Office 365 E-Mail Security Webinar
18. & 23. März 2021

cisco Secure

Cisco Cloud Mailbox Defense

Tobias Mayer
Technical Solutions Architect
March 2021

M365 - Deployment

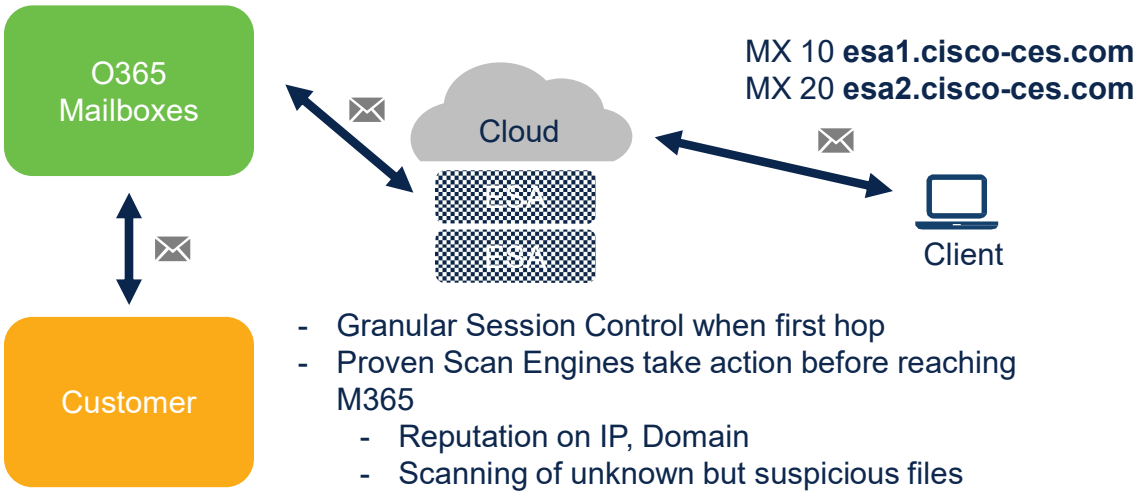
AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

Things you might realize a bit later (or faster…)

- EOP/E3 + ATP or E5 is not very cheap….
- IP address is shared among many customers…
  - SPF Record has to allow all of Microsoft
- Not really many options for granular rules
  - Many functions is mainly a turn on or turn off such as Antispam
- Too much SPAM and suspicious links in emails are passing through M
- Message Tracking is limited , cumbersome
  - Time delay when going back more than a couple of days
  - Delivered via CSV
  - Not able to search for something like an URL
- Reporting is limited

Cloud Email Security



- Granular Session Control when first hop
- Proven Scan Engines take action before reaching M365
  - Reputation on IP, Domain
  - Scanning of unknown but suspicious files

AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

"I do not want to change my Infrastructure and my mail routing, but I want something to enhance my M365 capabilities"

Source: Unicorn

Cisco Cloud Mailbox Defense

AVANTEC
Competence. Security. Trust.

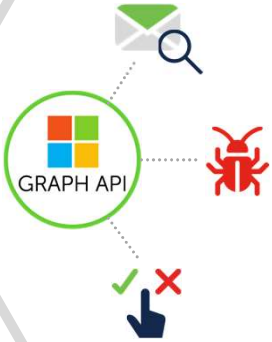
Office 365 E-Mail Security Webinar
18. & 23. März 2021

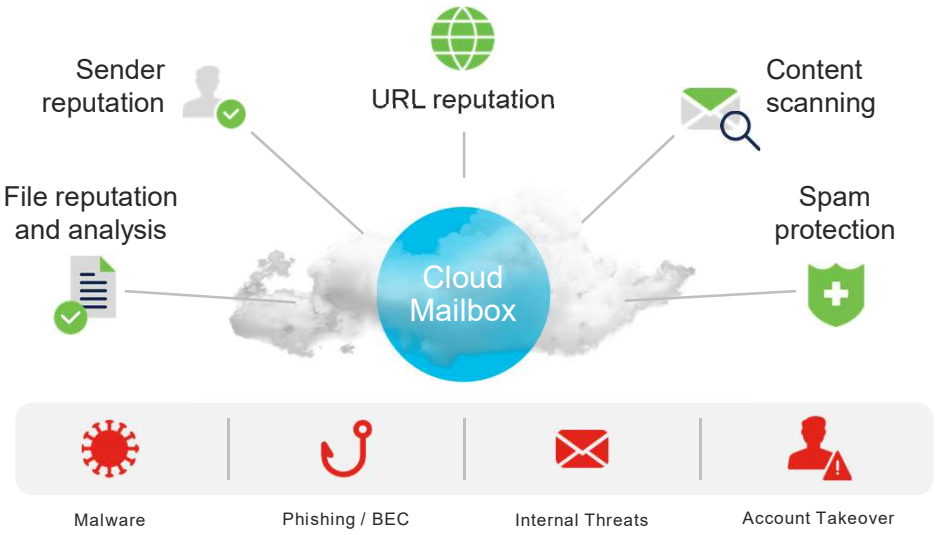
Cloud brings new email security capabilities

Faster and more powerful

Evolving defense and detection strategies

Integration is essential for securing cloud email





AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

Cisco Security inside Microsoft's Cloud

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

Bringing Cisco threat intelligence as close to the mailbox as possible

[1]Cloud file analysis is optional

Gateway vs. CESS

MX record changed to CES address

CES scans messages and takes an action

Message is delivered

MX record is unchanged

Copy of each message is sent to Cloud Mailbox

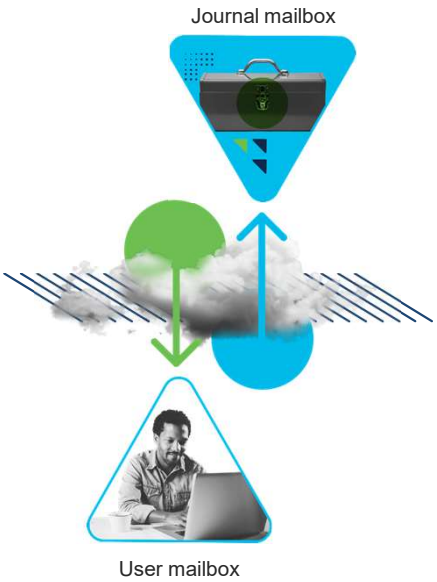
Cloud Mailbox scans and remediates using an API

AVANTEC
Competence. Security. Trust.

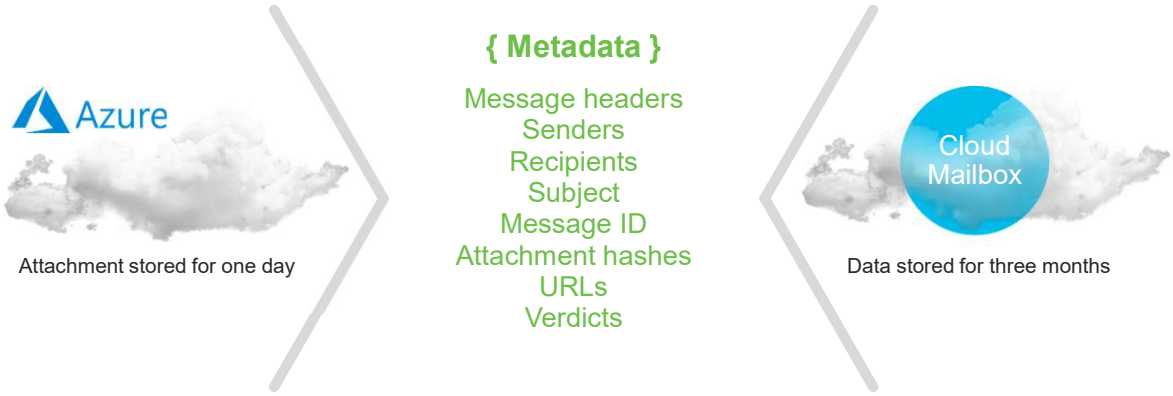
Office 365 E-Mail Security Webinar
18. & 23. März 2021

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



Cloud brings new email security capabilities



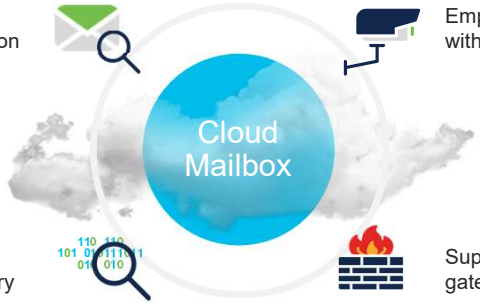
AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

Take command of your mailbox

Simplify your email administration with easy searching and remediation

Empower your security operations with triage and open APIs



Enrich your IR investigations with conversation tracking and trajectory

Supplement your secure email gateway with internal visibility

Administrators | Operations | Incident Response

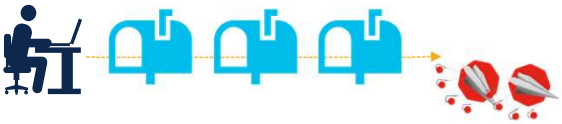
Scenario
A phishing link has been reported by a user

What do I want to know?

Who else received this link

- *From additional senders?*
- *With the same subject?*

What do I want to do?



Remove the link from all inboxes

- *Regardless of sender*
- *Regardless of subject*

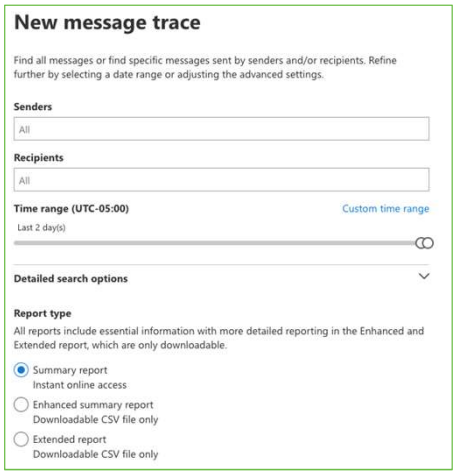
AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

Scenario
A phishing link has been reported by a user

Microsoft workflow

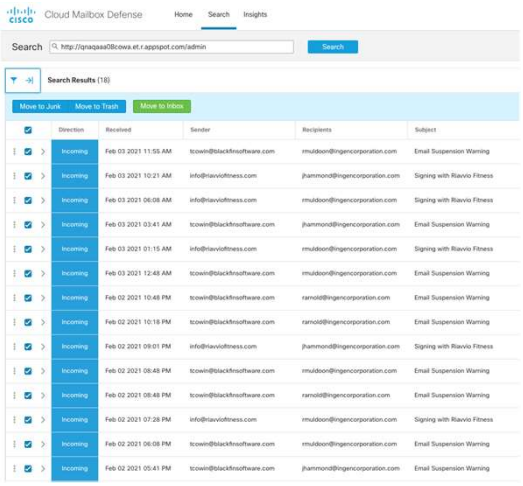
- Message Trace query
  - *Cannot search by subject or URL*
  - *Slow to return results*
  - *Generates a report only*
- Cannot take any action from the results
  - *Writing a PowerShell script is the next step to remediate.*
- Total time is in minutes or hours



Scenario
A phishing link has been reported by a user

Cloud Mailbox workfow

- Search for any message detail
  - *Sender, Recipient, URL, etc.*
  - *Lightening fast results*
- Select and remediate instantly
  - *One or multiple messages at once*
  - *Actions taken directly from the results*
- Total time is in seconds



AVANTEC
Competence. Security. Trust.

Office 365 E-Mail Security Webinar
18. & 23. März 2021

POV made easy

- Fully functional in 5 minutes
- No operational risk
- No changes to mail flow or DNS
- Track all messages, including internal

Two-step deployment

Instant tracking and reporting

No risk to mail delivery

17

cisco Secure

AVANTEC
Competence. Security. Trust.