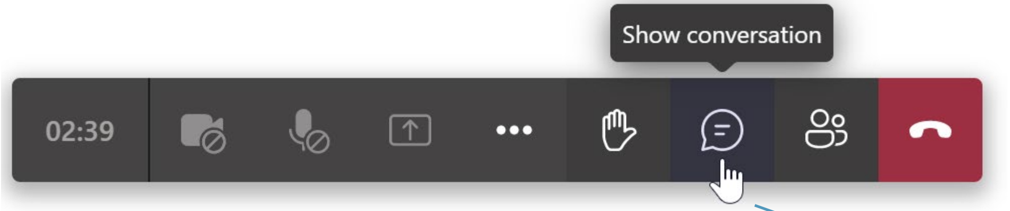
CENTARIS™

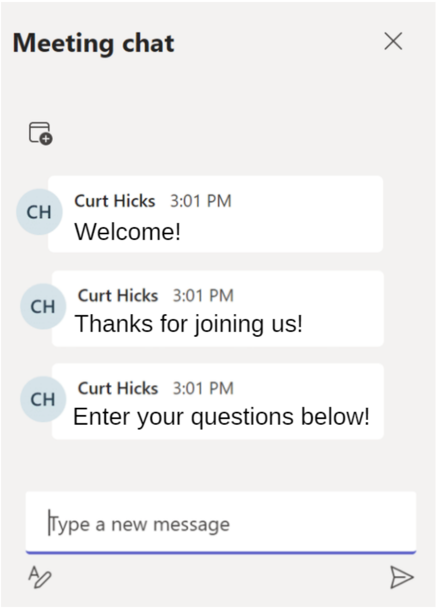
Office 365 Email Security Solution

The most advanced email and collaboration security tool on the market.

Office 365 Microsoft Teams OneDrive SharePoint Dropbox box CITRIX ShareFile

Use the Teams Chat to post any questions





CH Curt Hicks 3:01 PM
Welcome!

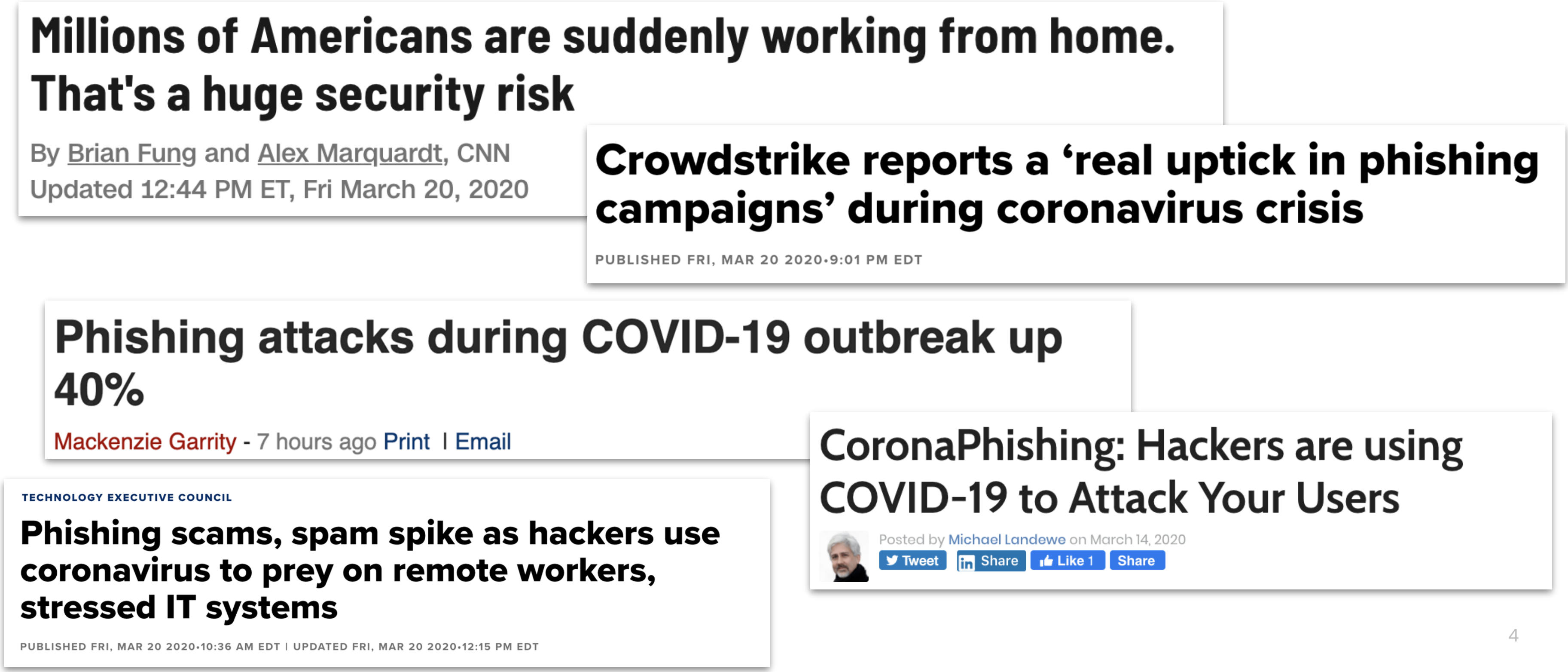
CH Curt Hicks 3:01 PM
Thanks for joining us!

CH Curt Hicks 3:01 PM
Enter your questions below!

Techie Definitions

- **Phishing -** the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
- **Spear Phishing** - the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.
- **Malware -** software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
- **Email Filter -** A technique used to organize incoming (and in some cases outbound) emails and to block email based on the specific and identifiable senders, keywords in the subject line, or by the quality of the content of an email.
- **Threat Actor** - A threat actor, also called a malicious actor, is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact -- an organization's security.
- **Attack Vector** - An attack vector is a pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities.

Attacks are Increasing more than ever Across Multiple Attack Vectors



Millions of Americans are suddenly working from home. That's a huge security risk

By Brian Fung and Alex Marquardt, CNN
Updated 12:44 PM ET, Fri March 20, 2020

Crowdstrike reports a 'real uptick in phishing campaigns' during coronavirus crisis

PUBLISHED FRI, MAR 20 2020•9:01 PM EDT

Phishing attacks during COVID-19 outbreak up 40%

Mackenzie Garrity - 7 hours ago Print | Email

TECHNOLOGY EXECUTIVE COUNCIL

Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems

PUBLISHED FRI, MAR 20 2020•10:36 AM EDT | UPDATED FRI, MAR 20 2020•12:15 PM EDT

CoronaPhishing: Hackers are using COVID-19 to Attack Your Users

Posted by Michael Landewe on March 14, 2020

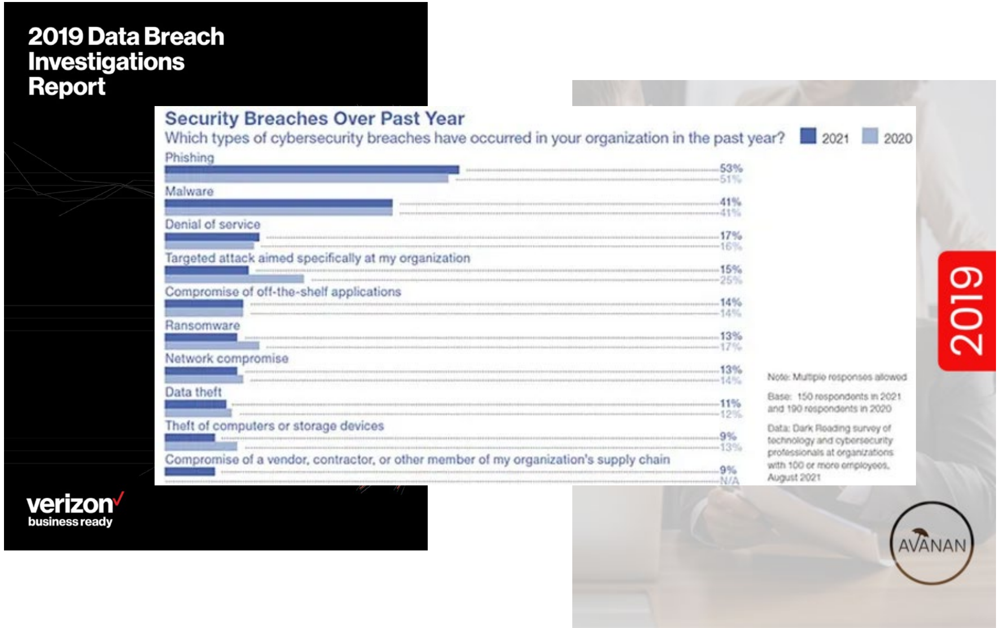
What experts and professionals are seeing: Your Inbox(es) Are Under Attack

#1 threat resulting in breaches is phishing

90% of attacks start with email

94% of malware incidence was delivered via email

Microsoft misses at least 30% of phishing attacks



Security Breaches Over Past Year

Which types of cybersecurity breaches have occurred in your organization in the past year?

Note: Multiple responses allowed

Base: 150 respondents in 2021 and 190 respondents in 2020

Data: Dark Reading survey of technology and cybersecurity professionals at organizations with 100 or more employees, August 2021

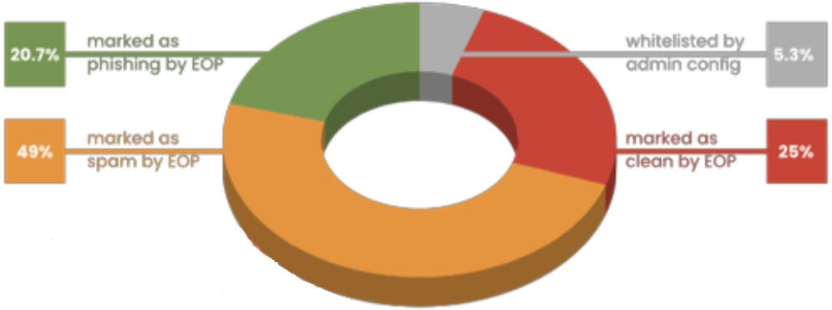
The Problem with Phishing

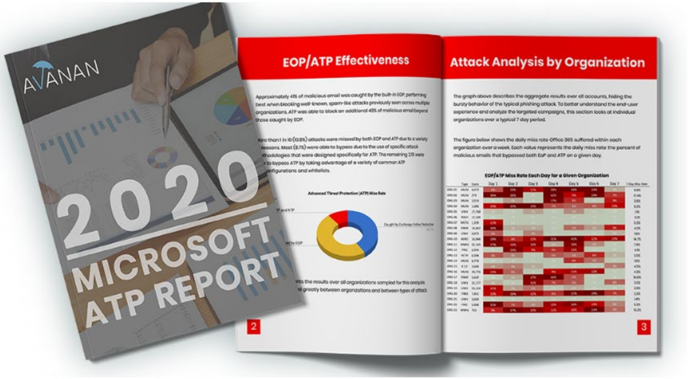
90% of cyber attacks start with a phishing email.

Email Security analyzed 55 million emails to Office 365 users

30.3% of malicious/phishing emails were missed by Microsoft EOP.

11% Miss Rate on Average by ATP




AVANAN

2020 MICROSOFT ATP REPORT

EOP/ATP Effectiveness

Attack Analysis by Organization

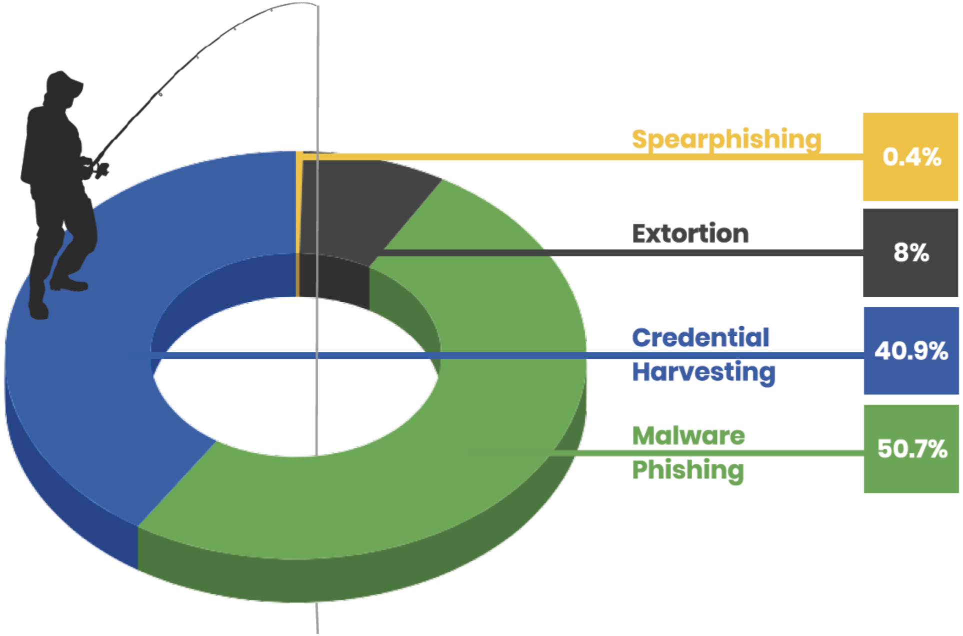
The Problem with Phishing and Microsoft

Why does Microsoft miss so many attacks?

- Hackers are testing their own malicious attacks against O365 security tools.
- Because of how large and diverse the Office 365 user base is, Microsoft must keep the false positive rate low to guarantee deliverability and business continuity.

Dissecting Email Attacks: By The Numbers

Is this happening to you?



Malware Phishing: Beware the Attachment

While users have been trained to be suspicious, hackers still send malicious files via email

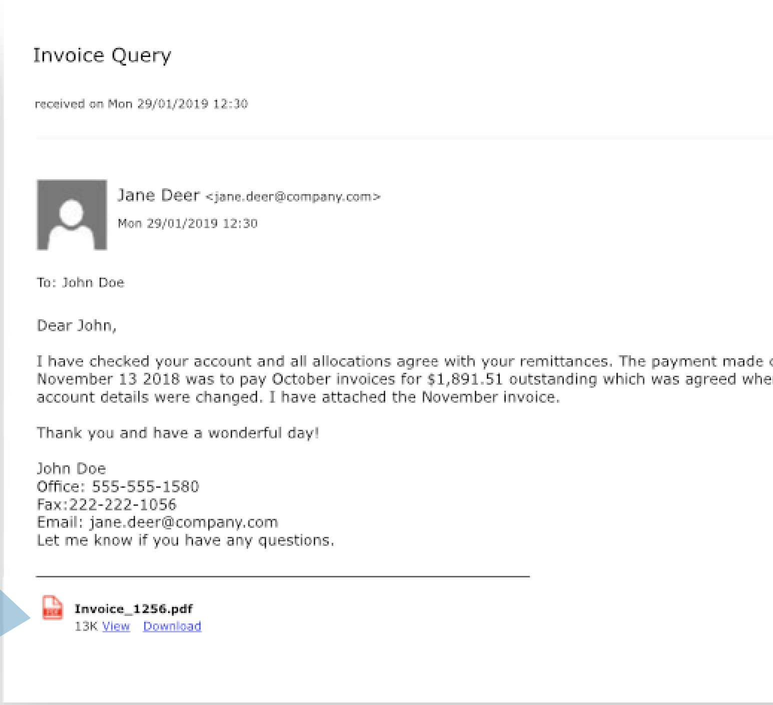
50.7% of email phishing attacks contain malware

Common traits of Malware Phishing emails

- Has an attachment
- Contains a link that triggers a file download

Attachments that evade default security:

- Zero day malware files
- Evasive malware
- Files stored on trusted file share sites



Invoice Query

received on Mon 29/01/2019 12:30

Jane Deer <jane.deer@company.com>
Mon 29/01/2019 12:30

To: John Doe

Dear John,

I have checked your account and all allocations agree with your remittances. The payment made November 13 2018 was to pay October invoices for $1,891.51 outstanding which was agreed whe account details were changed. I have attached the November invoice.

Thank you and have a wonderful day!

John Doe
Office: 555-555-1580
Fax:222-222-1056
Email: jane.deer@company.com
Let me know if you have any questions.

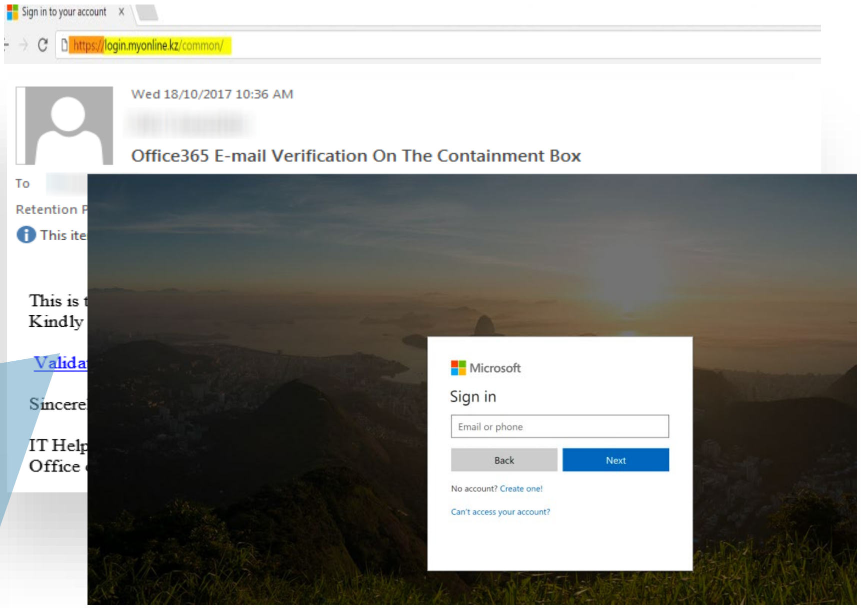
Invoice_1256.pdf
13K View Download

Credential Harvesting: Scam the Keys to the Front Door

Any user can be a compromised; key executives, admin accounts highly targeted

40.9% of email phishing attacks feature credential harvesting

- Microsoft is most impersonated
- Link to pointing to login page
- Misleading URL not always obvious



Sign in to your account ×

https://login.myonline.kz/common/

Wed 18/10/2017 10:36 AM

[redacted]

Office365 E-mail Verification On The Containment Box

To [redacted]

Retention P

This ite

This is t
Kindly

Valida

Sincere

IT Help
Office

Microsoft

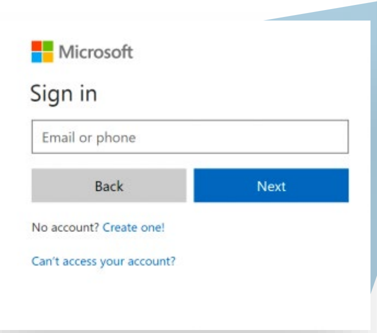
Sign in

Email or phone

Back | Next

No account? Create one!

Can't access your account?



Microsoft

Sign in

Email or phone

Back | Next

No account? Create one!

Can't access your account?

Extortion Emails: Probable Targets, Real Passwords

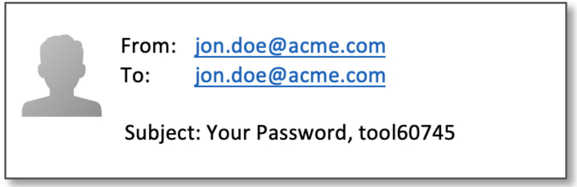
Digital blackmail - hackers after money spew vague mass emails

8% of phishing attacks are extortion emails

Often demand ransom, usually in the form of crypto-currency

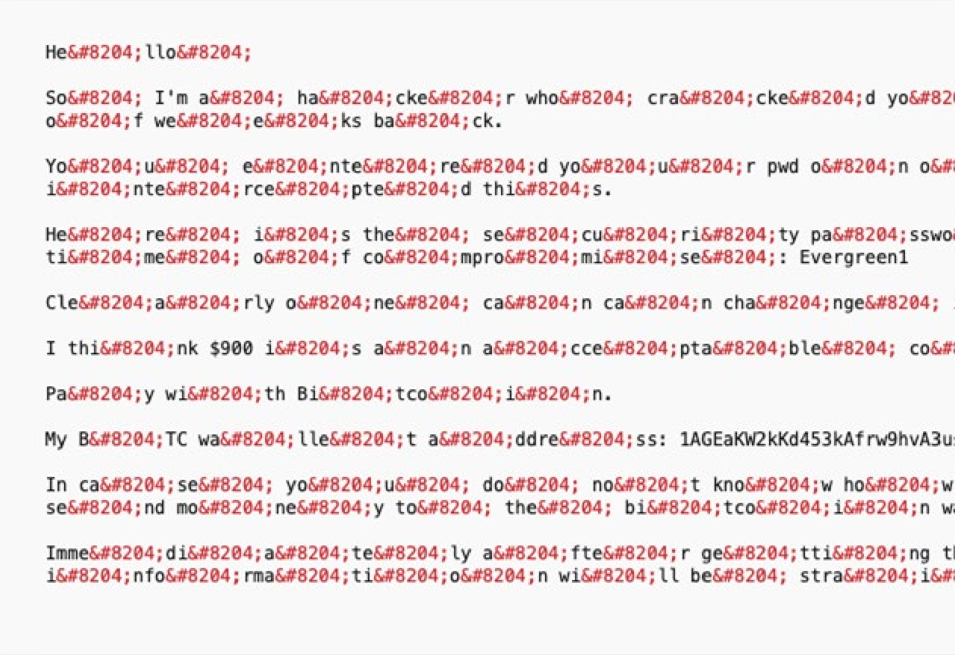
Common features:

- Contain a crypto-wallet address
- Nickname, domain impersonation



From: jon.doe@acme.com
To: jon.doe@acme.com

Subject: Your Password, tool60745



```
He&#8204;llo&#8204;

So&#8204; I'm a&#8204; ha&#8204;cke&#8204;r who&#8204; cra&#8204;cke&#8204;d yo&#82
o&#8204;f we&#8204;e&#8204;ks ba&#8204;ck.

Yo&#8204;u&#8204; e&#8204;nte&#8204;re&#8204;d yo&#8204;u&#8204;r pwd o&#8204;n o&#
i&#8204;nte&#8204;rce&#8204;pte&#8204;d thi&#8204;s.

He&#8204;re&#8204; i&#8204;s the&#8204; se&#8204;cu&#8204;ri&#8204;ty pa&#8204;sswo
ti&#8204;me&#8204; o&#8204;f co&#8204;mpro&#8204;mi&#8204;se&#8204;: Evergreen1

Cle&#8204;a&#8204;rly o&#8204;ne&#8204; ca&#8204;n ca&#8204;n cha&#8204;nge&#8204;

I thi&#8204;nk $900 i&#8204;s a&#8204;n a&#8204;cce&#8204;pta&#8204;ble&#8204; co&#

Pa&#8204;y wi&#8204;th Bi&#8204;tco&#8204;i&#8204;n.

My B&#8204;TC wa&#8204;lle&#8204;t a&#8204;ddre&#8204;ss: 1AGEaKW2kKd453kAfrw9hvA3u

In ca&#8204;se&#8204; yo&#8204;u&#8204; do&#8204; no&#8204;t kno&#8204;w ho&#8204;w
se&#8204;nd mo&#8204;ne&#8204;y to&#8204; the&#8204; bi&#8204;tco&#8204;i&#8204;n w

Imme&#8204;di&#8204;a&#8204;te&#8204;ly a&#8204;fte&#8204;r ge&#8204;tti&#8204;ng t
i&#8204;nfo&#8204;rma&#8204;ti&#8204;o&#8204;n wi&#8204;ll be&#8204; stra&#8204;i&#
```

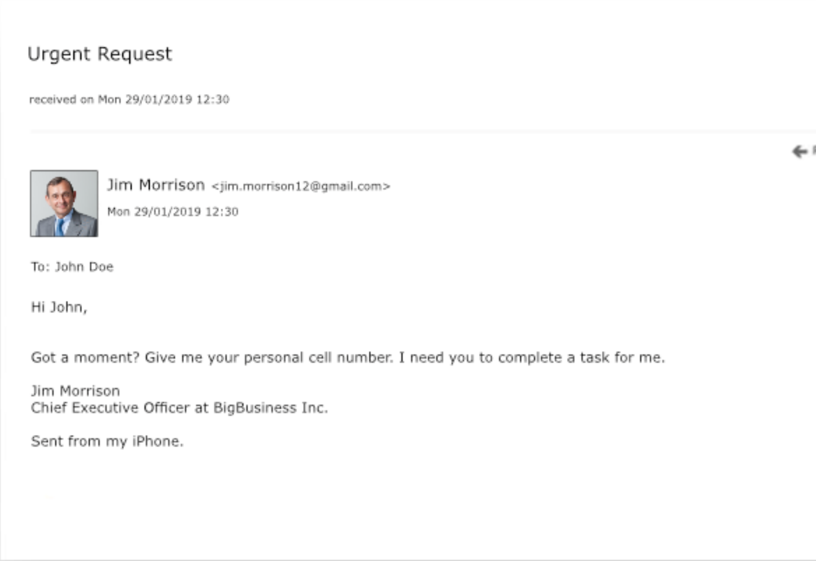
Spear Phishing: Less common, but high impact

Difficult to detect for most anti-phishing tools, due to lack of attachments or links

0.4% of email phishing attacks are spear phishing attacks

Common traits of Spear Phishing emails

- Sent to high level employees who have access to finances or other sensitive information
- This is sometime referred to as impersonation emails
- No link or attachment
- Sense of urgency



Urgent Request

received on Mon 29/01/2019 12:30

Jim Morrison <jim.morrison12@gmail.com>
Mon 29/01/2019 12:30

To: John Doe

Hi John,

Got a moment? Give me your personal cell number. I need you to complete a task for me.

Jim Morrison
Chief Executive Officer at BigBusiness Inc.

Sent from my iPhone.

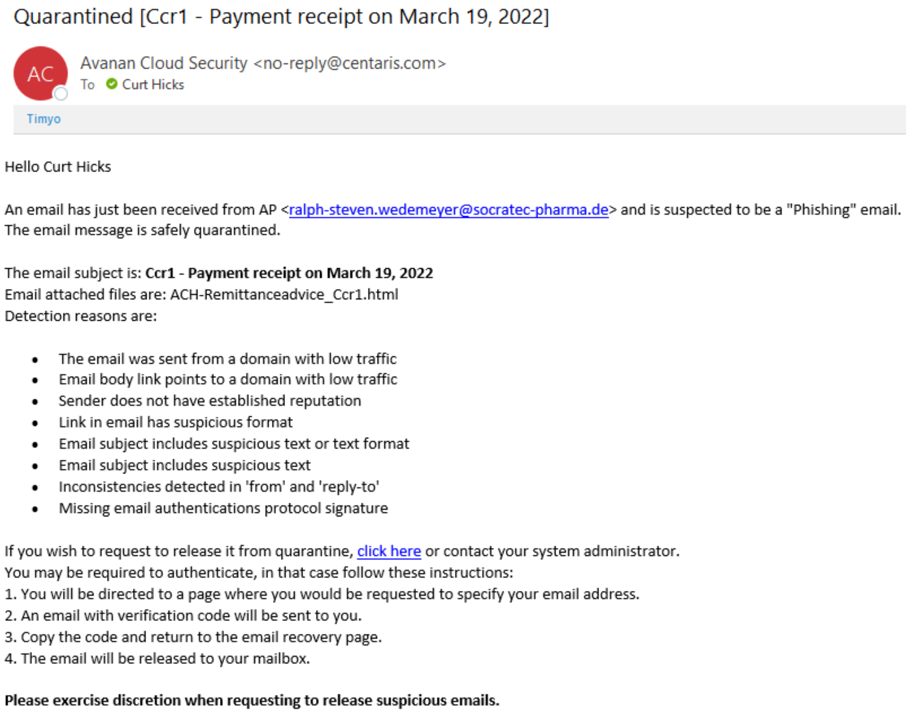
Spear Phishing: Less common, but high impact

Difficult to detect for most anti-phishing tools, due to lack of attachments or links

0.4% of email phishing attacks are spear phishing attacks

300+ Phishing Indicators

- Here is what our Email Security solution does to analyze and eliminate these types of email messages before they even land in your inbox!



Quarantined [Ccr1 - Payment receipt on March 19, 2022]

Avanan Cloud Security <no-reply@centaris.com>
To Curt Hicks

Hello Curt Hicks

An email has just been received from AP <ralph-steven.wedemeyer@socratec-pharma.de> and is suspected to be a "Phishing" email. The email message is safely quarantined.

The email subject is: **Ccr1 - Payment receipt on March 19, 2022**
Email attached files are: ACH-Remittanceadvice_Ccr1.html
Detection reasons are:

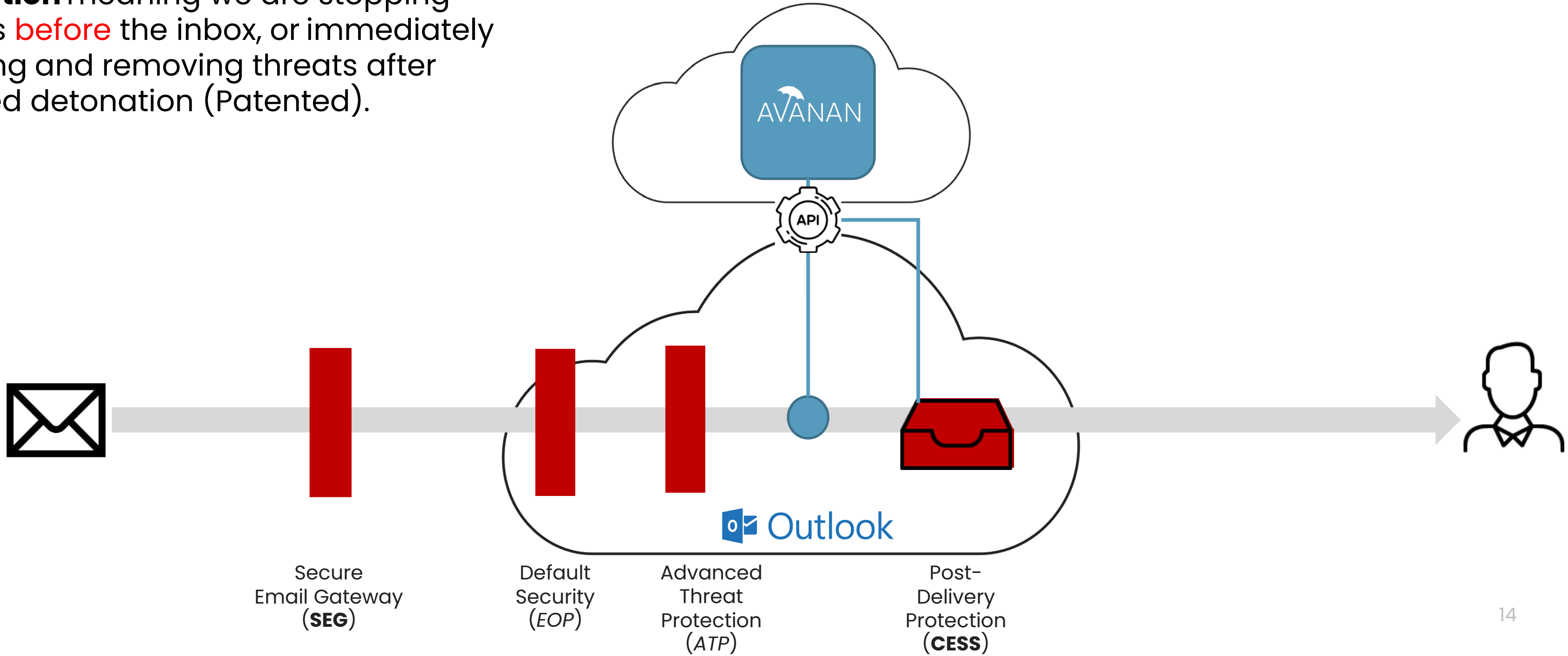
- The email was sent from a domain with low traffic
- Email body link points to a domain with low traffic
- Sender does not have established reputation
- Link in email has suspicious format
- Email subject includes suspicious text or text format
- Email subject includes suspicious text
- Inconsistencies detected in 'from' and 'reply-to'
- Missing email authentications protocol signature

If you wish to request to release it from quarantine, click here or contact your system administrator.
You may be required to authenticate, in that case follow these instructions:
1. You will be directed to a page where you would be requested to specify your email address.
2. An email with verification code will be sent to you.
3. Copy the code and return to the email recovery page.
4. The email will be released to your mailbox.

Please exercise discretion when requesting to release suspicious emails.

The Solution to eliminationg bad messages lies in what makes our solution different.

Inline defense with post-delivery protection meaning we are stopping threats before the inbox, or immediately blocking and removing threats after delayed detonation (Patented).

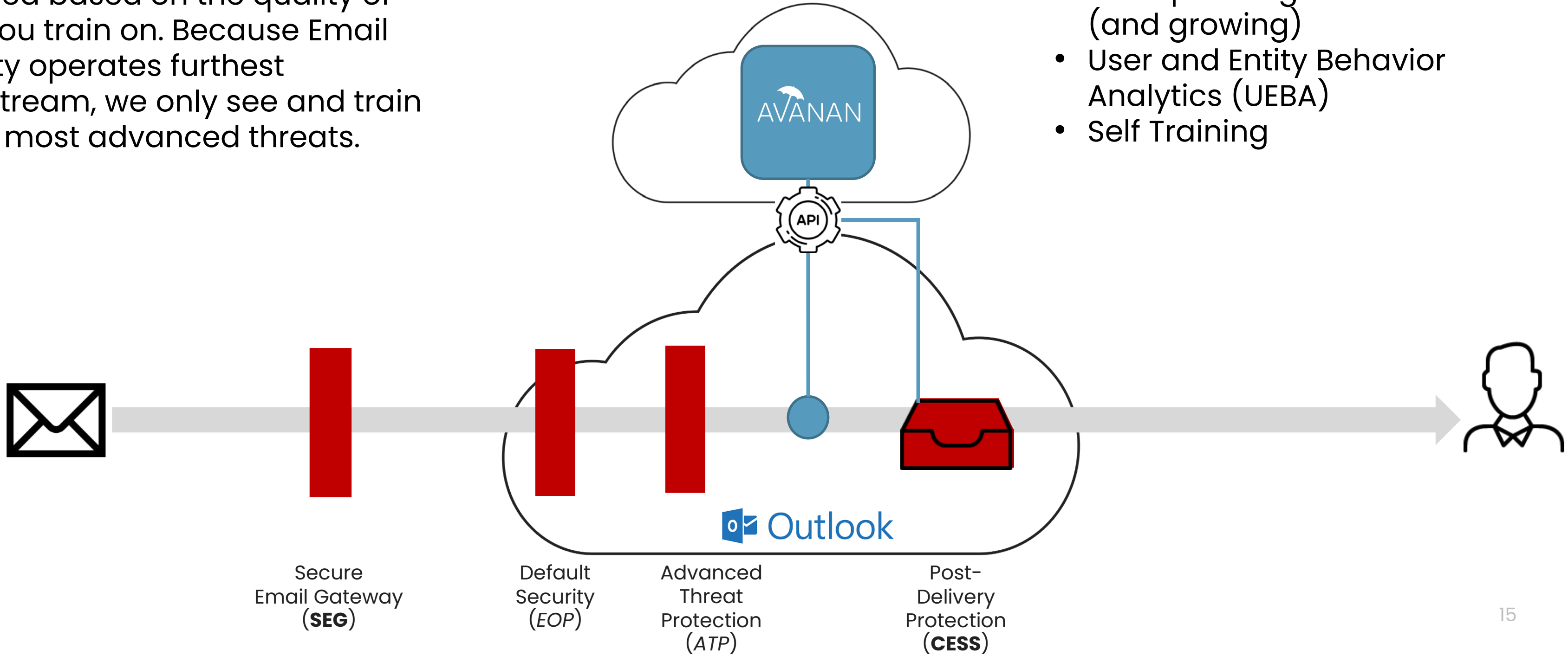

AVANAN
API
Outlook
Secure Email Gateway (**SEG**)
Default Security (*EOP*)
Advanced Threat Protection (*ATP*)
Post-Delivery Protection (**CESS**)

The Solution to eliminationg bad messages lies in what makes our solution different.

Next-Generation AI & ML is achieved based on the quality of data you train on. Because Email Security operates furthest downstream, we only see and train on the most advanced threats.

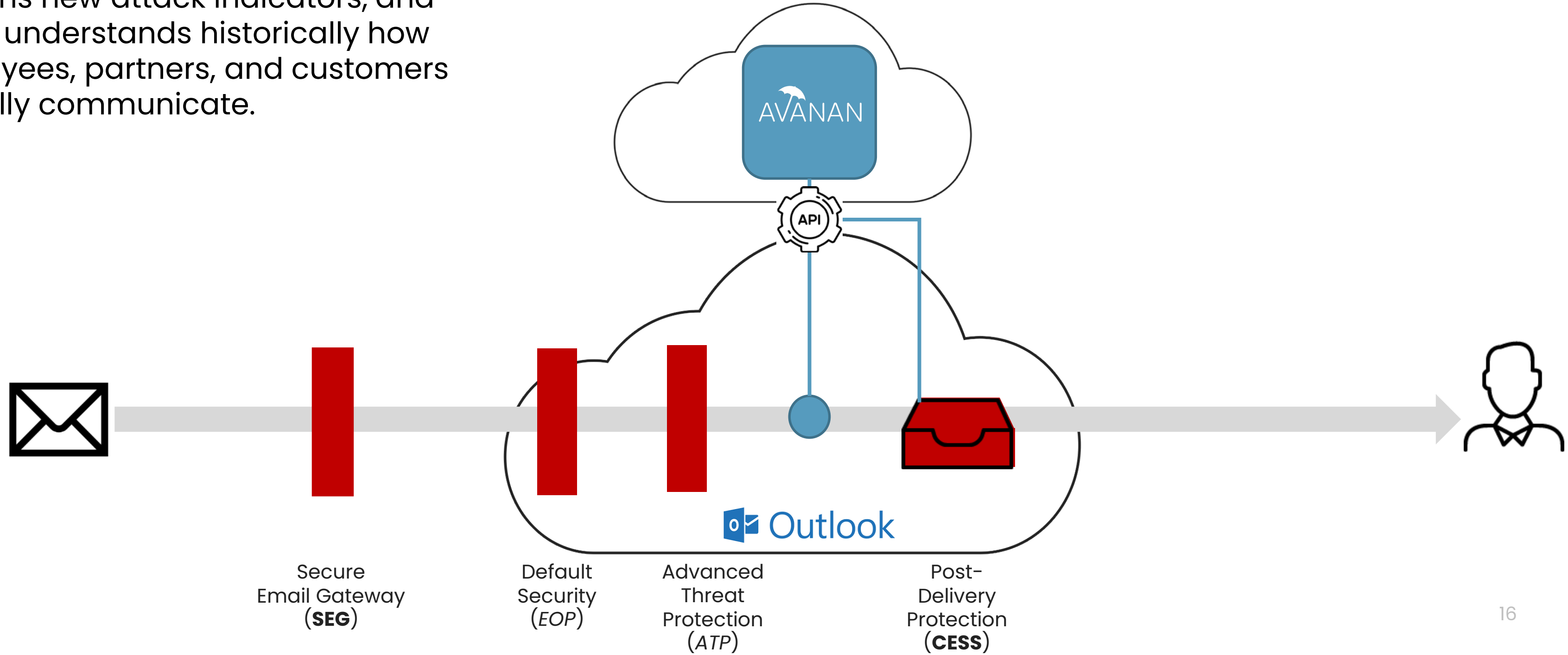
SmartPhish Alone Leverages

- 300+ phishing indicators (and growing)
- User and Entity Behavior Analytics (UEBA)
- Self Training


AVANAN
API
Outlook
Secure Email Gateway (**SEG**)
Default Security (*EOP*)
Advanced Threat Protection (*ATP*)
Post-Delivery Protection (**CESS**)

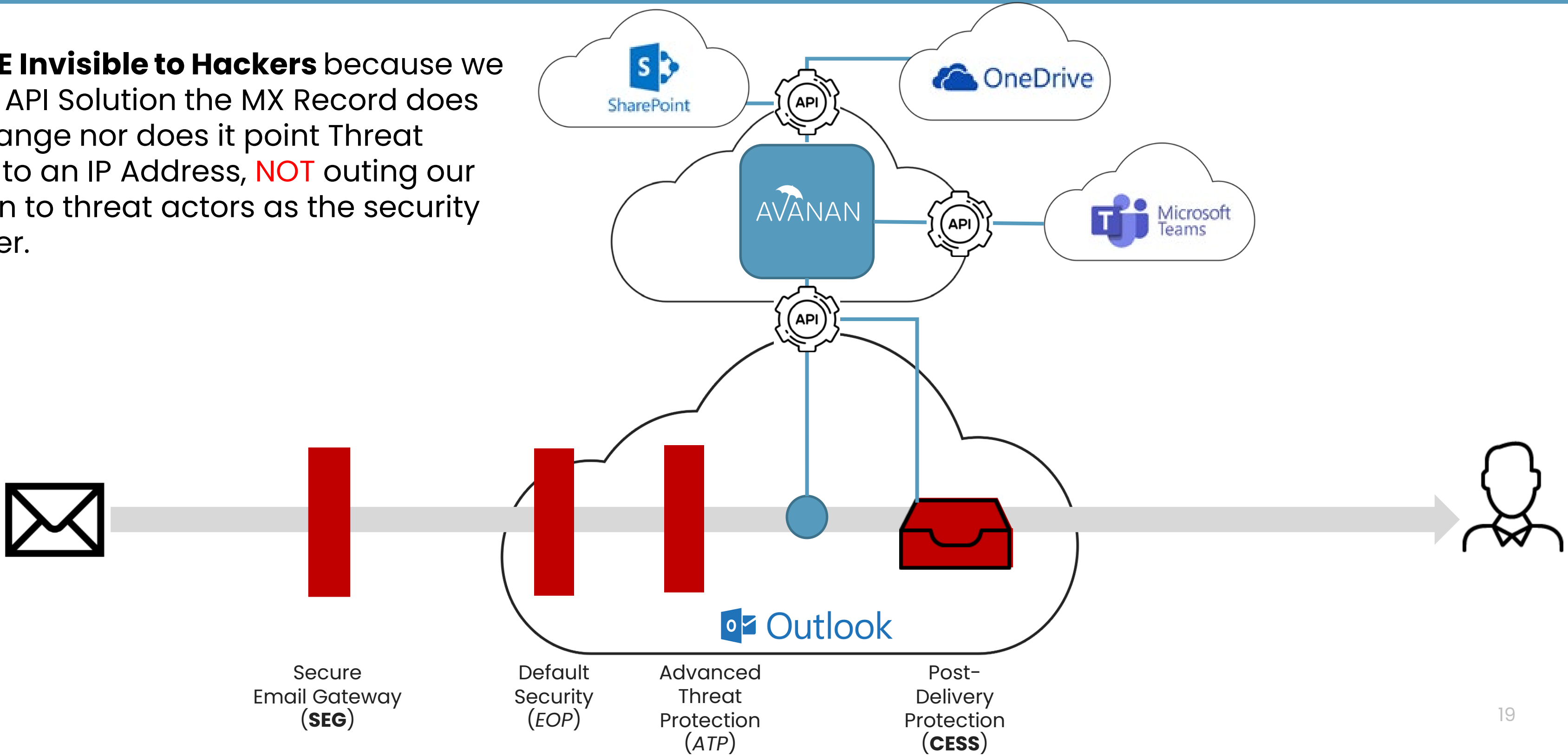
The Solution to eliminationg bad messages lies in what makes our solution different.

Self-training with every bad email, the AI learns new attack indicators, and better understands historically how employees, partners, and customers typically communicate.


AVANAN
API
Outlook
Secure Email Gateway (**SEG**)
Default Security (*EOP*)
Advanced Threat Protection (*ATP*)
Post-Delivery Protection (**CESS**)

The Solution to eliminationg bad messages lies in what makes our solution different.

We ARE Invisible to Hackers because we are an API Solution the MX Record does not change nor does it point Threat Actors to an IP Address, NOT outing our solution to threat actors as the security provider.

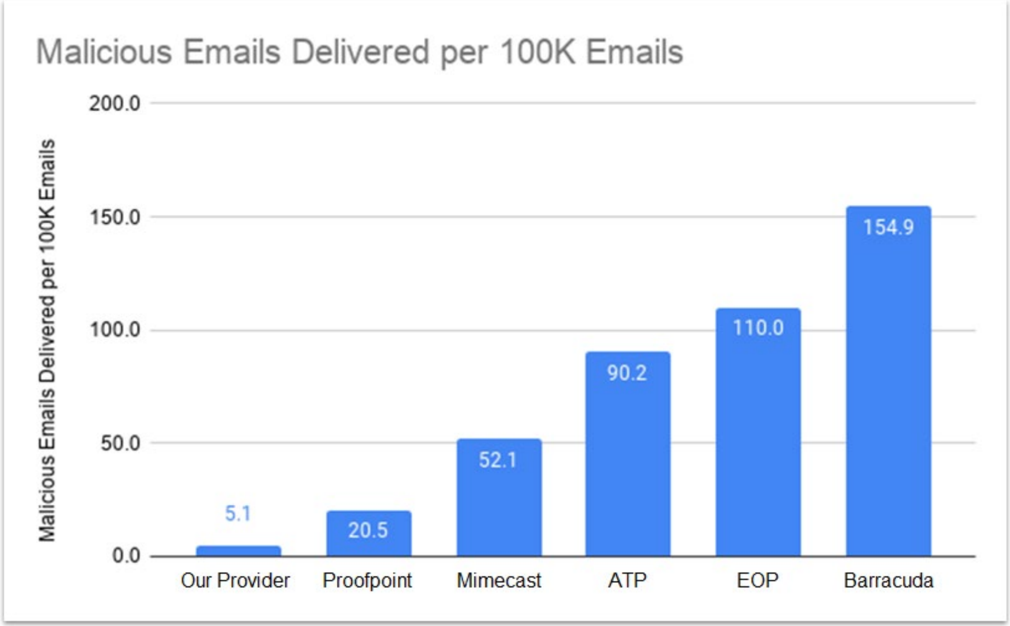

SharePoint
OneDrive
API
API
API
AVANAN
Microsoft Teams
Outlook
Secure Email Gateway (**SEG**)
Default Security (*EOP*)
Advanced Threat Protection (*ATP*)
Post-Delivery Protection (**CESS**)

Case Study vs Closest Competitors

360 million email sent through Email Security Providers Detection Engines, and this was the result.

Percentage Increase between the other study participants and **Our Provider**:

Proofpoint
302% Worse
Mimecast
922% Worse
ATP – Microsoft Adv Threat Protect
1669% Worse
Exchange Online Protection – Microsoft Default Security 2057% Worse
Barracuda
2937% Worse



The Solution: A new approach to email security

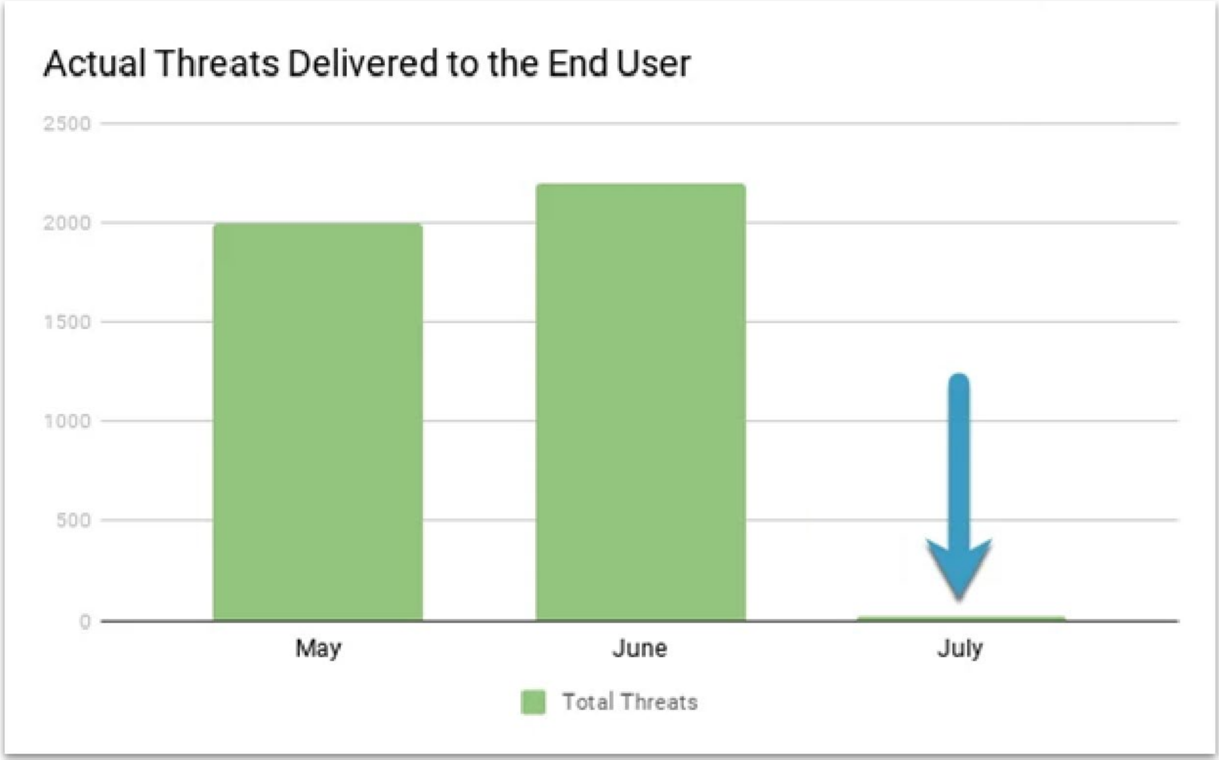
Case Study: Large Chemical Distributor

Case Study Results: 11K Mailboxes

With Our Solution they achieved:

- 99.2% Reduction in phishing attacks
- 71% Reduction in end user requests to SOC

In days, not months or years

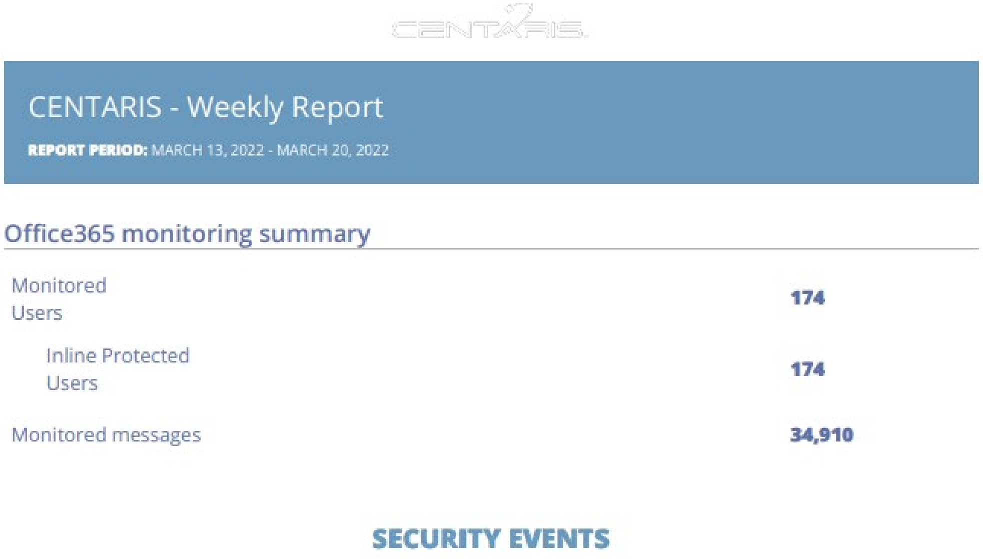


7/24/365 Security Operations Center (SOC) Support

Weekly Report

Weekly Report

- Phishing – top attacked users
- Phishing attacks – 5 week trend
- Malware attacks – 5 week trend
- Phishing - attacks per category
- User Interactions



CENTARIS - Weekly Report

REPORT PERIOD: MARCH 13, 2022 - MARCH 20, 2022

Office365 monitoring summary

Monitored Users	**174**
Inline Protected Users	**174**
Monitored messages	**34,910**

SECURITY EVENTS

Report Link

What else do we protect?

Connect any additional cloud applications during the 14-Day Assessment Period

OneDrive

SharePoint

Microsoft Teams

box

Office 365

Dropbox

CITRIX ShareFile

Two CCare Solution Offerings

- **CCare Email Security**
  - Advanced Anti-Phishing and Advanced Malware Protection
    - Smartphish Anti-Phishing
    - URL Click Protection
    - Configuration Security
    - Malware Sandboxing
- **CCare Email Compliance**
  - Include Advanced Anti-Phishing and Advanced Malware Protection plus
    - Data Loss Prevention (DLP)
    - Encryption for Office 365

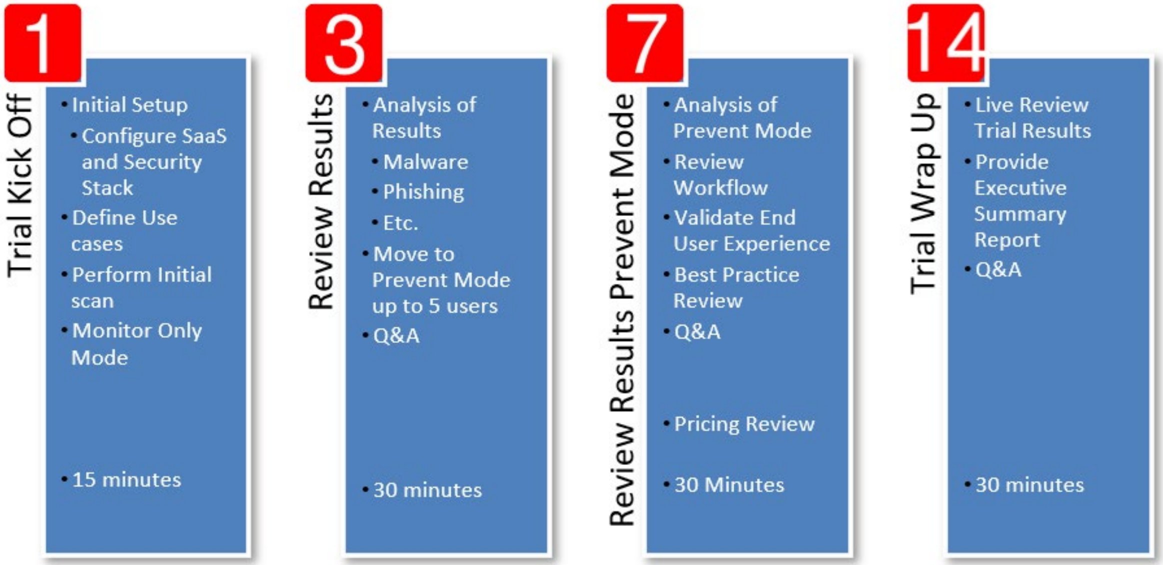
Next Steps … Sign up for an Assessment

Hassle-free Interactive 14-Day Assessment (2 Meetings)

To see how your environment stacks up this 14-Day Hassle-free Interactive Assessment takes a total time investment 45 to 60 minutes .. Can combine 7 & 14 days

To start it takes 5-Minutes to connect your O365 Applications with your Admin Credentials

The bulk of that time investment coming from reviewing your own data and learning about your very real risks and satisfying your curiosity



1

Trial Kick Off

- Initial Setup
  - Configure SaaS and Security Stack
- Define Use cases
- Perform Initial scan
- Monitor Only Mode
- 15 minutes

3

Review Results

- Analysis of Results
  - Malware
  - Phishing
  - Etc.
- Move to Prevent Mode up to 5 users
- Q&A
- 30 minutes

7

Review Results Prevent Mode

- Analysis of Prevent Mode
- Review Workflow
- Validate End User Experience
- Best Practice Review
- Q&A
- Pricing Review
- 30 Minutes

14

Trial Wrap Up

- Live Review Trial Results
- Provide Executive Summary Report
- Q&A
- 30 minutes

Next Centaris Webinar

Next Webinar in our Security Education Series

Managed Detection and Response … MDR is a 24x7 cybersecurity services that rapidly detects, analyzes, investigates, contains and actively responds to security threats.

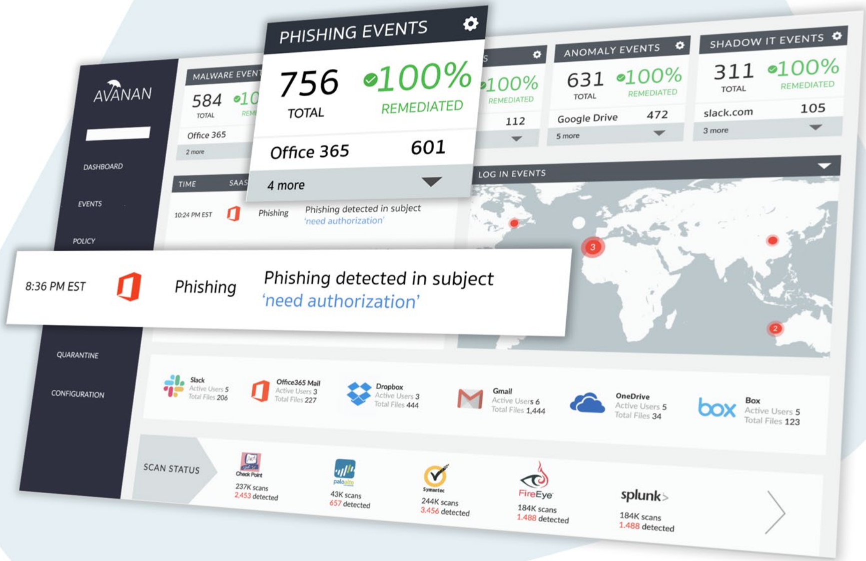
March 31, 2022 @ 1:30 pm

Thank You for Joining Us!

- A recording of this session will be emailed to all attendees.
- Please feel free to share the recording with your staff.

Thank You

CENTARIS™


AVANAN
DASHBOARD
EVENTS
POLICY
QUARANTINE
CONFIGURATION
MALWARE EVENTS
584 TOTAL
Office 365
2 more
PHISHING EVENTS
756 TOTAL
100% REMEDIATED
Office 365 601
4 more
100% REMEDIATED
112
ANOMALY EVENTS
631 TOTAL
100% REMEDIATED
Google Drive 472
5 more
SHADOW IT EVENTS
311 TOTAL
100% REMEDIATED
slack.com 105
3 more
LOG IN EVENTS
TIME
SAAS
10:24 PM EST
Phishing
Slack Active Users 5 Total Files 206
Office365 Mail Active Users 3 Total Files 227
Dropbox Active Users 3 Total Files 444
Gmail Active Users 6 Total Files 1,444
OneDrive Active Users 5 Total Files 34
Box Active Users 5 Total Files 123
SCAN STATUS
Check Point 237K scans 2,453 detected
paloalto 43K scans 657 detected
Symantec 244K scans 3,456 detected
FireEye 184K scans 1,488 detected
splunk 184K scans 1,488 detected

Phishing detected in subject 'need authorization'

8:36 PM EST Phishing Phishing detected in subject 'need authorization'