
SWS COMPUTERSYSTEME AG
Cisco Security für Microsoft 365
Schützen Sie Ihre Microsoft 365 E-Mails vor komplexen Bedrohungen

Ihre Referenten

Hans-Martin.Kuhn@sws.de
Senior Security Consultant

Lukas.Schwarzfischer@sws.de
System Engineer

Agenda

- Überblick
- Bedrohungslage
- M365 E-Mail Portfolio
- Cisco E-Mail Portfolio
  - Cloud Mailbox Defense
  - Cloud Email Security
  - Secure Access by DUO

Überblick

Microsoft O365 Networking Best Practices

- All offices of your organization should have local Internet connections.
- Each local Internet connection should be using a regionally local DNS server for outbound Internet traffic from that location.
- Whenever possible, configure your edge routers to send trusted Microsoft O365 traffic directly, instead of proxying or tunneling through a gateway.
- Configure your edge devices to forward traffic without processing. This is known as traffic bypass.

Sender Policy Framework (SPF)

- Allows recipients to verify sender IP addresses by looking up DNS (TXT) records listing authorized Mail Gateways for a domain. (RFC7208)
- What does an SPF record look like?

```
$dig TXT pipershark.com +short
"v=spf1 ip4:139.138.32.156 ip4:139.138.56.31 include:mailgun.org -all"
```

Version

Verification Mechanisms

- The record is evaluated in order from right to left, checks all mechanisms until it either passes one or fails all checks.
- The “all” setting is traditional at the end, handling anything that did not match the rest.

Domain Keys Identified Mail (DKIM)

- Specifies methods for gateway-based cryptographic signing of outgoing messages, embedding verification data in an e-mail header, and ways for recipients to verify integrity of the messages
- Uses DNS TXT records to publish public keys
- DKIM Signatures (RFC5585 + RFC6376)
- DKIM Development, Deployment and Operation (RFC5863)
- Author Domain Signing Practices (ADSP)(RFC561)

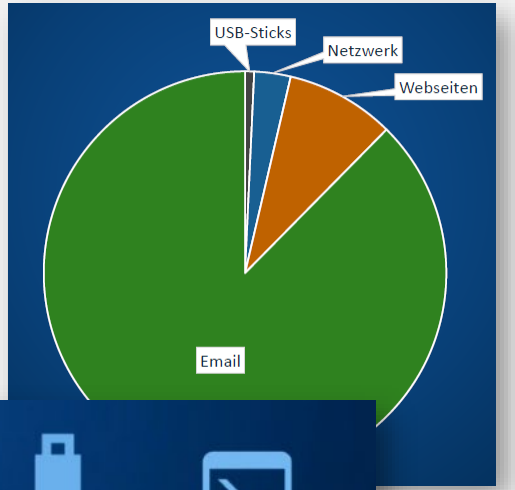
Domain-based Message Authentication, Reporting And Conformance (DMARC)

- Both DKIM and SPF have shortcomings, not because of bad design, but because of different nature of each technology... (enter)... DMARC (RFC7489)!
- Leveraging great existing technologies, providing a glue to keep them in sync, and allowing **senders** to mandate rejection policies and have visibility of offending traffic
  - Provides:
    - SPF authentication
    - DKIM verification
    - **Synchronization between all sender identities (Envelope From, Header From)**
    - Reporting back to the spoofed entity

Bedrohungslage

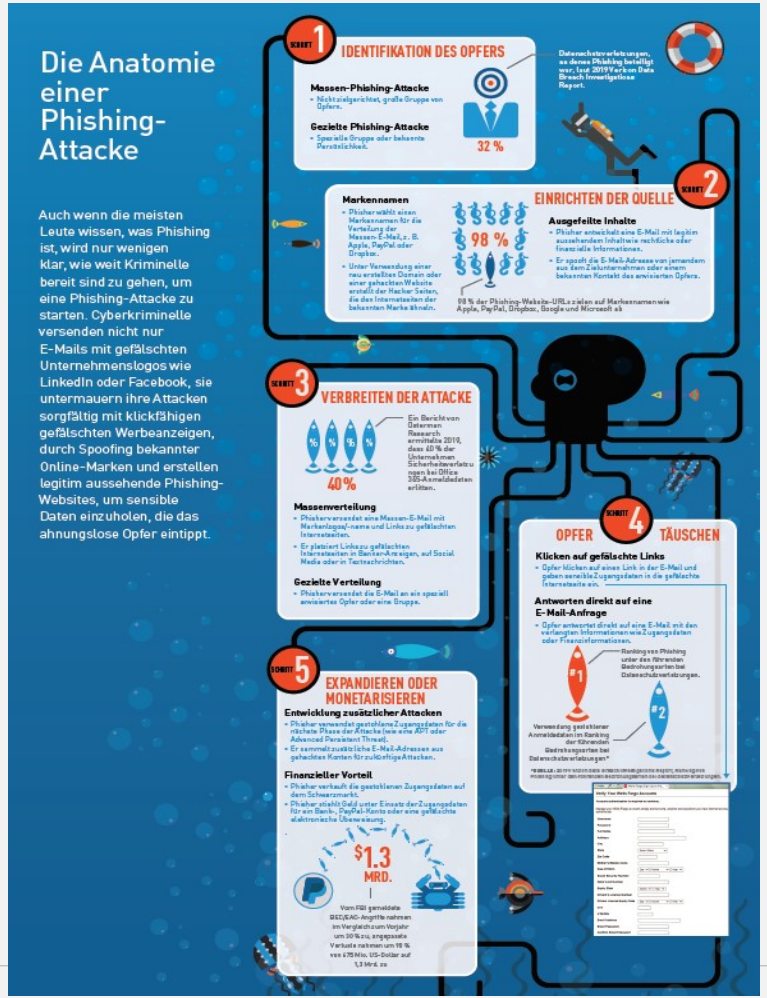
Bedrohungen

- Malware / Ransomware / APTs
  - Mail
  - Websites
  - Netzwerk
  - Wechseldatenträger



Quelle: Sophos

Infiltration mithilfe von Panikmache – Stellen Sie sich vor, Sie sind ein Mitarbeiter der mittleren Führungsebene eines kleinen bis mittelgroßen Unternehmens und finden plötzlich eine E-Mail in Ihrem Postfach, in der Ihnen mitgeteilt wird, dass Ihr Office 365-Unternehmenskonto kurzzeitig suspendiert ist, weil Ihr Passwort abgelaufen ist und Ihre E-Mail-Adresse wieder aktiviert werden muss. Sie klicken auf den Link und gelangen dadurch auf ein Internetformular auf einer Website, die die Microsoft Office 365-Site zu sein scheint. Sie werden aufgefordert, Ihre Unternehmens-E-Mail-Adresse und Ihr aktuelles Passwort sowie personenbezogene Informationen wie Firmennamen und Titel anzugeben, um das Konto wieder zu aktivieren.

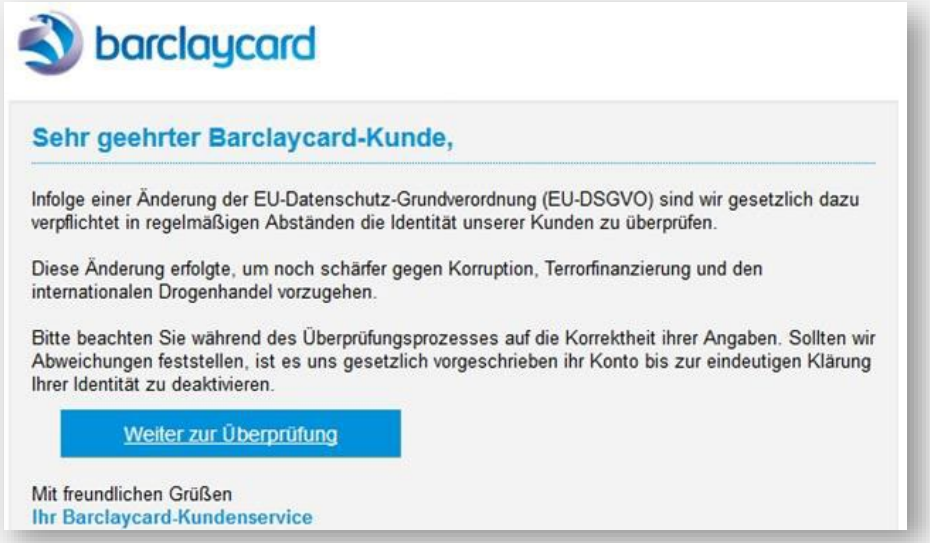


Quelle: Heiseonline

„ 365 ist eine beliebte Zielscheibe für Cyberkriminelle. Die Office-Lösung ist nicht nur weit verbreitet und wird immer beliebter, ihre Standard-Security-Vorkehrungen lassen sich auch relativ leicht knacken. Haben die Angreifer erst einmal das Secure E-Mail Gateway (SEG) überwunden, steht ihnen der Weg zu Account Übernahme, Datendiebstahl und Betrug offen.“ (Quelle Heiseonline)

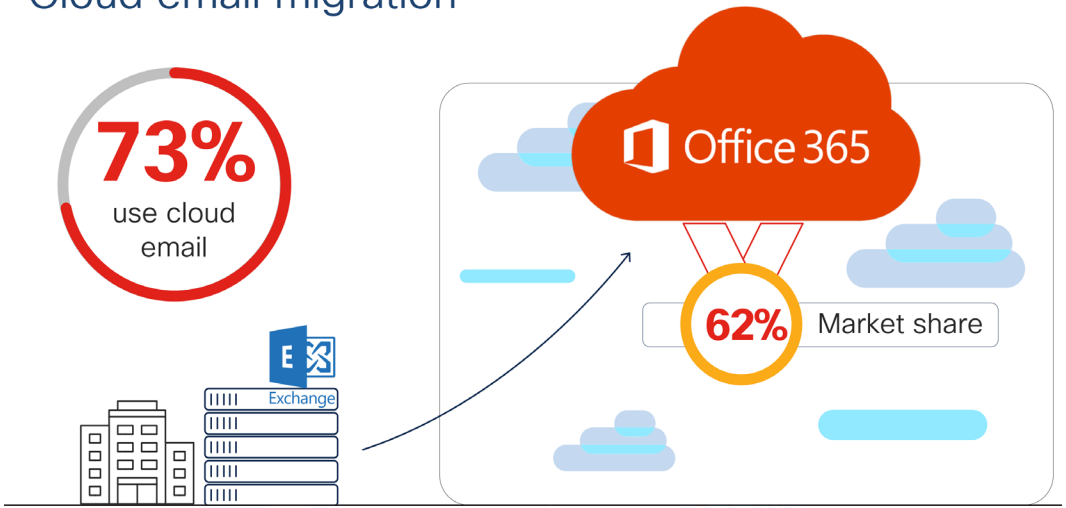
Bedrohungen

- Malware gelangt ins Unternehmen über



Phishing E-Mails

Cloud email migration



Headline Grabbing Misses

A quarter of phishing emails bypass Office 365 security

By Ian Barker | Published 1 year ago | Follow @IanDBarker

https://betanews.com/2019/04/10/phishing-emails-bypass-office-365-security/

Hackers target Office 365 business accounts

By Anthony Spadafora May 03, 2019

Account takeover attacks are on the rise

https://www.techradar.com/au/news/hackers-target-office-365-business-accounts

Business Email Attacks on the Rise; Office 365 Users Hardest Hit: Beazley

July 31, 2018

Email This | Subscribe to Newsletter

https://www.insurancejournal.com/news/national/2018/07/31/496500.htm

200M+ Users At Risk: New Malicious .slk Files Are Bypassing Microsoft 365 Security

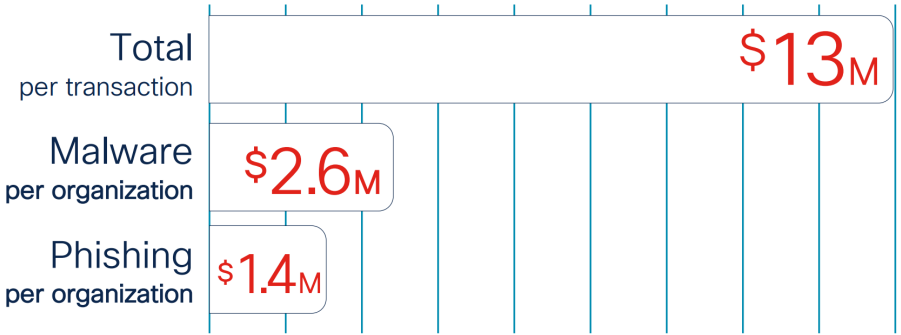
By Avanan's Security June 26, 2020 3408 0

https://www.avanan.com/blog/sylkin-attack-bypassing-microsoft-365-security-risking-users

The number one threat vector

$1.2 Billion in losses to BEC in 2018[1]

$125,439 average per transaction[1]



Office365

is the second most targeted brand in phishing attacks[2]

1 FBI IDC Report 2019
2 Openphish

Attackers use multiple ways to get in

Business Email Compromise (BEC)

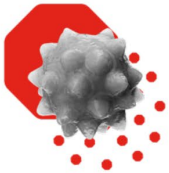
Estimated exposed losses due to BEC between 2016 and 2019 totaled $26 billion.[1]

Ransomware

Predicted to hit $20 billion in 2021[2]

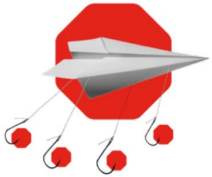
Domain Compromise

54% of legitimate domains used in phishing campaigns[3]



Malware

10.52 billion malware attacks in 2018[4]



Phishing

27% of data breaches in 2019 involved the theft of credentials such as logins or encryption keys[5]

On February 26, 2020...

Companies have lost $26 billion to email wire fraud since 2016

"This morning I wired $388,000 into a false bank account in Asia."

– "Shark Tank" star Barbara Corcoran

"People influence security more than technology or policy and cybercriminals know how to exploit human behaviors"

Gartner

Magic Quadrant for Security Awareness Computer-based Training report

Top 3 Attacks: Advanced Phishing

"52% of breaches featured hacking, 28% involved malware and 32–33% included phishing or social engineering, respectively."

– Verizon 2019 Data Breach Investigations Report

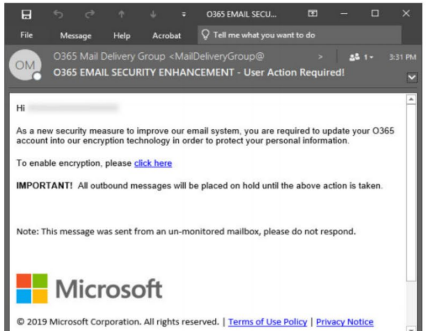
"Over 3.4 billion email scams or phishing emails are sent every day. This adds up to one trillion email scams per year"

– Security Magazine (June 11, 2019)

Office365

is the second most targeted brand in phishing attacks

OpenPhish



Top 3 Attacks: Account Takeover

- Office 365 account takeover through credential phishing is one of the top three most common email threats, but creates many other follow on attacks
  - Targeted phishing attacks sent from a valid email account
  - Very dangerous BEC messages sent form an internal email account
  - Compromise of the user's contacts
  - Hijacking legitimate email threads, i.e. Valak

- *Attackers are actively distributing the Valak malware family around the globe, with enterprises, in particular, being targeted.*
- *These campaigns make use of existing email threads from compromised accounts to greatly increase success.*
- *The overwhelming majority of campaigns occurred over the last couple of months and targeted organizations in the financial, manufacturing, health care and insurance verticals.*
- *Valak is a modular information-stealer*

Top 3 Attacks: BEC

- Most BEC occurs in low-volume campaigns, averaging approx. 10 to 20 messages per day
- Almost all BEC messages come from free webmail services, led by Gmail, Yahoo, Hotmail, Comcast, Zoho, Yandex, Outlook.com and Spectrum/Time Warner cable
- 84% do not bother to spoof the domain in the 'from' field
- Evolved across many trends from encouraging wire transfers to gift card purchases to most recently payroll changes

Privileged Access Management	CARTA-Inspired Vulnerability Management	Detection and Response	Cloud Security Posture Management	Cloud Access Security Broker
Business Email Compromise	Dark Data Discovery	Security Incident Response	Container Security	Security Ratings Services

Gartner: Top 10 Security Projects for 2019

cisco Live!

Email Priorities

ESG Survey across US & Canada

ESG Enterprise Strategy Group

APRIL 2020

MOST IMPORTANT EMAIL SECURITY PRIORITIES OVER THE NEXT 12-18 MONTHS

- **27%** Phishing detection and prevention
- **22%** End-user training
- **22%** Email encryption services
- **21%** Ransomware/extortion protection
- **21%** Improved spam/malware filtering

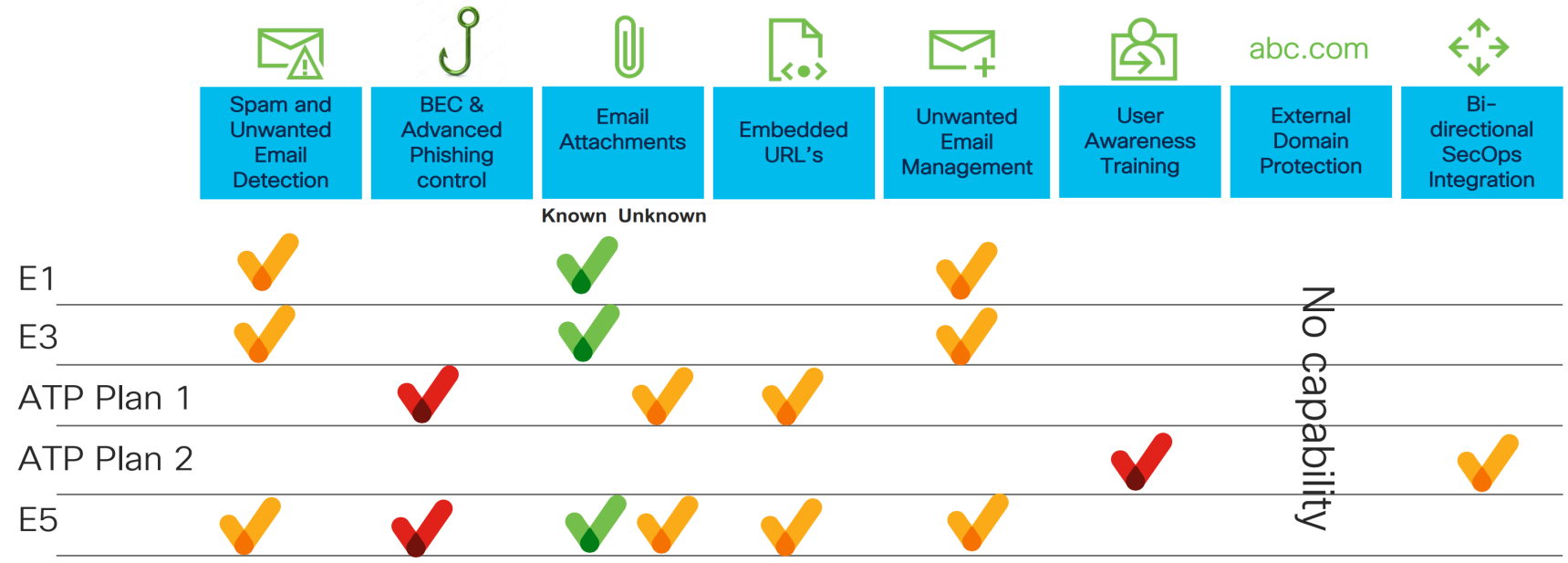
cisco Live!

Email Security Recommendations in 2020

Spam and Unwanted Email Detection	BEC & Advanced Phishing control	Email Attachments	Embedded URL's	Quarantined Email Management	User Awareness Training	External Domain Protection	Bi-directional SecOps Integration
• Maximise connection filtering capabilities • Ensure solid combination of not only IP but also Domain Reputation filtering • Ensure checking of full DMARC scores to include SPF & DKIM	• Gateway based controls to detect 'known bad' • Non-gateway based AI based controls to identify 'known good' • Executive identification lists	• Known malware detection • Active content dis-arm & reconstruction • Unknown malware detection • Retrospective scanning combined with automated Remediation	• Domain reputation • Domain categorization • Advanced URL analysis by threat intelligence, sandboxing etc.	• Maximize connection filtering to minimize future management • End-user spam management for appropriate spam messages with regular digests	• Phishing simulation with closed loop integration to cyber education offerings to deliver just-in-time response to simulations	• Attain 100% DMARC compliance for all domains • Monitor DMARC reporting statistics for any unauthorized usage of your domains, externally	• Integration of external threat intelligence • Sending email log data to SIEM or other SecOPs tools • Creating SecOPs playbooks to automate incident response via API's with a central toolset

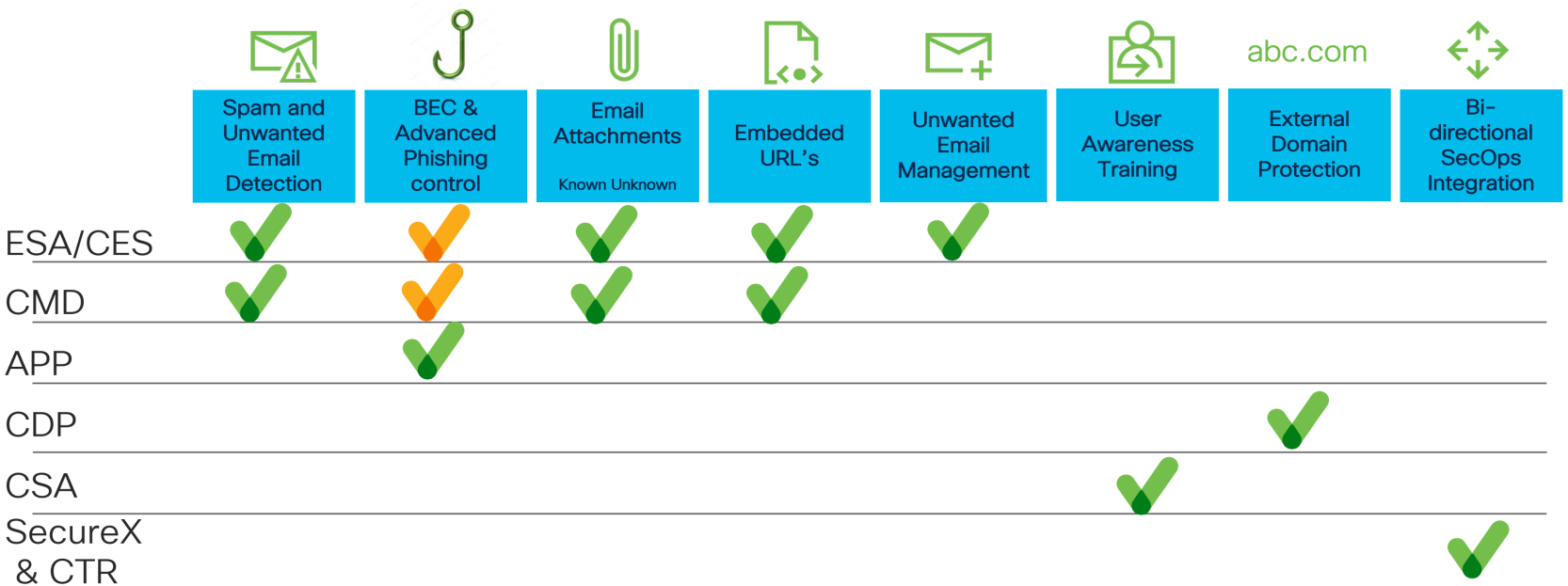
M365 E-Mail Portfolio

Office 365 Score Card

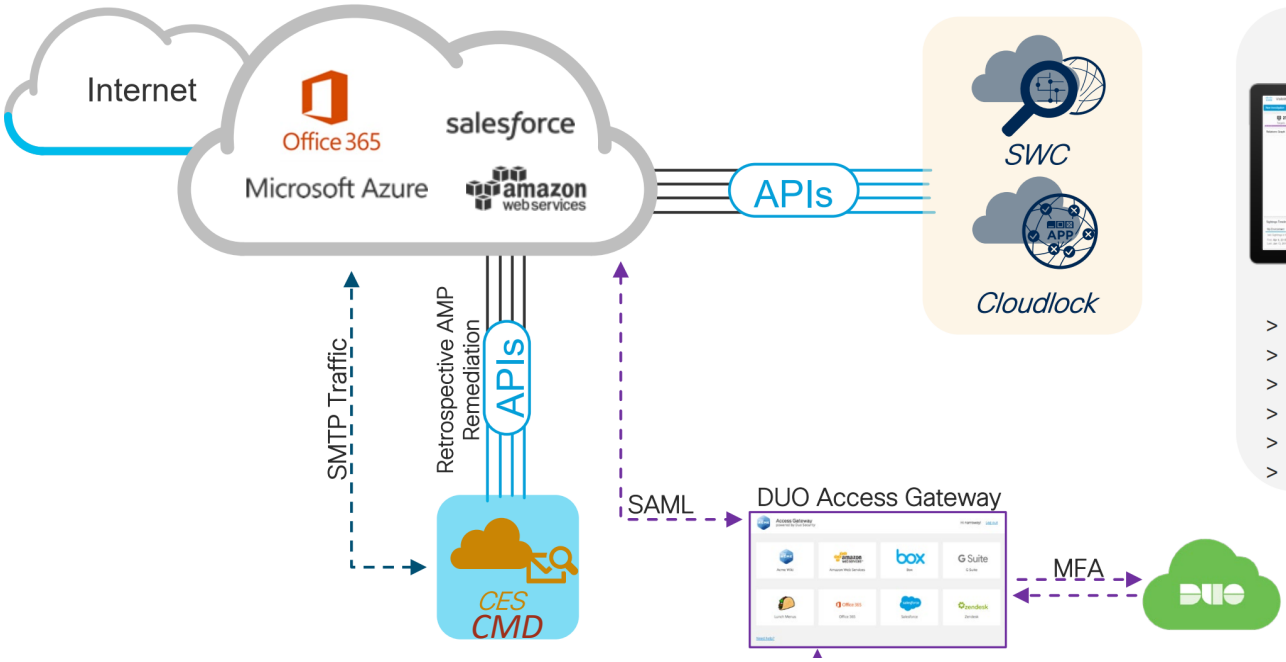


SWS COMPUTERSYSTEME
Member of ACP Group

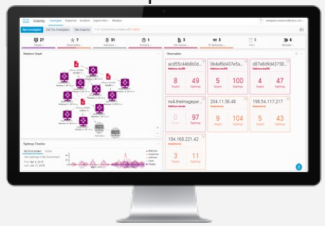
Cisco Score Card



Cisco E-Mail Portfolio



Cisco Threat Response



- > Umbrella
- > AMP(4E)
- > Threat Grid
- > FTD
- > CES / ESA
- > more!

1. Detect
2. Investigate
3. **Remediate**

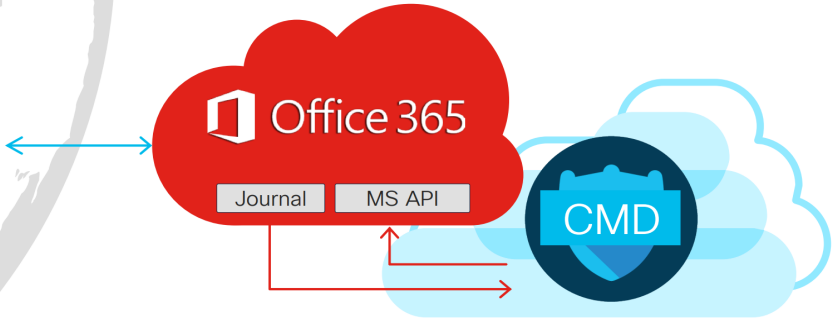
TALOS

- ✓ Umbrella and OpenDNS
- ✓ AMP(4E)
- ✓ Threat Grid
- ✓ FTD and Snort
- ✓ CES / ESA
- ✓ WSA
- ✓ Cloudlock
- ✓ Stealthwatch
- ✓ Cognitive

Gateway vs. CESS

Cloud Email Security (Gateway)

1. MX record changed to CES address
2. CES scans messages and takes an action
3. Message is delivered



Cloud Mailbox Defense (CESS)

1. MX record is unchanged
2. Copy of each message is sent to CMD
3. CMD scans and remediates using an API

Primary use-case

- Pure O365 deployments
- Additional security protections
  - Spam / Phishing / BEC
  - Malware
- Simplicity and ease-of-use
  - No tweaking
  - No mail flow changes

When to use a secure email gateway?

- Connection time filtering
- Per-user or group policies
- Custom message filters
- Quarantine options
- DLP integration
- On-premises or hybrid mailboxes

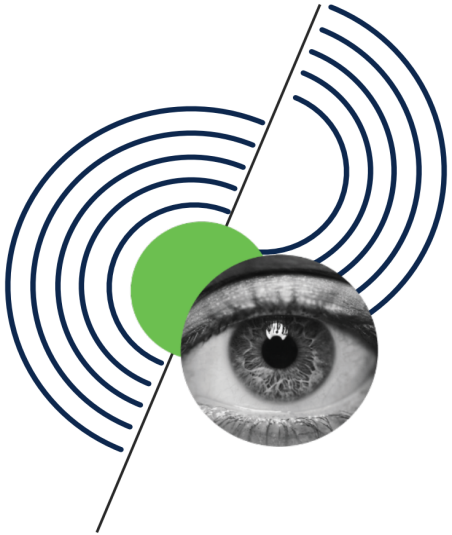
Superior threat intelligence from Cisco Talos

Visibility across all vectors from a best in class portfolio

TALOS

Automated Analysis

Specialized Tools



Daily Analysis

- 100TB of Data
- 1.5M Malware Samples
- 16 Billon Web Requests
- 600 Billion Emails

Telemetry Delivered

- Domain
- Network
- URL
- IP
- File
- Flow

What value does Talos bring to O365?

Main Source	Daily Amount	Type	Benefit to O365?
ESA/CES	600B	Email	Sender Domain Reputation, Phishing, BEC
UMB/OpenDNS	150B	DNS Request	Domain Reputation, Block Malicious Web
AMP	1.5M	Unique Malware	Malware Protection
WSA	16B	Web Request	Domain Reputation, Block Malicious Web
Cloudlock	300K	Cloud Apps	Risk Score on Shadow IT Apps
SW Cloud	~	Security Intelligence	Talos IP and Domain blacklist can be added to watchlist

Cisco Cloud Mailbox Defense

Primary use-case

- Pure O365 deployments
- Additional security protections
  - Spam / Phishing / BEC
  - Malware
- Simplicity and ease-of-use
  - No tweaking
  - No mail flow changes

Cloud Mailbox Defense

Cloud-native email security platform that focuses on

Simplicity

Visibility

Integration

Powered by Cisco Talos threat intelligence

Cloud Mailbox Defense

Simplicity

Deployment

- No MX record changes
- No change to mail flow
- Two-step process
- Fully functional in 5 minutes

Powered by Cisco Talos threat intelligence

Cloud Mailbox Defense

Simplicity

Deployment

Effective out-of-the-box

Configuration

One-page with minimal settings

No required add-ons

Powered by Cisco Talos threat intelligence

Cloud Mailbox Defense

Simplicity

Deployment

Configuration

Management

No specialized training

Point-and-shoot remediation

Easy search and triage

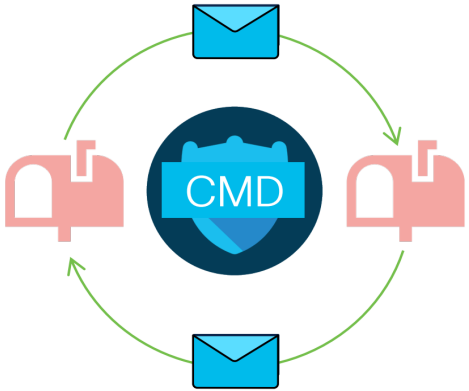
Powered by Cisco Talos threat intelligence

Cloud Mailbox Defense

Visibility

All messages...

even between internal users



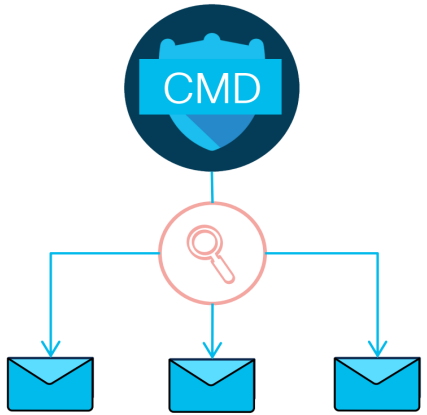
Powered by Cisco Talos threat intelligence

Cloud Mailbox Defense

Visibility

Every message at your fingertips

with lightening fast search



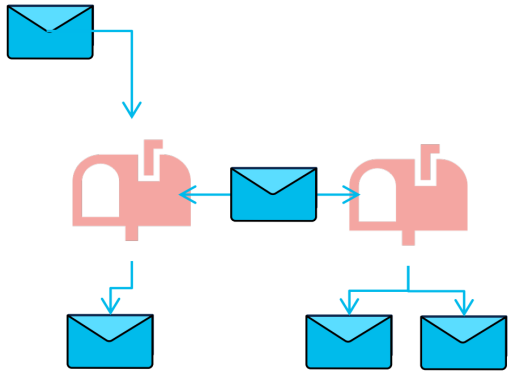
Powered by Cisco Talos threat intelligence

Cloud Mailbox Defense

Visibility

Understand the whole picture with

conversation view



Powered by Cisco Talos threat intelligence

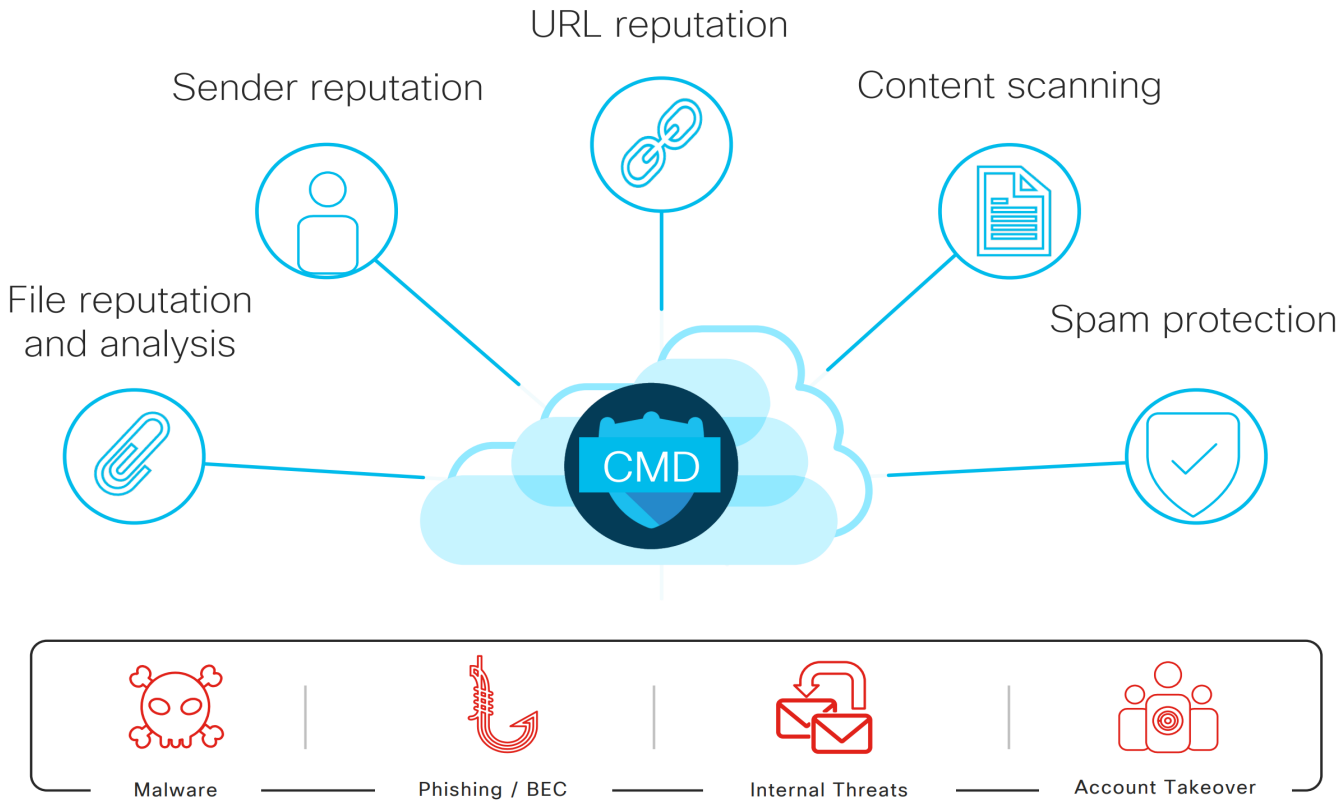
Cloud Mailbox Defense

Cisco Security inside Microsoft's Cloud

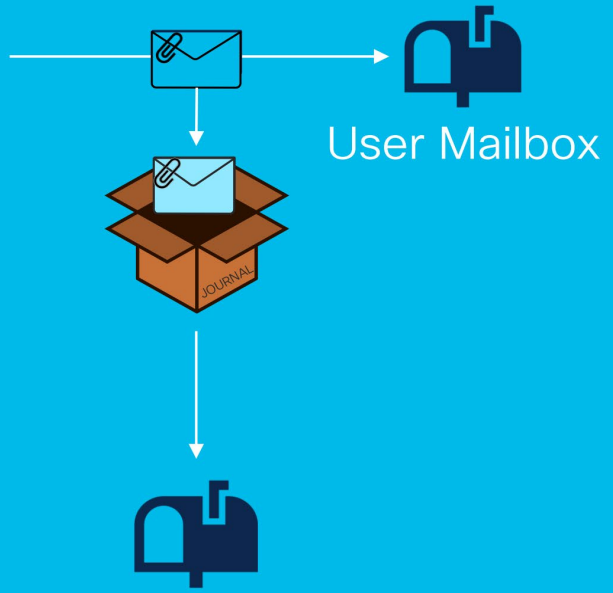
- No MX record changes
- Messages scanned in MS cloud
- Metadata sent to CMD
- Attachments stay in MS cloud[1]

Bringing Cisco threat intelligence as close to the mailbox as possible

[1]Cloud file analysis is optional


URL reputation
Sender reputation
Content scanning
File reputation and analysis
Spam protection
CMD
Malware
Phishing / BEC
Internal Threats
Account Takeover

Journaling

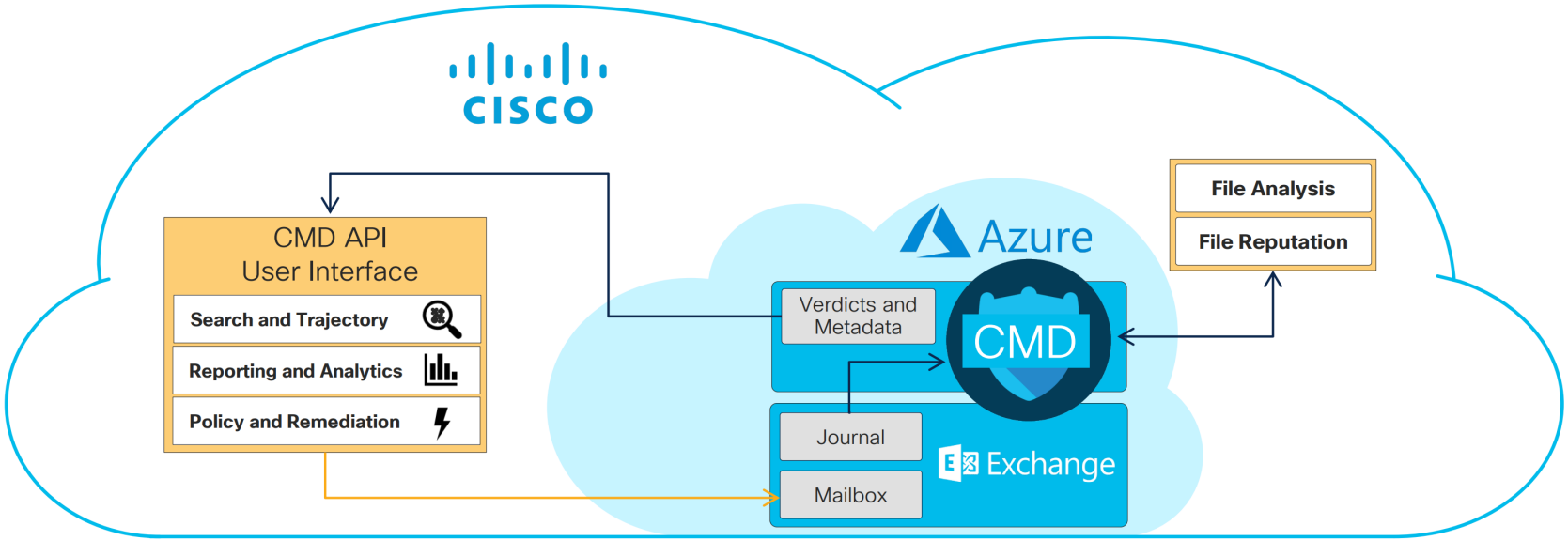


Invented for legal archiving and record retention

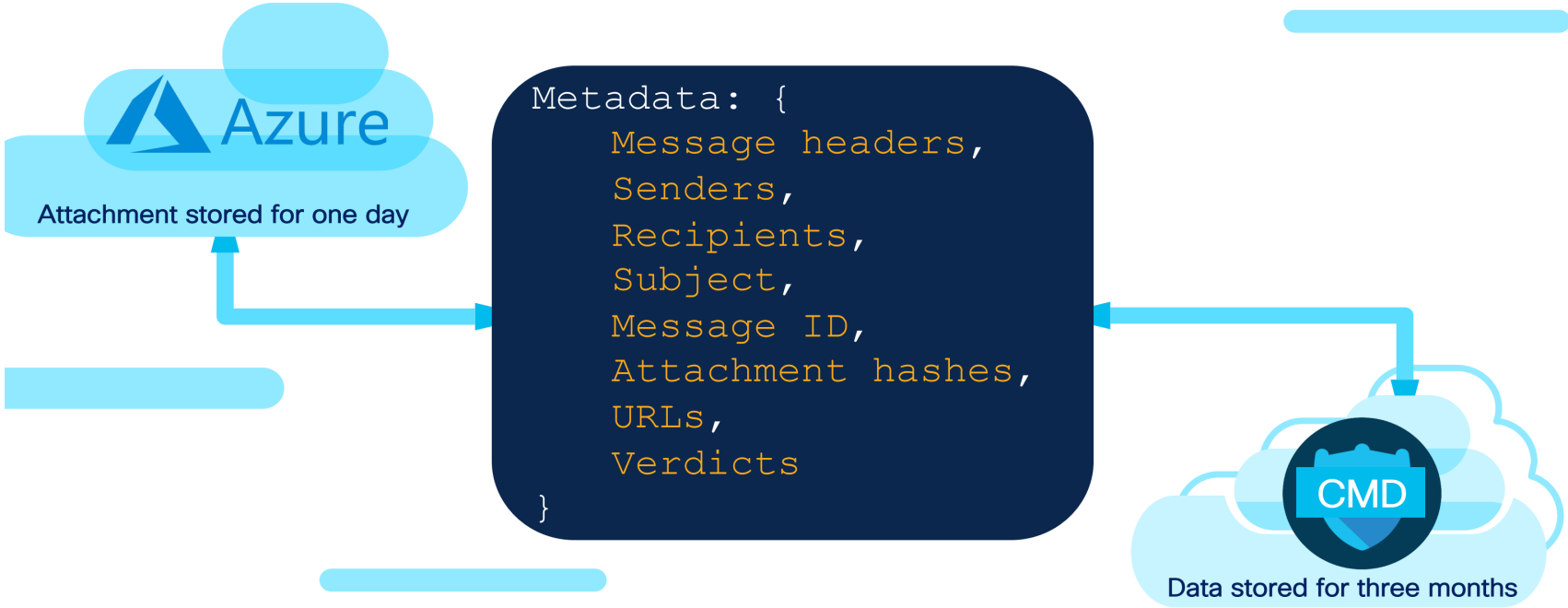
Creates a new copy of every message sent or received

Copy is sent to an external mailbox with all the original headers intact

A true multi-cloud solution



Metadata indexed in CMD



Cisco Cloud Email Security

Cisco Email Security: deployment options

http://cs.co/9009DdIRN

Cloud

Dedicated email security deployments in multiple resilient Cisco data centers provide the highest levels of service availability and data protection

On-premises

The Cisco Email Security Appliance is a gateway typically deployed in a network edge outside the firewall (the so - called demilitarized zone)

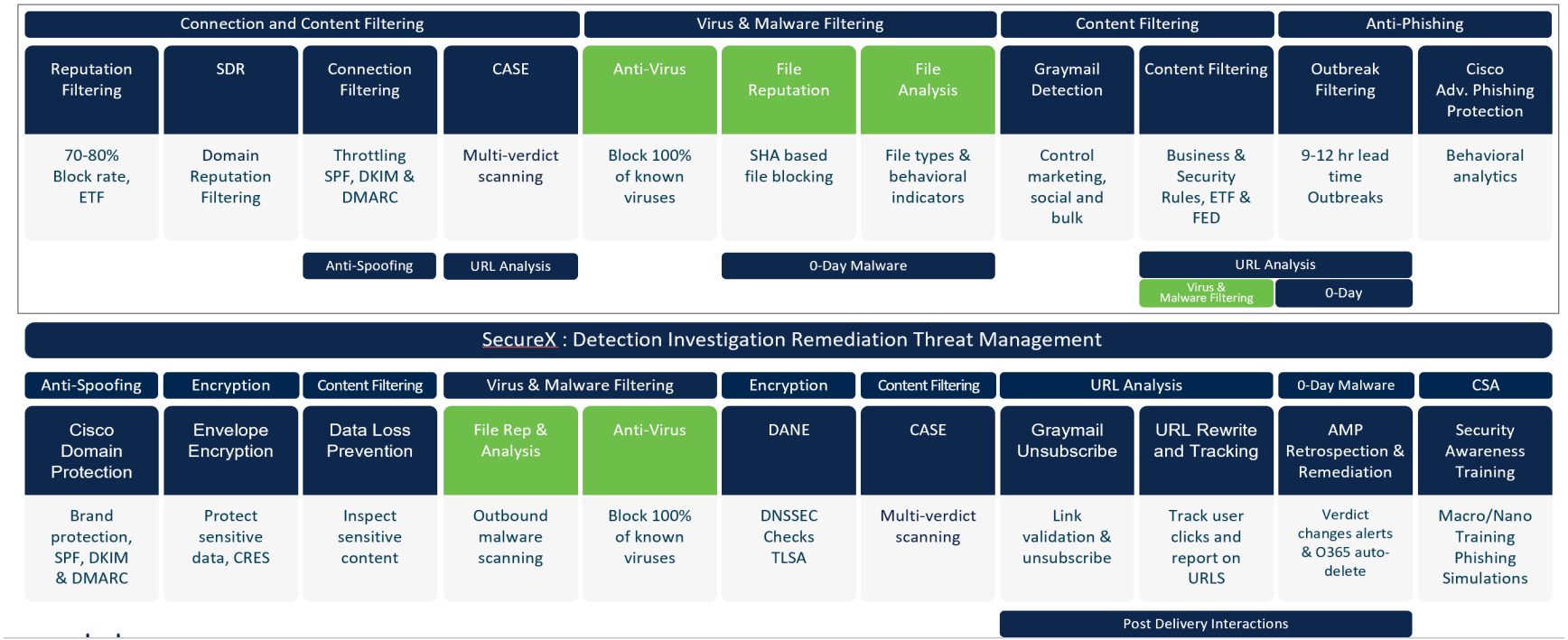
Virtual

A software version of the physical appliance runs on top of a VMware ESXi hypervisor and Cisco Unified Computing System™ (Cisco UCS®) servers

Hybrid

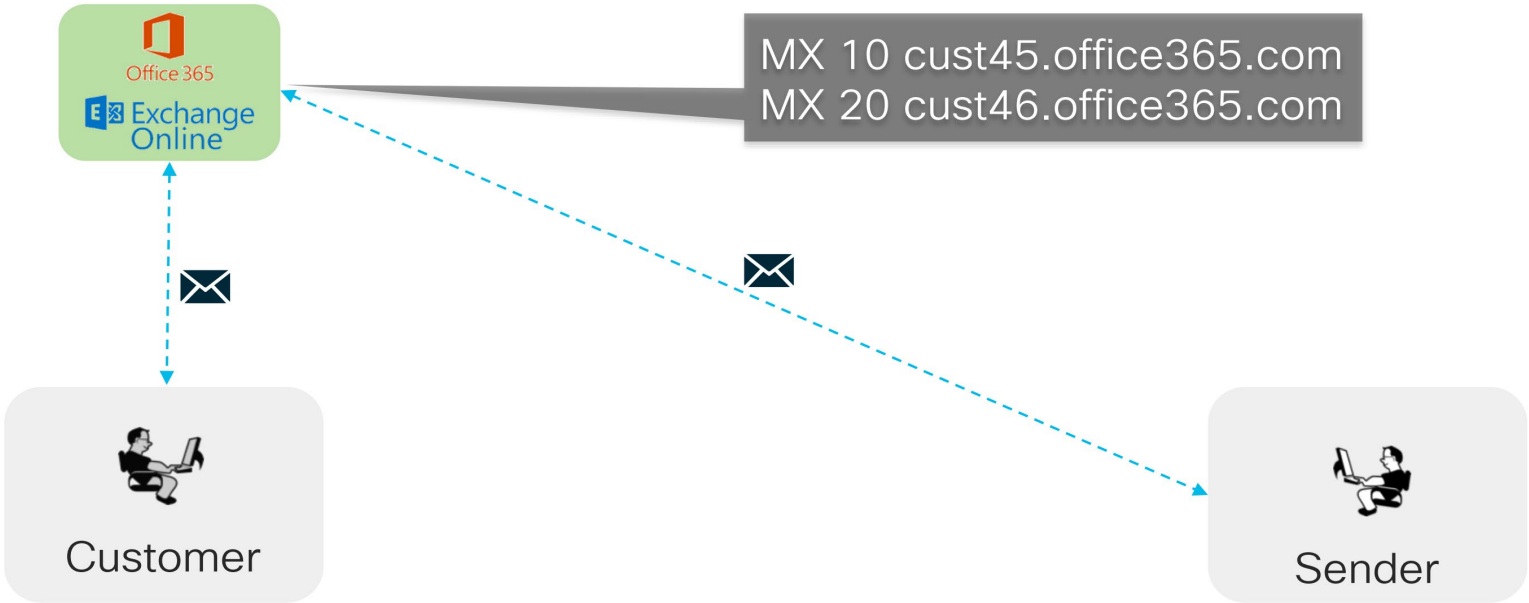
With Cisco Email Security in the cloud Run on-premises and virtual Cisco Email Security in the same deployment

Cisco Email Security: strengthening the email pipeline

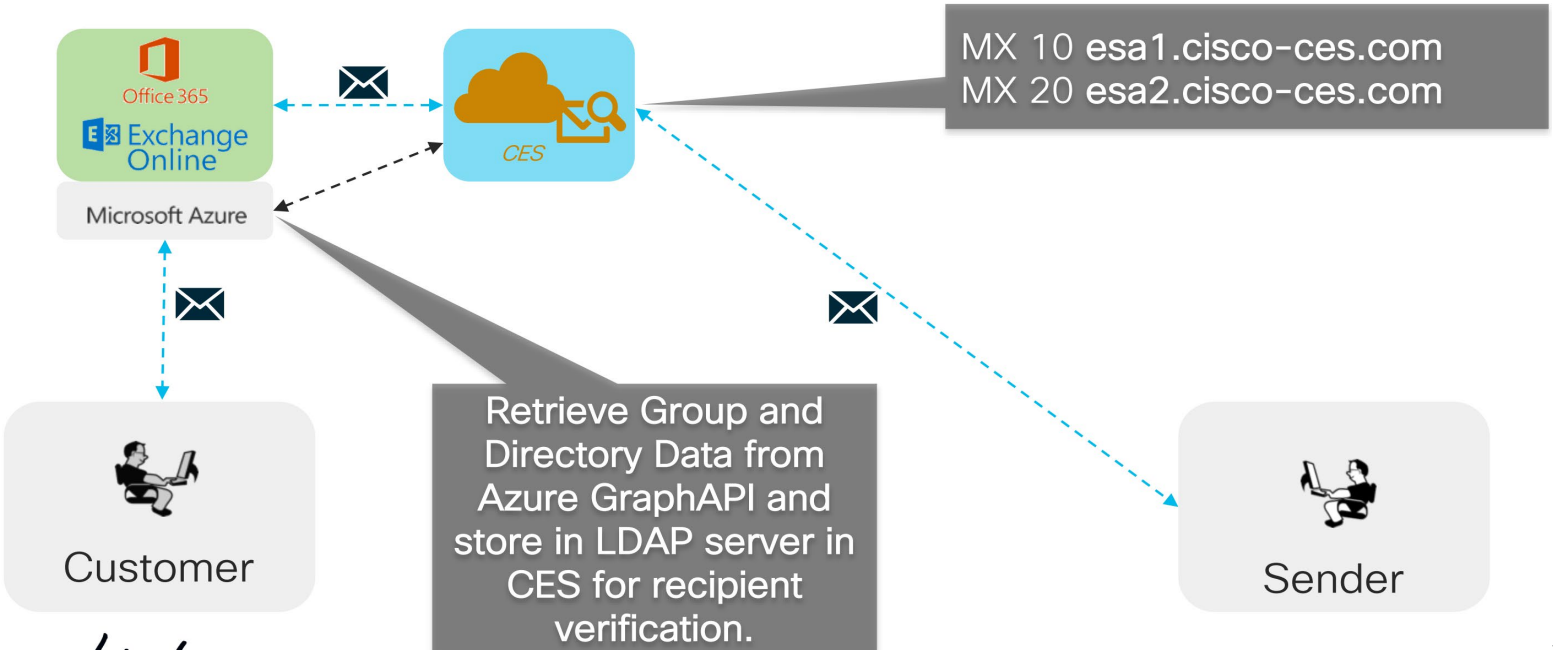


Microsoft O365 E3 licenses	Cisco CES Premium licenses
	Sender Base Reputation
	Sender Domain Reputation
Anti-Spam Filters	Anti-Spam Filters
	Graymail Detection
Antivirus Protection	Antivirus Protection
Safe Links (ATP) *	URL Reputation & Category filters
	Outbreak Filter (Anti-Phishing)
	Web Interaction Tracking and Shortened URL support
Safe Attachments (ATP) *	AMP File Analysis
Retrospective Alerts	Retrospective Alerts and Remediation up to 7 Days
Basic Message Tracking	Detailed Message Tracking**
Basic Reporting	Detailed Reporting**
S/MIME, TLS	S/MIME, TLS
DLP	DLP with higher catch rate**
	Envelope Encryption
	DANE (mandatory in most EU countries)
	STIX/TAXII Third Party feeds
	Advanced Phishing Protection***
	Domain Protection (DMARC hosting and reporting)***

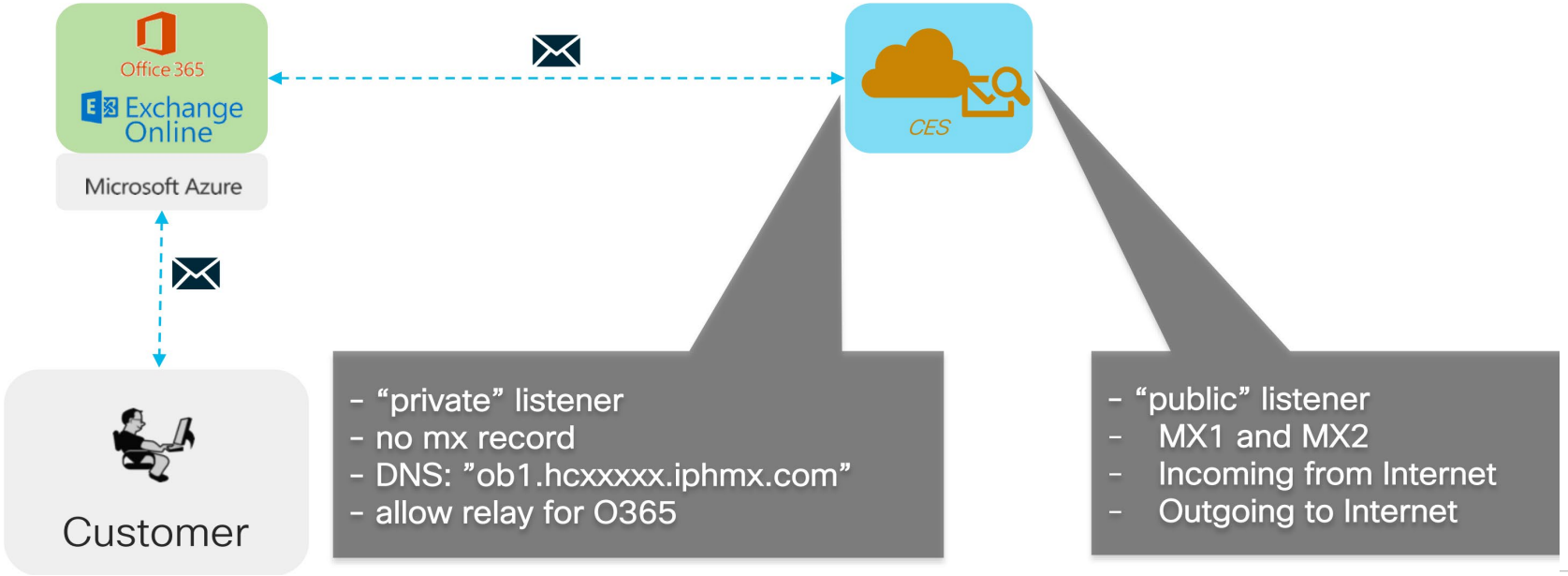
Office 365 without Cisco Email Security



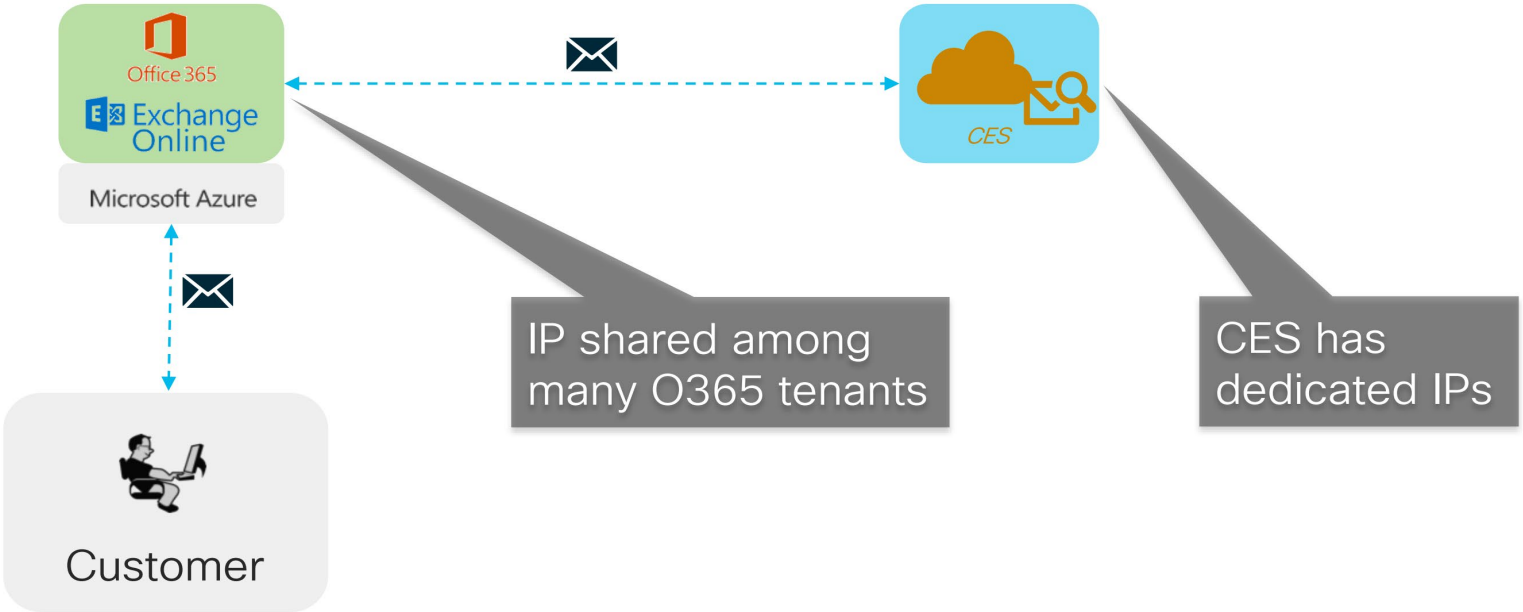
Office 365 with Cisco Email Security



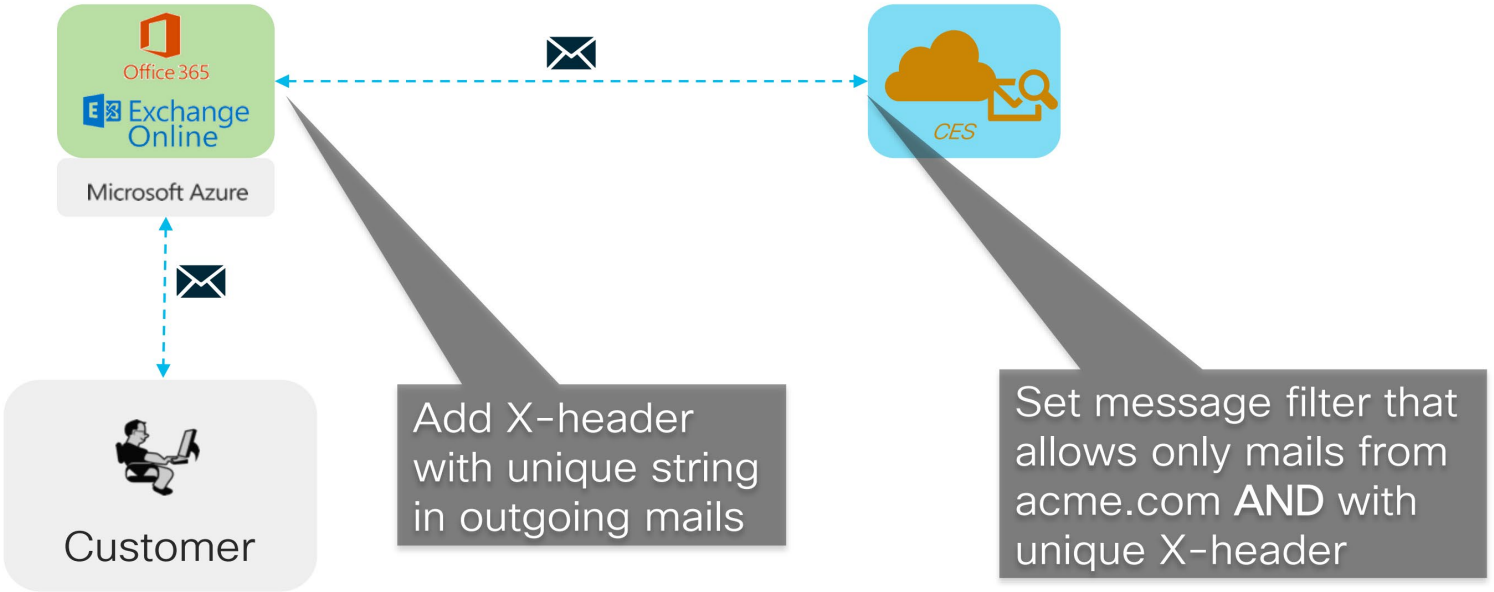
Office 365 with Cisco Email Security



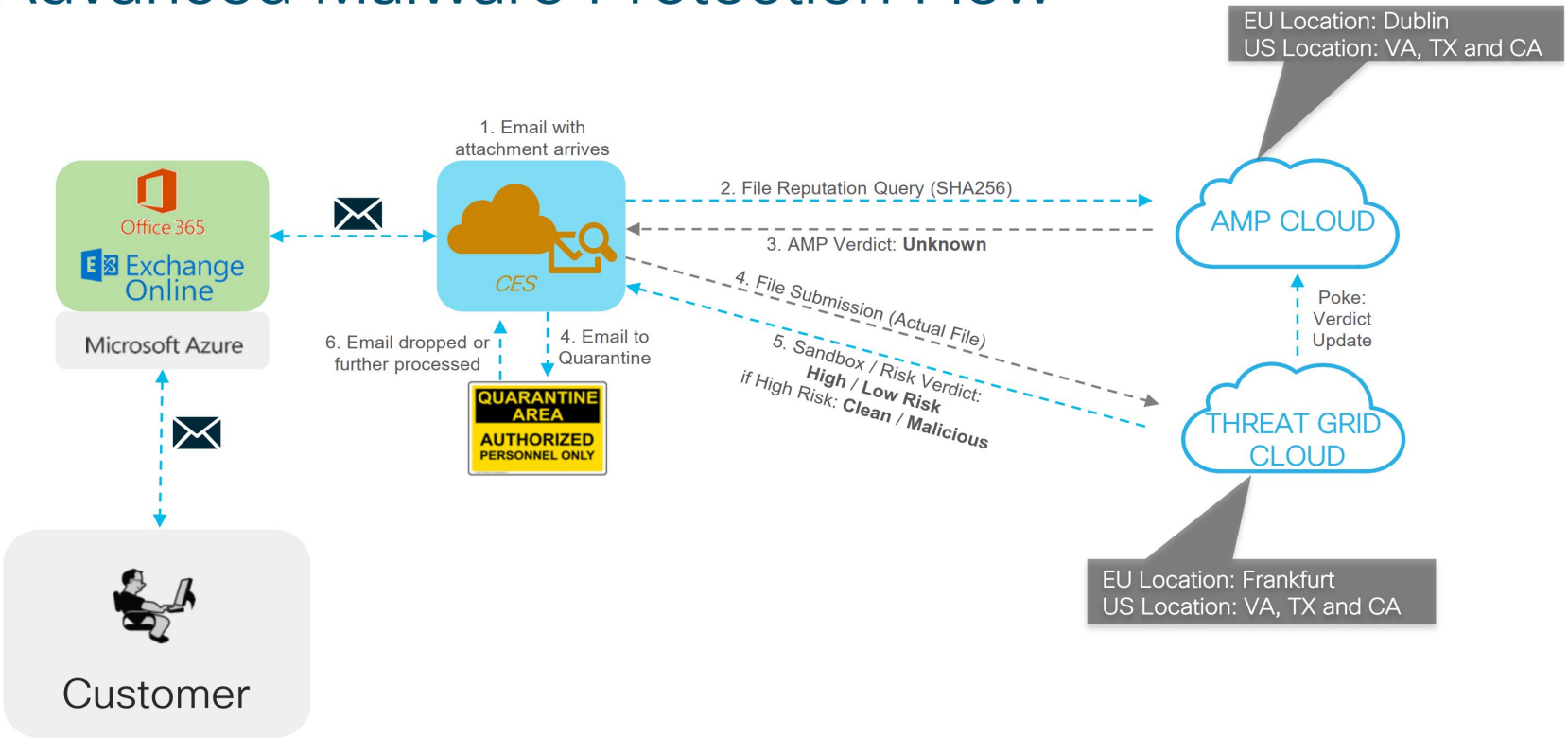
Office 365 with Cisco Email Security



Office 365 with Cisco Email Security



Advanced Malware Protection Flow



SWS COMPUTERSYSTEME
Member of ACP Group

Retrospective Verdict Change

Verdict Update for a threat that has a disposition change at later point in time

Advanced Malware Protection Verdict Updates

[**Incoming Messages** | Outgoing Messages]

Click here to view reports prior to AsyncOS 10.0

Printable PDF

Time Range: Year — **View Data for:** Group: Hosted_Cluster

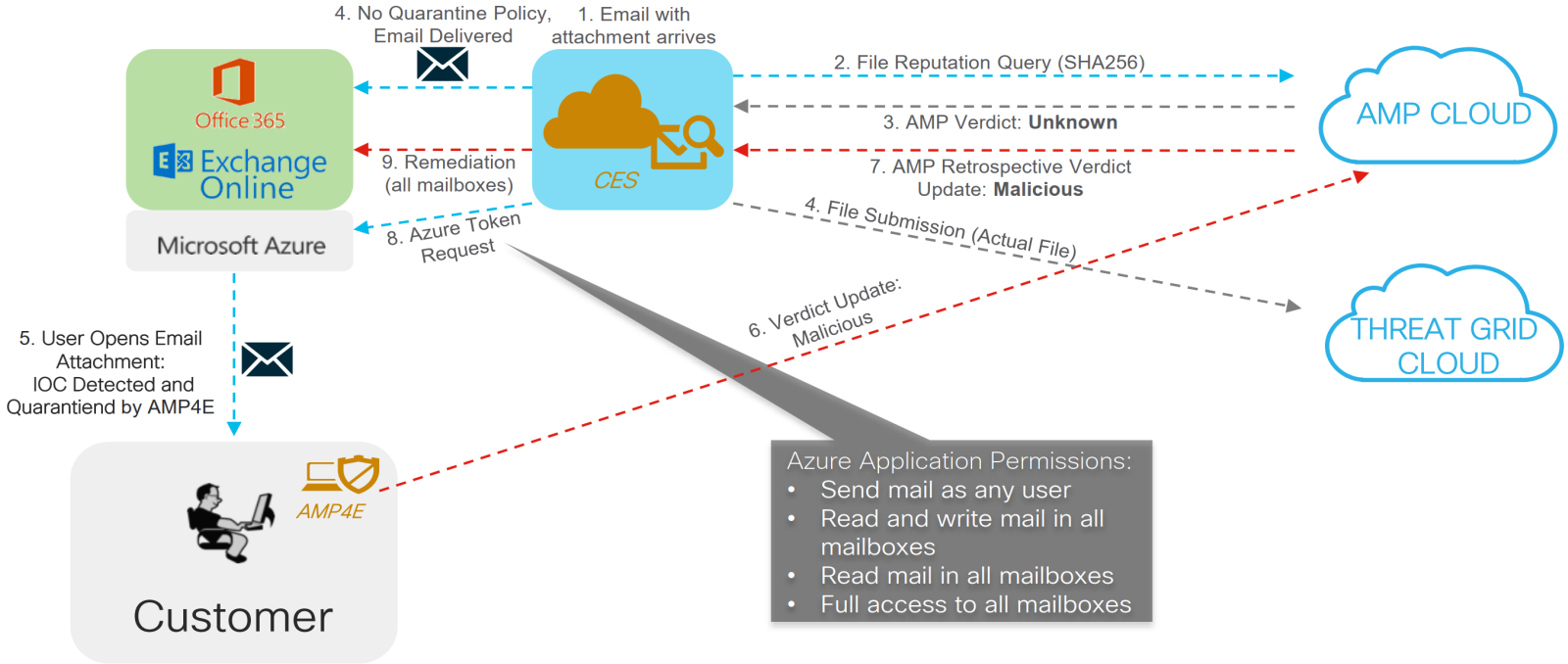
01 Jan 2018 00:00 to 11 Jan 2019 12:55 (GMT +01:00) — Data in time range: 100.0 % complete

Files with Retrospective Verdict Changes

Items Displayed 10

File SHA256	Filename	Time of Retrospective Verdict Change	Old Disposition	Current Disposition	Message Tracking
35c8963e...4861cf82	TEST-GAS.xlsm	06 Nov 2018 13:41:07	Unknown	MALICIOUS	Details
b4cc35fe...99da1e93	HACENDADO.xlsm	26 Sep 2018 13:41:07	Unknown	MALICIOUS	Details
a3520988...74a358ae	Recent activity report.pdf	09 Jul 2018 18:37:01	LOWRISK	MALICIOUS	Details
11ffedf6...67e40472	TEST-INPS-2.xlsm	06 Jun 2018 14:37:34	Unknown	MALICIOUS	Details

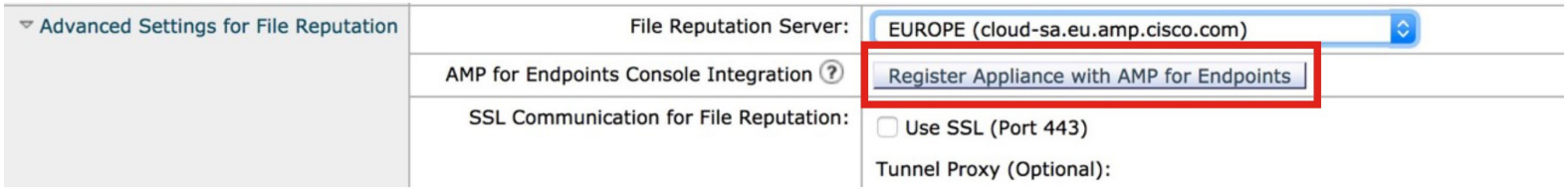
AMP Unity Retrospective Event Flow



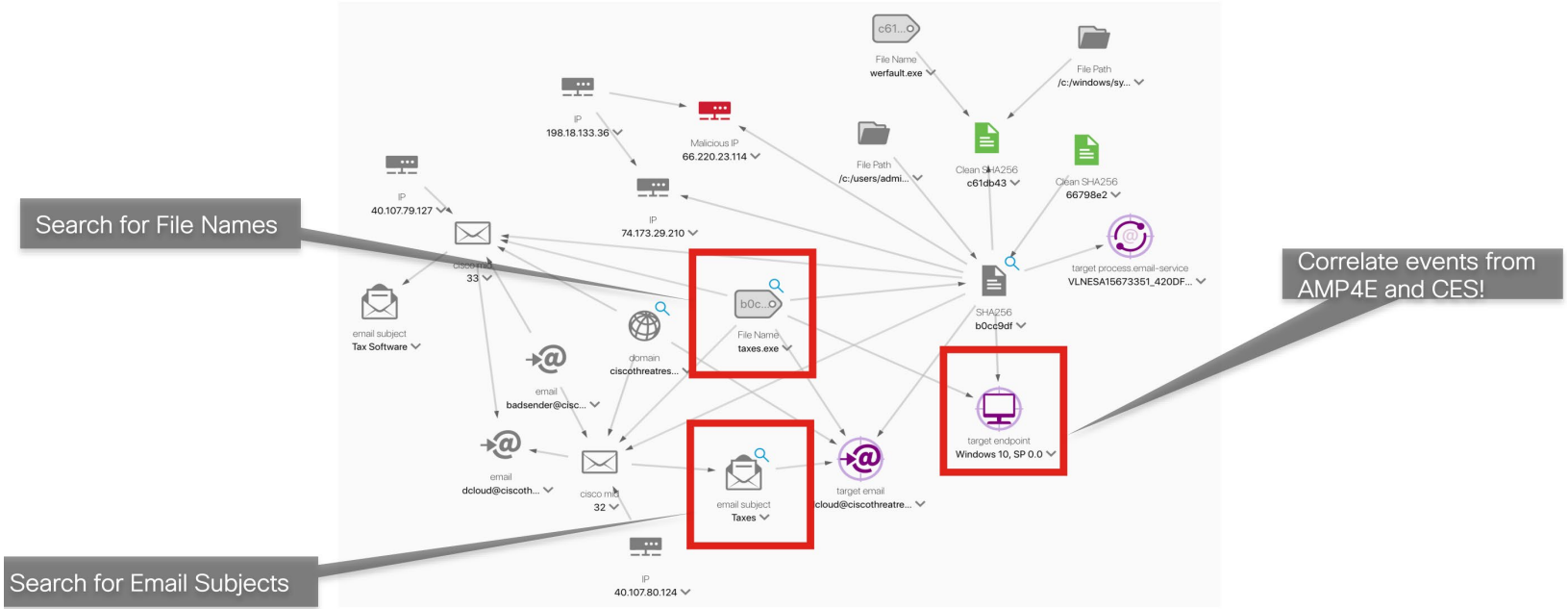
AMP Unity Integration

Pro Tip

- Integrate ESA / WSA / FP with AMP4E Console
- Group multiple ESA / WSA / FP together & share common policy
- Whitelist / Blacklist SHA256 values
- Share IoC & get File Trajectory across Organization



CES + Cisco Threat Response Integration



Cisco Advanced Phishing Protection

With Cisco Advanced Phishing Protection (APP):

- Gain a real-time understanding of senders, learn, and authenticate email. identities and behavioral relationships to protect against BEC attacks.
- Remove malicious emails from users' inboxes to prevent wire fraud or other advanced attacks.
- Get detailed visibility into email attack activity, including total messages secured and attacks prevented.
- Augment phishing and BEC detection and blocking capabilities offered in Cisco® Email Security.

Cisco Advanced Phishing Protection

Cisco Advanced Phishing Protection (APP) provides:

- Advanced intelligence that authenticates senders in real-time.
- A self-learning network that models your organization's unique inbound traffic patterns to detect fraud quickly.
- Efficient removal of malicious emails from users' inboxes
  - even from Office365 mailboxes.

Cisco Domain Protection

With Cisco Domain Protection (CDP or DP)(sometimes DMP)

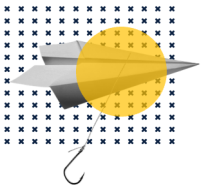
- Automates the DMARC email authentication process to achieve DMARC compliance.
- Gives you visibility into all your email senders via an easy-to-read
- Helps you block unauthorized senders to reduce or eliminate phishing emails from your domain.

Cisco Secure Access by DUO

Enabling Secure Access

Take a zero-trust approach to secure access across your entire IT environment

Prevent Risks



Reduce risk of a breach before it happens

Gain Visibility

Identify risks and indicators of a breach of trust

Reduce Attack Surface

Contain breaches and stop attacker lateral movement

The Zero Trust Approach

Enable policy-based controls for every access request in a corporate environment

See who and what is accessing applications, workloads and the network

Segment your network and workloads by enforcing granular controls

SWS COMPUTERSYSTEME
Member of ACP Group

Broadest Range of Multi-Factor Authentication (MFA) Options

- Configure authentication options for each application or group of users
- Enable multiple option for users for ease of use and flexibility


Wearables


Push


Phone Call

Soft Token


Biometrics


U2F


Hardware Tokens


SMS

What information does Duo gather?

Mobile Devices

- Corp managed asset status
- Biometrics (Touch/Face) status
- Screen lock status
- OS condition (tampered) status
- Encryption status
- Platform type
- Device OS type
- Device OS version
- Device owner
- Duo Mobile version

Laptops / Desktops

- Disk encryption
- Firewall enabled
- Device password
- OS patch level (Win 10)
- Third party agents
- Corp managed asset status*
- OS type & versions
- Browser type & versions
- Flash & Java plugins versions
- OS, browser and plugins status

New!

Duo Device Health App

Secure Any Corporate Application

Proprietary Apps (APIs)

Microsoft Environments

Cloud Services

Unix Devices (SSH Sessions)

Internal Applications (VPNs)

Cloud Applications

Web Applications

SAML 2.0 Applications

Duo Can Easily Secure O365

Duo Access Gateway

Integration with DAG/Duo SSO

Native SSO and IdP Support

Integration with ADFS

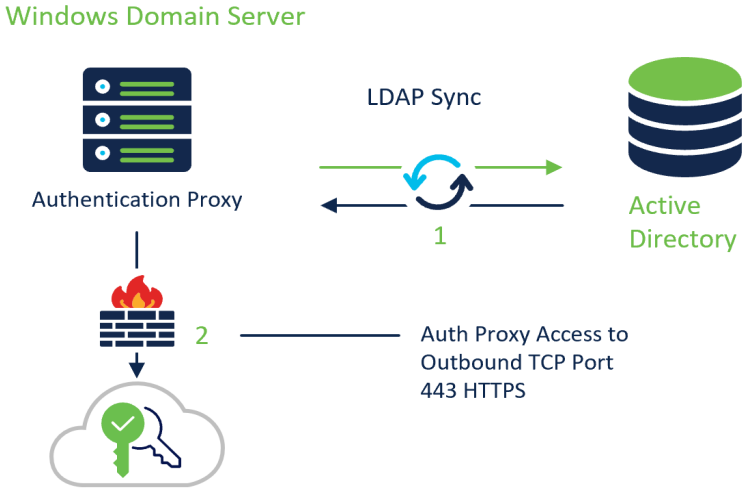
Native Azure-AD Conditional Access

Integration with Azure AD

Easily Provision Users from AD, LDAP or Azure

Import users directly into Duo from Azure without any on-premises software

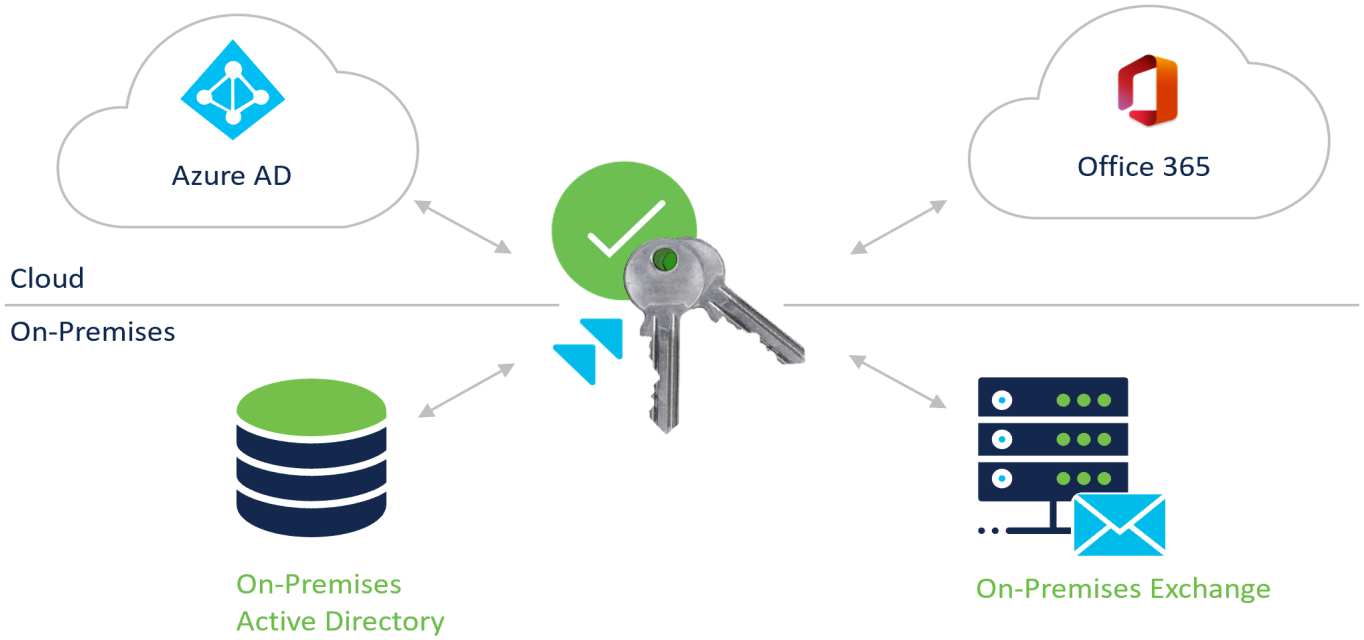
Import users via LDAP from AD or OpenLDAP directories. Requires installation of Duo Authentication proxy



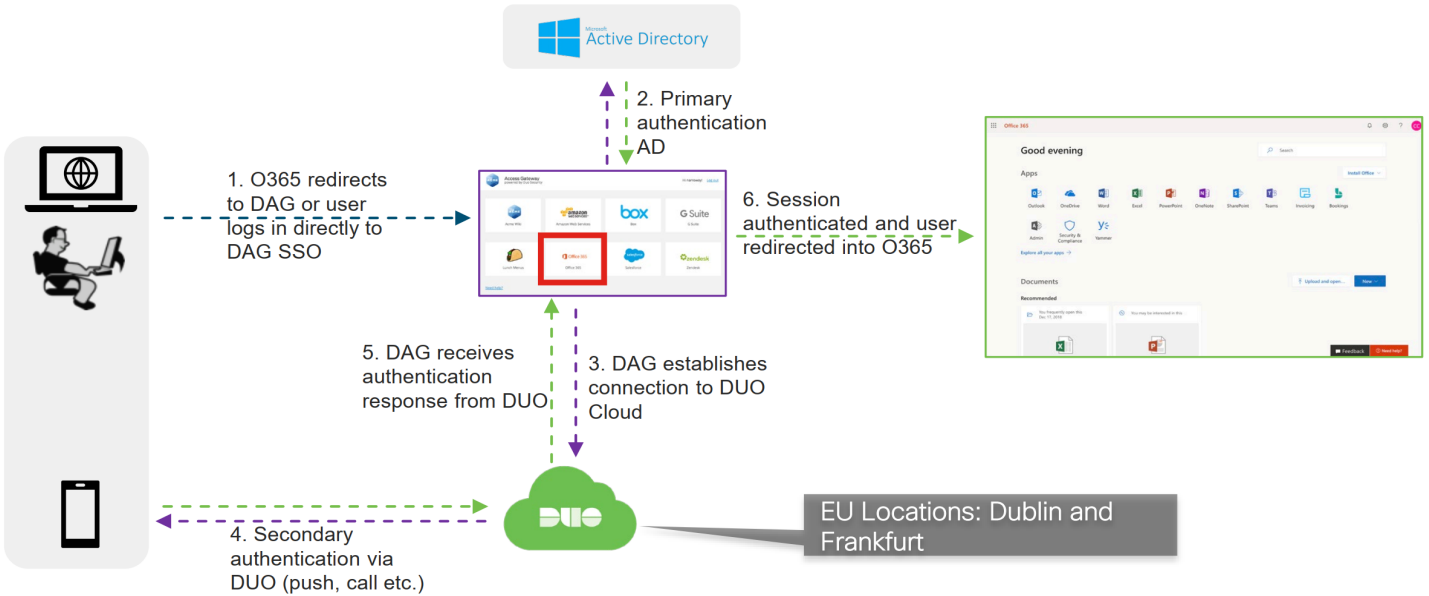
SWS COMPUTERSYSTEME
Member of ACP Group

Duo for Microsoft

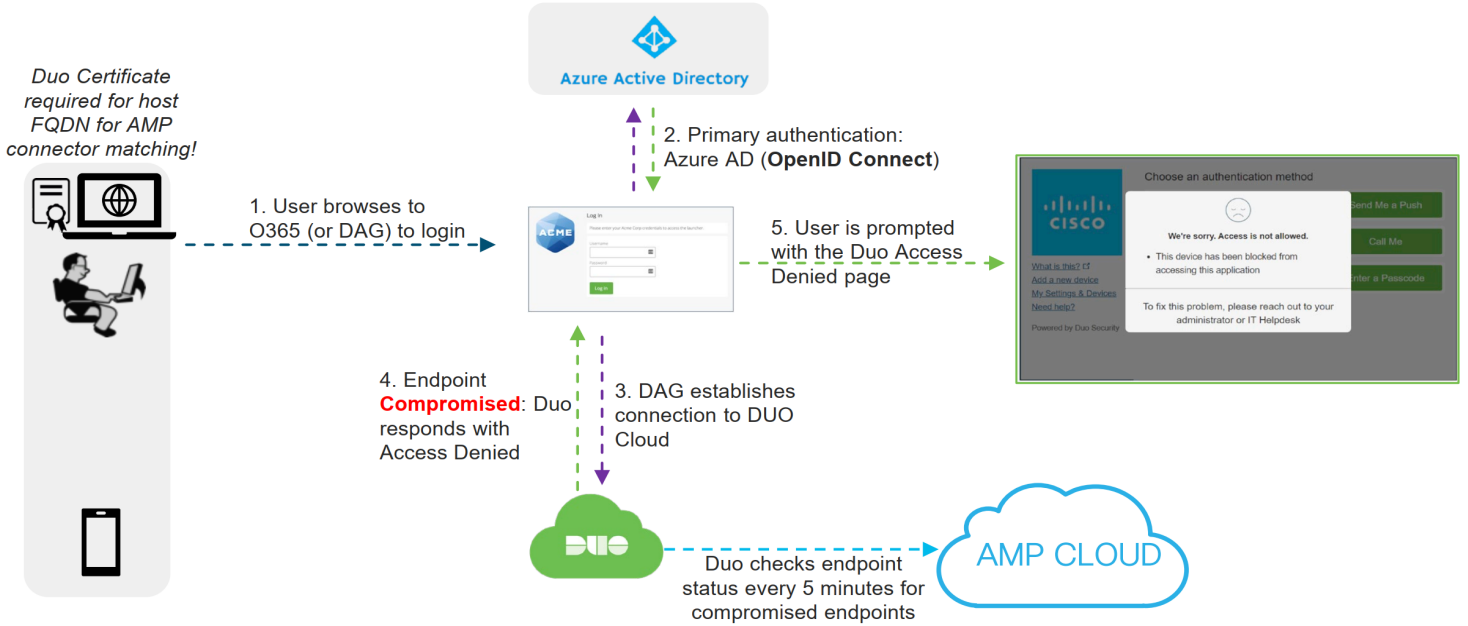
O365, RDP/Windows Logon, and Azure AD use cases



DUO + O365 Authentication Flow (On-prem AD)



DUO + AMP4E Adaptive MFA



Result: Duo Authentication Logs shows AMP4E

Full authentication log

Timestamp (UTC)	Result	User	Application	Access Device	Second Factor
9:53 PM OCT 30, 2019	✕ Denied Blocked by AMP for Endpoints	[redacted]	Microsoft Azure Active Directory	› Windows 10.0.18362.449	Unknown
9:40 PM OCT 30, 2019	✓ Granted User approved	[redacted]	Microsoft Azure Active Directory	› Windows 10.0.18362.449	› Duo Push South Jordan, UT

Fragen?