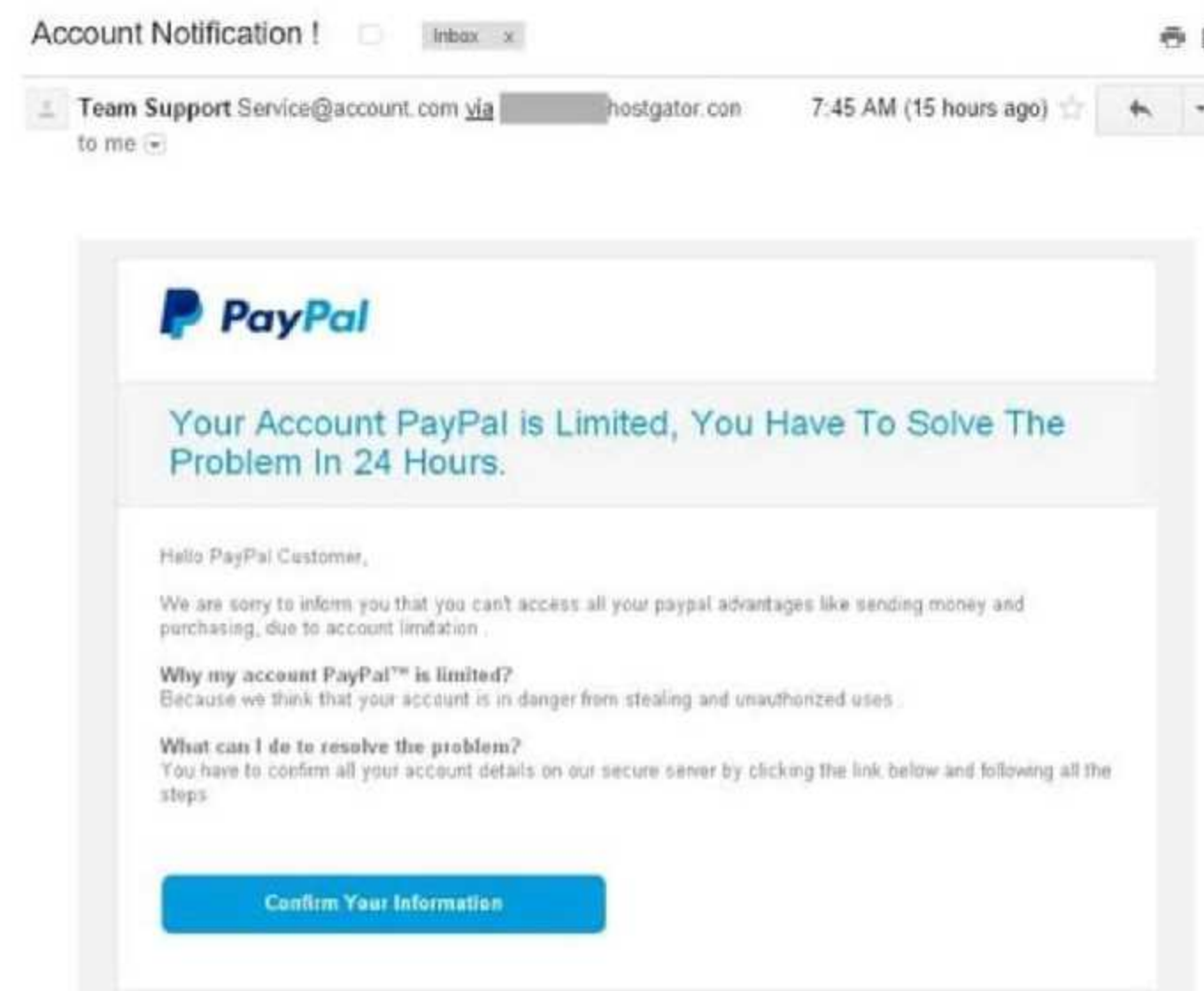
Social Engineering

- Social engineering is the practice of obtaining confidential information by manipulation of legitimate users.
- A social engineer will commonly use e-mail, the internet, or the telephone to trick people into revealing sensitive information or get them to do something that is against policy.



Types of CyberSecurity Attacks

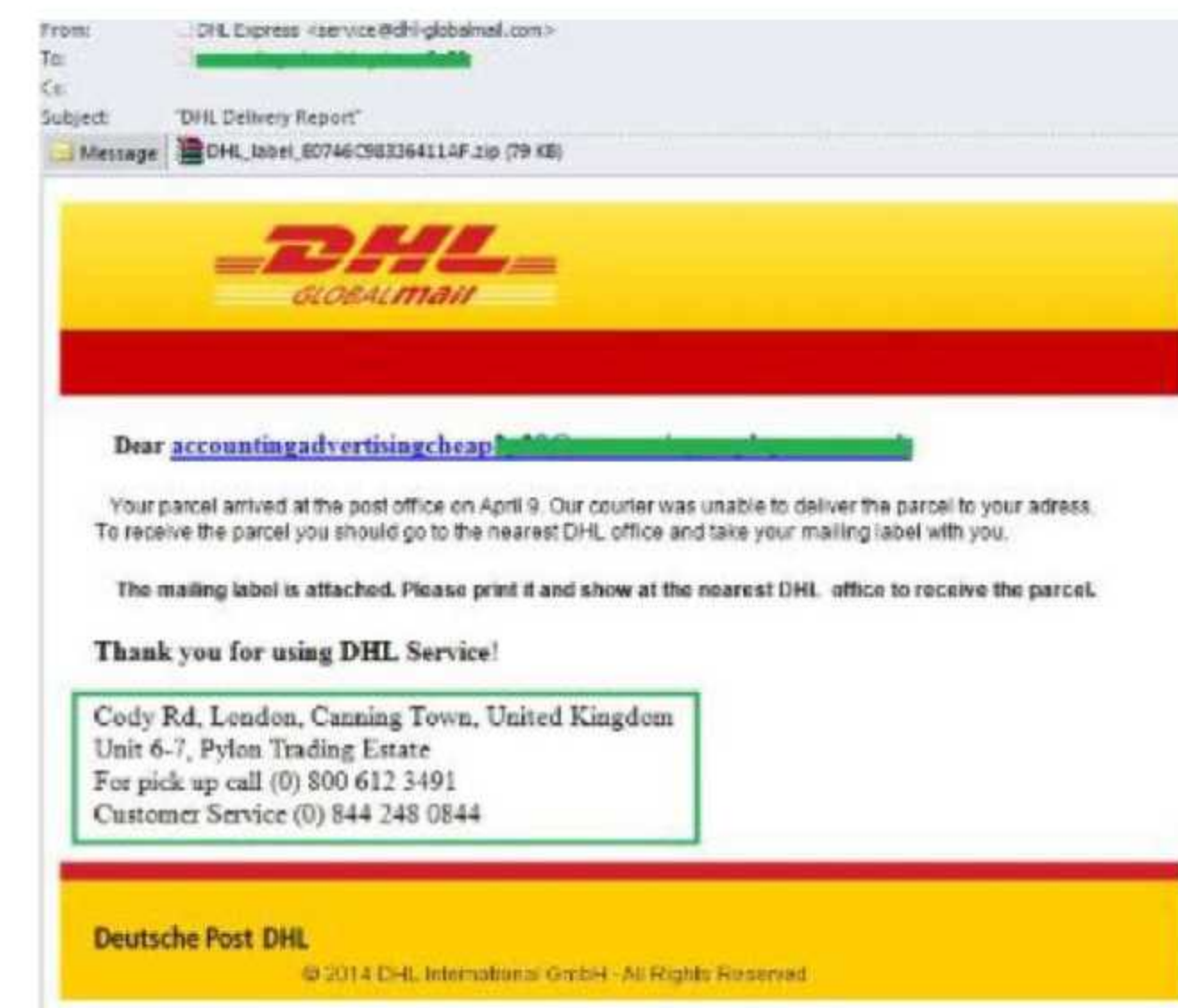
Phishing - is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity



Types of CyberSecurity Attacks

Deceptive Phishing

- Most common type
- Steals information by imitating a legitimate provider.
- To avoid, look out for generic salutations, grammar mistakes, spelling errors found on the malicious email.
- Users must also inspect URLs carefully and check for legitimacy.



Attn: Your-150 Dollar Prime Credit Expires on 12/28. Shopper: [redacted] Spam x

Amazon Update <AmazonUpdate@efficaciouscrbays.xyz> to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. [Learn more](#)

amazon.com
Prime

The Amazon Marketplace

-----SHOPPER/MEMBER:4726
-----DATE-OF-NOTICE: 12/22/2015

Hello Shopper [redacted]! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with \$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this \$100 reward, simply go below to get your coupon-card and then just use it during checkout on your next purchase. That's all there is to it!

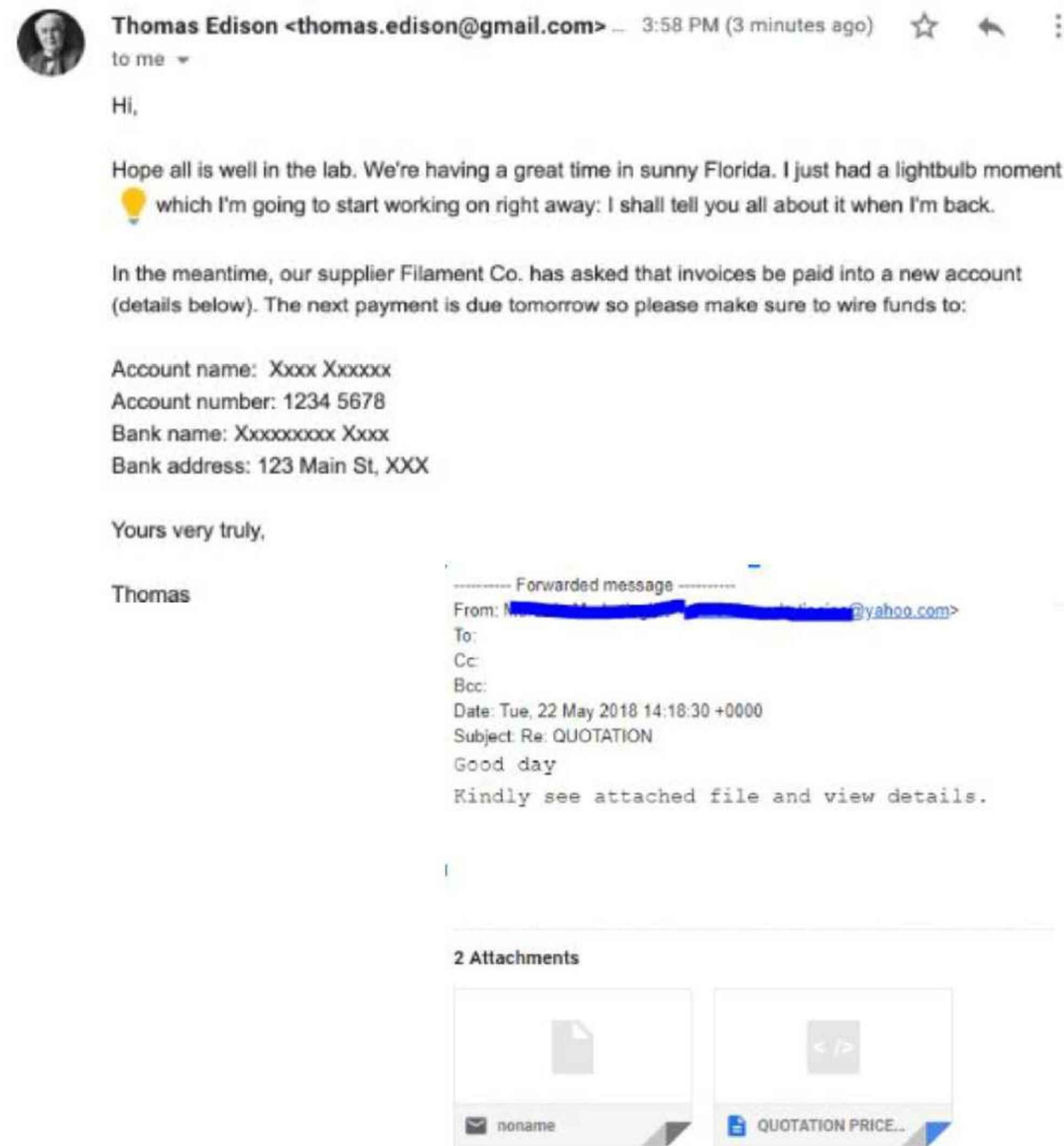
[Please visit here now to get your reward](#)

***DON'T WAIT! The Link Above Expires on 12/28!

Types of CyberSecurity Attacks

Spear Phishing

- Most common on social media sites.
- Email from recognized sender.
- Uses personalized information.
- To avoid, limit sharing of sensitive personal information



Types of CyberSecurity Attacks

Whaling

- Targets executives in the organization.
- This is a type of spear phishing that focuses on a high-ranking target within an organization.
- This scam is mostly used for fraudulent financial transfers.

Types of CyberSecurity Attacks


Vishing

- Contacts target using phone.
- This type of scam is used to steal sensitive data/funds.
- To avoid, don't give personal information over the phone and avoid calls from unknown numbers.



crying baby defcon

FILTER




And I can't remember what email address we used to log in to the account and the baby's crying -

2:30

This is how hackers hack you using simple social engineering

oracle mind • 1M views • 4 years ago

Simple Social Engineering Trick with a phone call and crying baby.




11:36

Real Future What Happens When You Dare Expert Hackers To Hack You Episode 8

Lexihut Professional Advisory Platform • 188K views • 4 years ago

This Documentary Is about cyber hacking and how easily hackers can fish for your information and thus can have the power to ...



6:55

Hacking challenge at DEFCON

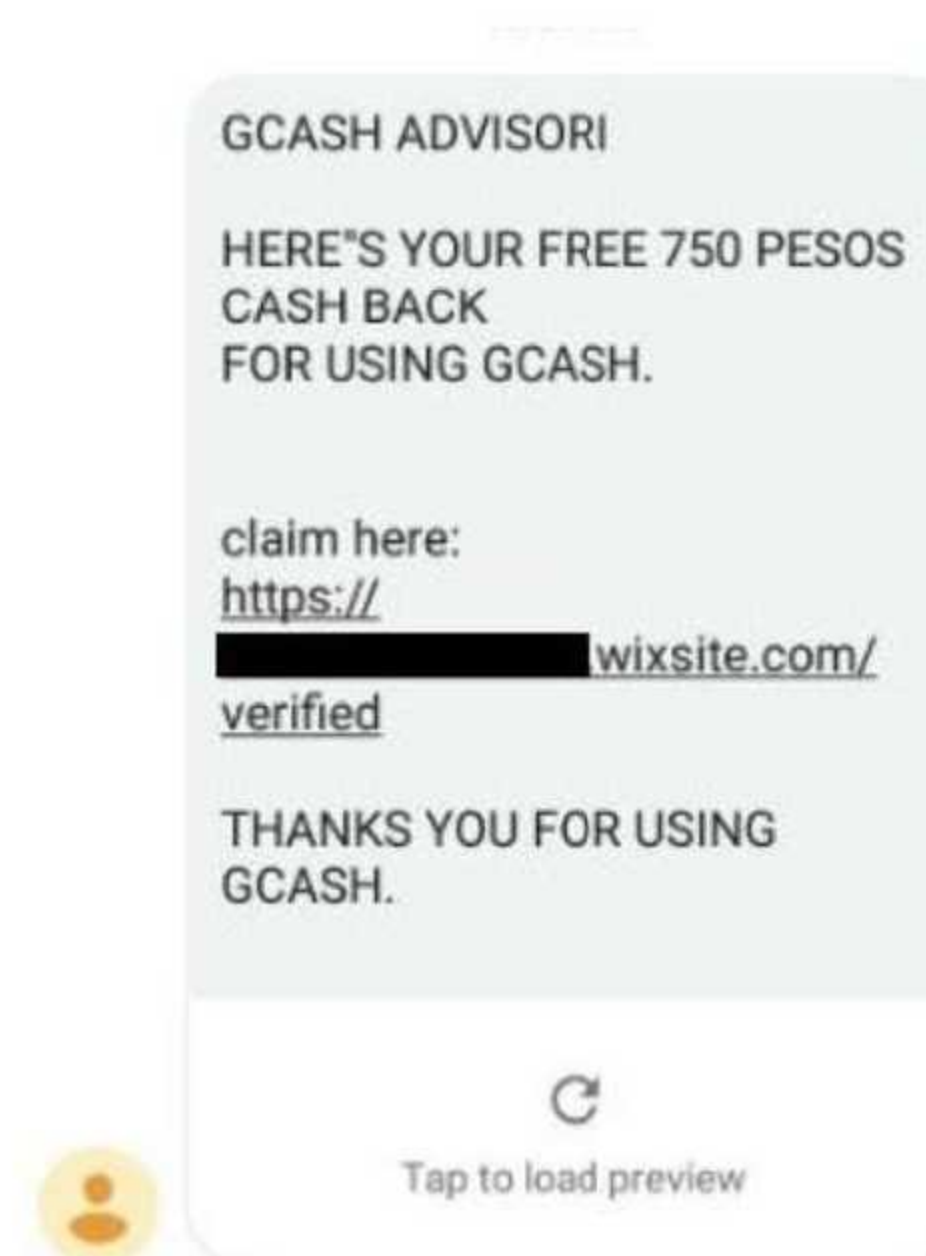
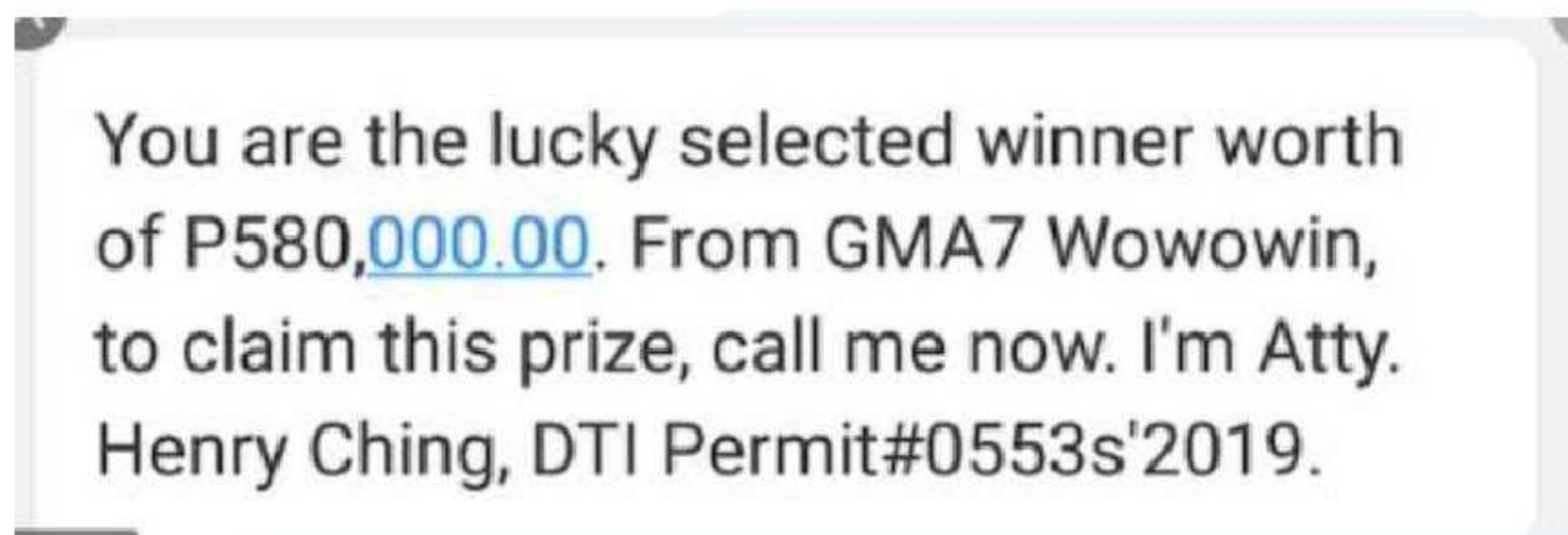
Conflict International • 80K views • 3 years ago

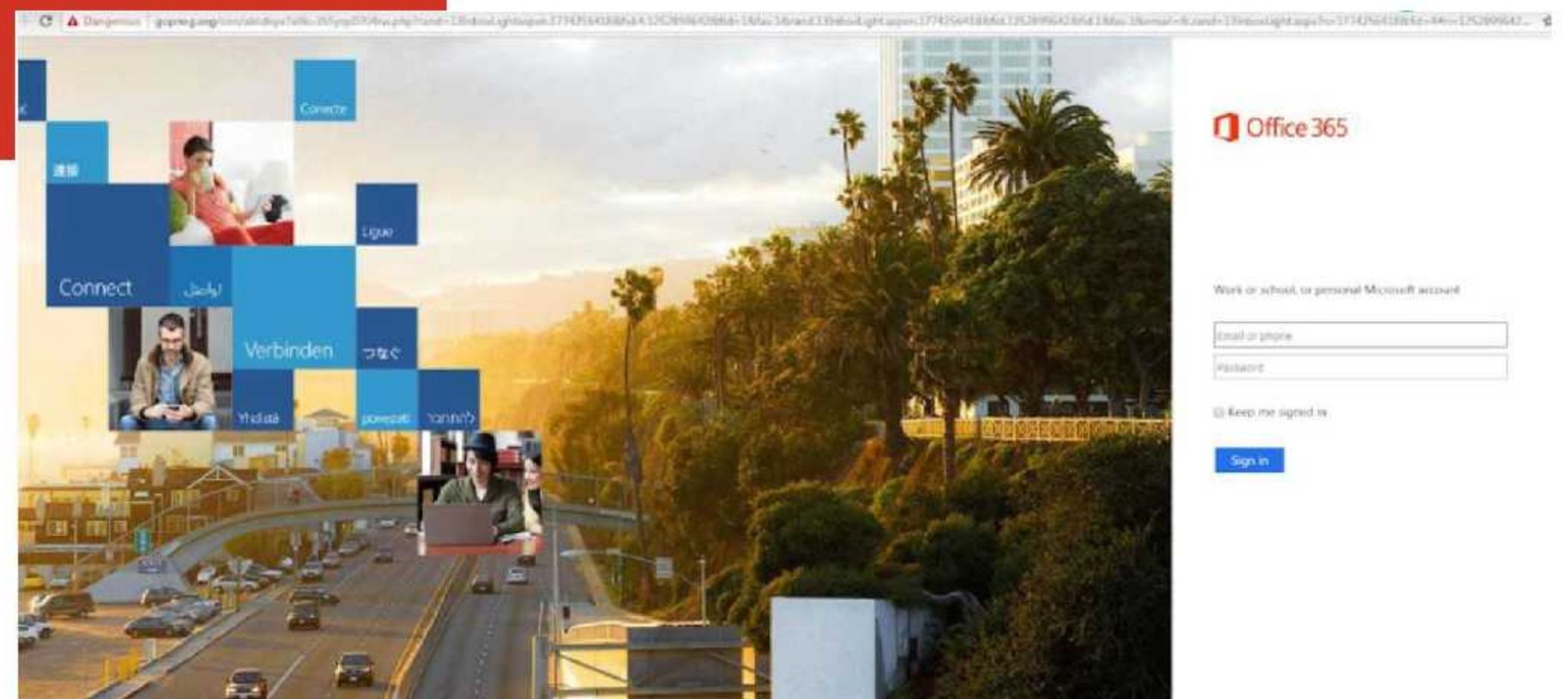
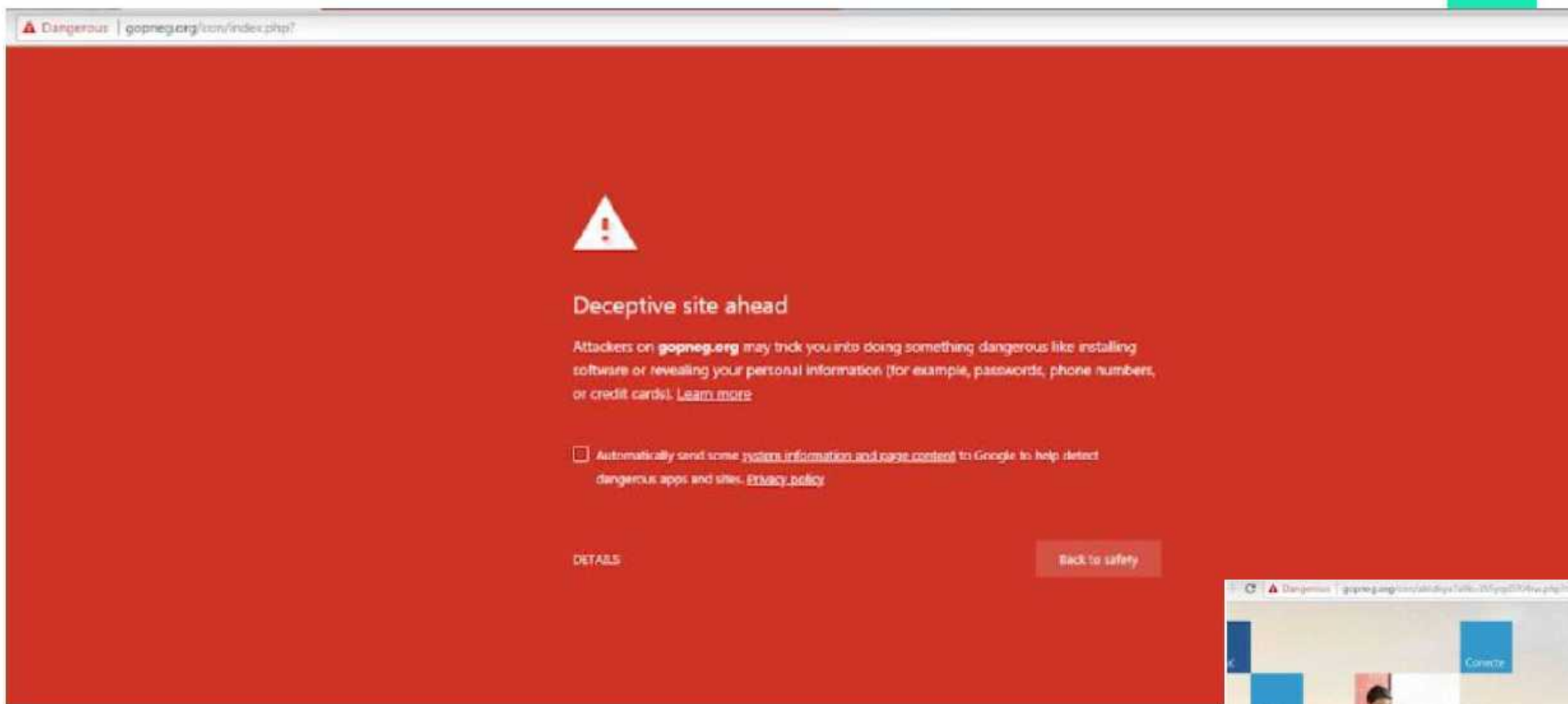
Watch what happens when journalist Kevin Roose challenges hackers to hack him. CREDIT: FUSION MEDIA NETWORK 2015.

Types of CyberSecurity Attacks

SMS Phishing/Smishing

- Contact target using SMS or text message.
- This type of scam is also used to steal sensitive data and funds.





Solidarity Response Fund. Help WHO fight COVID-19

2:16 PM (2 hours ago)

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe

The world has never faced a crisis like COVID-19. The pandemic is impacting communities everywhere. **It's never been more urgent to support the global response.** The humanity, solidarity and generosity of people and organizations everywhere is also unprecedented. But we can't stop now.

The World Health Organization (WHO) is leading and coordinating the global effort with a range of partners, supporting countries to prevent, detect, and respond to the pandemic. **Donations support WHO's work, including with partners, to track and understand the spread of the virus; to ensure patients get the care they need and frontline workers get essential supplies and information; and to accelerate research and development of a vaccine and treatments for all who need them.**

See below for more ways to give, Via BTC (Bitcoin). Every donation helps support life-saving work for the world.

BTC Address: *****

Re: COVID-19 Adjustment !

Admin Department

to me

1:20 PM (2 hours ago)

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe

Dear Staff

New notification ,Please due to COVID-19, all staff & Employee are expected to kindly Click [PROCEED](#) and complete the required directive to be added to March and April benefit payroll directory as compilation is ongoing and will last within 48hours.

Thank you,
Admin Department

Coronavirus (2019 -nCoV) Safety Measures



Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

General Internist

Intensive Care Physician

WHO Plague Prevention & Control



← → ↻ coronavirus.jhu.edu

JOHNS HOPKINS UNIVERSITY & MEDICINE | CORONAVIRUS RESOURCE CENTER

Home Maps & Trends Testing News & Information COVID-19 Basics Videos & Live Events

COVID-19 Case Tracker

Follow global cases and trends.
Updated daily.

Global Confirmed
5,168,433

Global Deaths
335,936

Total Test Results in US
13,056,206

View the COVID-19 Global Map → View the COVID-19 U.S. Map → **NEW** Explore Critical Trends →

Hubei Timeline

How did events unfold in Hubei, China?

Major events and actions taken in Hubei Province at the start of the outbreak.

Learn More →

U.S. State Data Availability

NEW

Which states have released breakdowns of Covid-19 data by race?

Visual representations of released state data.

Learn More →

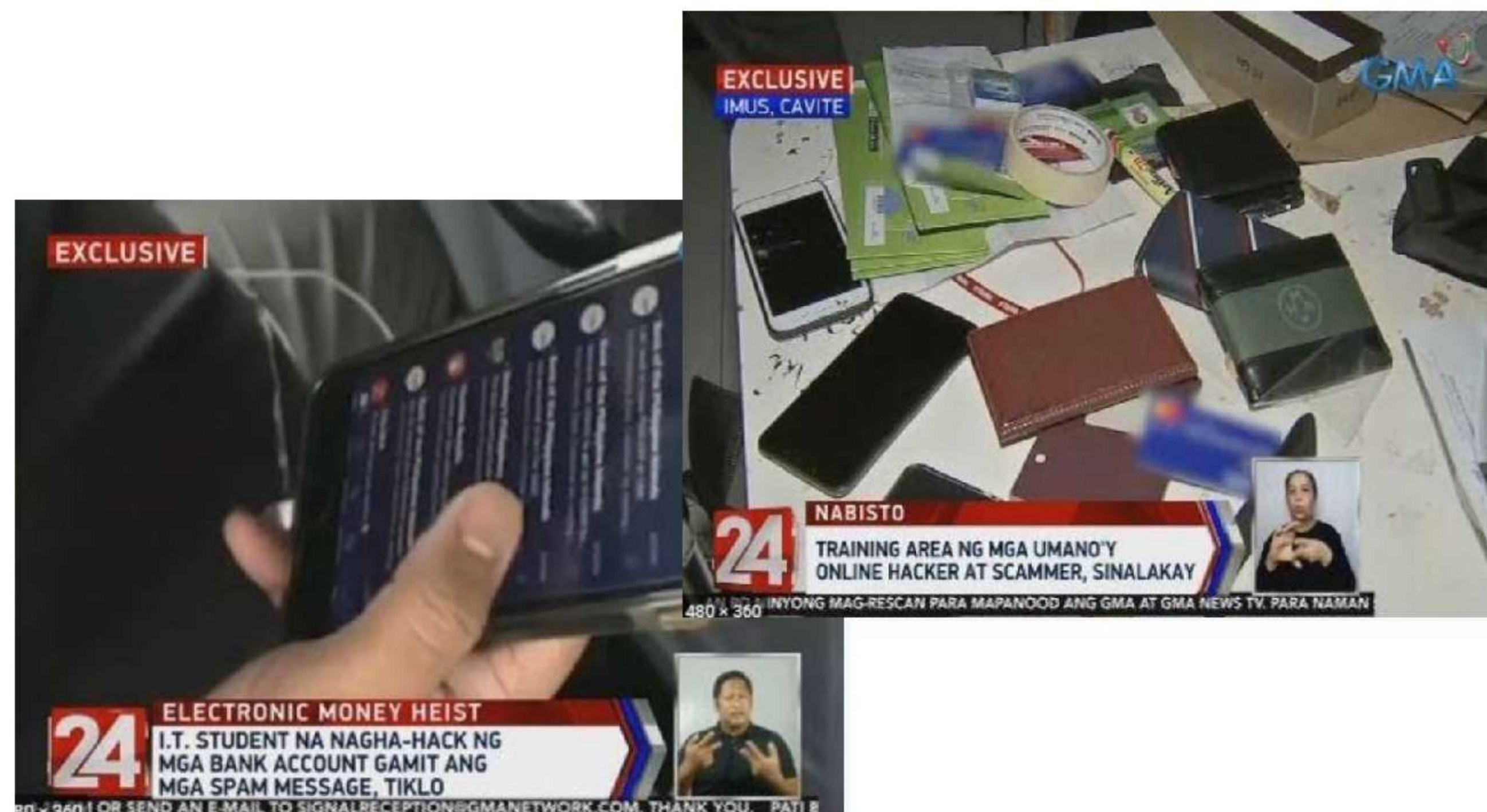
Animated Maps

Where a



Types of CyberSecurity Attacks

Phishing scams exploiting fear of this pandemic are on the rise.
Many of these contains information regarding the COVID-19 virus



In time of Social Distancing, we are all
Vulnerable

Work Is No Longer Where We Go, But What We Do

Security needs to follow the user and happen inside the cloud itself

Users will access data **from anywhere, with any device**, and will try to **use any service** available to them to allow productive and flexible work.

A new approach to cloud security is needed as **current approaches** are inflexible, create friction, and are **not optimized for the cloud age**.



The New Reality of Modern Work

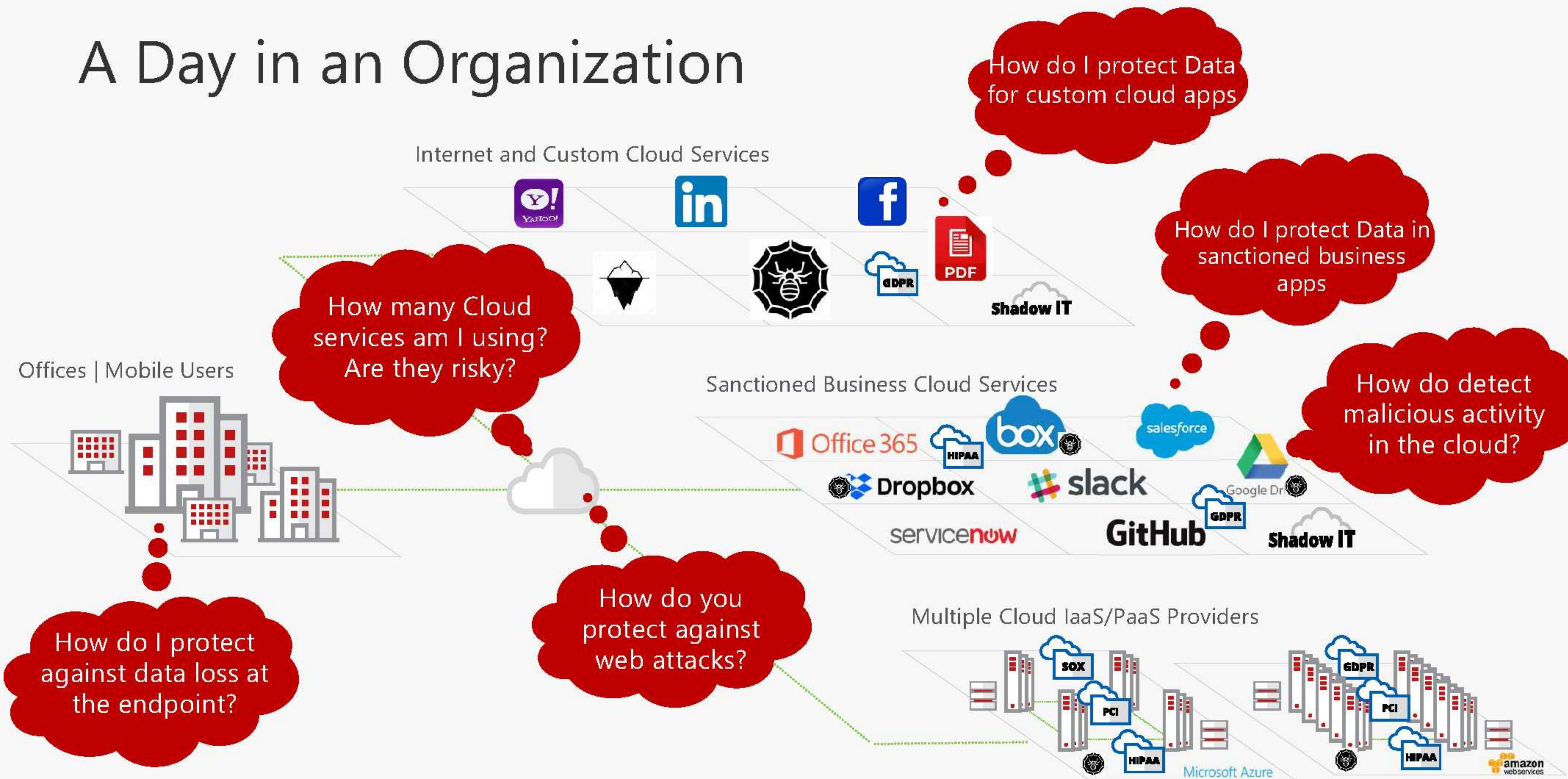
From...



...to

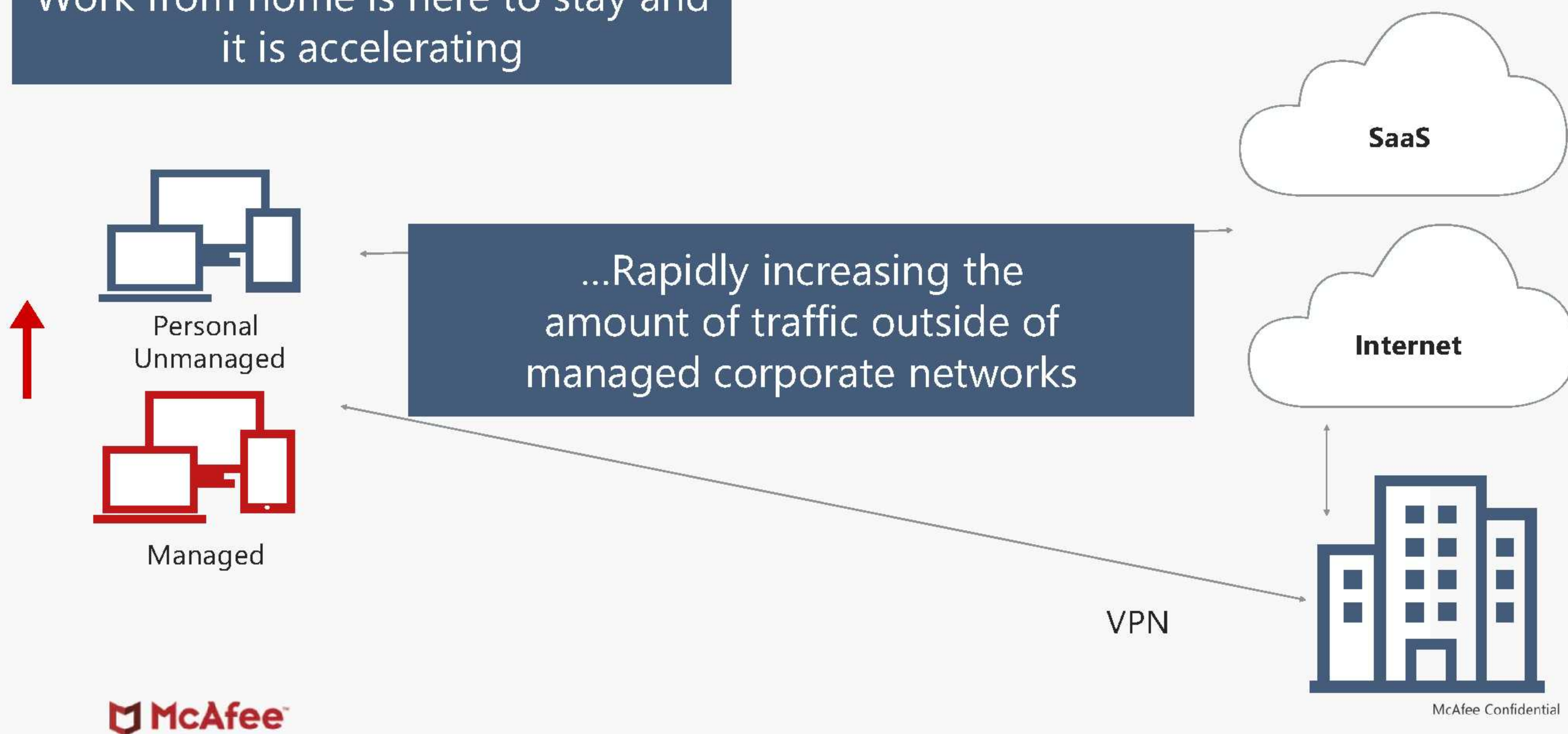


A Day in an Organization



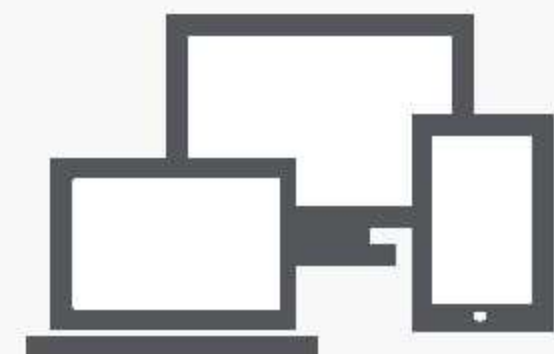
The Problem

Work from home is here to stay and it is accelerating

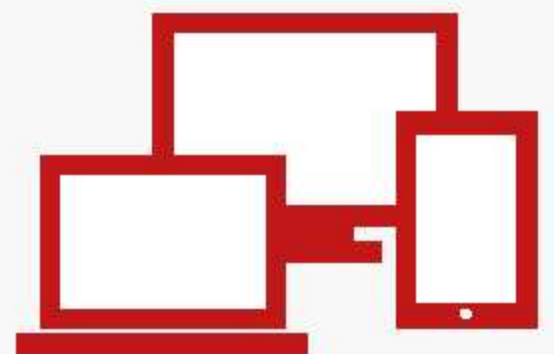


Security Implications

1 Vulnerable Personal and Enterprise Devices at Home

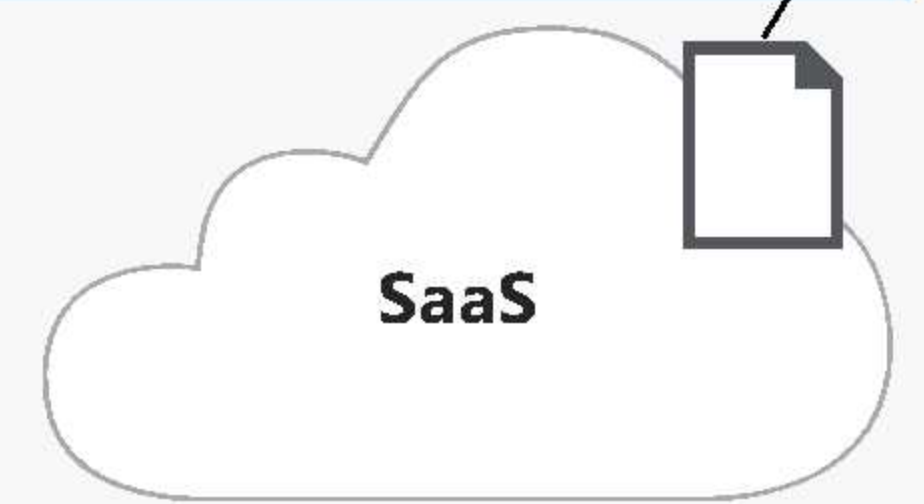


Personal
Unmanaged



Managed

3 Cloud Data Exfiltration via Collab (Teams...) and SaaS Use Outside of Corporate Network



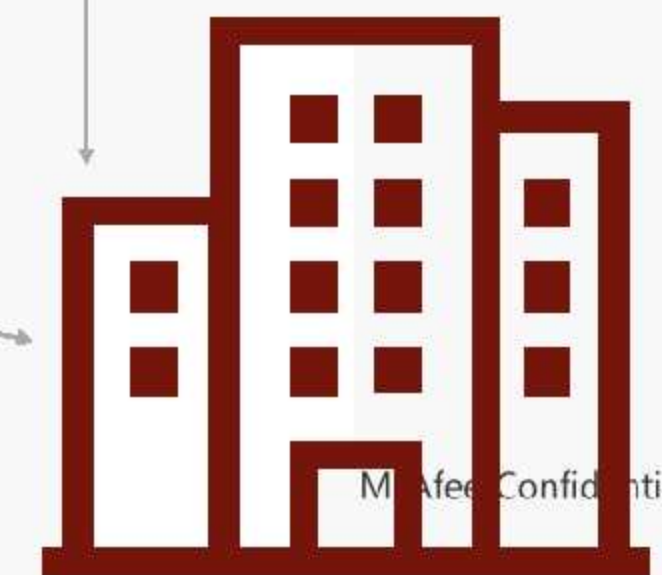
SaaS



Internet

2 Strain and cost of provisioning additional VPN connections

VPN



McAfee Confidential

Meet Maria, Dave, and Lee from GetItDone Financials



Maria
Account Executive



Dave
IT Security Manager



Lee
Network Manager



Maria

Account Executive

- Manages named accounts
- Loves technology and runs a blog for working moms
- Breaks glass and gets things done
- **Always makes quota**

Maria—Sharing and Collaboration



GetItDone Office 365



Partner Office 365

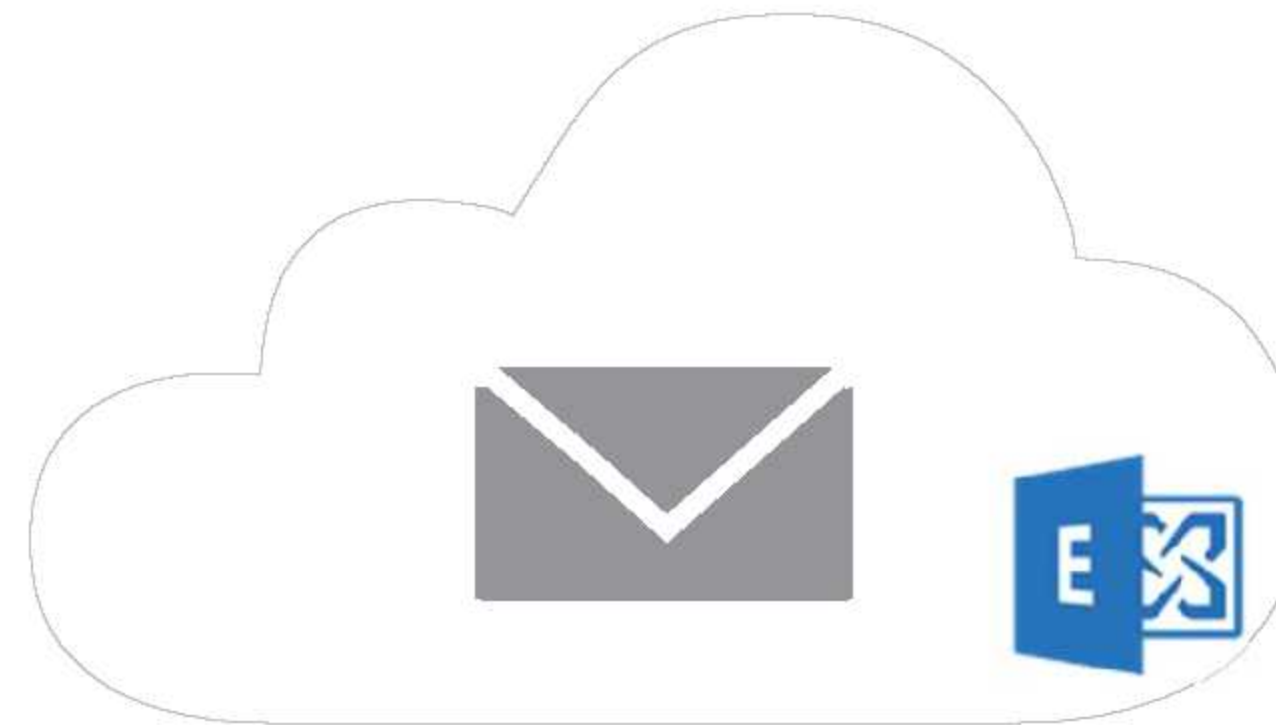
Collaboration puts
confidential data at risk

Maria—Copying Sensitive Data to a USB



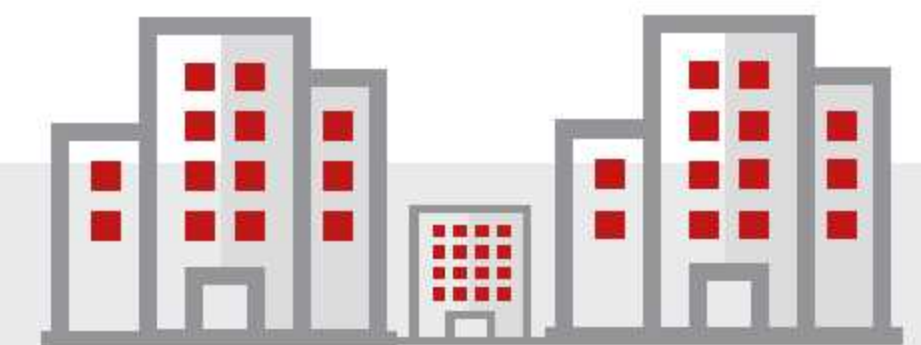
Sensitive data copied to local USBs and personal drives can be **lost** or **stolen**

Maria—Working at Home



Office 365

Email synced to a personal device is **gone** forever

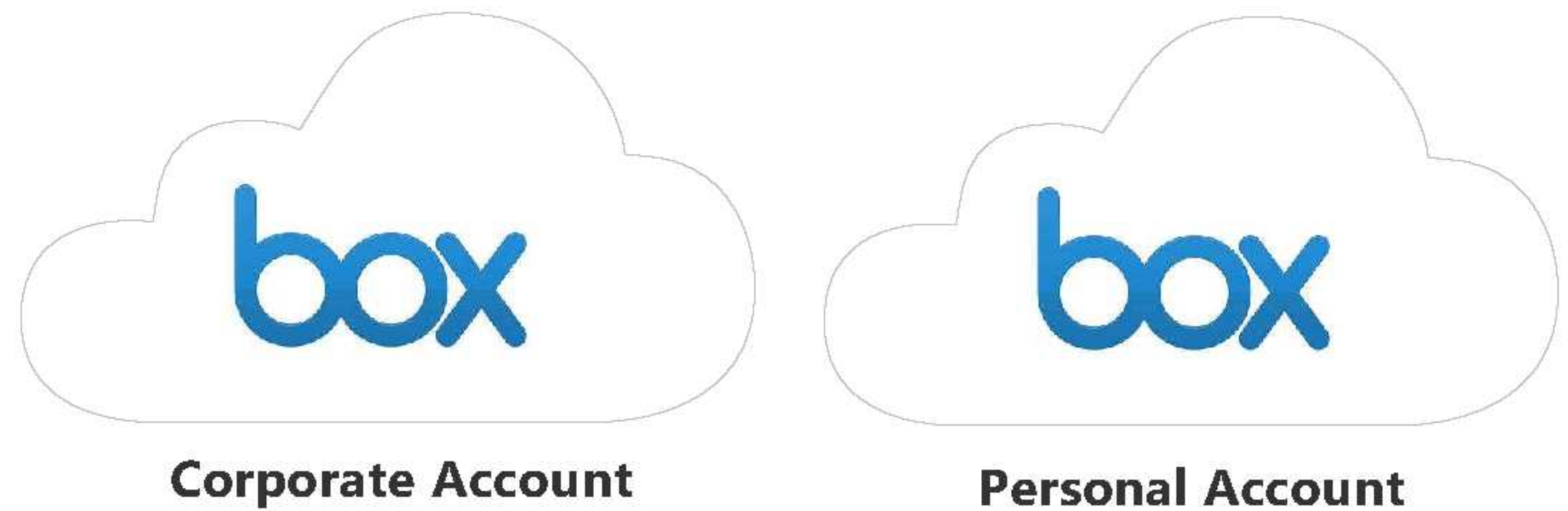


Maria—Uploading Sensitive Data to an Unsanctioned Service at Work



Sensitive data uploads to Shadow IT increases risk of **data loss**

Maria—Accessing a Personal Box Account at Work



Personal accounts **lack
enterprise control**

Maria—Downloads Malware While at Home



Shadow IT accessed at home increases risk of **malware** download



Maria—Downloads Malware from Sanctioned Cloud Service



Malware from sanctioned services can be downloaded and shared

Negative Consequences of Maria's Use Cases

Data can leak from cloud and devices by:

- Bypassing network controls
- User unintentional actions
 - Collaborating
 - Accessing data from personal devices
 - Using personal accounts
 - Using high-risk services
 - Ignoring coaching from IT
- Malware from sanctioned or shadow services



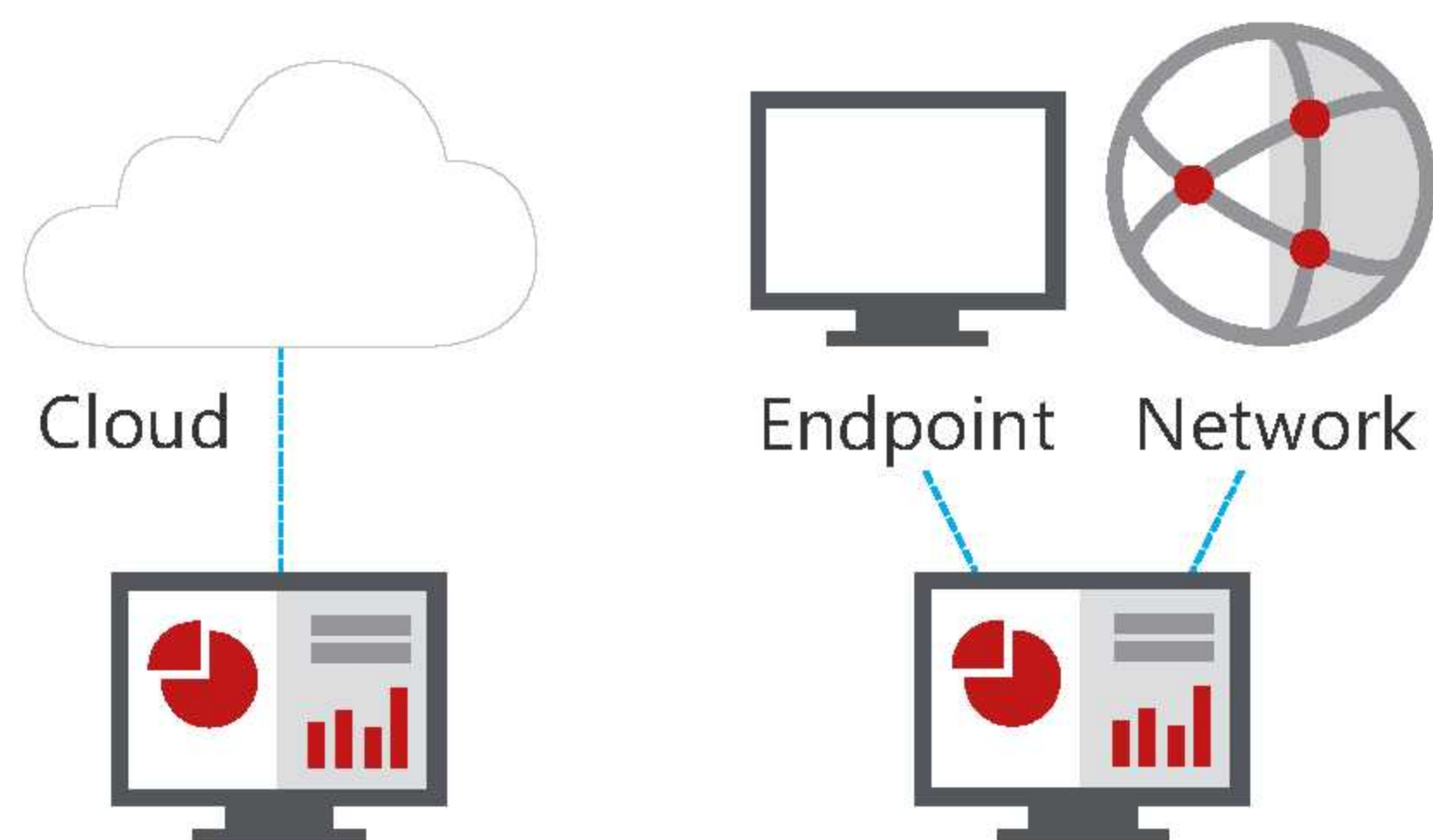
Dave

IT Security Manager

- Manages multiple security tools to keep the company compliant and out of the news
- Ensures the uptime, performance and security of managed devices
- Resolves 100% of the helpdesk tickets
- Always finds ways to improve efficiency
- **Proud to be the IT hero**



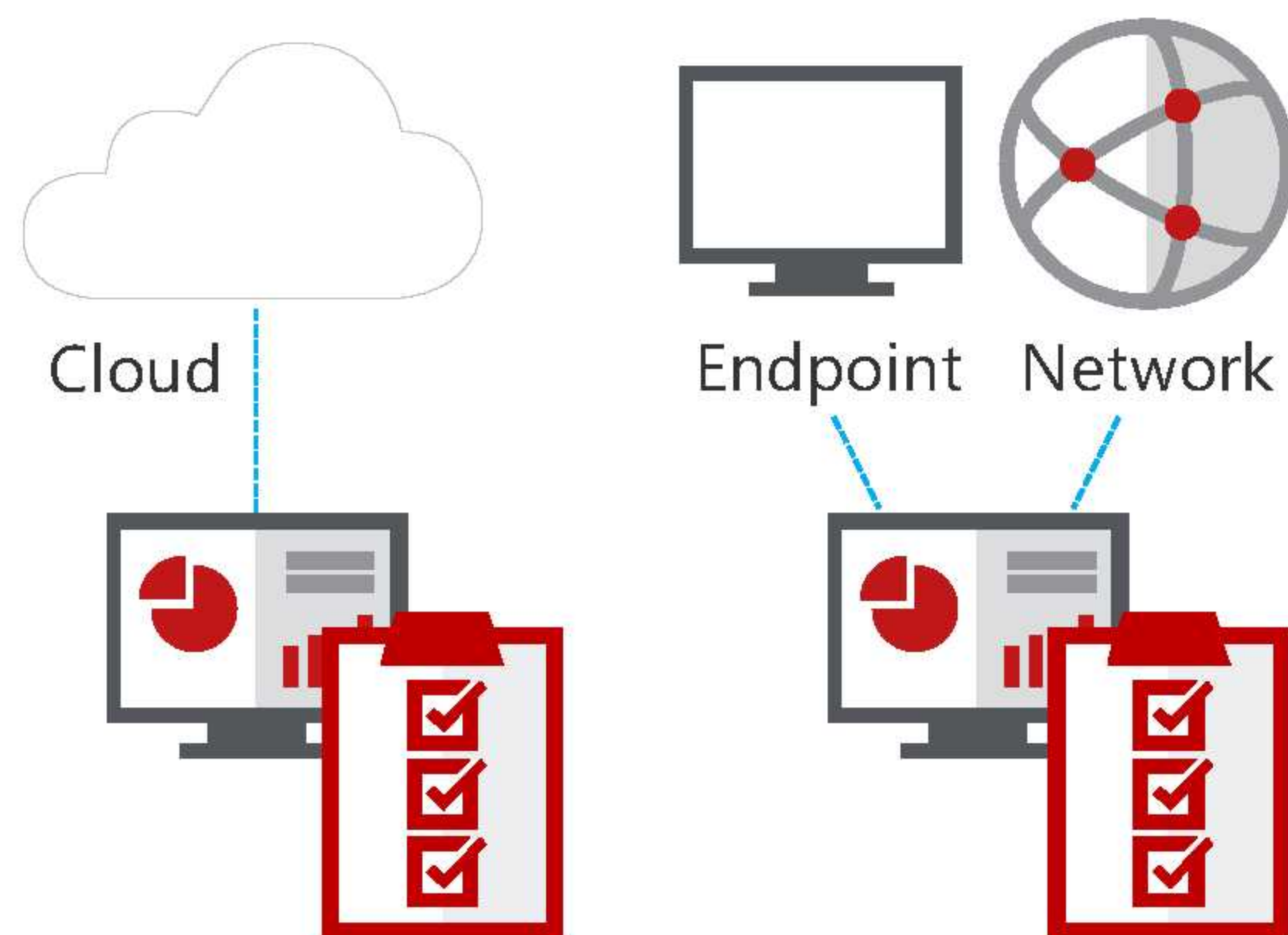
Dave—Duplicating Data Classifications from On-prem to Cloud



Weeks wasted rebuilding content rules to protect data in the cloud

- Public
- Confidential
- Partner

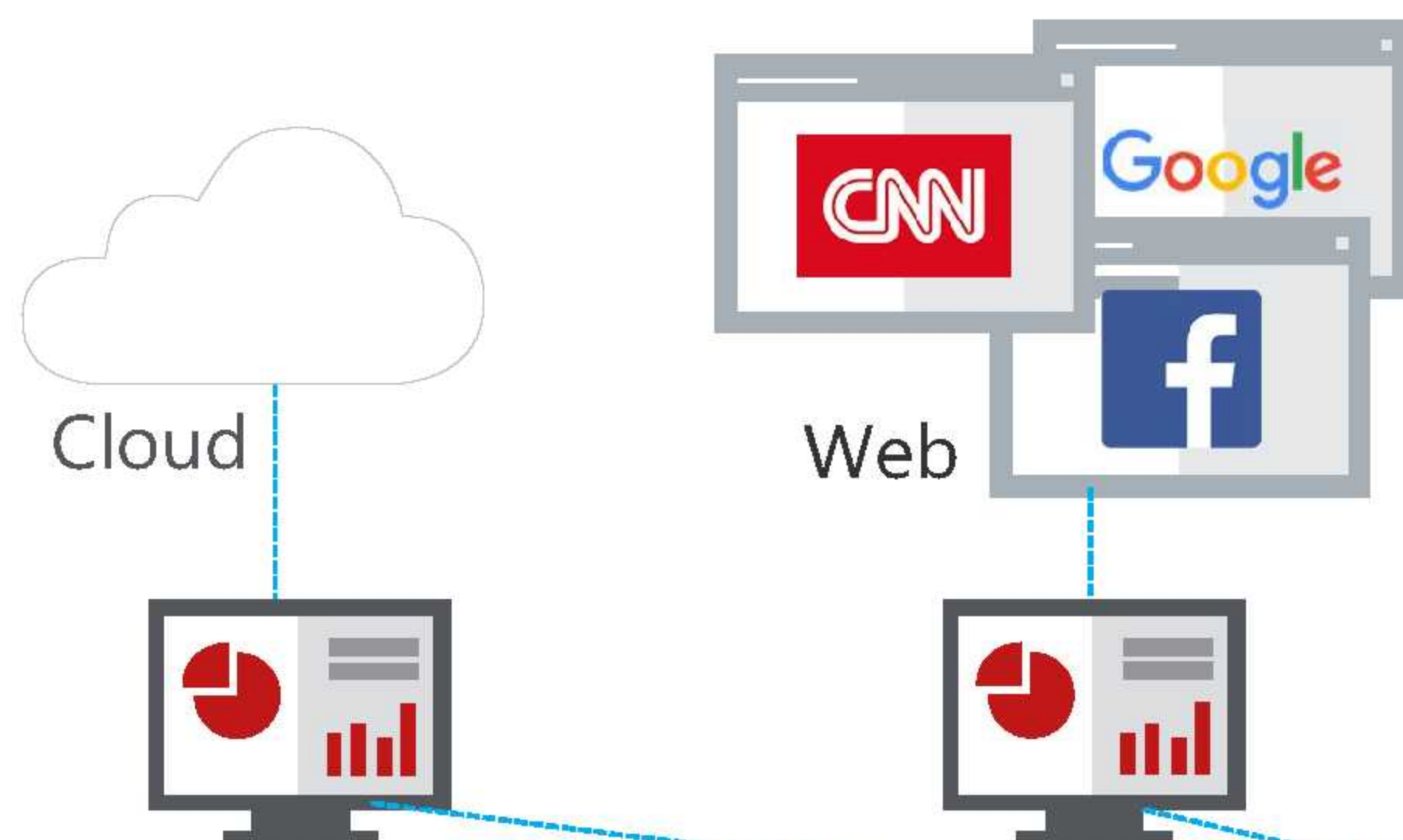
Dave—Managing Two Different Workflows for DLP Incidents



Complexity and mistakes
with two DLP workflows



Dave—Managing Disconnected Cloud and Web Security Policies



Inconsistent control and time wasted in two consoles

Negative Consequences of Dave's Use Cases

Complexity and control gaps from:

- Separate management consoles
- Manually duplicating and extending on-prem security controls to the Cloud
 - Data classifications
 - Policy engines
 - Workflows
 - Siloed risk databases
 - Incident reports



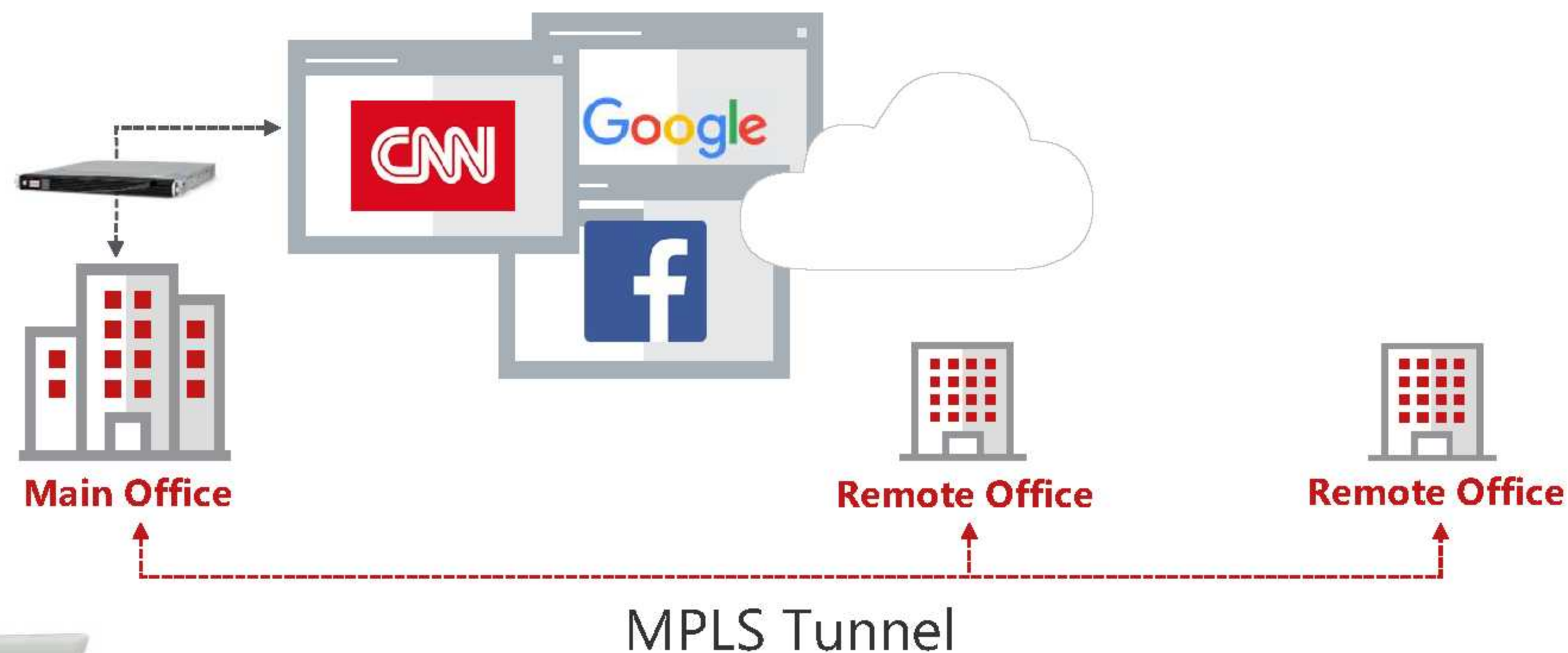


Lee

Network Manager

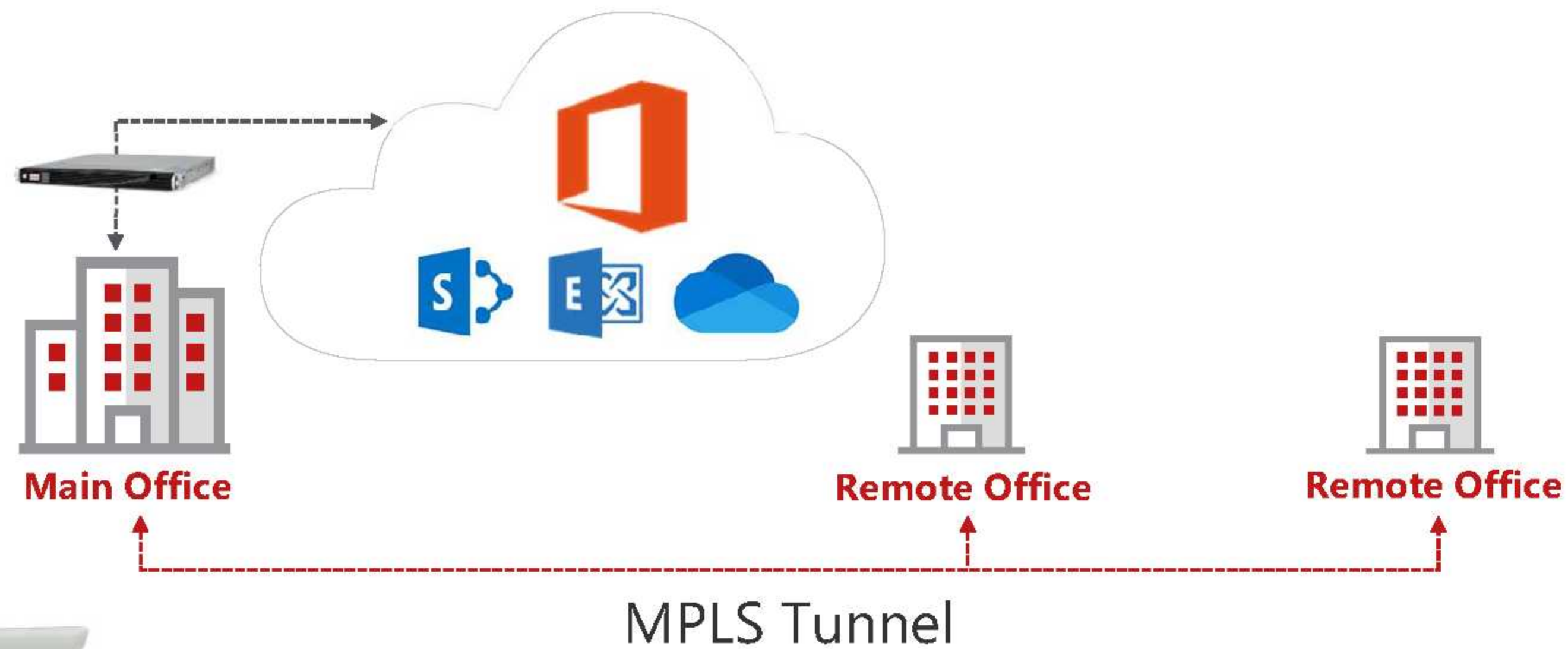
- Loses sleep over network outages
- Executive pressure to simplify architecture and lower costs
- Still manages data center hardware
- **Always on call for emergencies**

Lee—Pays for MPLS Tunnels to Connect Remote Offices to the Internet



Money wasted routing traffic back to HQ then out to the cloud

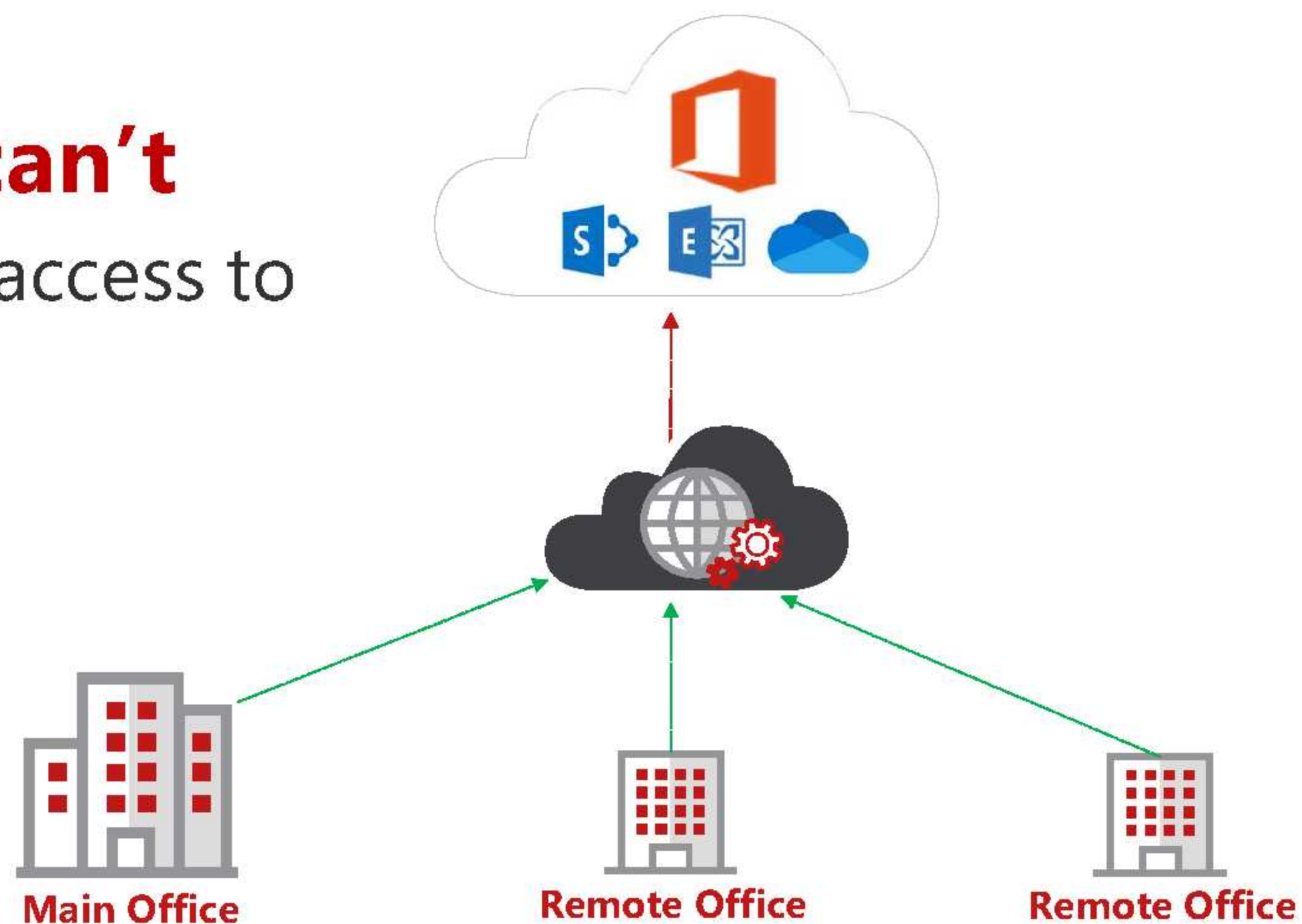
Lee—Network Slows When Traffic Spikes



Workforce **productivity drops**
with slow access

Lee—No Access when Cloud Proxy Has Outage

Employees can't work without access to the cloud



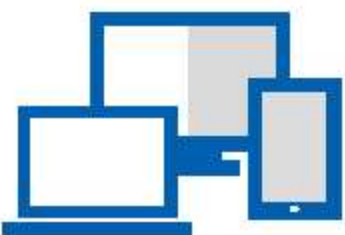
Negative Consequences of Lee's Use Cases



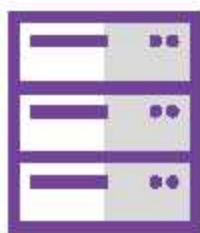
Cost and risk to uptime driven from:

- Outdated MPLS tunnels
- Aging proxy hardware
- New cloud proxy with poor SLA

Current Methodology for Data Security



Endpoint



Network



Web

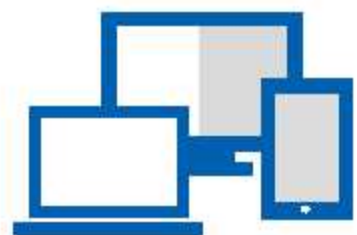


Cloud



Unified Cloud Edge –

Unifies Data Protection and Cloud Threat Prevention



Endpoint



Network



Web



Cloud

McAfee Unified Cloud Edge (UCE)



Common policies & insights



Closed-loop Remediation



Merged business risk and threat database



Tenant restriction for cloud app access



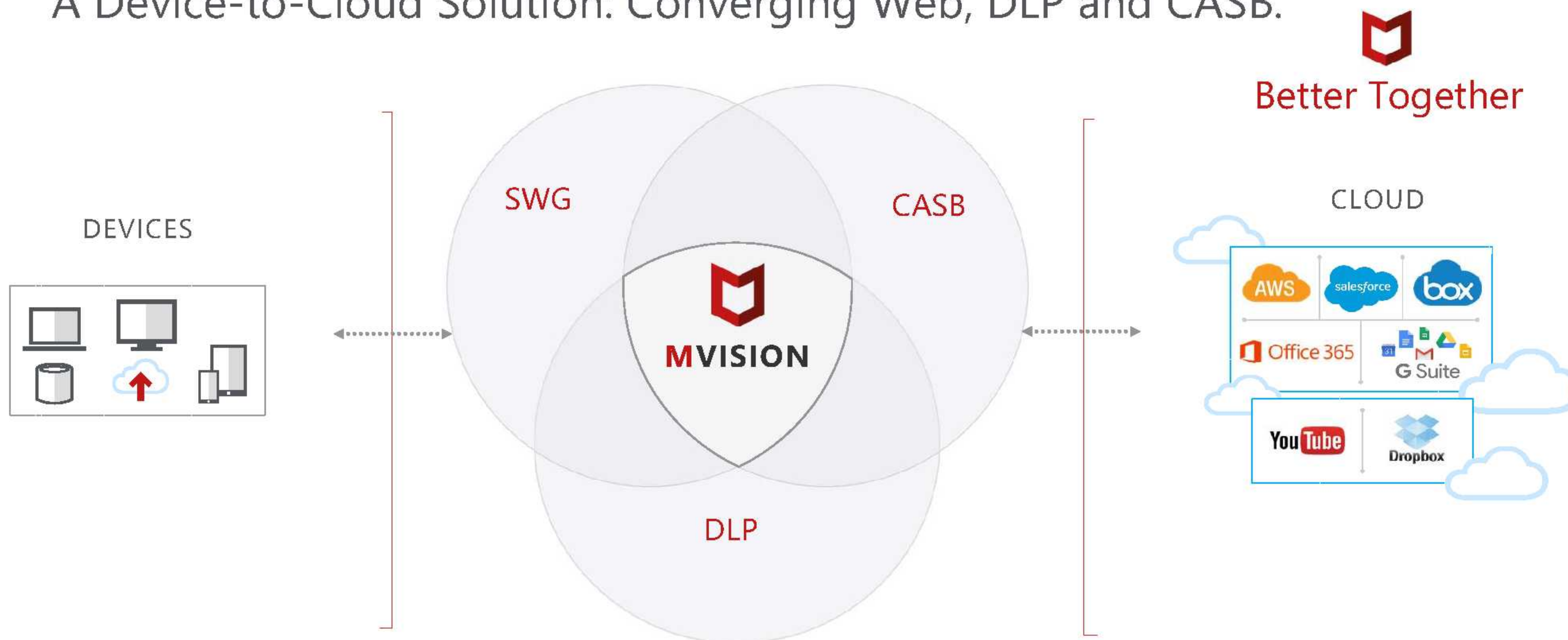
Unified incidents, workflows and investigations



Complete context awareness

What is Unified Cloud Edge (UCE)?

A Device-to-Cloud Solution: Converging Web, DLP and CASB.

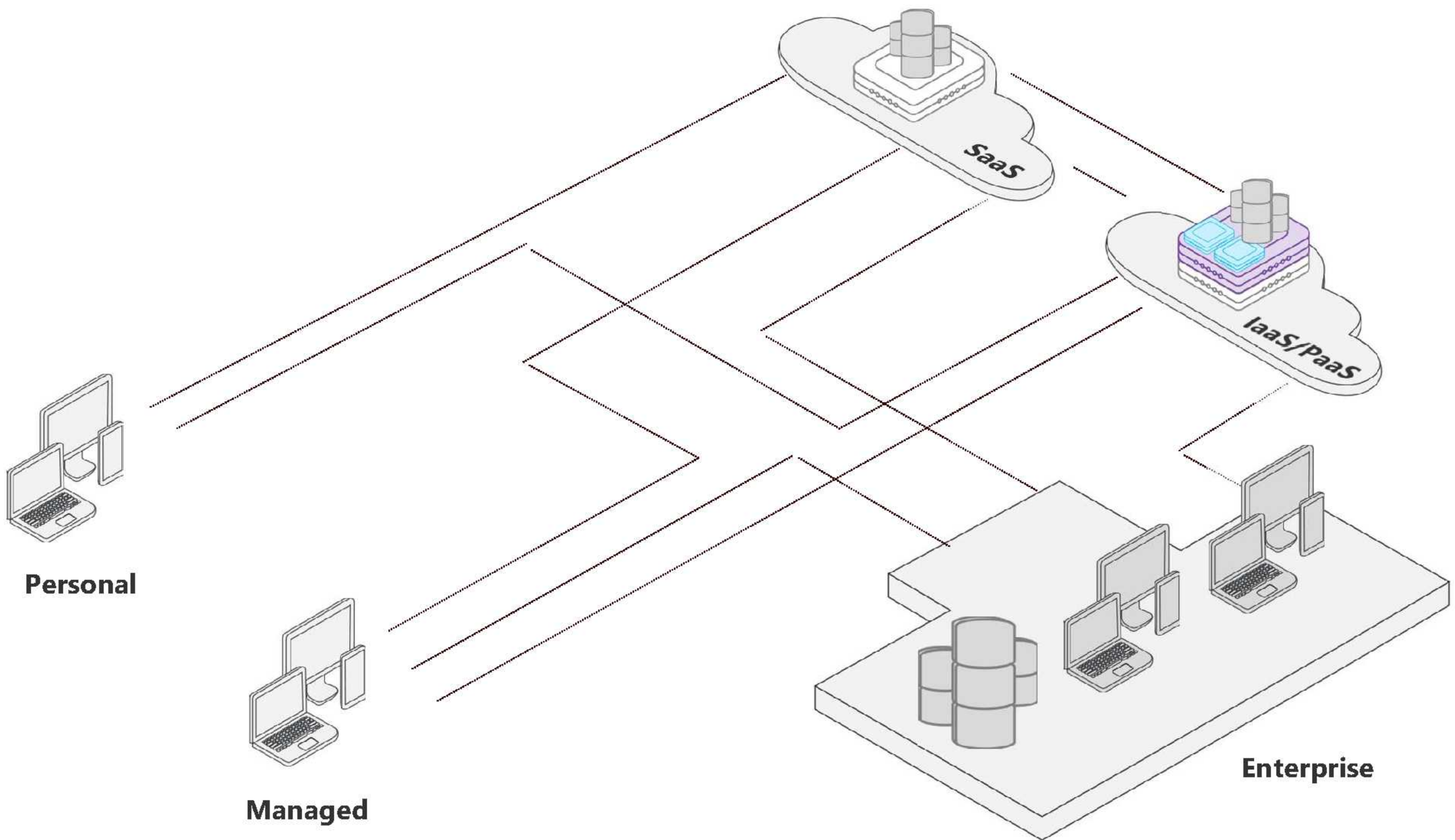


Integrated = Complexity ▪ Converged = Simplicity

What is Unified Cloud Edge

McAfee Unified Cloud Edge is a product for cloud-native security that enables consistent data and threat protection controls from device to cloud. It consists of three core technologies that are converging into a single solution:

- Cloud Access Security Broker (**McAfee® MVISION Cloud**): Direct API and reverse proxy-based visibility and control for cloud services
- Secure Web Gateway (**McAfee® Web Protection**): Proxy-based visibility and control over web traffic and unsanctioned cloud services
- Data Loss Prevention (**McAfee® DLP Endpoint**): Agent-based visibility and control over sensitive data



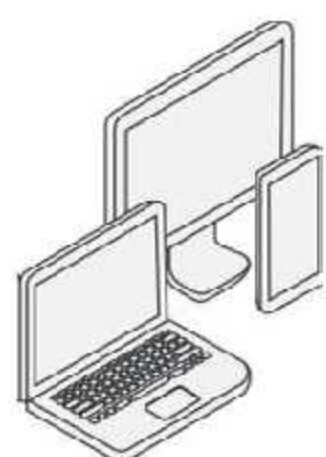
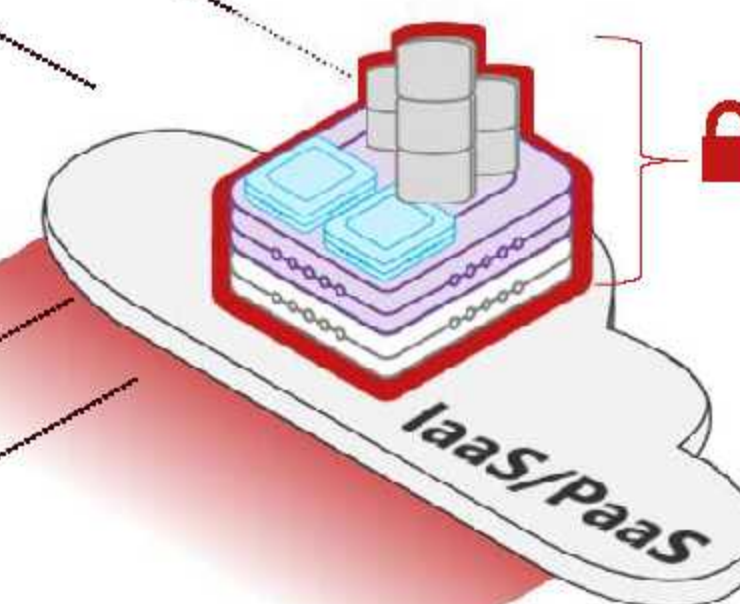
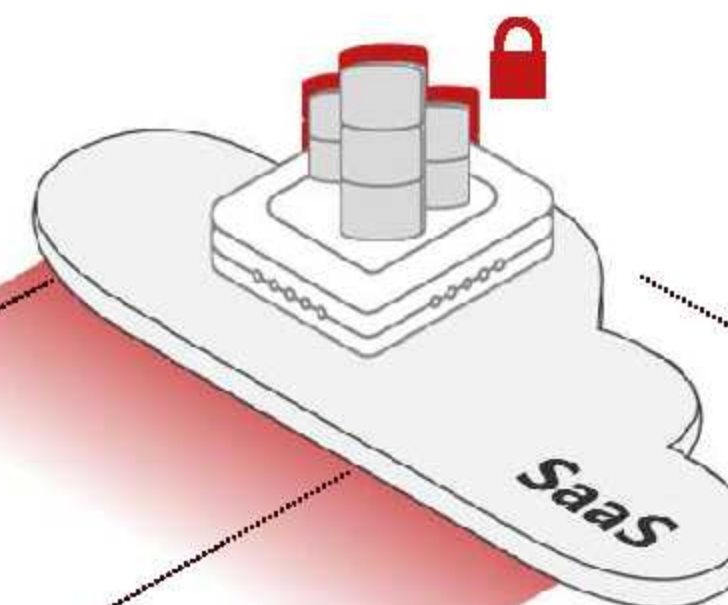


1

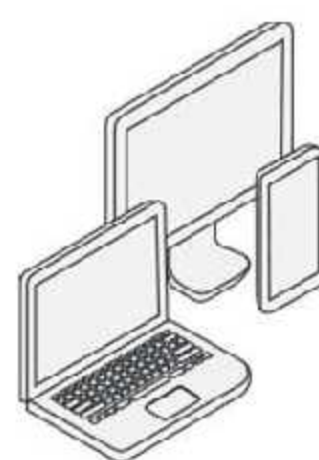
**Data Security Across Clouds
...and In and Out of the
Cloud: Device & Enterprise**

2

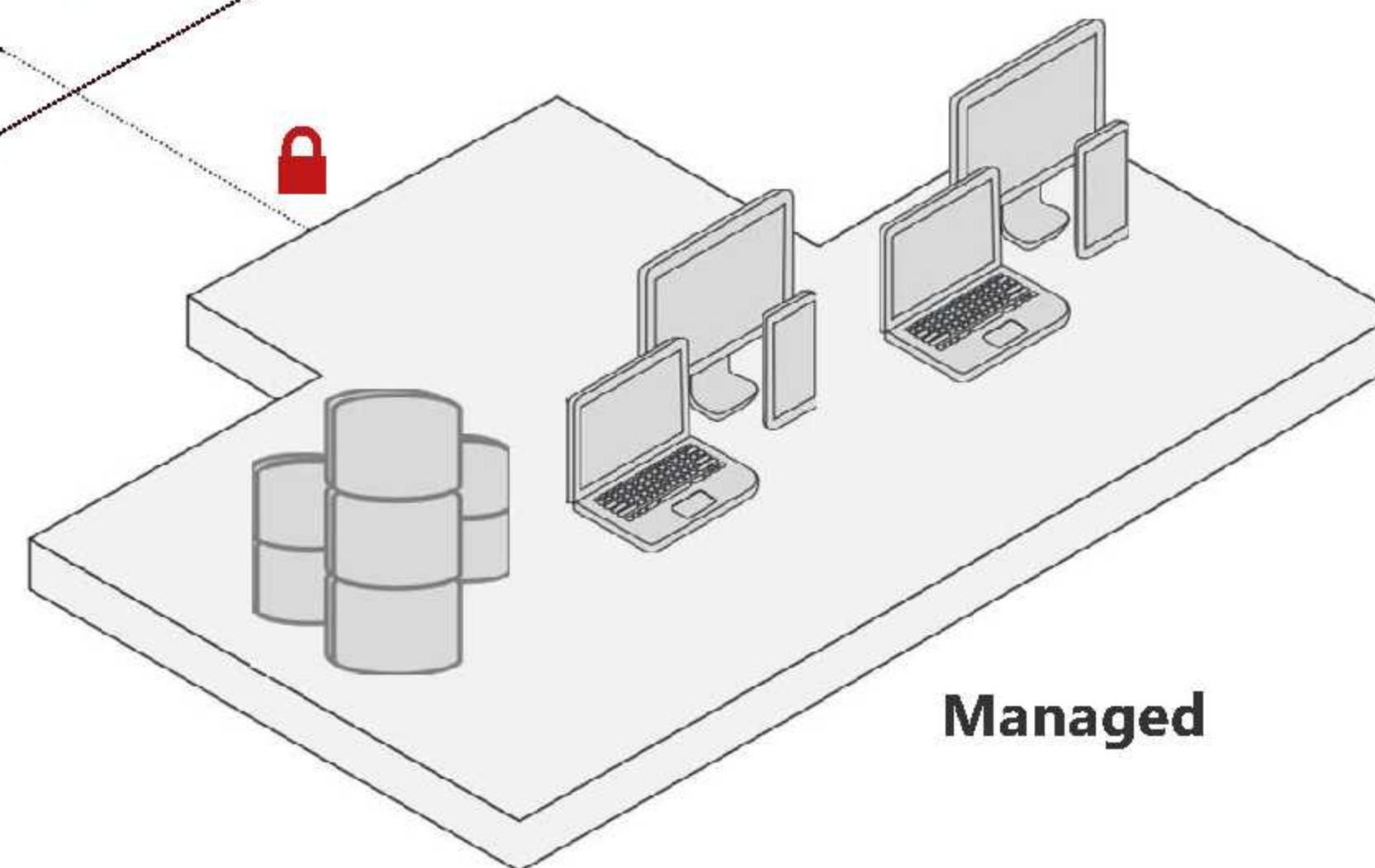
**Public Cloud
Infrastructure
Security**



Personal



Managed

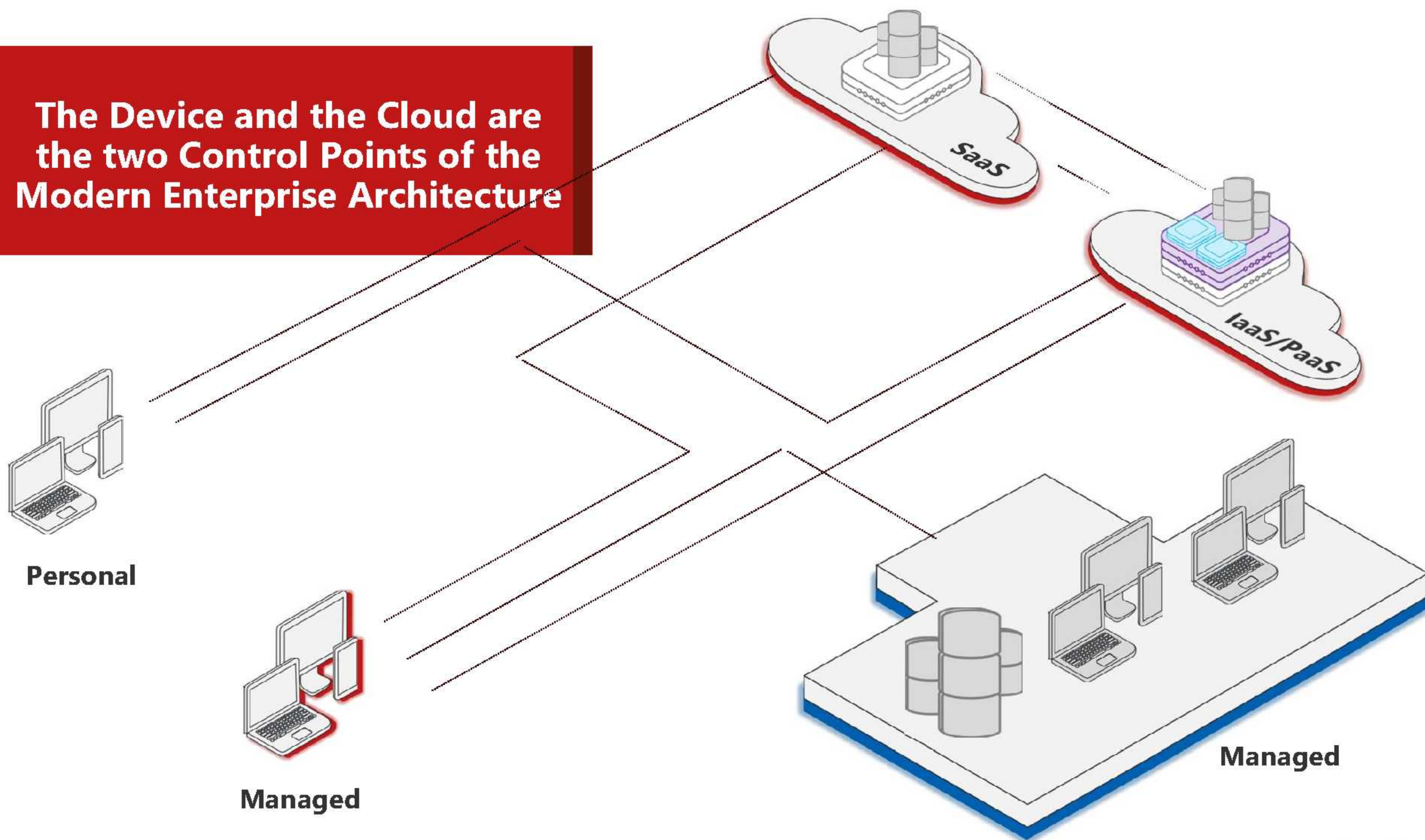


Managed

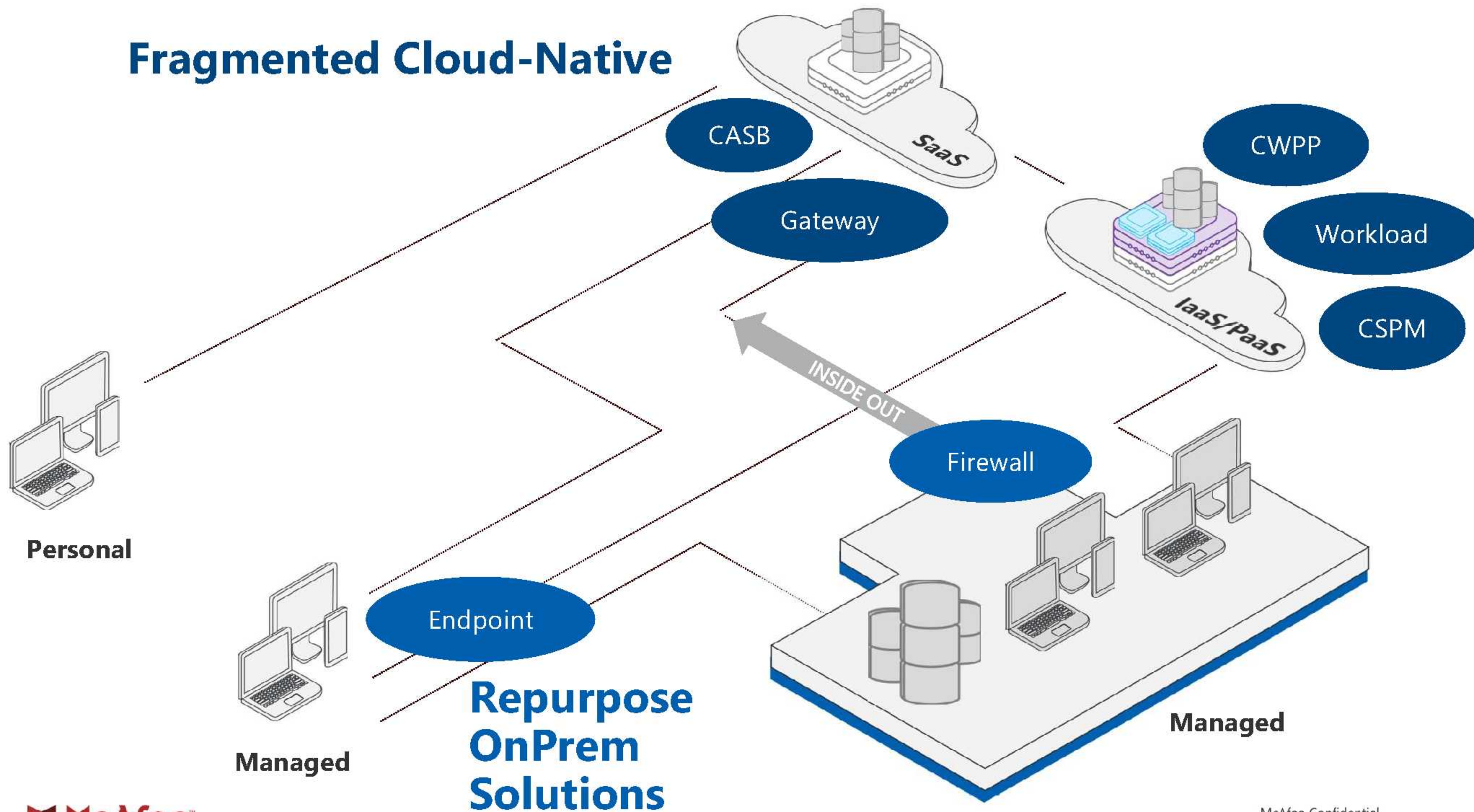


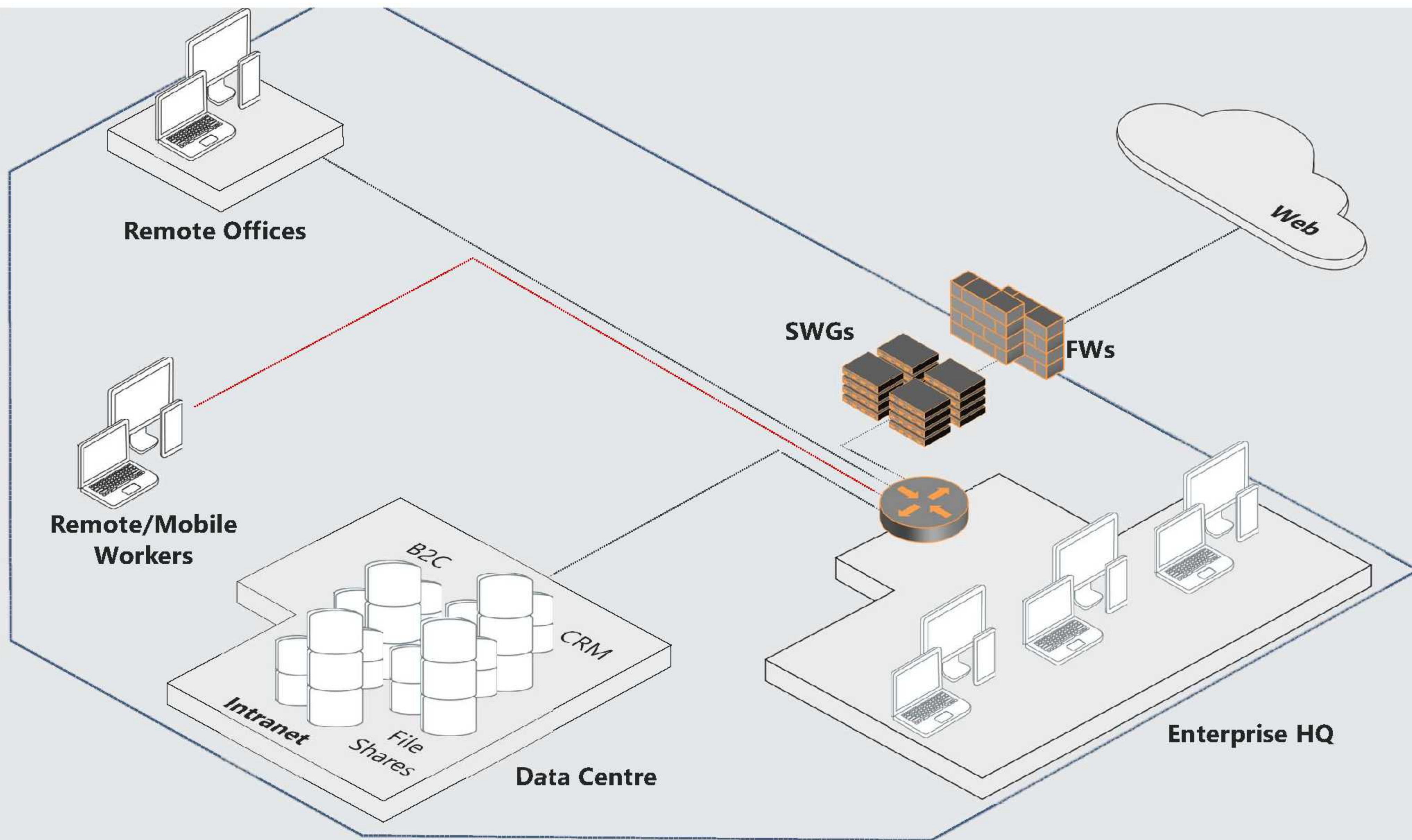
McAfee Confidential

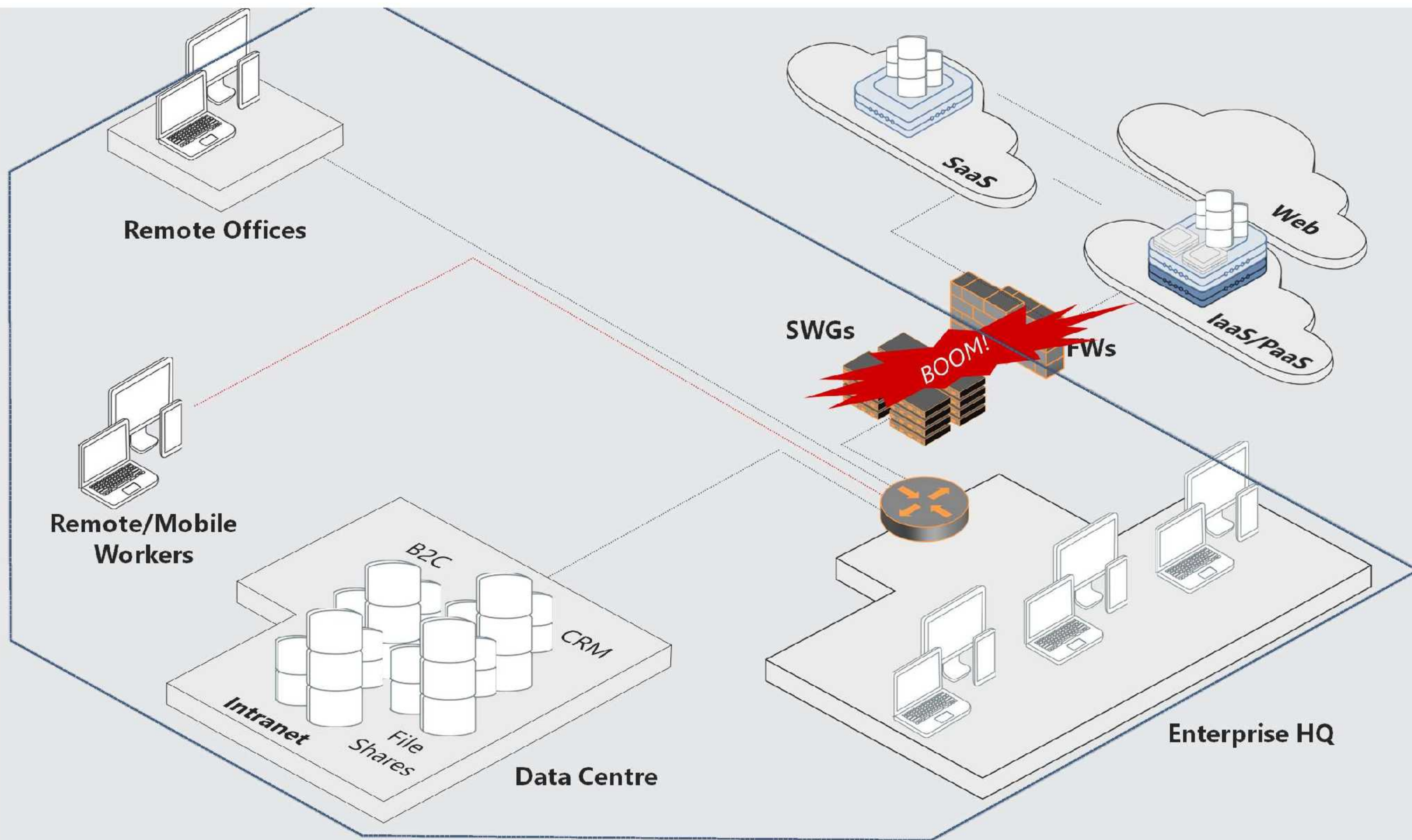
**The Device and the Cloud are
the two Control Points of the
Modern Enterprise Architecture**



Fragmented Cloud-Native







The McAfee Strategy

*To Protect Data and Defend Against Threats where
Modern Work Gets Done: **On Devices and in the Cloud***



Device

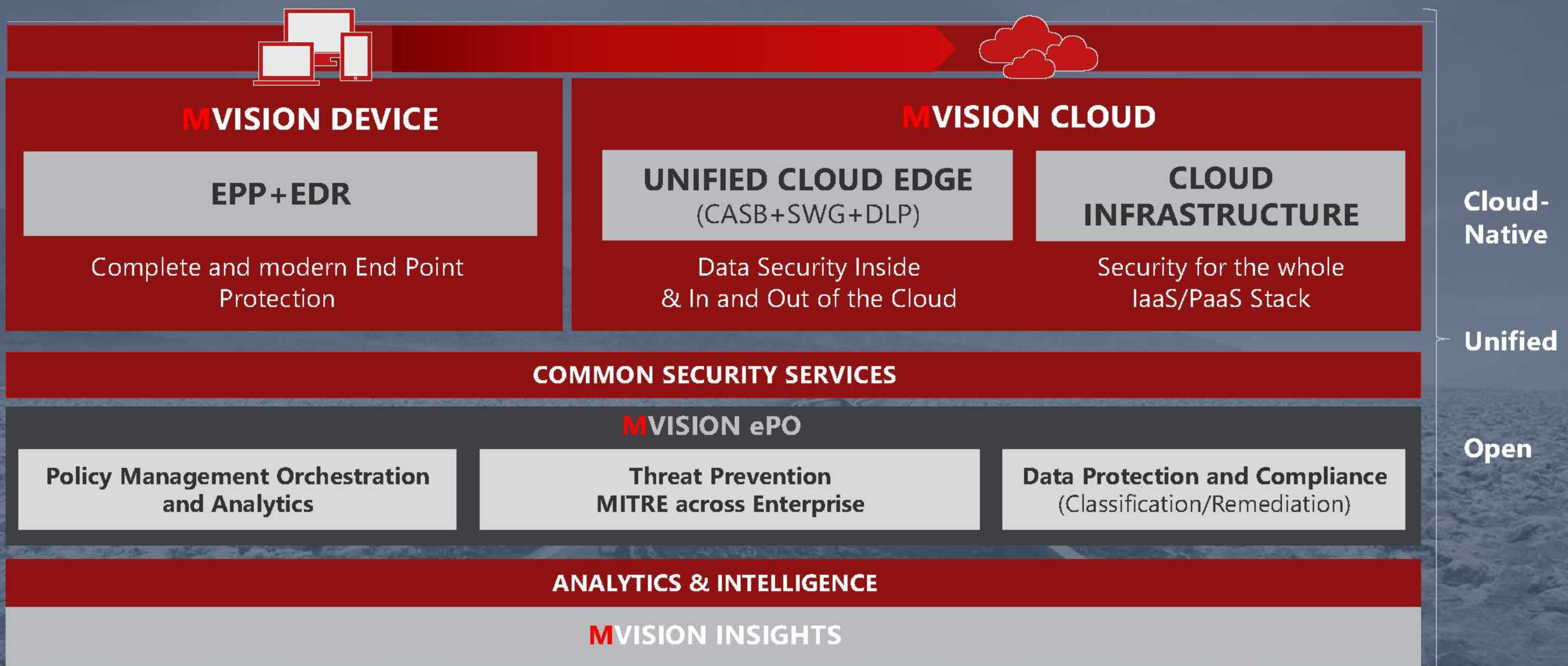


Cloud



Device to Cloud

McAfee Device-to-Cloud Security Platform

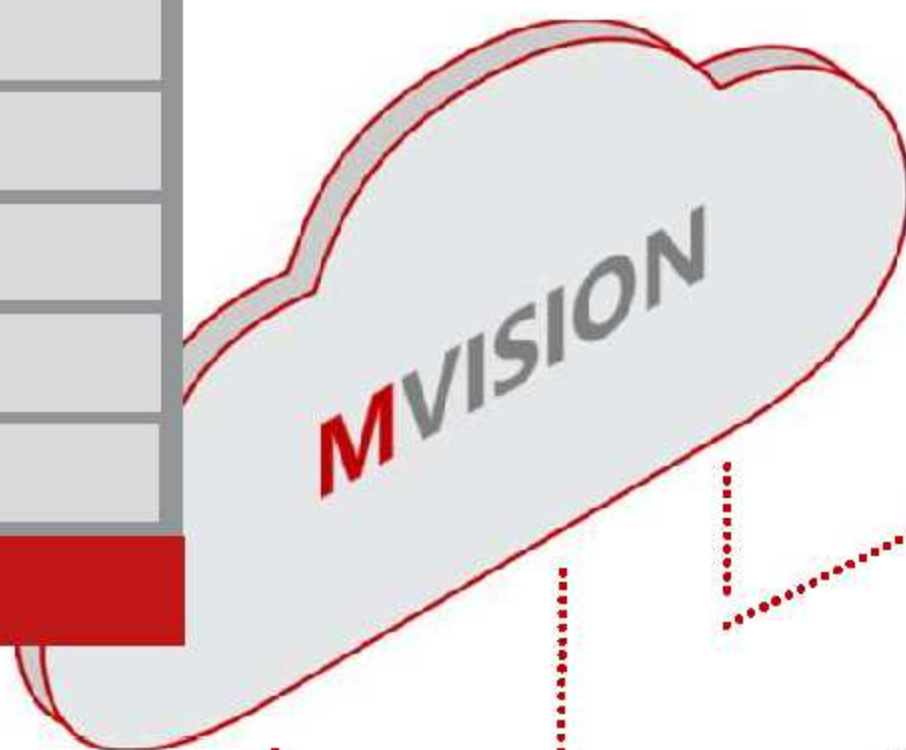




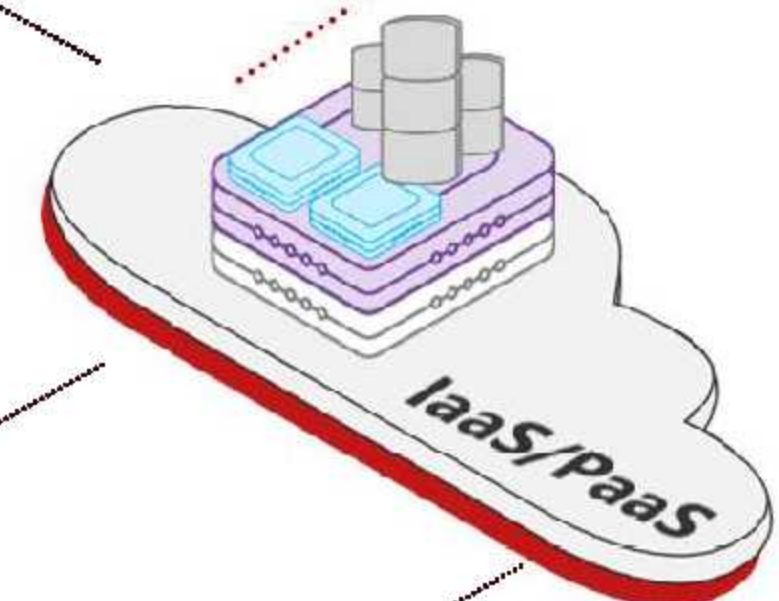
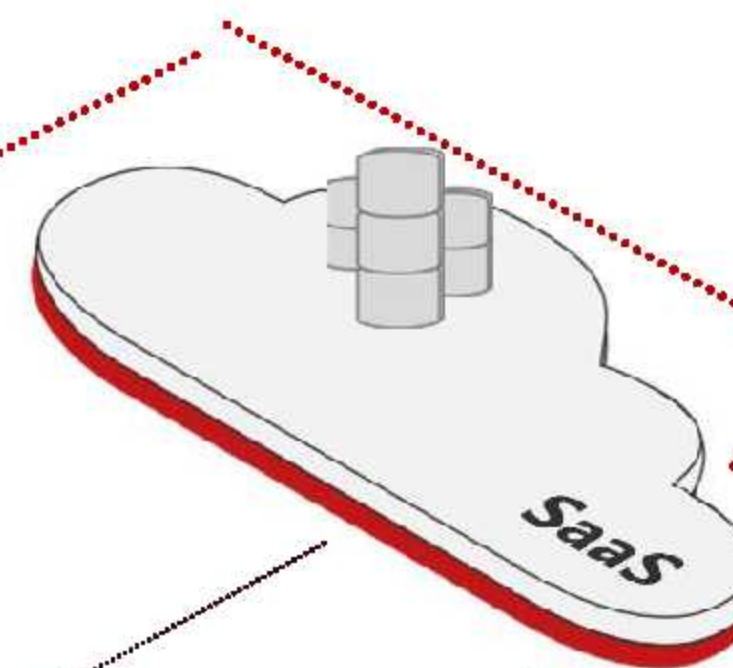
McAfee Unified Cloud Security Approach



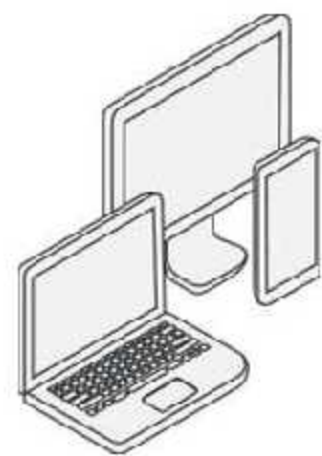
Visibility
Unified Policies
Data Protection
Threat Prevention
Incident Reporting
...ACROSS



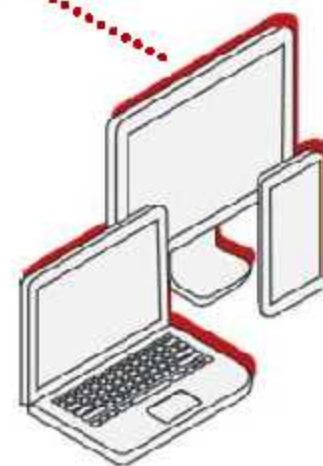
1 In the Cloud



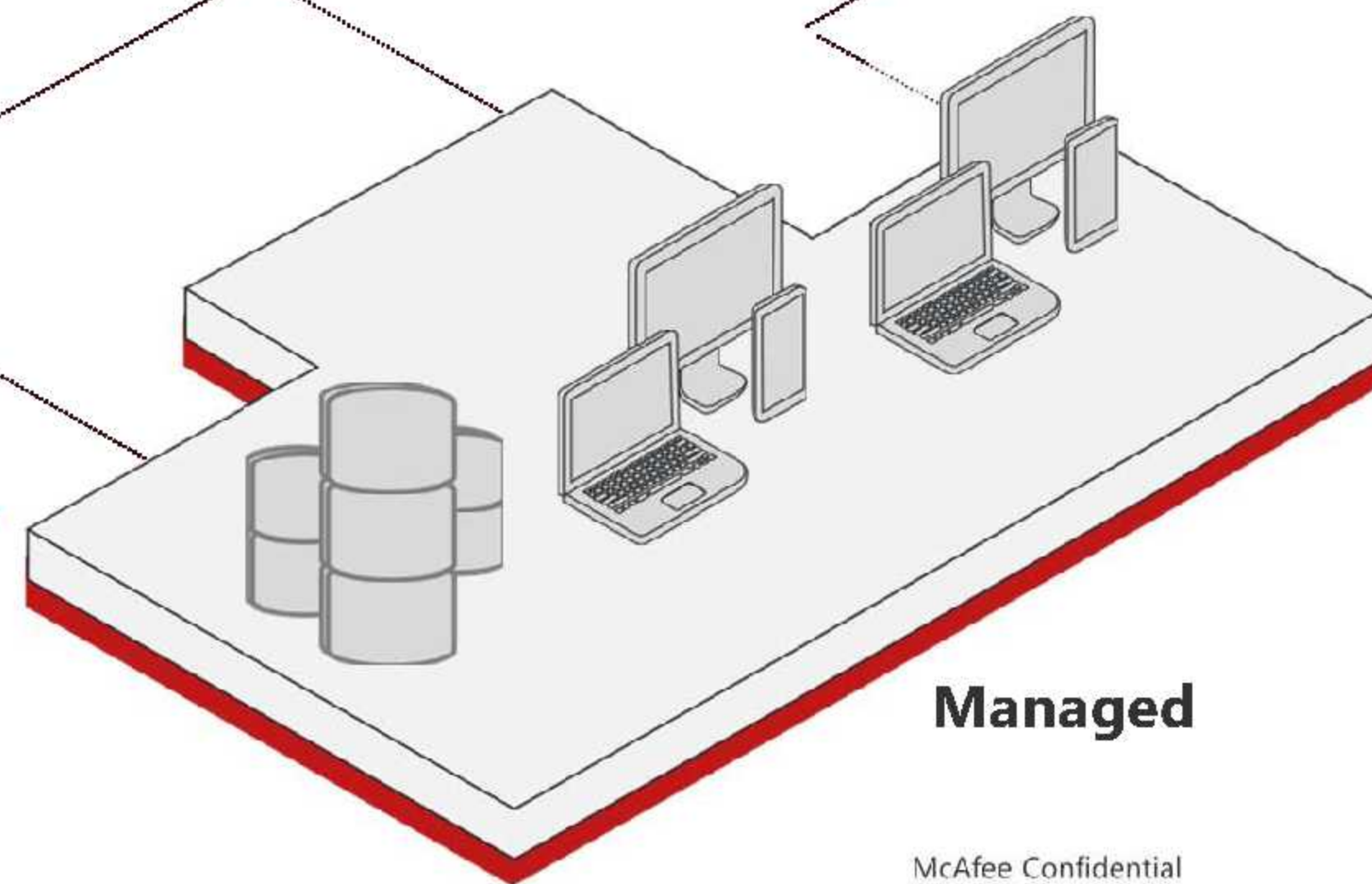
2 In and Out of the Enterprise



Personal



Managed



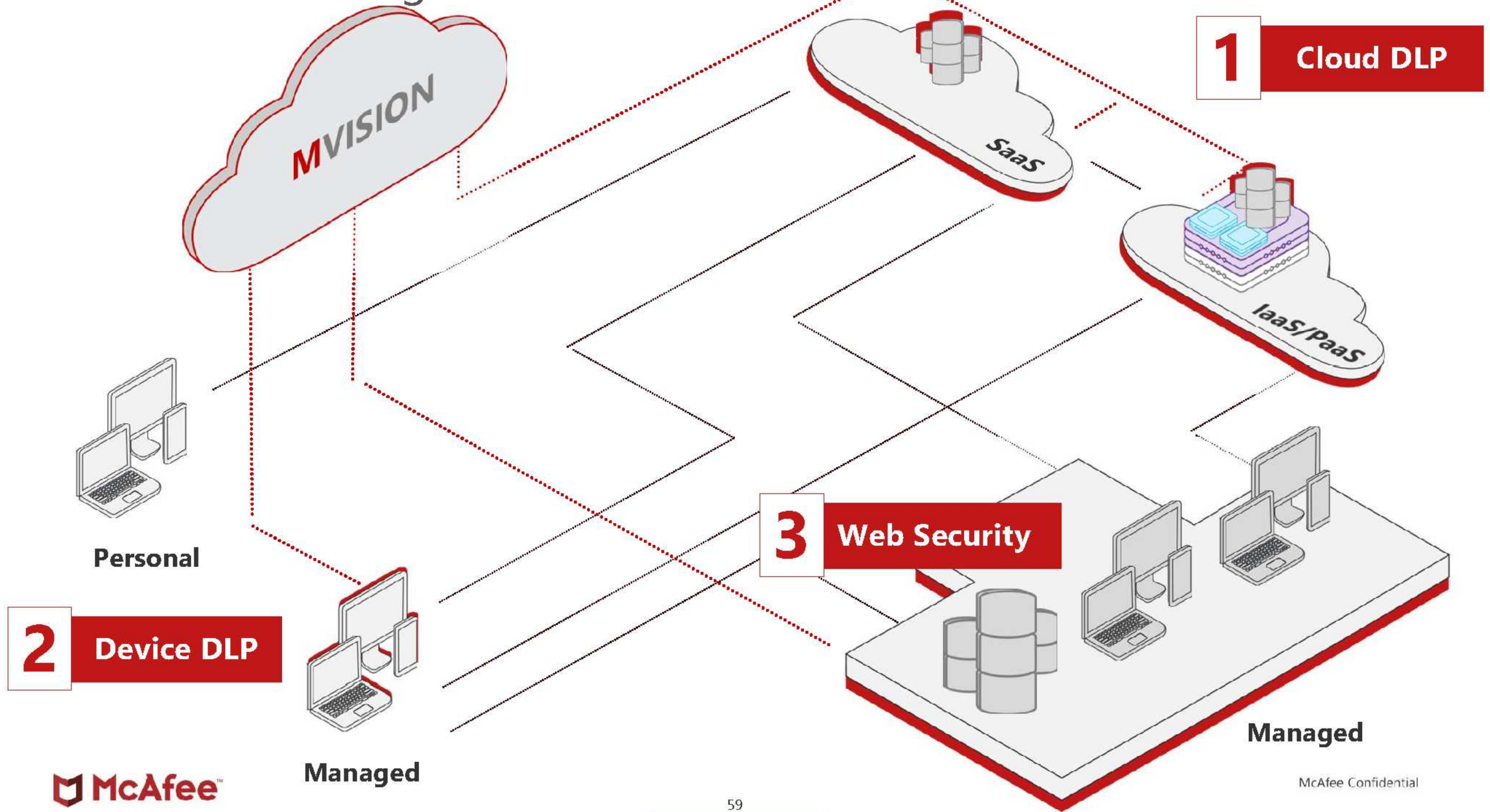
Managed

3 On Devices

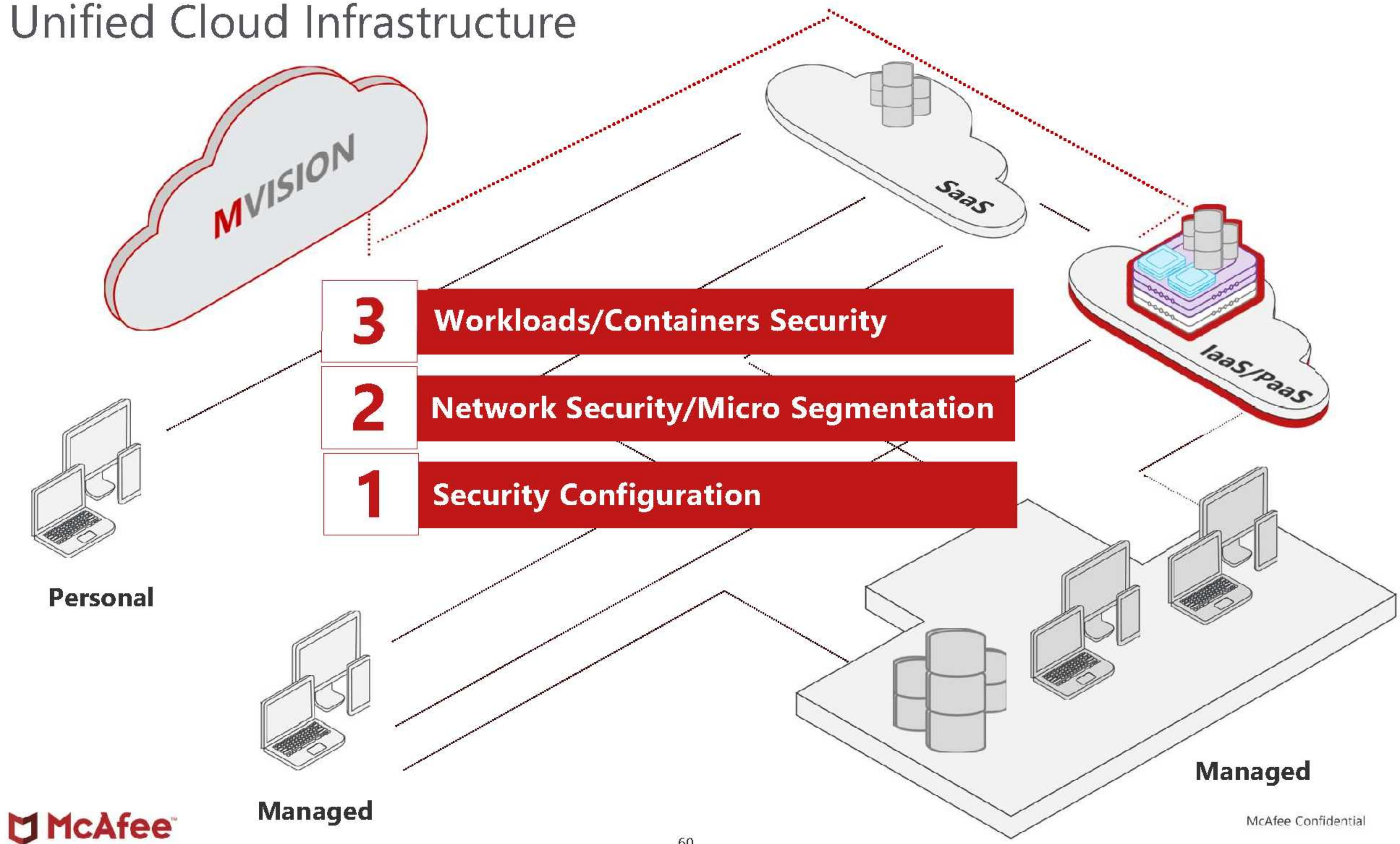


McAfee Confidential

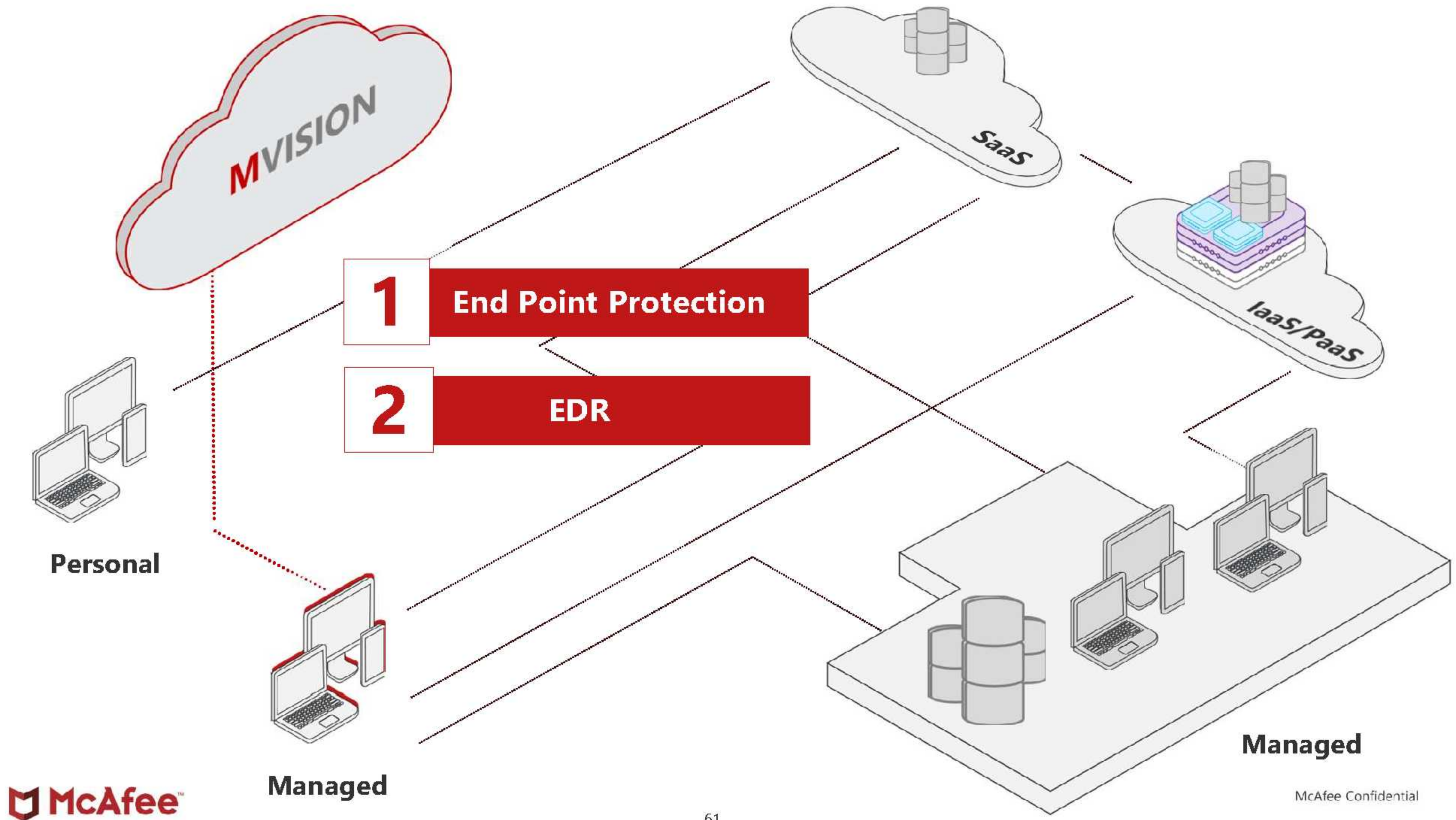
Unified Cloud Edge **CASB + Web + DLP**



Unified Cloud Infrastructure

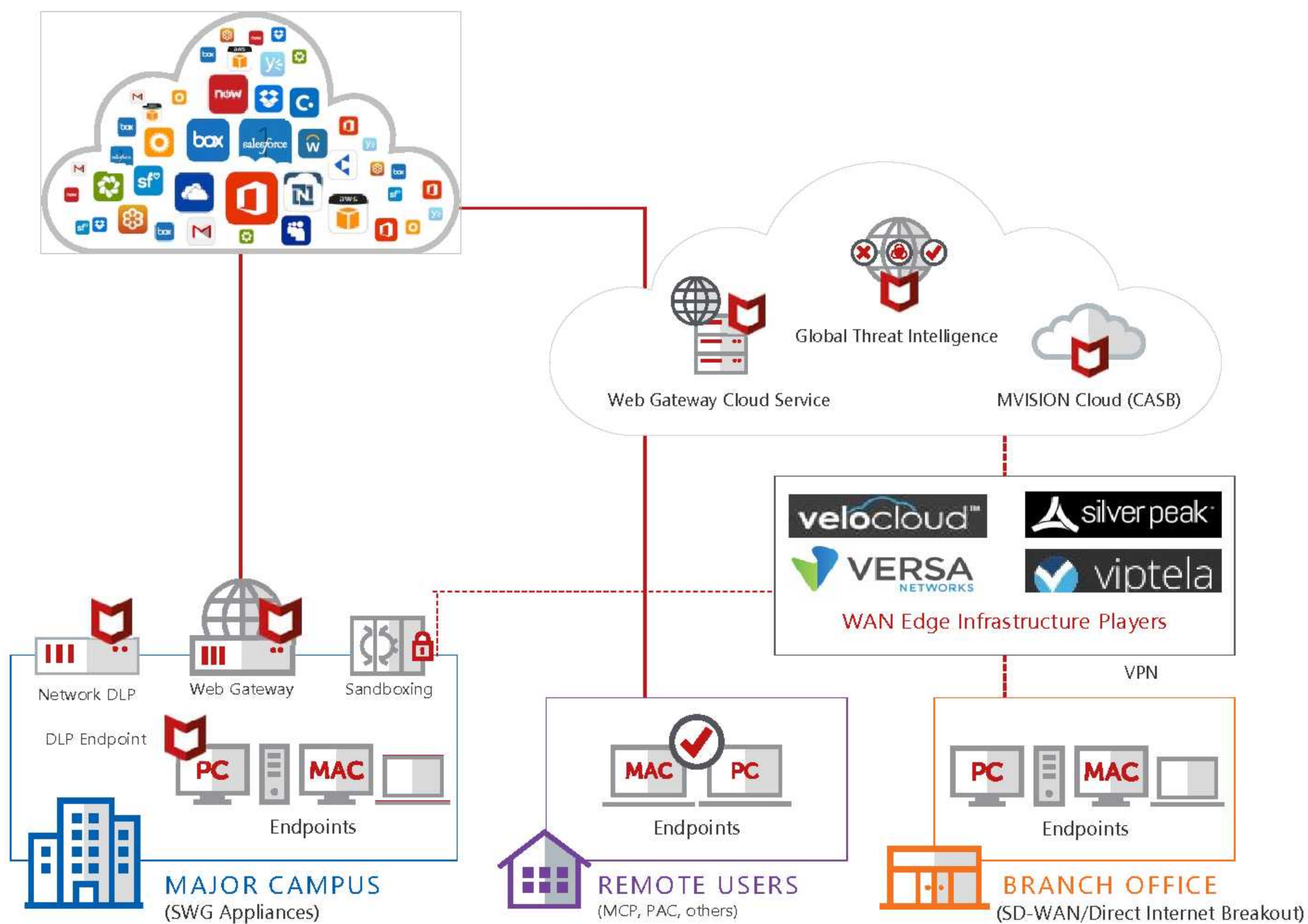


Endpoint

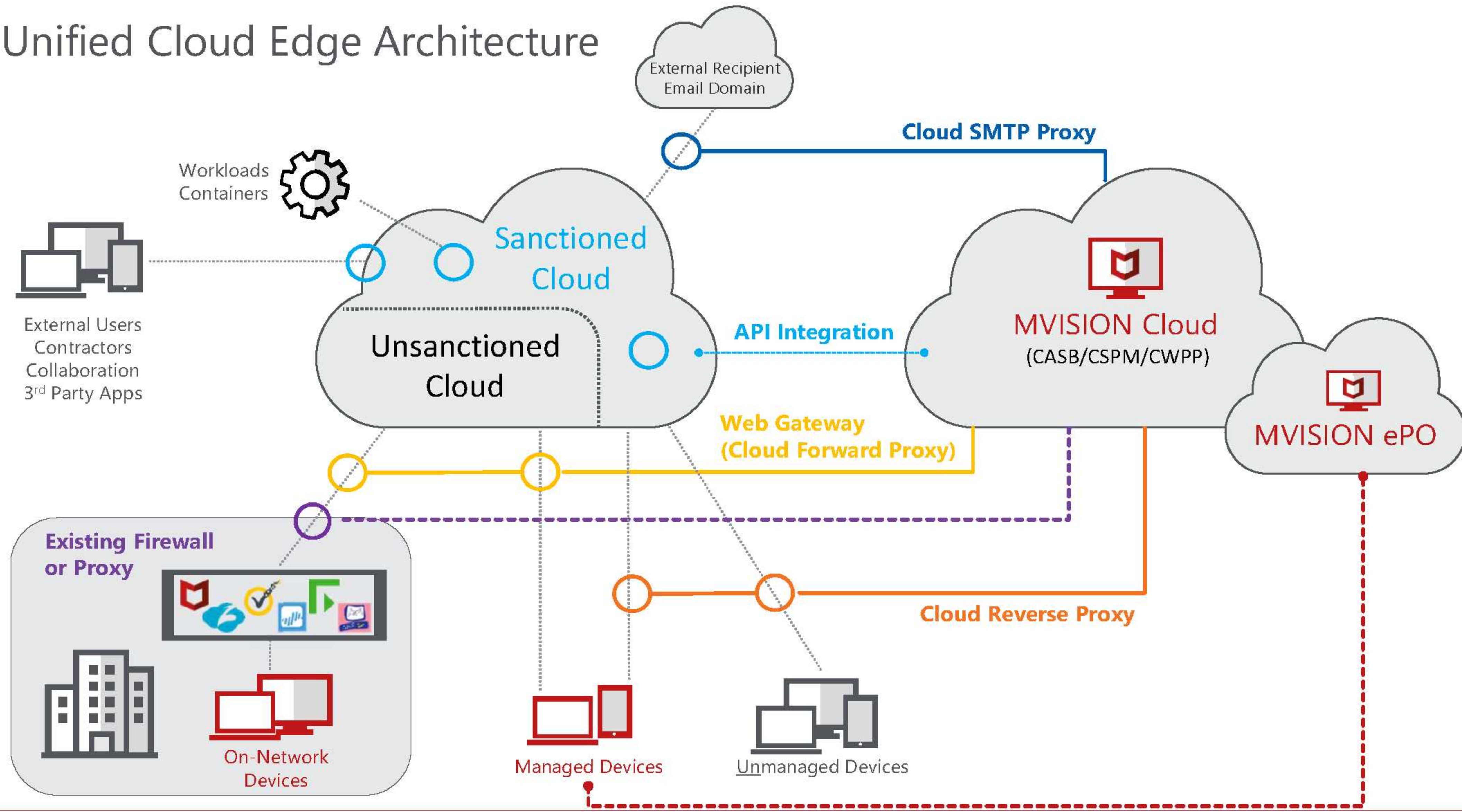


Architecture

Unified Cloud Edge Architecture

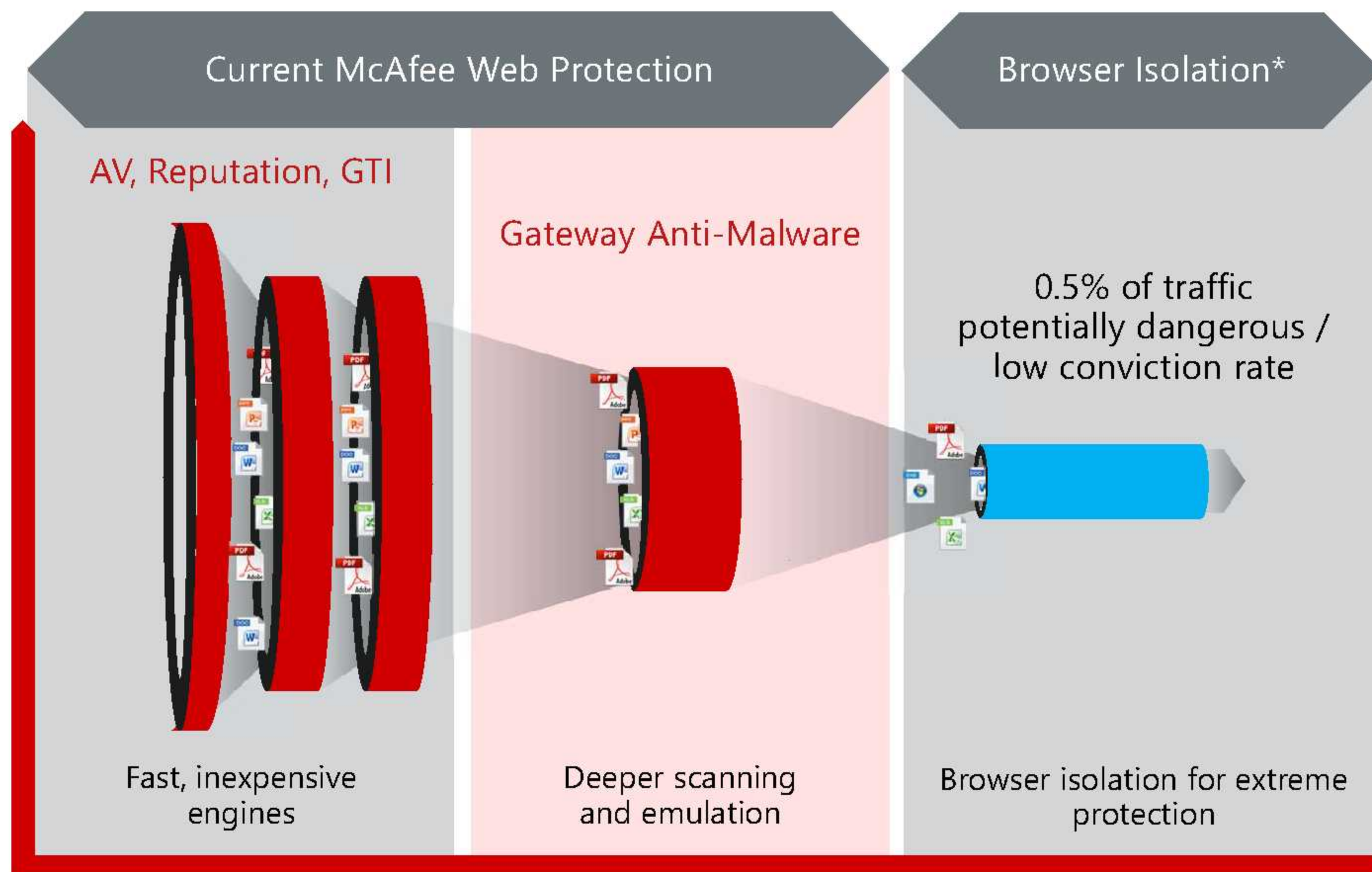


Unified Cloud Edge Architecture



Layered Threat Prevention, including Browser Isolation

- Provide best-in-class threat effectiveness for web borne threats
- Deliver strong performance and user experience by isolating only risky or uncategorized websites where access is needed
- Converge management and policy into a unified user interface for simplicity of deployment



UCE Infrastructure

Web Gateway Cloud Service (CASB Forward Proxy)

- Cloud-based filtering using Web Gateway technology
- High availability SLA of **99.999%**
- 53 points of presence in 44 countries
 - trust.mcafee.com
- Data center peering used for improved performance
- Authentication: IP-based, SAML, and MCP Agent
- Two Malware Engines:
 - GTI Signature-based from 1+ Billion Sensors
 - Zero-Day Heuristics GAM Engine
- Native TLS 1.3 and HTTP/2 for SSL Inspection, no downgrading
- Web Gateway = CASB Forward Proxy
 - No Proxy Chaining or Splitting Traffic!!



99.999% Service Availability = True Cloud-grade Infrastructure

Service availability publicly documented on
<https://trust.mcafee.com>

Service Availability*	Last 7 Days	Last 30 Days	Last 90 Days
Global Routing Manager (GRM)	100%	100%	100%
North America Proxy Service**	100%	100%	99.999%
Europe Proxy Service**	100%	100%	100%
Asia Proxy Service**	100%	100%	100%
Global Proxy Service**	100%	100%	99.999%

*February 2020 Snapshot

Why five 9's matter

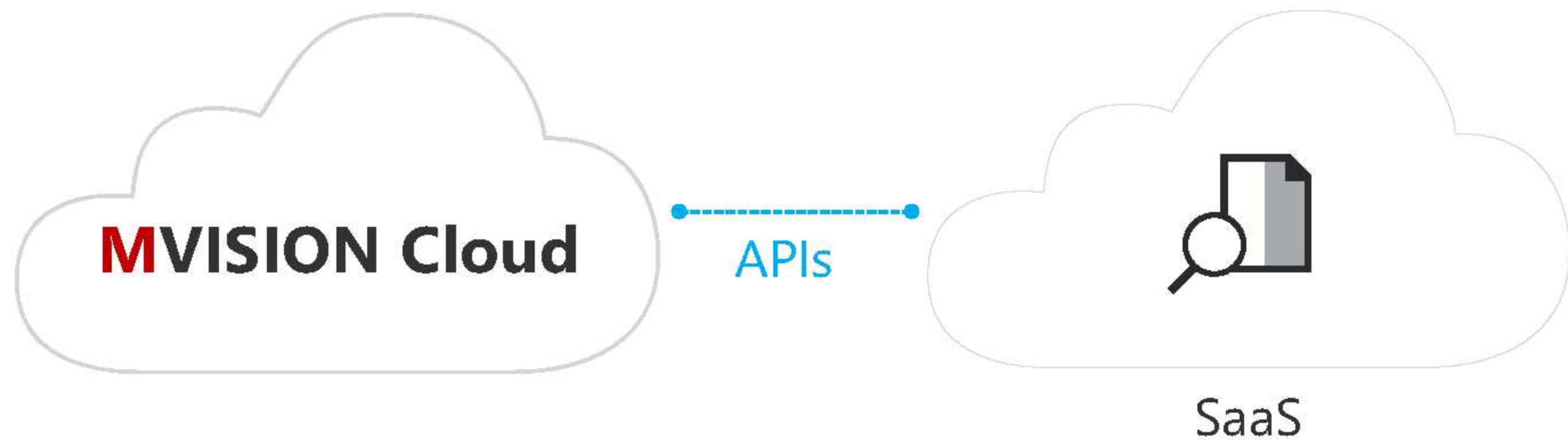
Difference in allowed downtime based on uptime SLA

	99.999% uptime	99.99% uptime	99.9% uptime
Day	0.9 sec	9 sec	86.4 sec
Week	6 sec	1min	10 min
Month	26 sec	4 min	44 min
Year	5 min	52 min	525 min

Use Cases

How a **Unified Cloud Edge** Addresses Cloud Security Use Cases

Maria—Collaboration Control and DLP



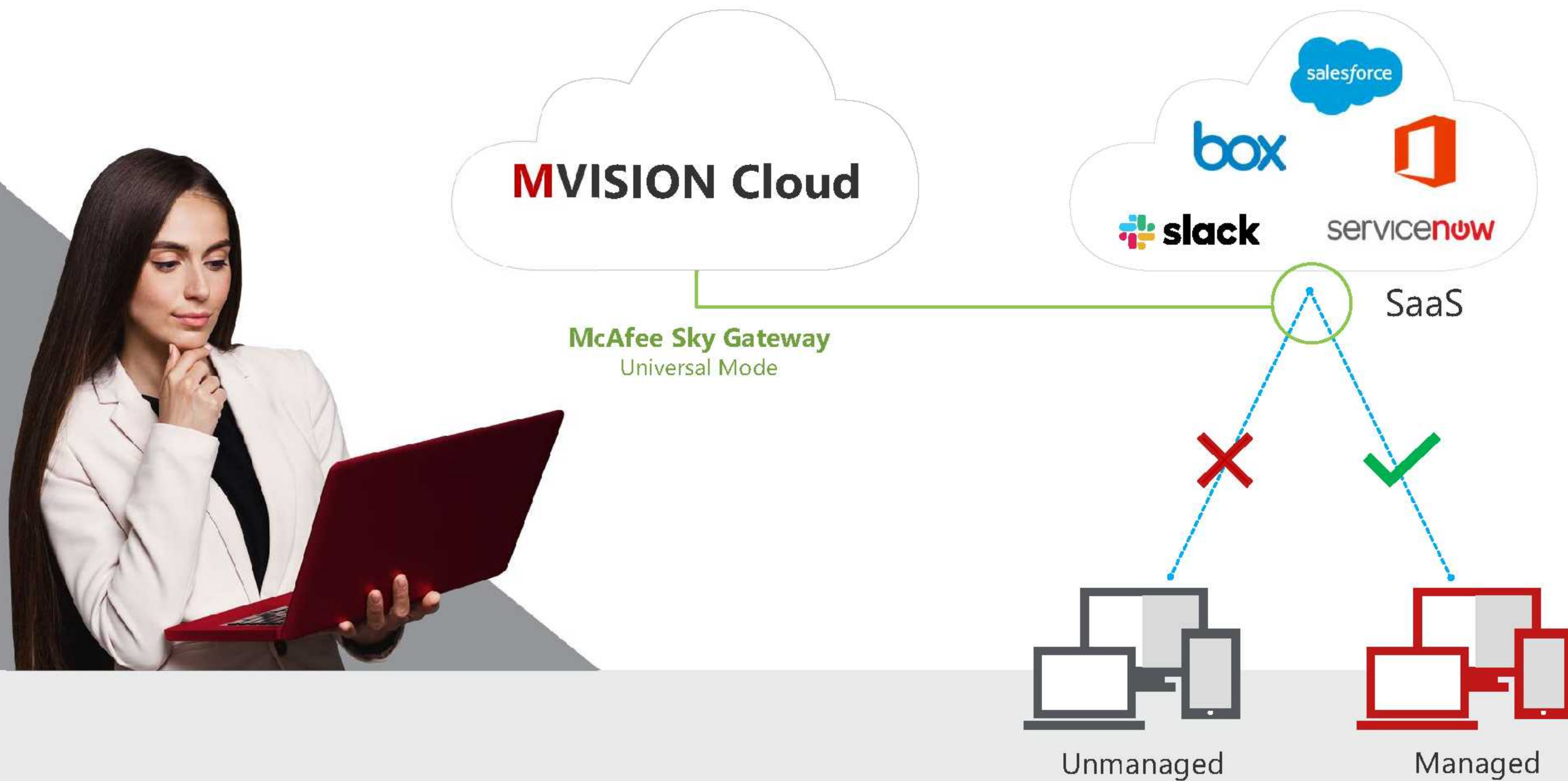
- Collaboration control
- Cloud-native DLP

Maria—Endpoint DLP

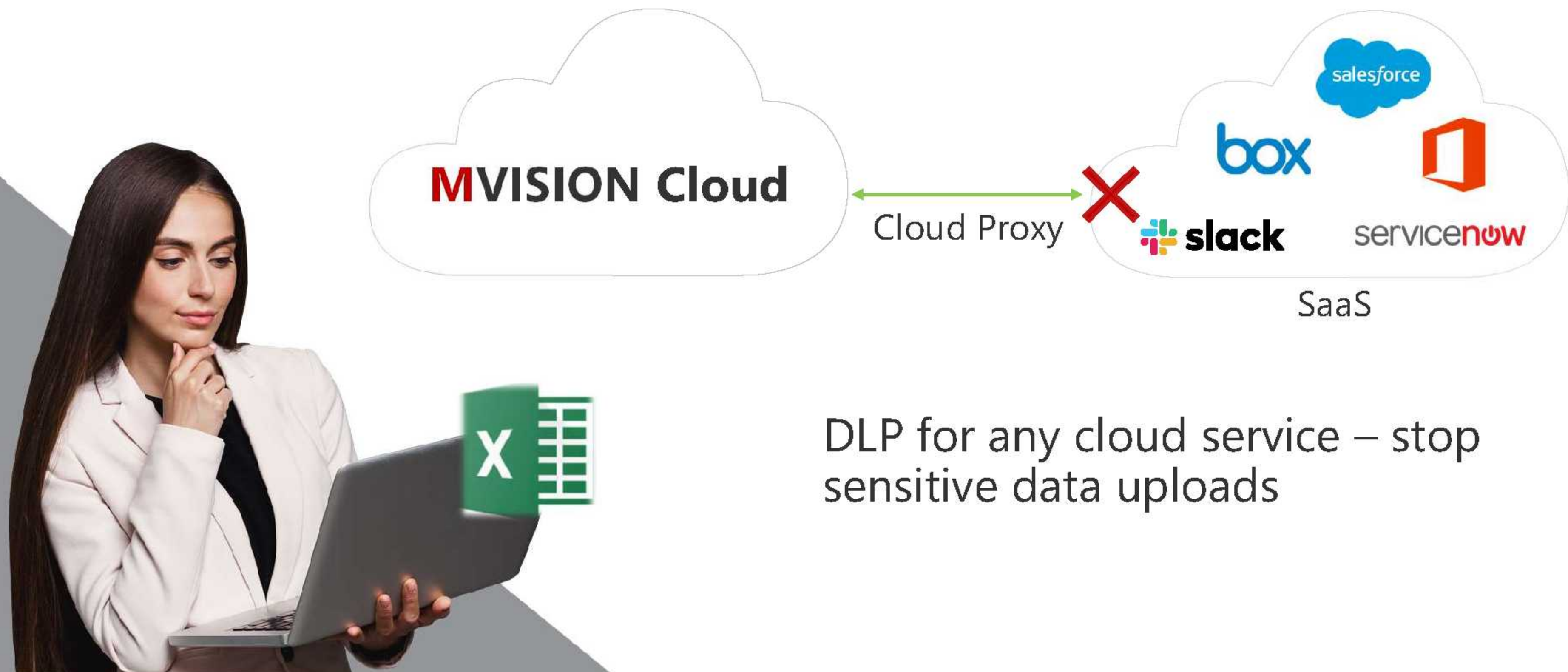


- Stop data loss to USB devices
- Block email attachments with sensitive data at the endpoint

Maria—Contextual Access Control



Maria—DLP for Shadow Cloud Services

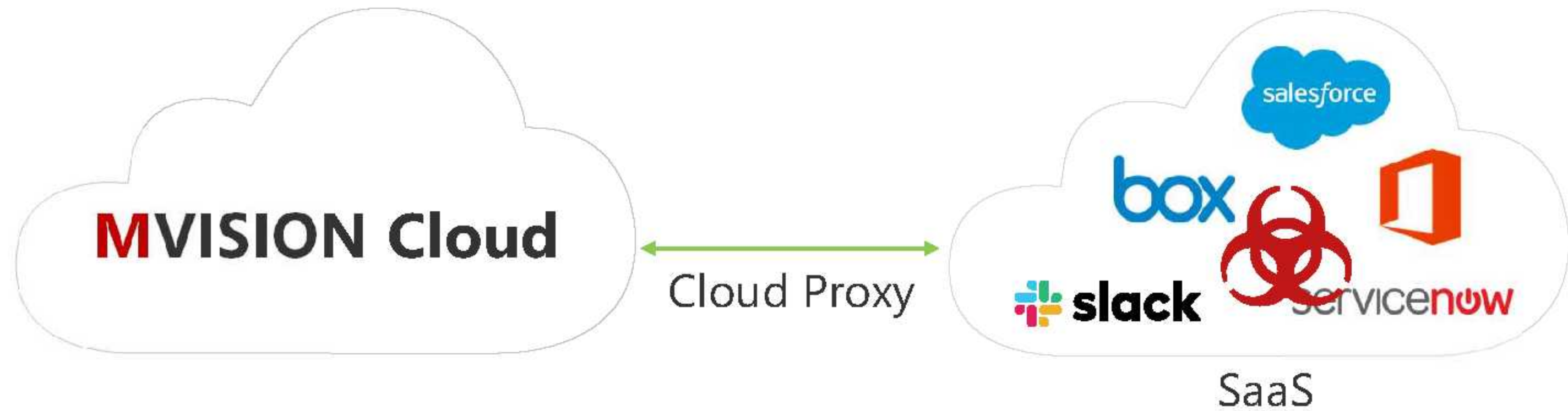


Maria—Cloud Application Control and Tenant Restrictions



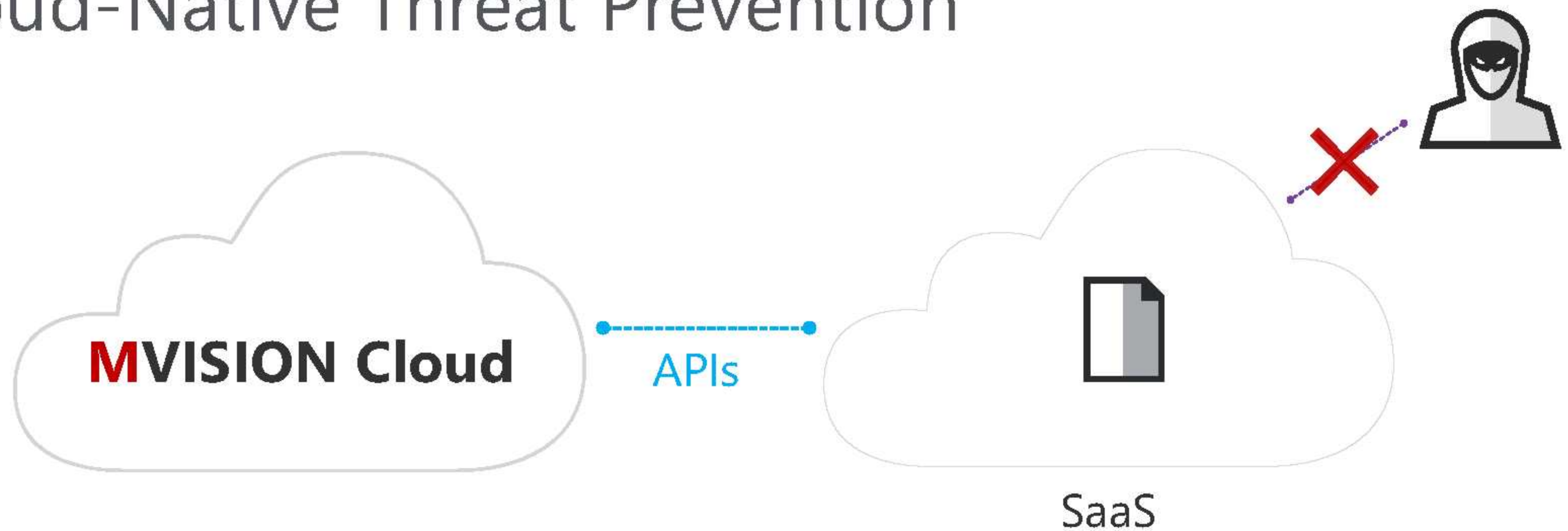
- Block uploads and access to high risk apps
- Block access to personal accounts

Maria—Zero-Day Malware Prevention



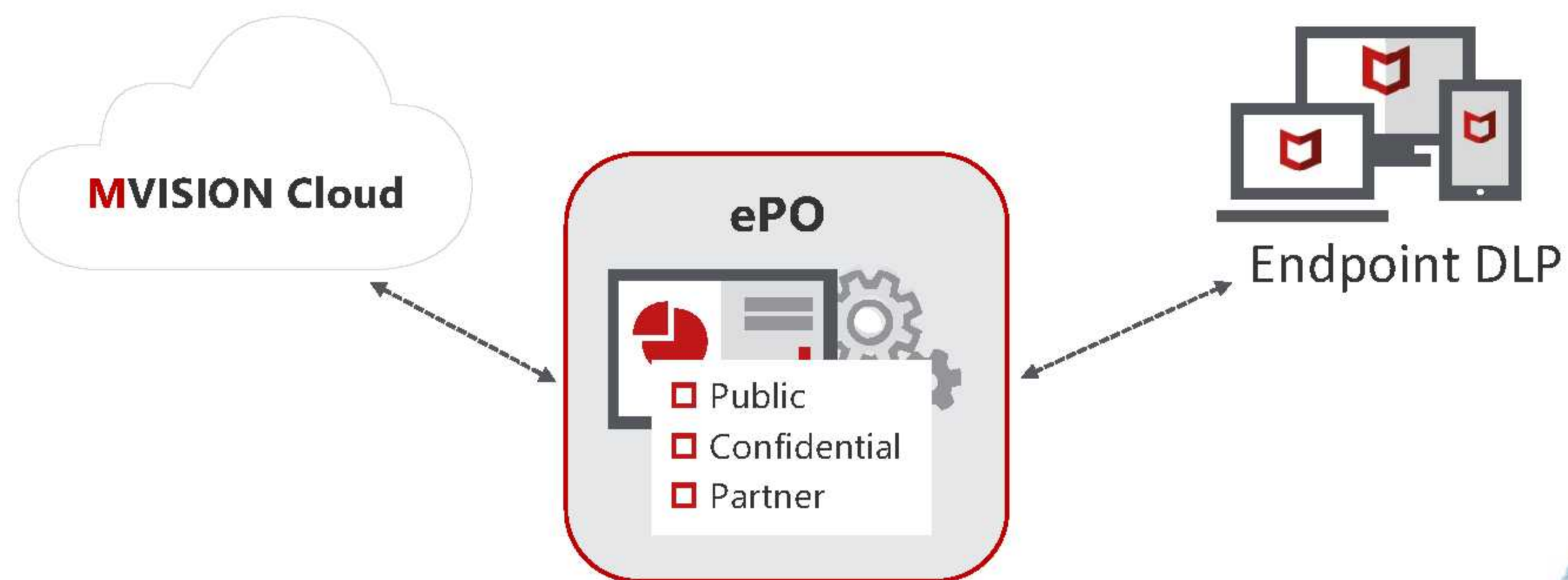
Stop zero-day malware download from
any cloud service or website

Maria—Cloud-Native Threat Prevention



Prevent cloud-native threats
and breach attempts

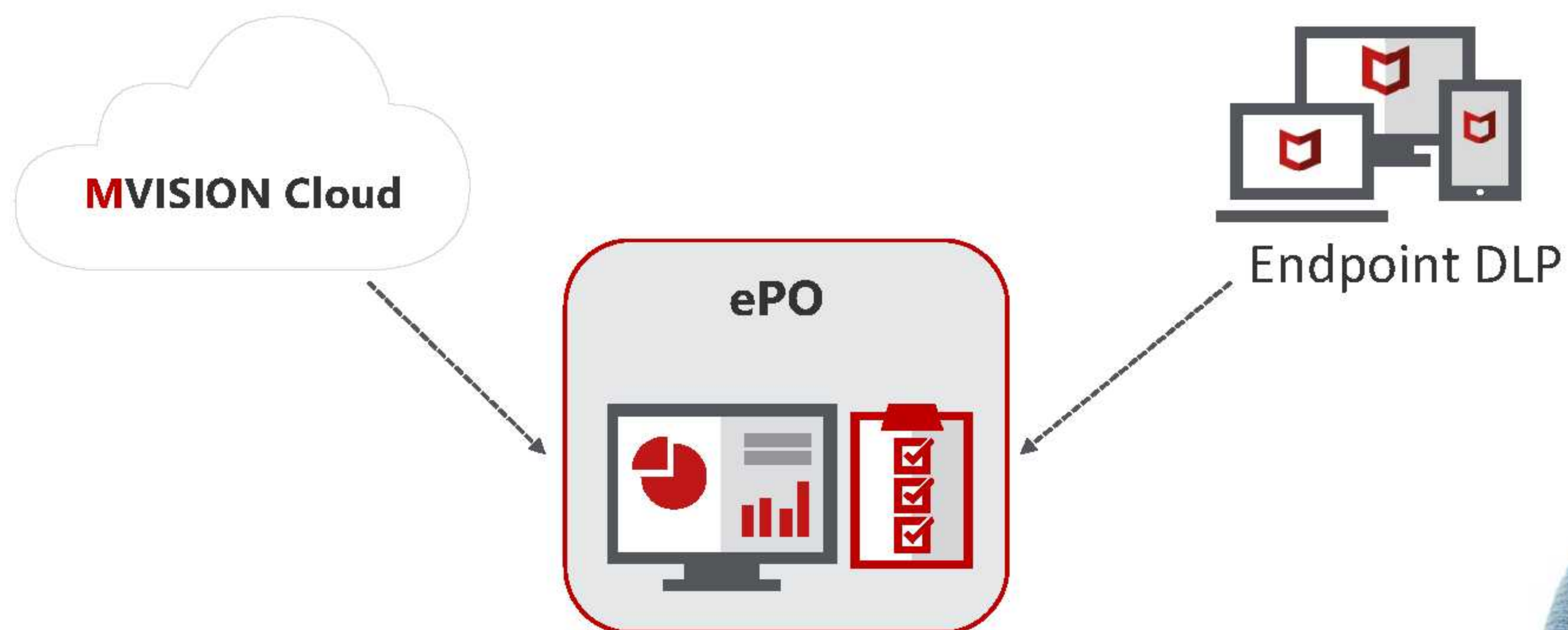
Dave—Device-to-Cloud DLP



- Saves time by creating DLP rules once and pushing everywhere
- Increases detection accuracy with one DLP engine running at device and cloud



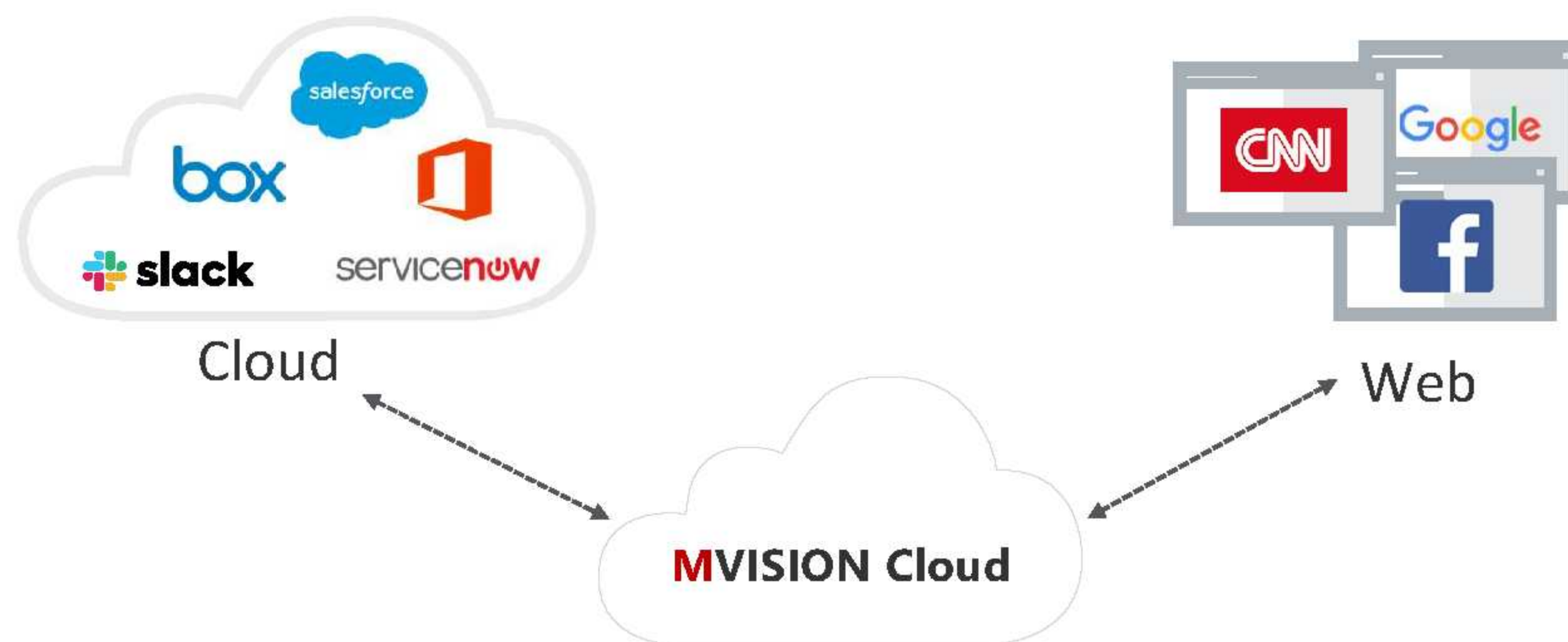
Dave—Unified DLP Workflows



- Reduce complexity with one console for cloud and endpoint DLP workflows and reporting



Dave—Unified Cloud and Web Security

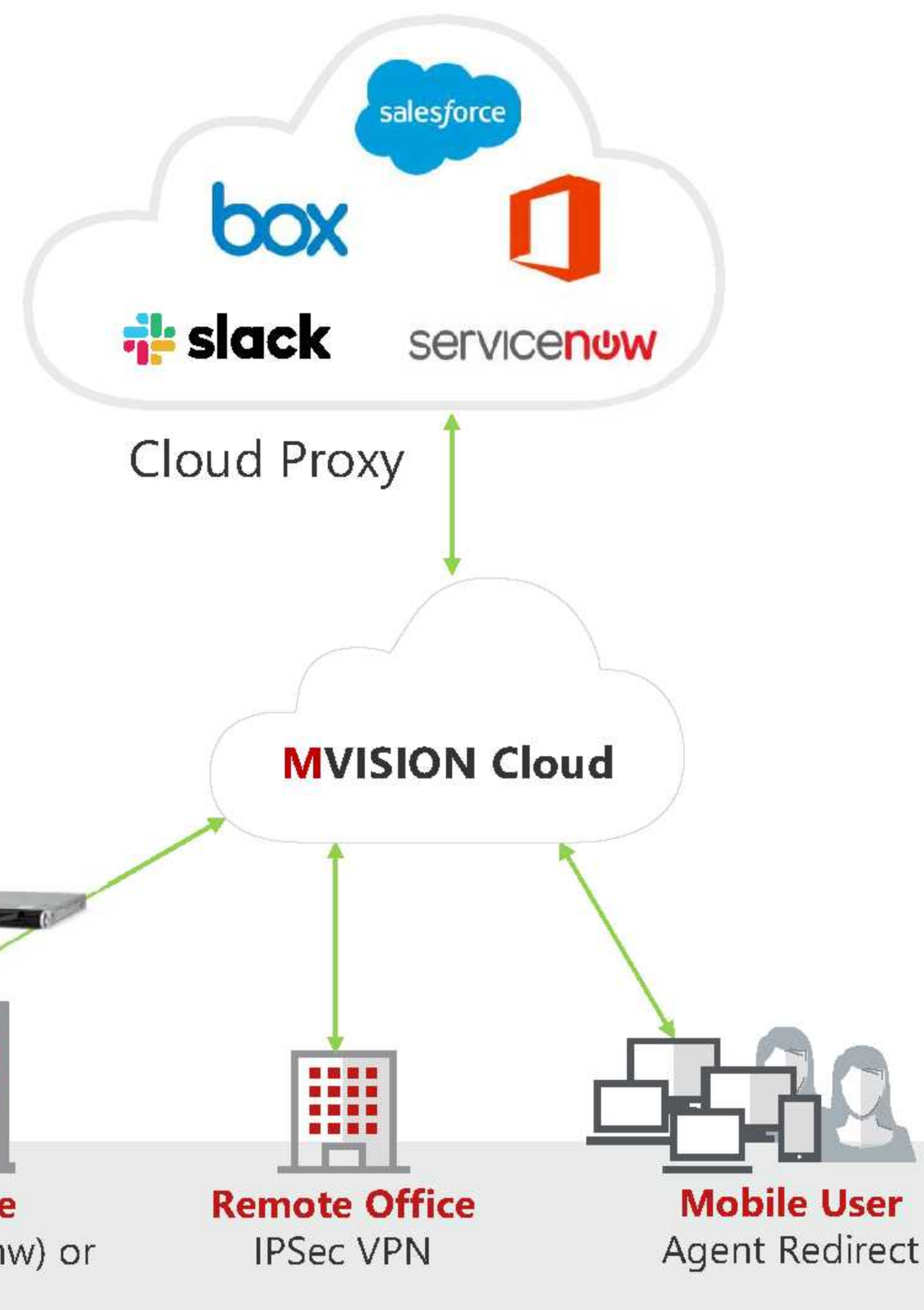


- One console for Cloud and Web security policy
- Shared risk database for cloud apps
- Closed-loop remediation for Shadow IT



Lee—Cloud-Native Proxy Architecture

- No hardware needed
- Reduced or eliminated MPLS
- Infinitely scalable
- 99.999% availability

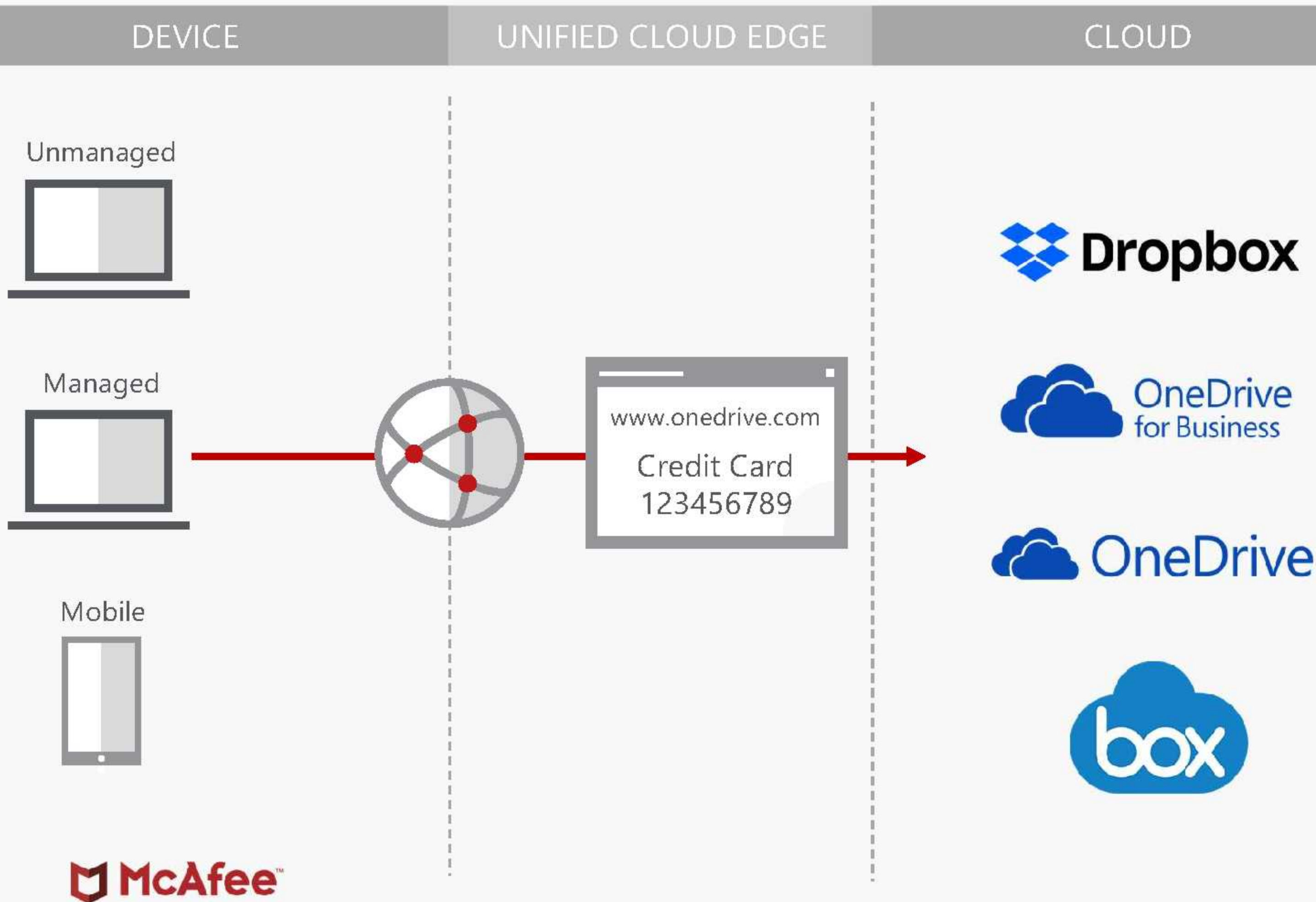




USE CASE

Shadow IT and Close Loop Remediation

Use Case Shadow IT



RISK

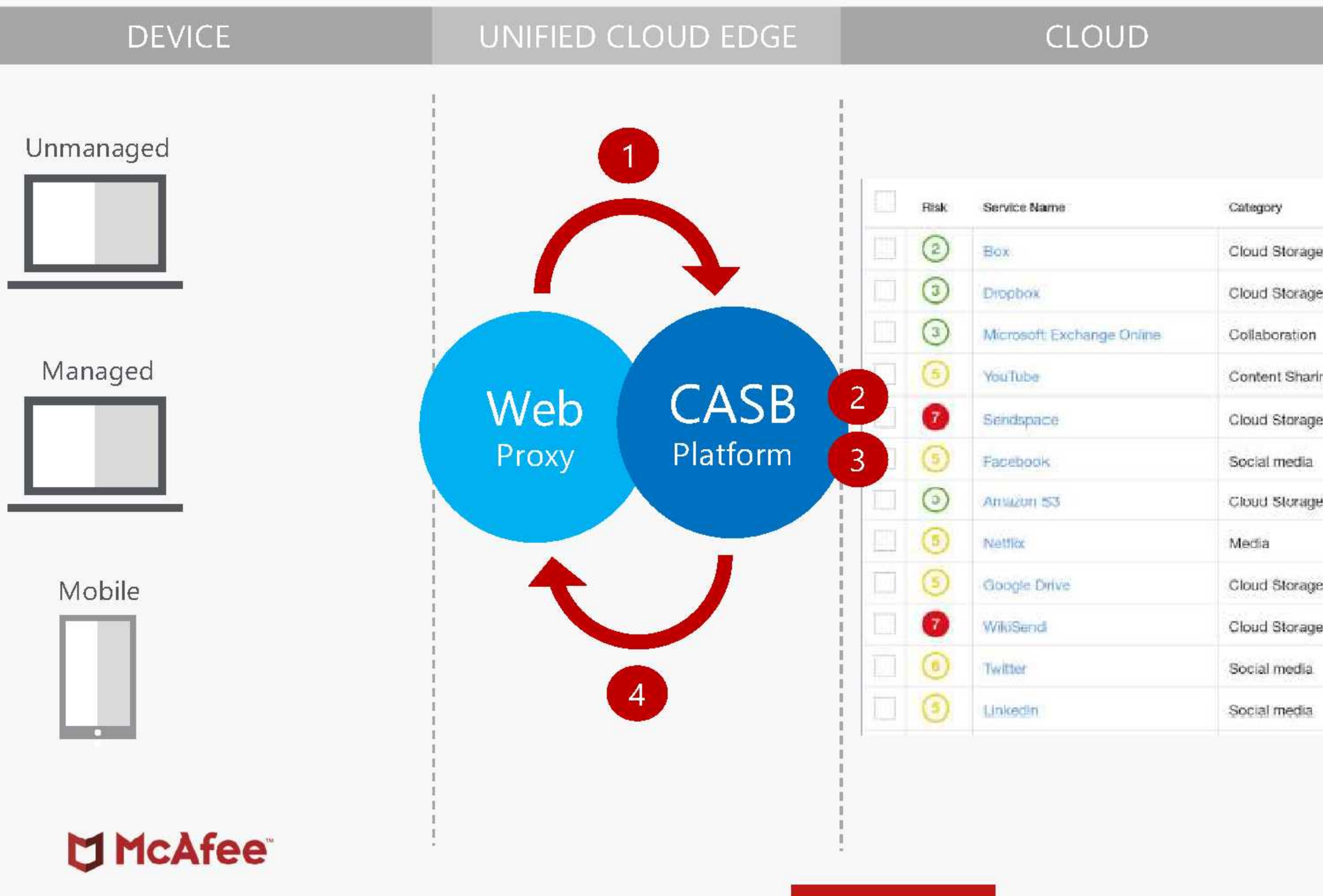
Uncontrolled Data Loss due to lack of visibility and control for Shadow IT applications.

CHALLENGE

IT lost control. Users just need a Browser and Credit Card to sign up for a new Cloud Services.

A standalone Web Proxy is not able to Stop all traffic. Only if the user uses the Browser only.

Use Case Shadow IT



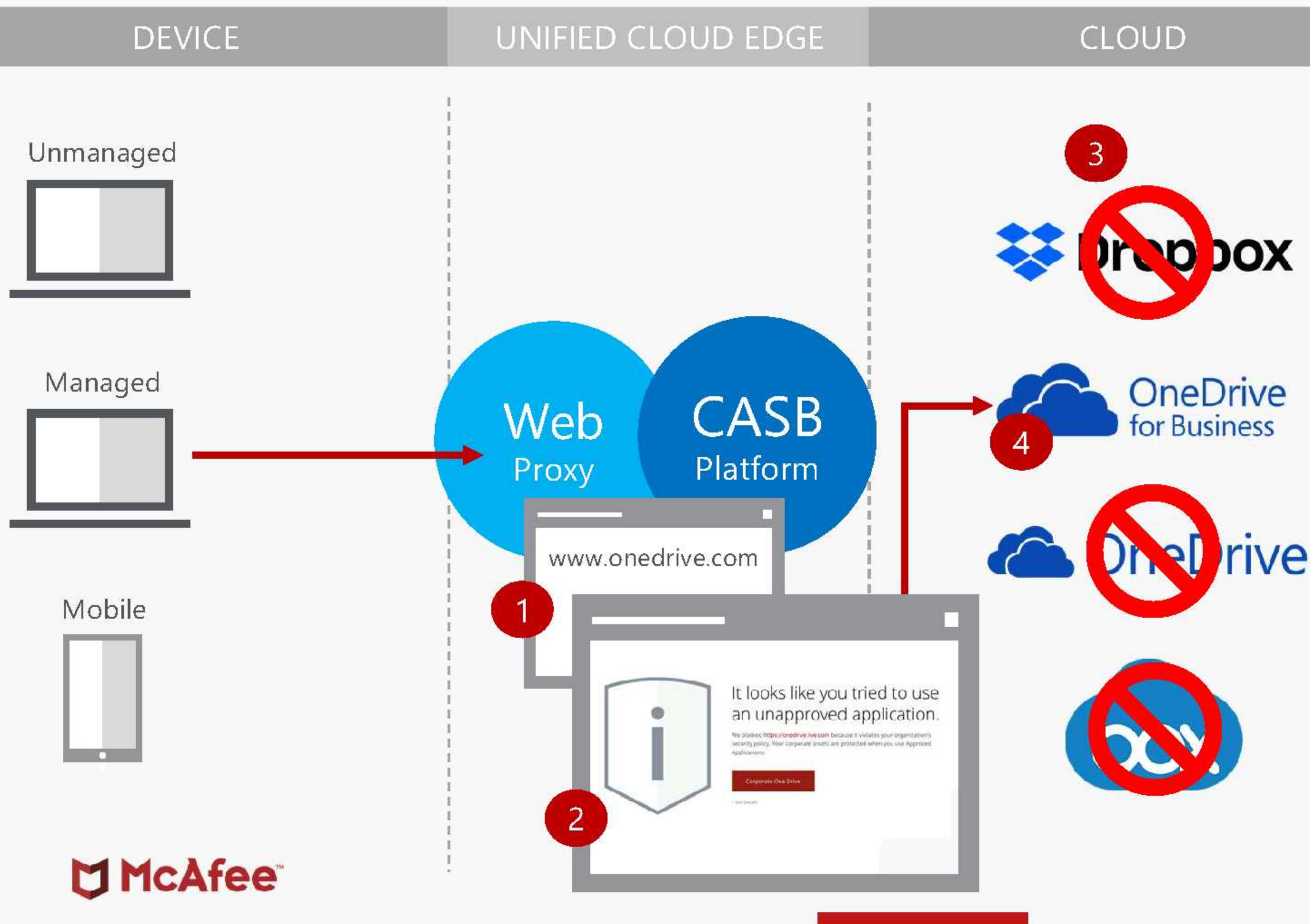
SOLUTION

Building a Close Loop Remediation process between a Web Proxy and CASB platform. Based on CASB Risk Scores customers can create Control Policies.

- 1 Web Proxy provides all data to CASB Platform
- 2 CASB will provide Shadow IT report including Risk Score
- 3 Create Control Policy in CASB – block all cloud Storage, except OneDrive for Business
- 4 Sync Policy to Web Proxy as enforcement point

Automated Proxy Configuration

Use Case Shadow IT



RESULT

Users cannot use any service anymore. For any blocked service they get a customized Block page and a corporate approved alternative service.

- 1 User opens Browser to download OneDrive
- 2 McAfee Web Proxy will bring up Block Page with link to corporate OneDrive
- 3 User can use OneDrive for Business only, all other Services will be blocked
- 4 User can upload Data securely to approved Cloud Storage Service

The background is a dark blue gradient with abstract geometric patterns. A large red arc curves across the frame. In the upper right, there are concentric circles with radial lines, resembling a radar or target. Faint dotted lines and small circles are scattered throughout the background.

USE CASE

Upload Data from unmanaged System

Data Upload from unmanaged System

RISK

High Risk for malware infections

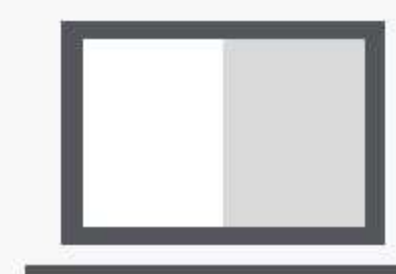
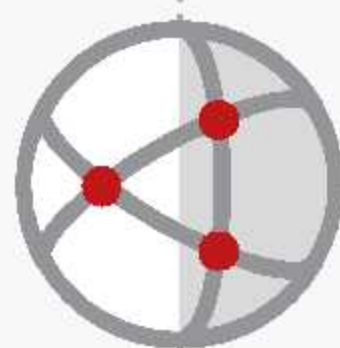
CHALLENGE

No Control in place. User bypasses any Web Control or VPN. The User can upload documents which might be infected without any Threat protection or Data control to a Corporate Cloud Storage

DEVICE

UNIFIED CLOUD EDGE

CLOUD

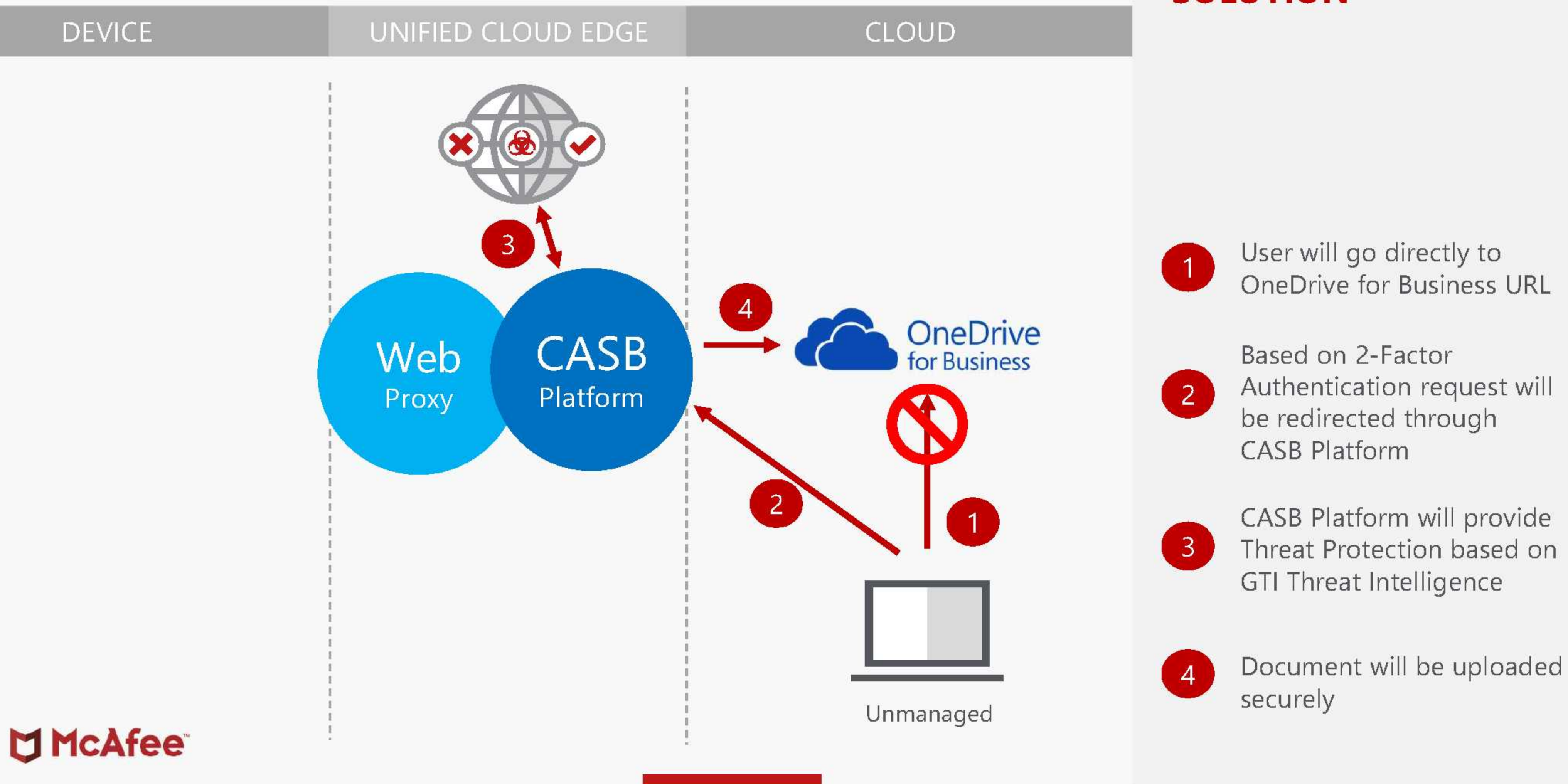


Unmanaged



Data Upload from unmanaged System

SOLUTION



The background is a dark blue gradient with abstract geometric patterns. A large red arc curves across the frame. In the upper right, there are concentric circles with radial lines, resembling a target or a radar screen. Faint dotted lines and small circles are scattered throughout the background.

USE CASE

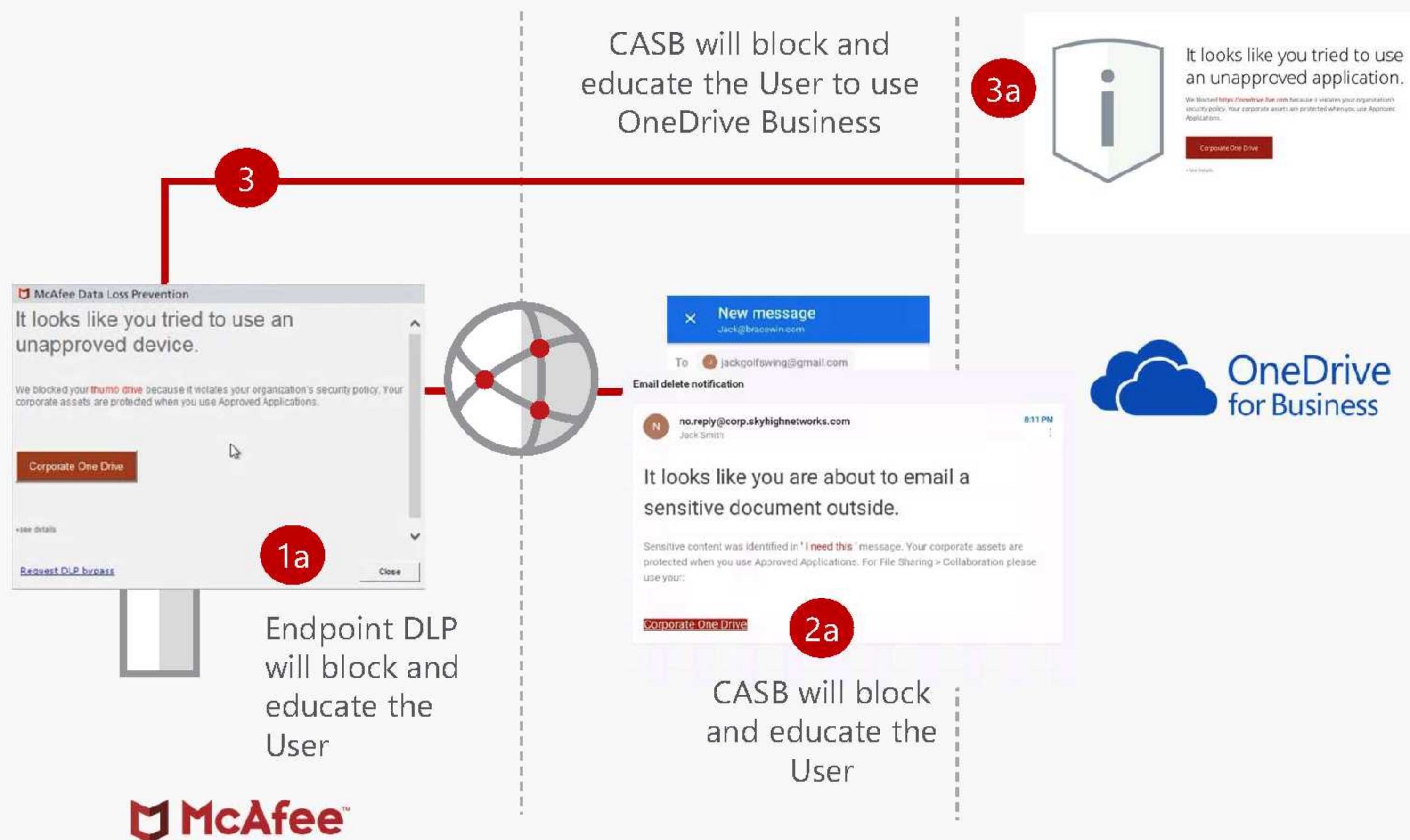
Device to Cloud Data Protection

Protect Confidential Data Everywhere

DEVICE

UNIFIED CLOUD EDGE

CLOUD

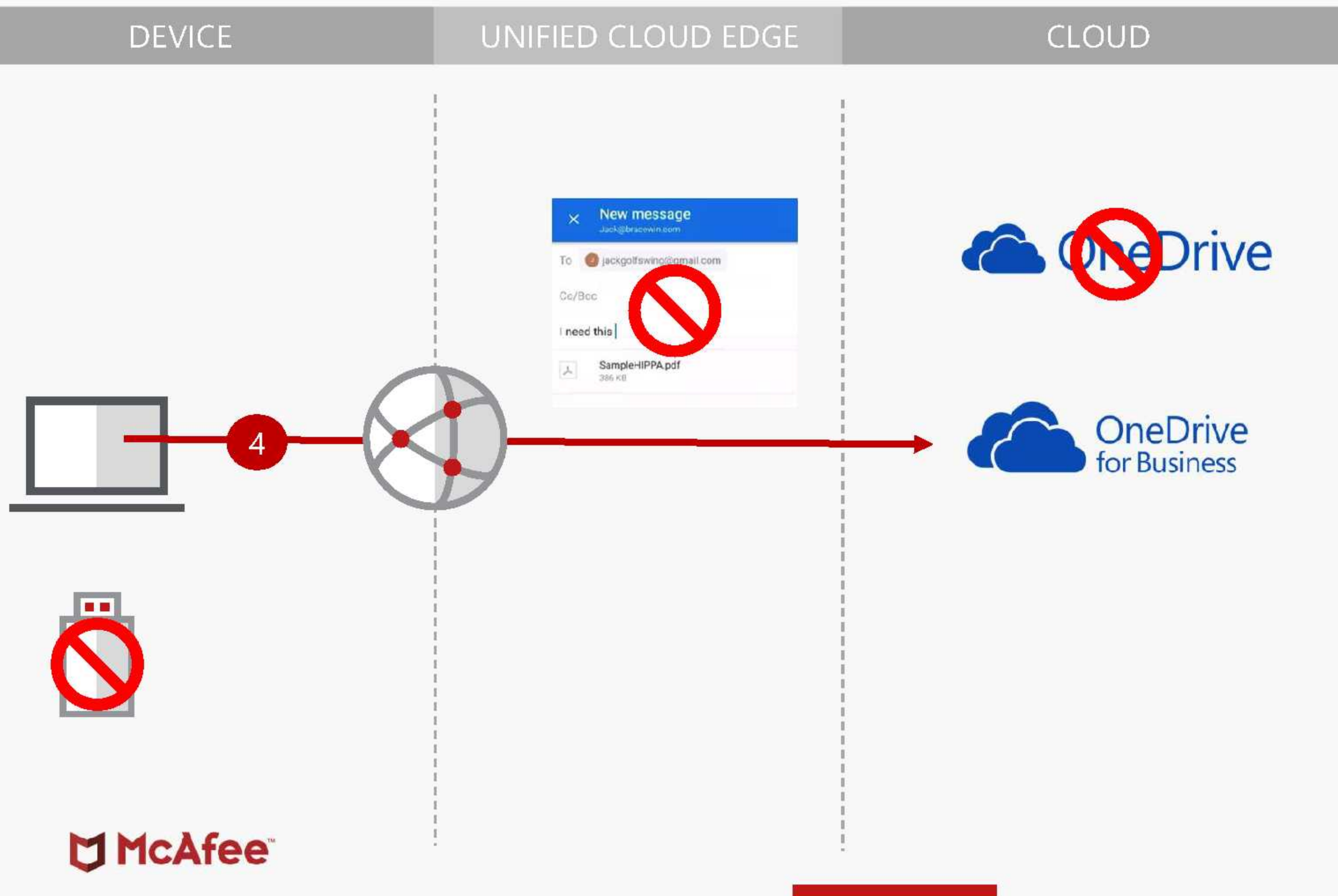


RISK

User has multiple ways to export confidential data. Especially with Cloud Email and non-approved Cloud Storage Services.

- 1 User tries to export sensitive document to USB
- 2 User tries to send same document to private Email
- 3 User wants to upload some document to Personal OneDrive

Protect Confidential Data Everywhere



RISK

User has multiple ways to export confidential data. Especially with Cloud Email and non-approved Cloud Storage Services.

- 1 User tries to export sensitive document to USB
- 2 User tries to send same document to private Email
- 3 User wants to upload some document to Personal OneDrive
- 4 User can upload document to corporate OneDrive

Licensing

UCE Offering

Unified Cloud Edge Basic

- **Per User** - provides new customer access to UCE. It includes CASB Shadow, Web Gateway Cloud Service, McAfee Web Security, Gateway Edition Software and Gateway Anti-Malware. In addition it includes access to McAfee Client Proxy and Content Security Reporter.

Unified Cloud Edge Advanced

- **Per User** - All components of UCEB and entitlements for endpoint DLP (DLPe) and 2.5 sanctioned apps for CASB. It also provides access to ePO and MVISION ePO to manage DLPe.

Leading SKUs

External/Public-Facing



What are the Differences Between the Bundles?

	Shadow IT	WSG	WPS	UCE-B	UCE-A
Gateway Web Protection		X	X	X	X
Gateway Edition Software		X	X	X	X
Gateway Anti-Malware			X	X	X
Web Gateway Cloud Service			X	X	X
McAfee® Web Gateway (MWG) On-premises		X	X	X (Web Gateway licences)	X (Web Gateway licences)
Policy Synchronization (Hybrid)			X		
Shadow IT	X			X	X
Sanctioned App (2.5)					X
Data Protection on the Endpoint (DLPe)					X
McAfee® Client Proxy (MCP)		X	X	X	X
McAfee® Mobile Cloud Service			X	X	X
Content Security Reporter		X	X	X	X

All features are available for the on-premises McAfee ePO™ platform.
For MVISION ePO, MCP is available and DLPe on the roadmap



McAfee Confidential

Summary

How UCE Evolves Your Security Posture

Cloud-native architecture increases scale and resilience while lowering TCO

Prevent cloud-native breach attempts with unified incident management

Consistent data protection at the device, through the web, and within the cloud

Convergence of CASB, SWG, and DLP technologies reduces complexity

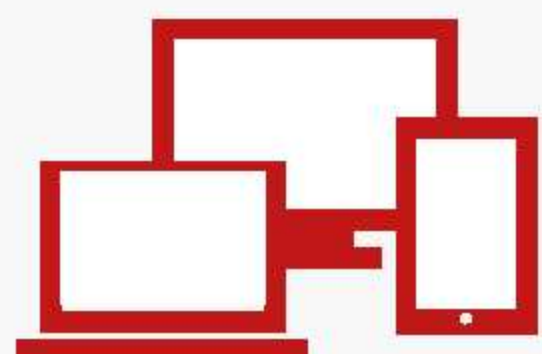
UCE

1

Protect Personal and/or Additional Corporate Device



Unmanaged



Managed



2

Secure Direct to Web Browsing



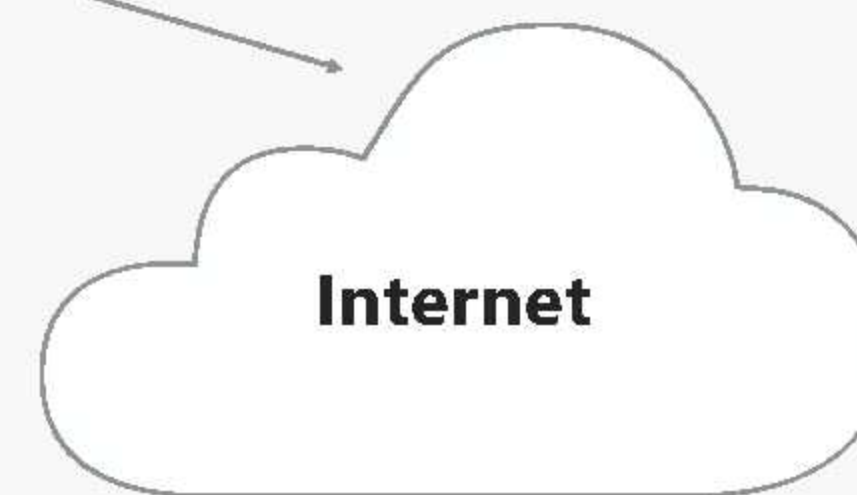
Web Gateway

3

Cloud Data Protection



SaaS



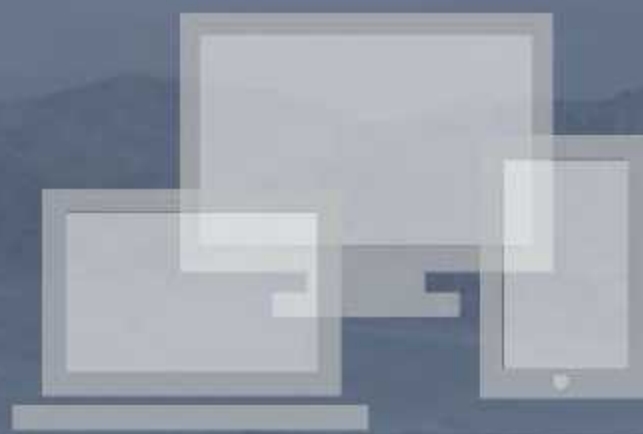
Internet



Why McAfee?

The McAfee Strategy

*To Protect Data and Defend Against Threats where
Modern Work Gets Done: **On Devices and in the Cloud***



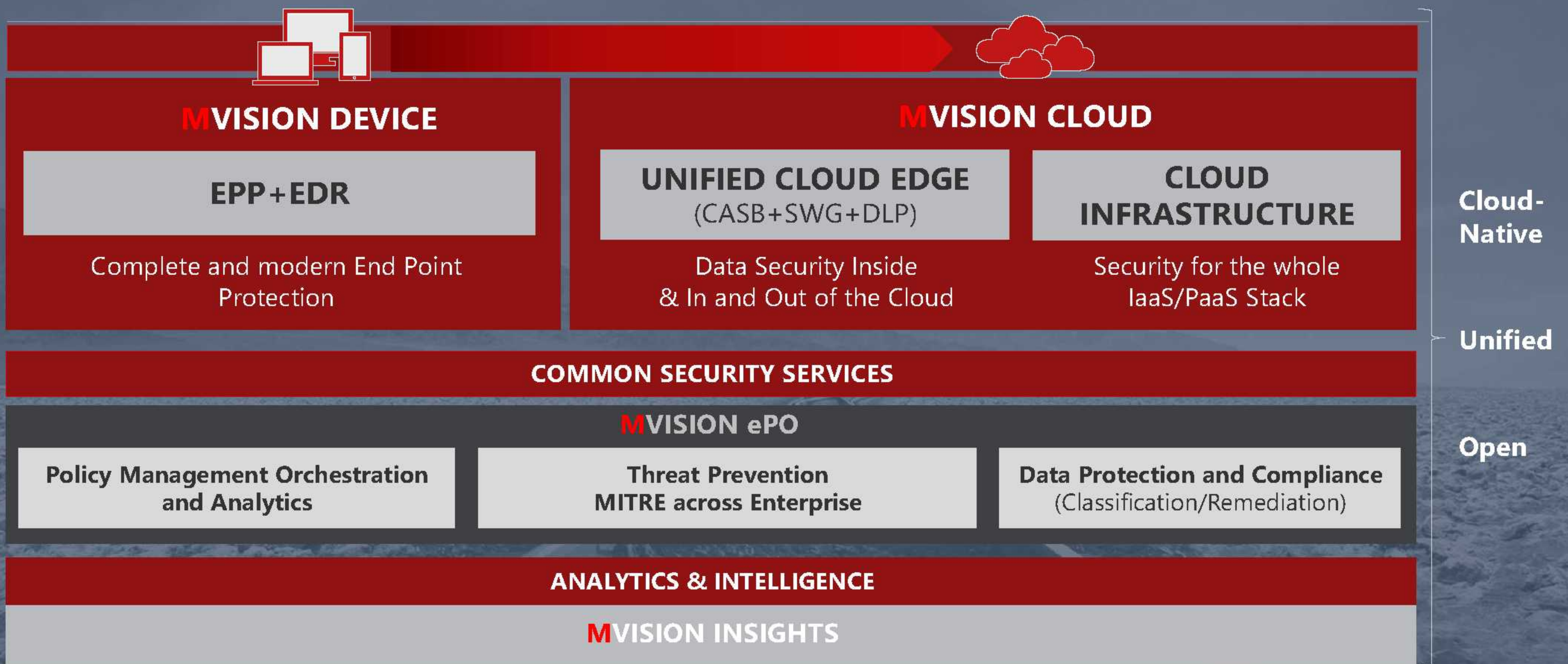
Device

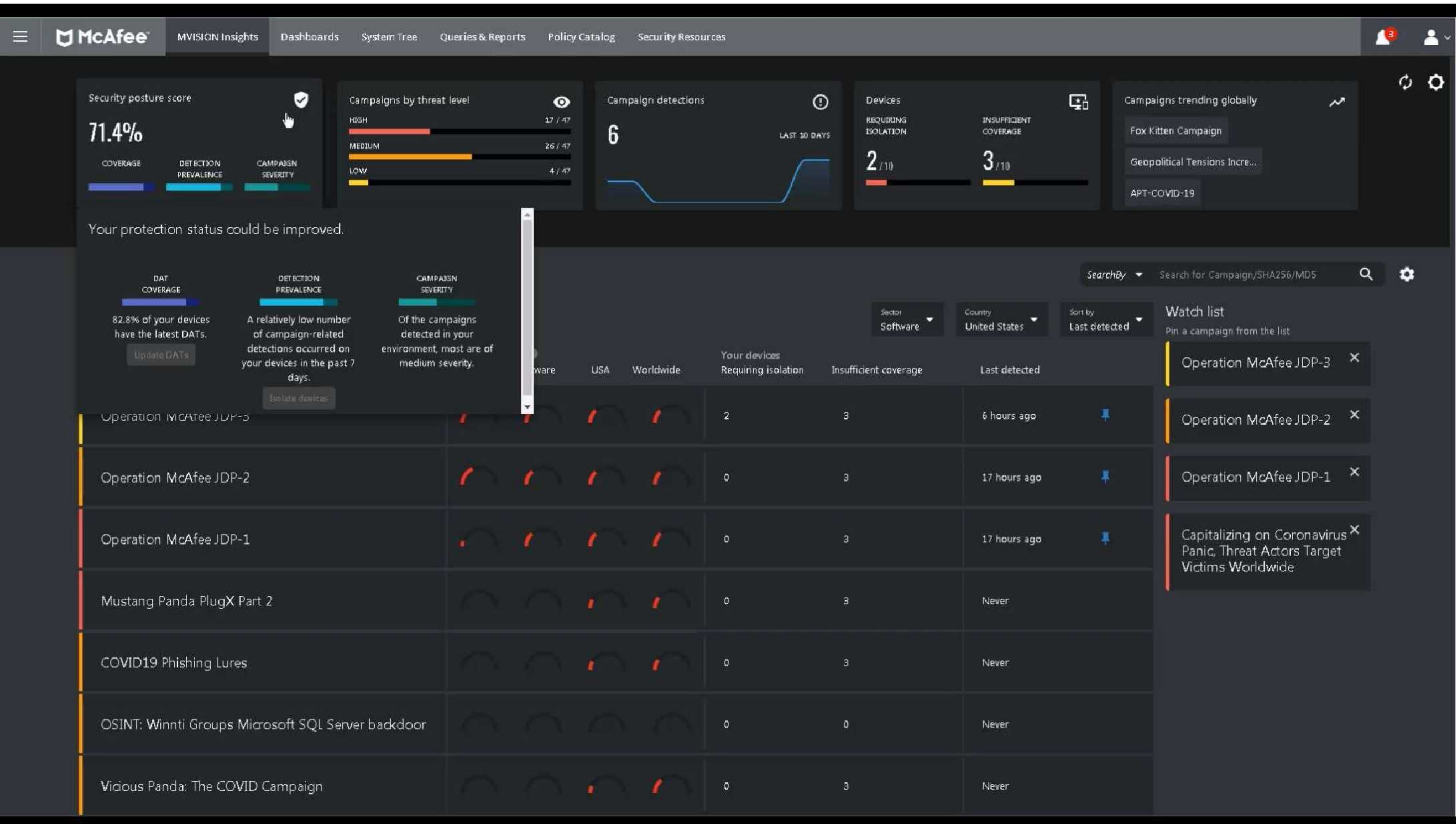


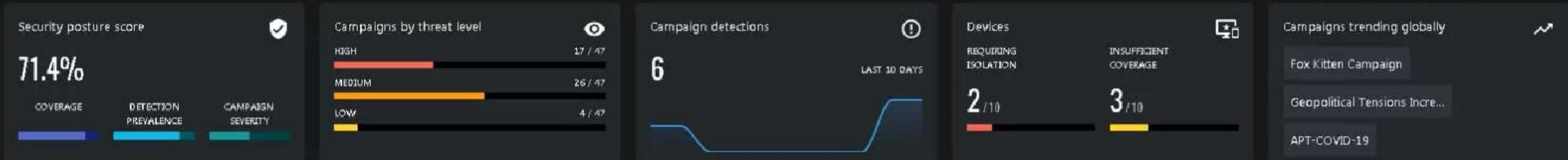
Cloud



McAfee Device-to-Cloud Security Platform







Campaigns > Geopolitical Tensions Increase Risk of Attacks

Overview Your environment

SearchBy Search for Campaign/SHA256/MD5

Description

Government backed cyber threat groups have been known to attack multiple sectors to deliver a range of malware including Shamoon, Dustman, and ZeroClear. The malicious software is used to perform multiple actions including disk/content wiping and service disruption. Various adversaries have been linked to similar attacks in the past including OilRig, APT34, MuddyWater, APT39, and Chafer.

Campaign severity

High

Aliases

-

Possible associations

-

Sources

https://kc.mcafee.com/corporate/index?page=content&id=KB92498

Min DAT Version

3983

Last detected

-



Infection rate comparison

Infection rate is the number of infected devices/total devices scaled over 10-100. An infected device has at least one campaign-related detection. Compare your infection rate against a selected sector and country.

Your organization

0

Sector

Software

0

Country

United States

23.6

Last 7 days

Associated Indicators (25)

905e3f74e5dcca58cf6bb3afaec88a3d6cb7529b6e4974e417b2c8392929148 20ec56029ec2dc6a0f86d172f12914d078fc679a8d01257394864413d01d7eda

Campaigns

SearchBy Search for Campaign/SHA256/MD5

Requiring attention (27) All campaigns (47)

Sector Software Country United States Sort by Last detected

Watch list






Pin a campaign from the list

Operation McAfee JDP-3

Operation McAfee JDP-2

Operation McAfee JDP-1

Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide

Campaign	Infection rate ⓘ				Your devices	Insufficient coverage	Last detected
	You	Software	USA	Worldwide	Requiring isolation		
Operation McAfee JDP-3	<div><div></div><div></div><div></div><div></div></div>				2	3	6 hours ago  
<div>Description</div> <div>This is a synthetic campaign created solely for the purpose of demonstrating the capabilities and use-cases of Insights to JDP-subscribed customers.</div> <div>Campaign severity</div> <div>Low</div> <div>Associated Indicators</div> <div><div>a4e5cfbeedb7f8be6a2efafb521bbc555e753225efa4380976fd5c6ea6bc9...</div><div>927efaa4a07a20773b5ce9a57eeca16ad44be6139aaa608465236391eb64...</div><div>e6c116f572abd074fea209f39cf9860945d5d229b2d0e361e13cbd0352df6...</div><div>3291ae00e69aaefdb7fe929433c324475c470004a2b842d6b463b992451f...</div><div>90c3a0505112e72ee527981fc8d71f4069350d9abd9bfec87471bbae3608...</div></div> <div>+ 3 more</div>	<div>Impact details</div> <div>Campaign is targeting you with an unusually high aggression when compared to others.</div> <div>Global prevalence</div> <div>Spain, United States</div> <div></div>	<div>Detections</div> <div>Status</div> <div>Unresolved</div> <div>Resolved</div> <div>Content package</div> <div>DAT Version</div> <div>4050.0</div> <div>3952.0</div> <div># of detections</div> <div>13</div> <div>10</div> <div># of devices</div> <div>2</div> <div>3</div> <div>7</div> <div>3</div> <div>Isolate devices</div> <div>Update DATs</div>					
Operation McAfee JDP-2	<div><div></div><div></div><div></div><div></div></div>				0	3	17 hours ago 
Operation McAfee JDP-1	<div><div></div><div></div><div></div><div></div></div>				0	3	17 hours ago 
Mustang Panda PlugX Part 2	<div><div></div><div></div><div></div><div></div></div>				0	3	Never

View Details



Campaigns > Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide

SearchBy Search for Campaign/SHA256/MD5 🔍 ⚙️

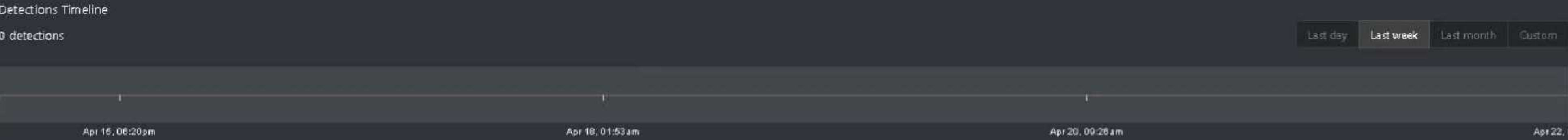
Overview

Your environment

Devices requiring isolation

0 of 10

0 unresolved detections on 0 devices.
3 devices have insufficient coverage to protect against this campaign.



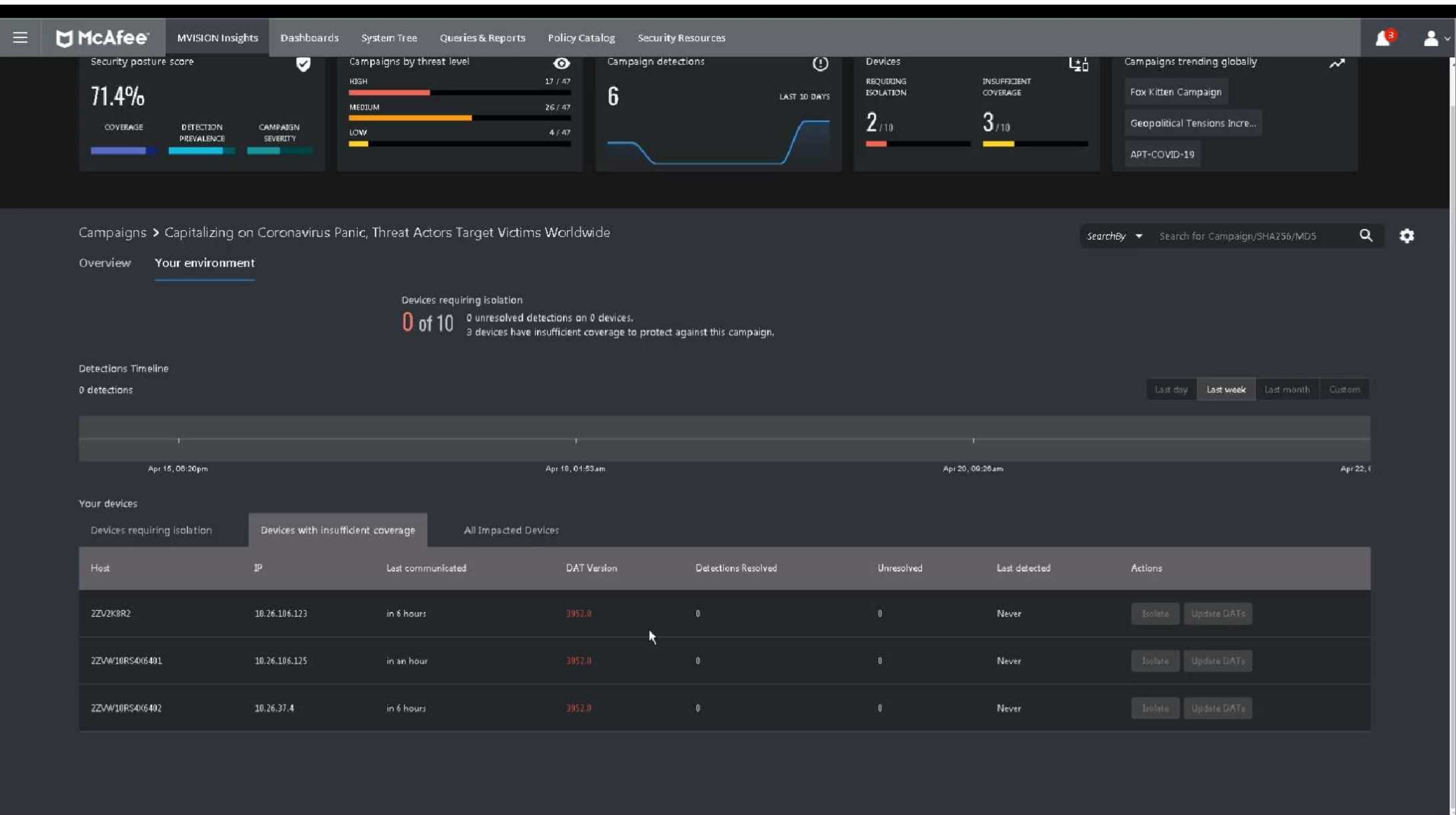
Your devices

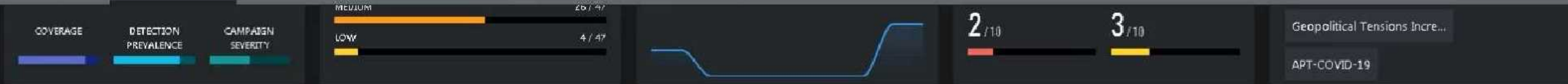
Devices requiring isolation

Devices with insufficient coverage

All Impacted Devices

Host	IP	Last communicated	DAT Version	Detections Resolved	Unresolved	Last detected	Actions
------	----	-------------------	-------------	---------------------	------------	---------------	---------





Campaigns > COVID19 Phishing Lures

SearchBy

Search for Campaign/SHA256/MD5

🔍

⚙️

Overview Your environment

Description

The Mustang Panda threat group is suspected to be behind a phishing campaign targeted toward users in Taiwan using the corona virus pandemic as the lure. Multiple techniques were used by the actor including creating a registry run key for persistence and domain fronting for command and control server communication.

Campaign severity

Medium

Aliases

-

Possible associations

-

Sources

<https://kc.mcafee.com/corporate/index?page=content&id=KB92635>

Min DAT Version

4015

Last detected

-

Global prevalence



Observed countries

United States Ukraine Spain

Observed sectors

-

Infection rate comparison

Infection rate is the number of infected devices/total devices scaled over 10-100. An infected device has at least one campaign-related detection. Compare your infection rate against a selected sector and country.

Your organization 0

Sector Software 0

Country United States 16

Last 7 days



Associated Indicators (2)

abeb1e2f027317a8d343acd03fadbbfb8362452489db734910a5189c0bb1cec2

f4e018db439526b3e836b505813e7dfd90221b59a53428bd4c68b678e7ed55d5

Be Resilient

Find information about COVID-19 at the official sites of the World Health Organization (WHO) , or the Department of Health (DOH)

<https://www.who.int/>

<https://www.doh.gov.ph/>



Be Resilient

Ensure Anti-Virus / Endpoint
Protection up to Date (For all
Devices)



Be Resilient

- Avoid using public wifi.
- Secure your home network
- When working, use VPN virtual private network.
- It can help protect the data you send and receive while you work from home. A VPN can provide a secure link between employees and businesses by encrypting data.
- Secure your home Wi-Fi with a strong password, in case VPN isn't an option or if it fails for some reason.

A man and a woman in business attire are looking at a tablet together in a modern office setting. The woman is pointing at the screen. The background shows large windows and a blurred office interior.

Be Resilient

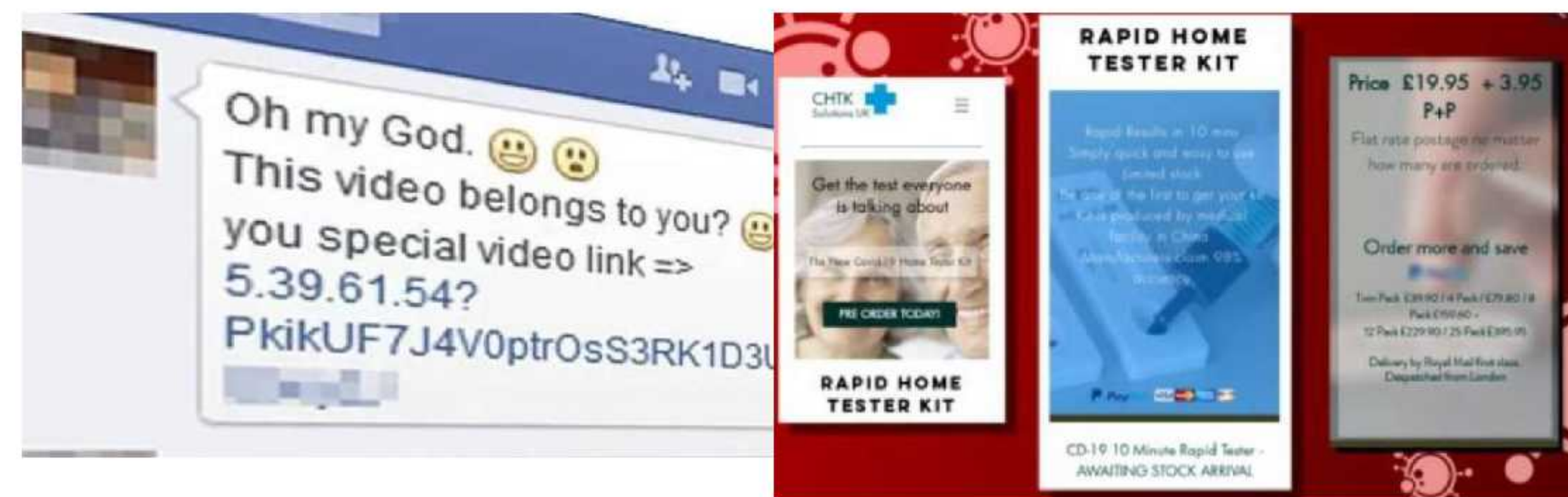
- Separate work and personal device.
- Carve out boundaries between work life and home life while working from home.

Be Resilient

- Exercise caution when providing personal information.
- Do not download or open email attachments from unknown senders. These could contain viruses and other malware.

Be Resilient

- Do not click on links in social media messages, even if they are from someone you know. Your contacts' accounts may have compromised.
- Do not click on ads or social media posts regarding COVID-19. They may be fake and contain malicious content.



Thank you!



Learn more at mcafee.com/unifiedcloud

McAfee, the McAfee logo, and MVISION are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the U.S. and/or other countries. Other names and brands may be claimed as the property of others. McAfee technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. No computer system can be absolutely secure.

Copyright © 2020 McAfee LLC.

External Facing Information / Public



To inquire, please call or email:

+63 2 8858 5555 / +63 2 7625 5900 • sales@wsiphil.com.ph

Metro Manila WSI Corporate Center, 1005 Metropolitan Avenue, Makati City, Philippines 1205 • Fax +63 2 8858 5511
Cebu 38 V. Sotto Street, Brgy. Tinago, Cebu City • Tel +63 32 255 1012 to 14 • Fax +63 32 255 1011
Davao Unit 11 Plug Holdings Bldg. 141 R. Castillo Street Agdao, Davao City 8000 • Tel +63 82 284 0098 • Fax +63 82 300 7463

