

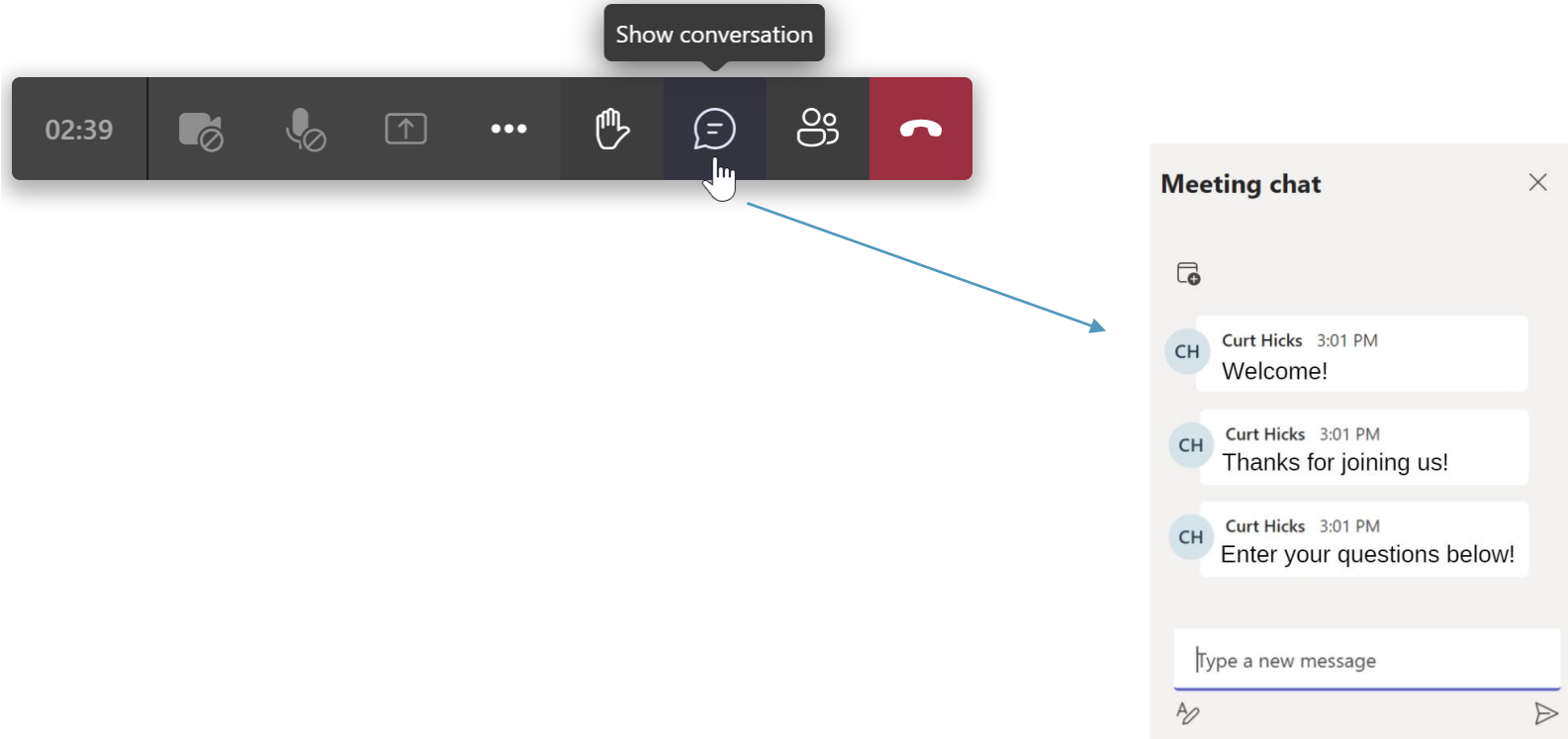


Office 365 Email & Collaboration Security Solution

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



Use the Teams Chat to post any questions



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

[Tweet](#)

[Share](#)

[Like 1](#)

[Share](#)

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

2019 Data Breach Investigations Report

Security Breaches Over Past Year

Which types of cybersecurity breaches have occurred in your organization in the past year? ■ 2021 ■ 2020



verizon
business ready

2019



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



The Problem with Phishing and Microsoft

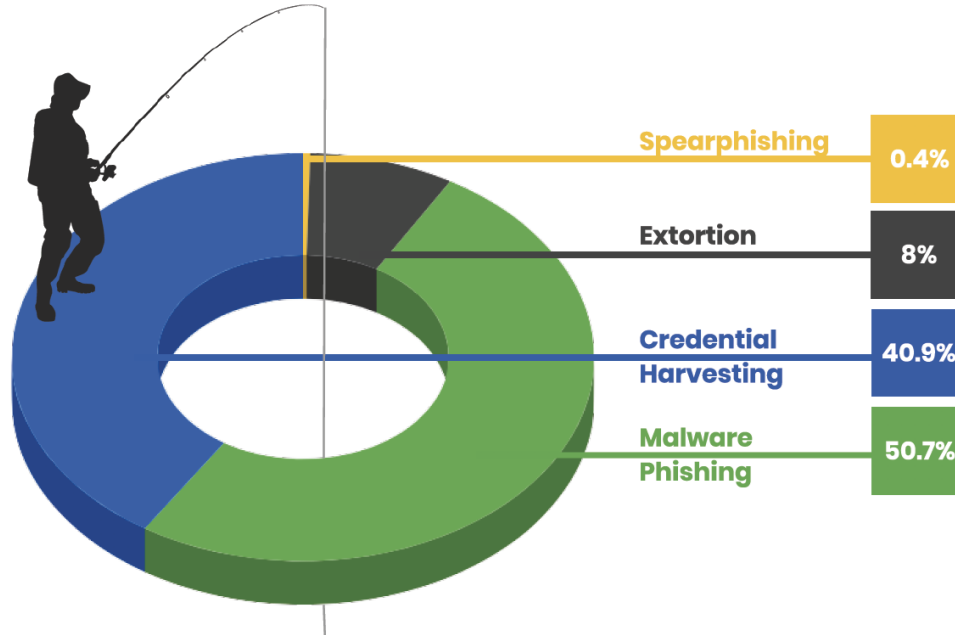
Why does Microsoft miss so many attacks?

- 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 on November 13 2018 was to pay October invoices for \$1,891.51 outstanding which was agreed when 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.



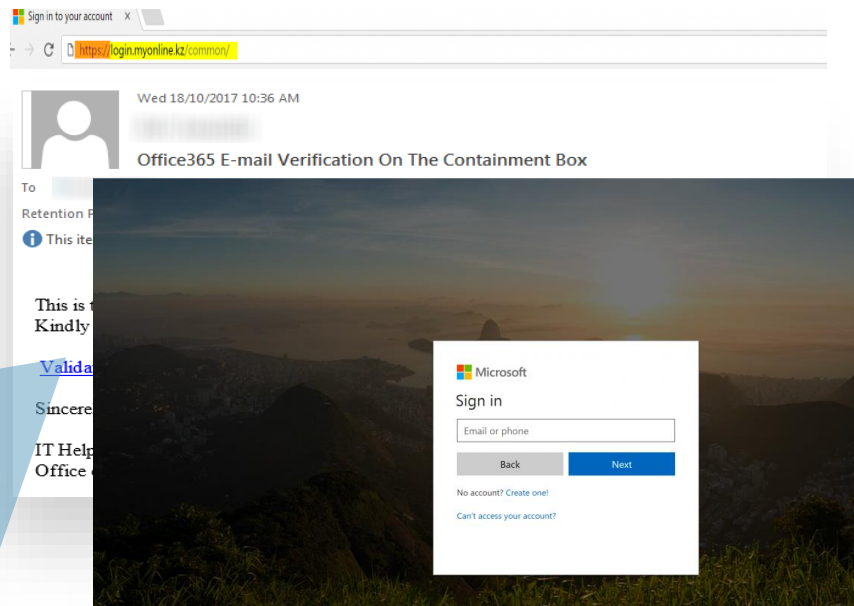
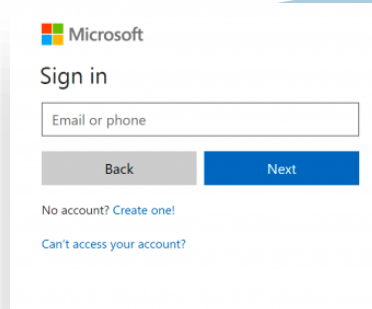
Invoice_1256.pdf
13K [View](#) [Download](#)

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



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

He‌llo‌

So‌I'm a‌ha‌cke‌r who‌ cra‌cke‌d yo‌o‌f we‌e‌ks ba‌ck.

Yo‌u‌e‌n‌re‌d yo‌u‌r pwd o‌n o‌i‌n‌rce‌pte‌d thi‌s.

He‌re‌i‌s the‌se‌cu‌ri‌ty pa‌sswo‌ti‌me‌o‌f co‌mpro‌mi‌se‌: Evergreen1

Cle‌a‌rly o‌ne‌ca‌n ca‌n cha‌nge‌:

I thi‌nk \$900 i‌s a‌n a‌cce‌pta‌ble‌co‌

Pa‌y wi‌th Bi‌tco‌i‌n.

My B‌TC wa‌lle‌t a‌ddre‌ss: 1AGEaKW2kKd453kAfrw9hvA3u

In ca‌se‌yo‌u‌do‌no‌t kno‌w ho‌w se‌nd mo‌ne‌y to‌the‌bi‌tco‌i‌n w

Imme‌di‌a‌te‌ly a‌fte‌r ge‌tti‌ng t‌i‌nfo‌rma‌ti‌o‌n wi‌ll be‌stra‌i‌

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

Timyo

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.

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

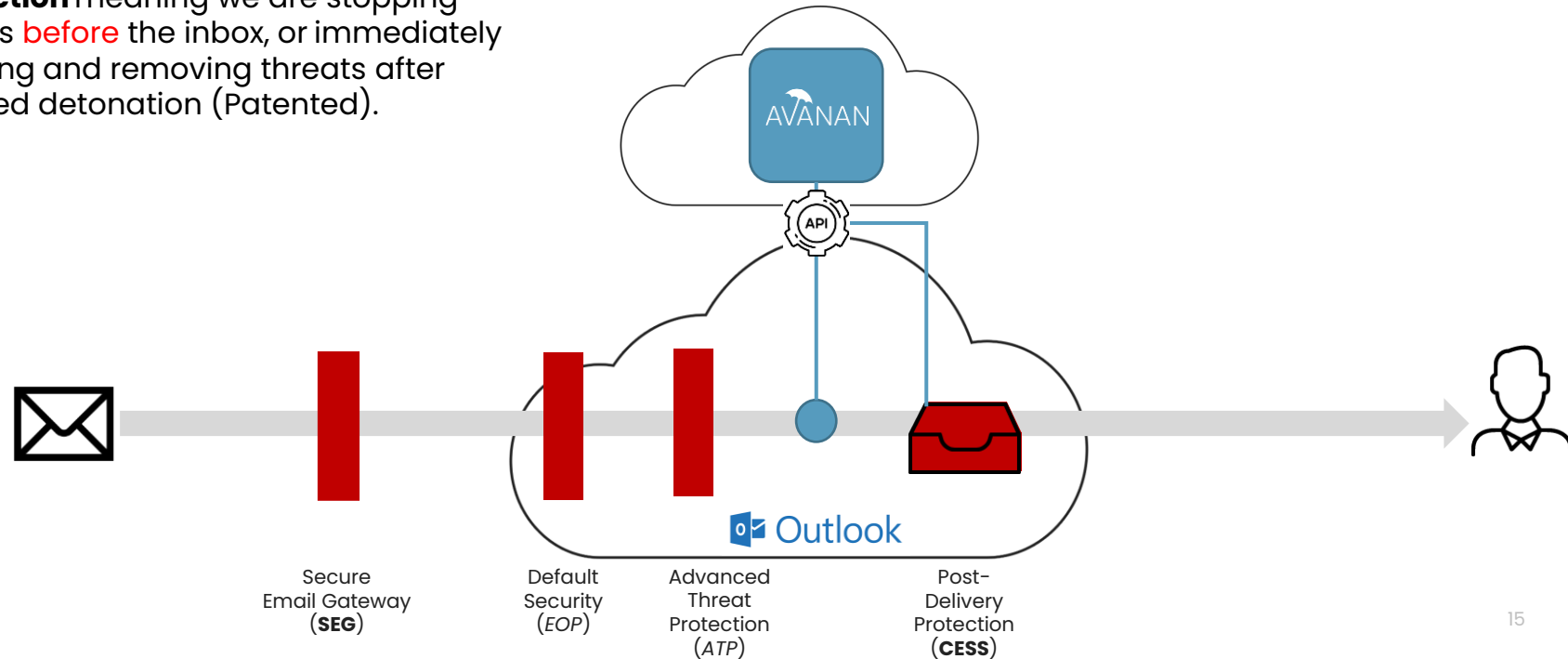
What if you think a flagged email is really legit?

Rely on our team of experts to manage end-user reports of suspicious emails and requests to release quarantined emails.

- 7/24/365 Remediation of all escalated tickets with an SLA within 30 minutes – and often less than 10.
- If a user is notified that an email was quarantined as malicious or phishing, they can request an investigation to ensure that it wasn't a false positive. If a user thinks an email is suspicious, all they have to do is press "Report as Phishing," and it opens a ticket in our system for our analysts to review. Our experts review the email and then choose from a variety of actions, such as:
 - Marking as Junk/Spam
 - Releasing from quarantine
 - Creating whitelists
 - Creating blacklists
 - Marking as phishing
 - Cross-customer mitigation

The Solution to eliminating 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).

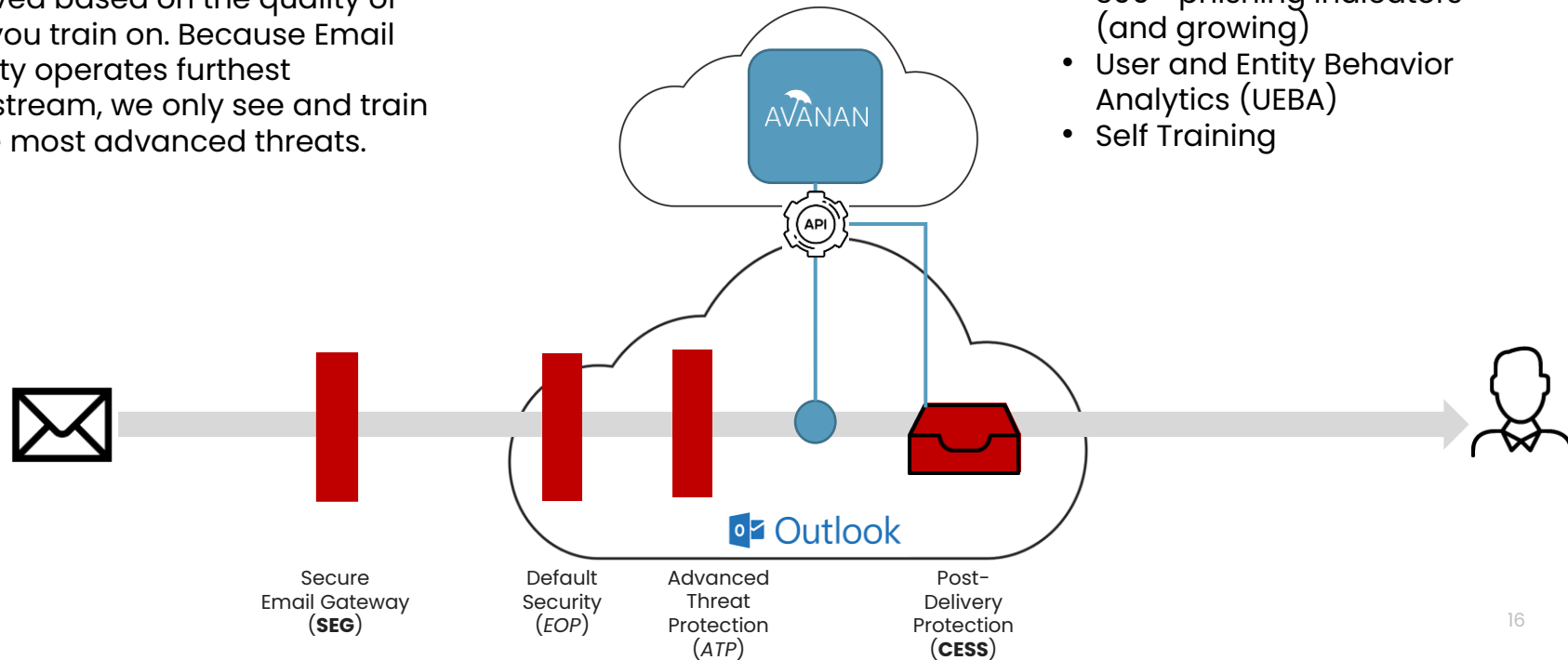


The Solution to eliminating bad messages lies in what makes our solution different.

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.

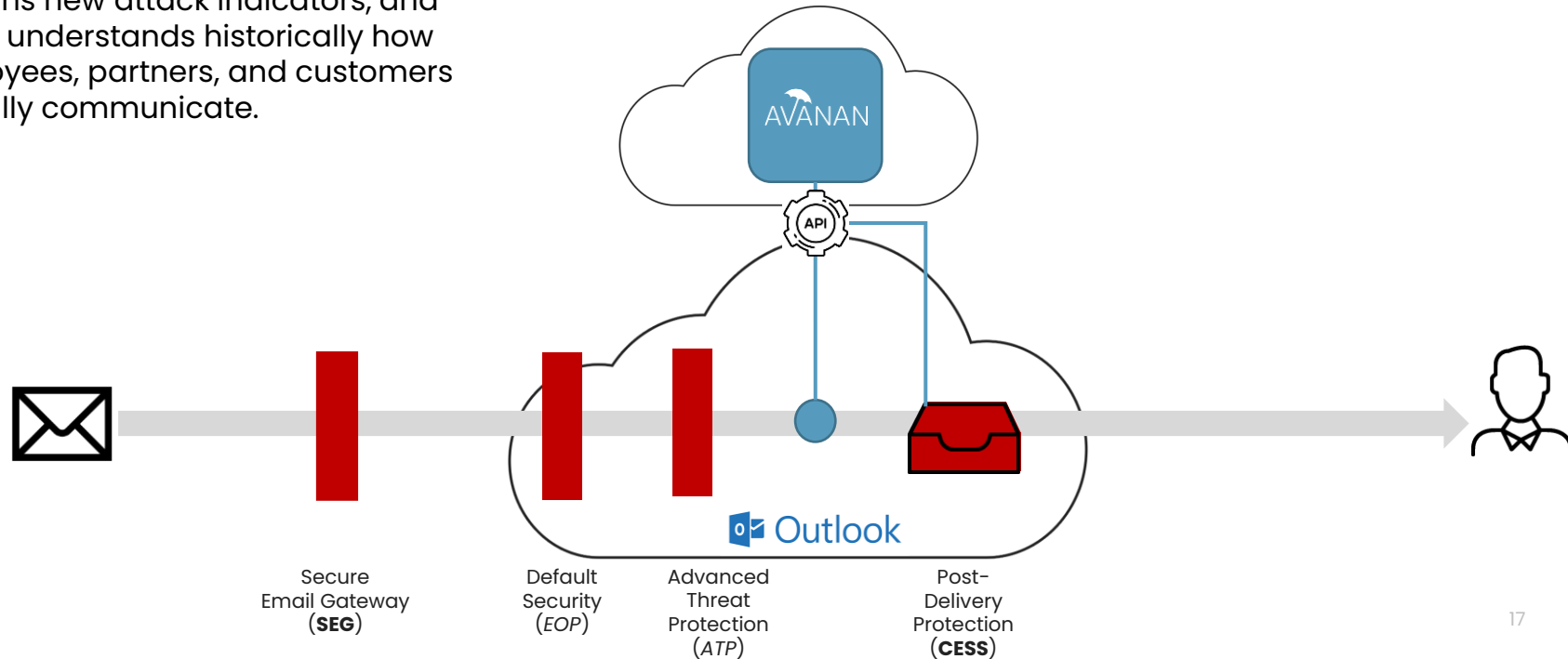
SmartPhish Alone Leverages

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



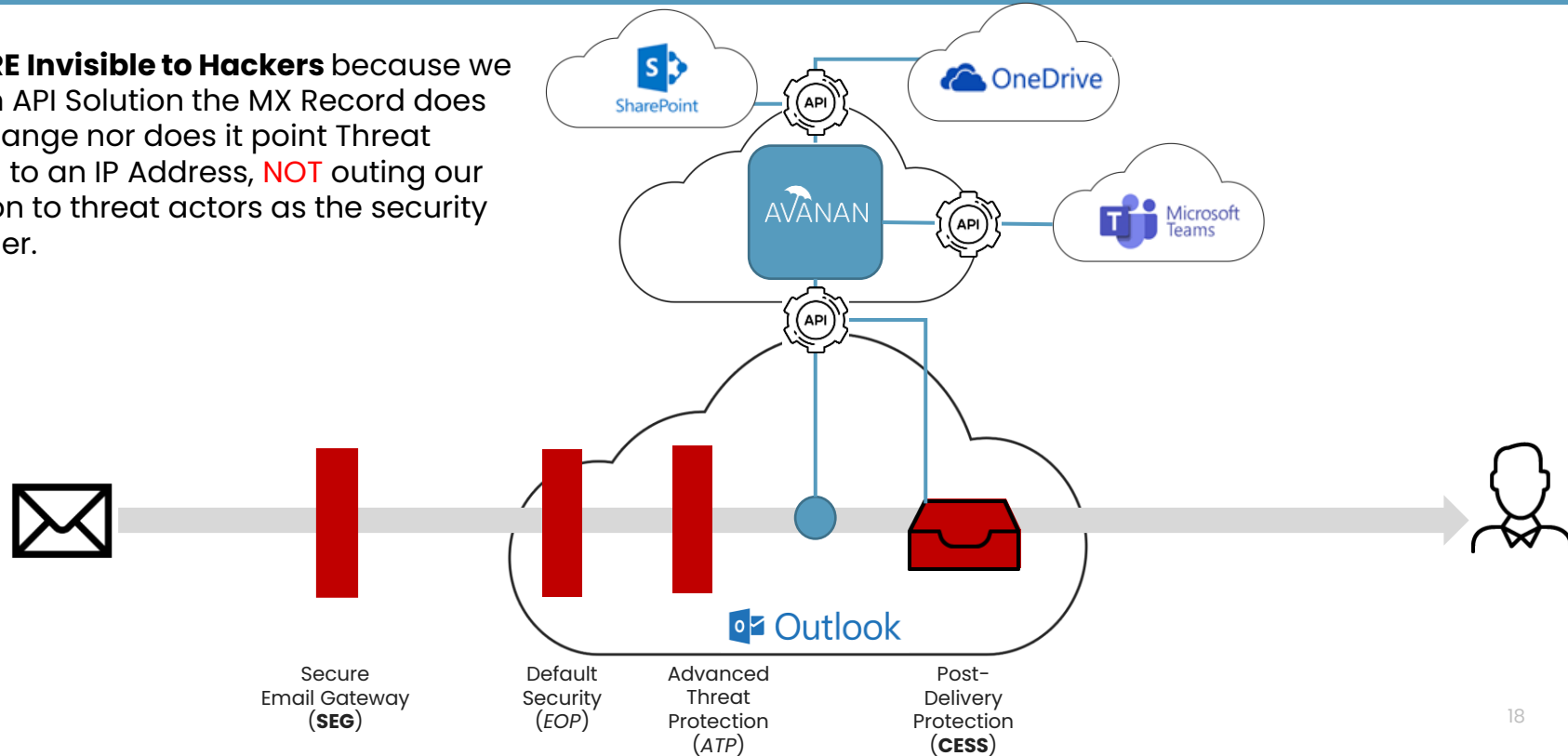
The Solution to eliminating bad messages lies in what makes our solution different.

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



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

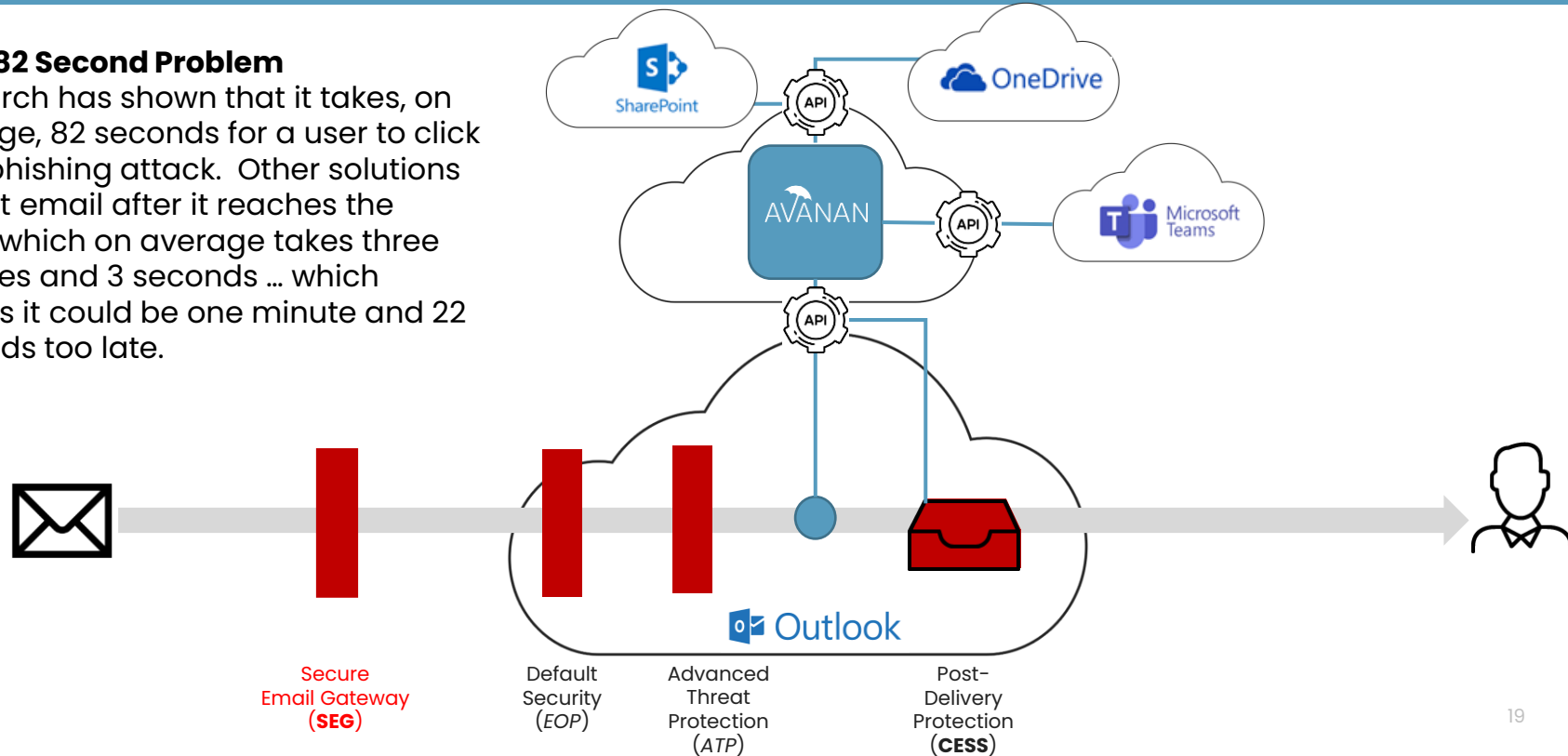
We ARE Invisible to Hackers because we are an API Solution the MX Record does not change nor does it point Threat Actors to an IP Address, **NOT** outing our solution to threat actors as the security provider.



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

API's 82 Second Problem

Research has shown that it takes, on average, 82 seconds for a user to click on a phishing attack. Other solutions retract email after it reaches the inbox which on average takes three minutes and 3 seconds ... which means it could be one minute and 22 seconds too late.



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

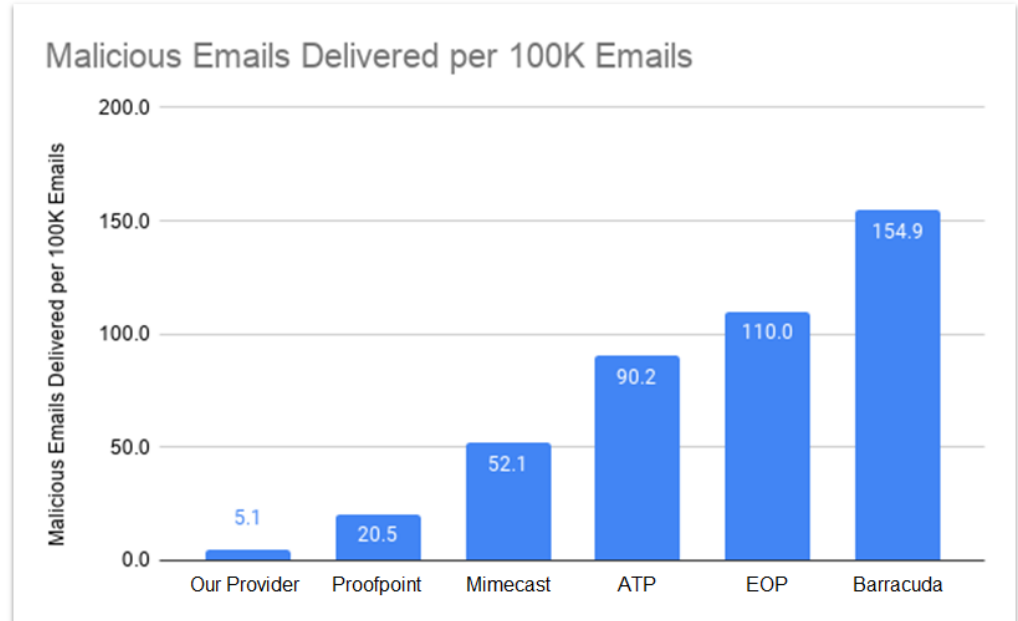
ATP – Microsoft Adv Threat Protect

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

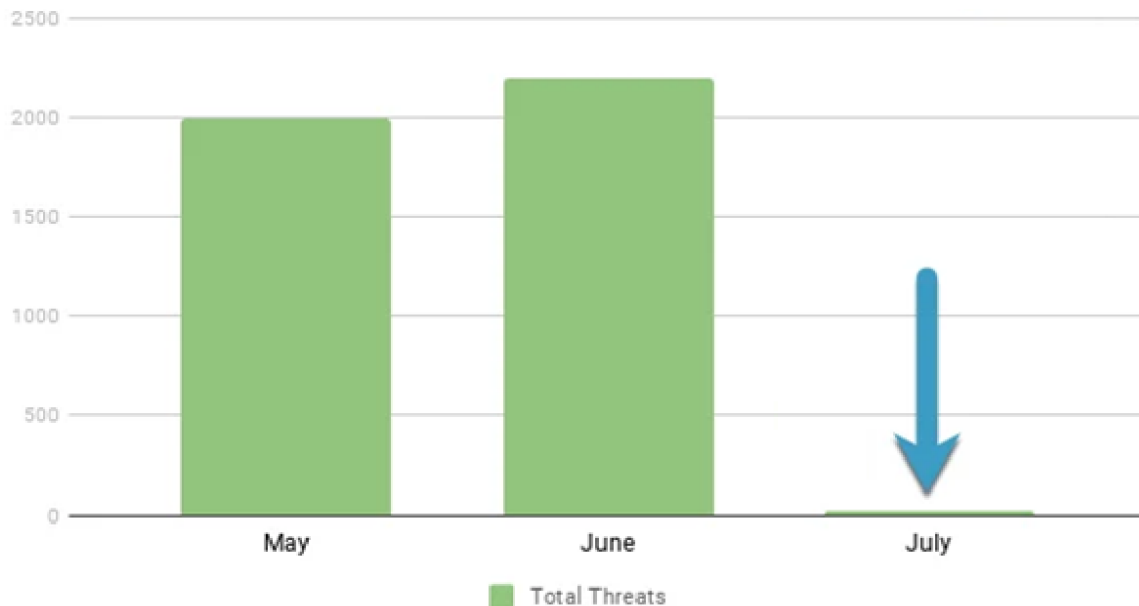
Case Study Results: 11K Mailboxes

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

Actual Threats Delivered to the End User



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](#)

Two CCare Solution Offerings

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

What else do we protect?

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



What do we do for Teams, OneDrive and SharePoint?

Malicious File Detection – Every file is sandboxed before downloading.

URL Filtering for File Sharing – Each file is scanned and analyzed for malicious links which are then blocked across all file share apps.

Malware Protection for File Sharing – All attachments are tested and executed to ensure there is no malicious content.



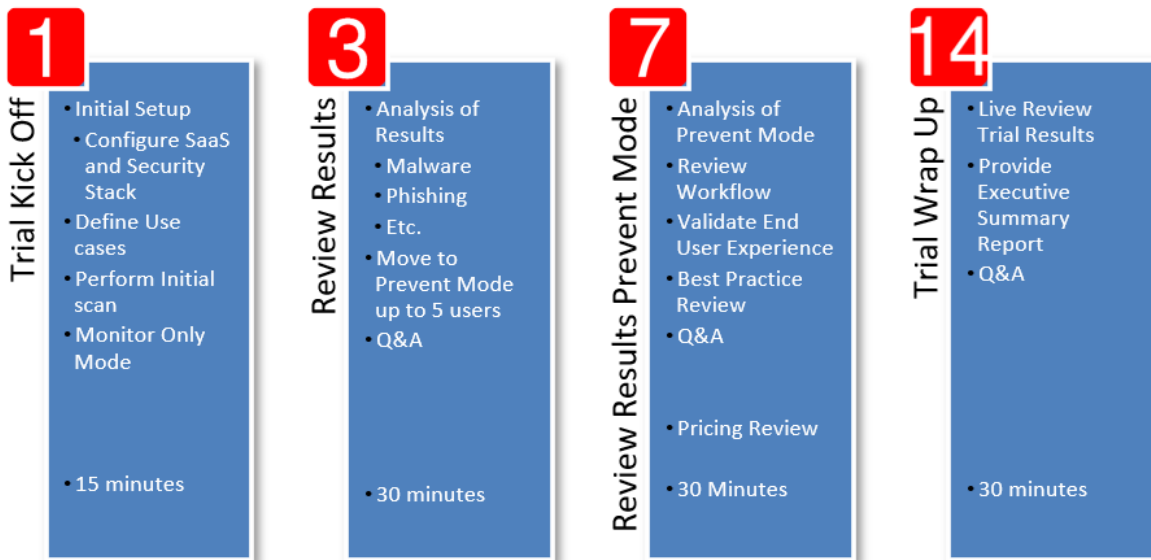
Next Steps ... Sign up for an Assessment

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



Next Centaris Webinar

Next Webinar in our Security Education Series

Security Journey ... The landscape has changed and what worked for security in the past is not anywhere near adequate for today's world. Learn what you need to plan for now.

May 12, 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™

