

13 email threat types

To defend against

Speakers



Name

Title, company



Name

Title, company



Name

Title, company



| [Partner] Overview



On average, there is a **cyberattack** every **39 seconds**



Cybint News' 15 Alarming Cyber Security Facts and Status



95% of all **cyber incidents** are **human-enabled**

ResearchGate December 2018 Holistica – Journal of Business and Public Administration



Impact of email attacks on organizations

\$20B

Ransomware costs
in 2021

43%

of organizations
fell victim to spear
phishing attacks

1 in 7

organizations
experienced an
account takeover

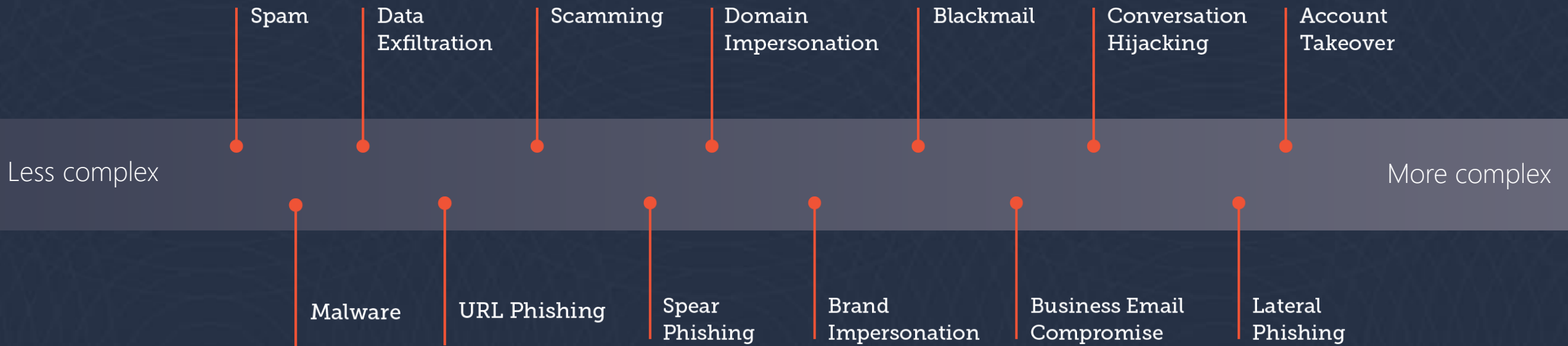


Email threat trends



Email attack complexity is increasing

Introducing the email threat taxonomy



Business Email Compromise decoded

To: Daniel Diamond <daniel_diamond@acme.org>
From: John McDonald <ceo.mail@acrne.net>
Reply to: John McDonald <ceo.mail@acrne.net>
Date: Dec 03, 2018
Subject: Wire Transfer Request

Hi Daniel,

Are you in the office today? I need you to process a wire transfer for me. Get back to me as soon as you get this.

Regards,
John

Sent from my iPad.

1. Impersonation techniques

2. Sense of urgency

3. From an authority / executive

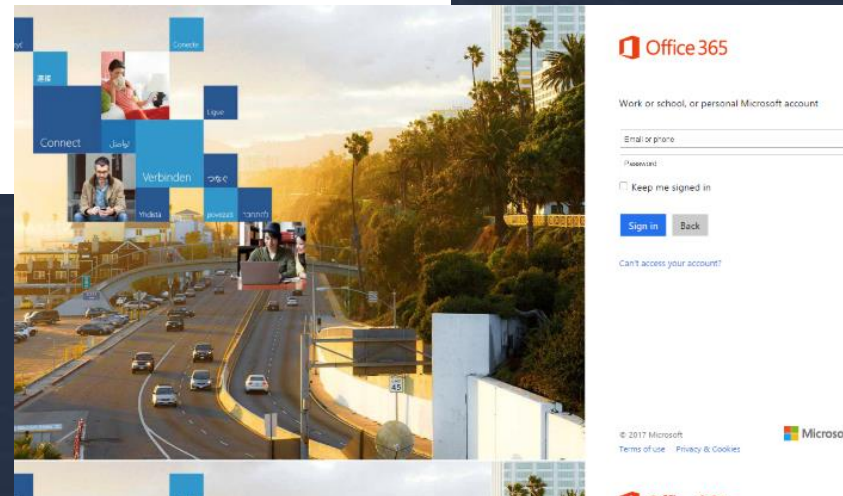
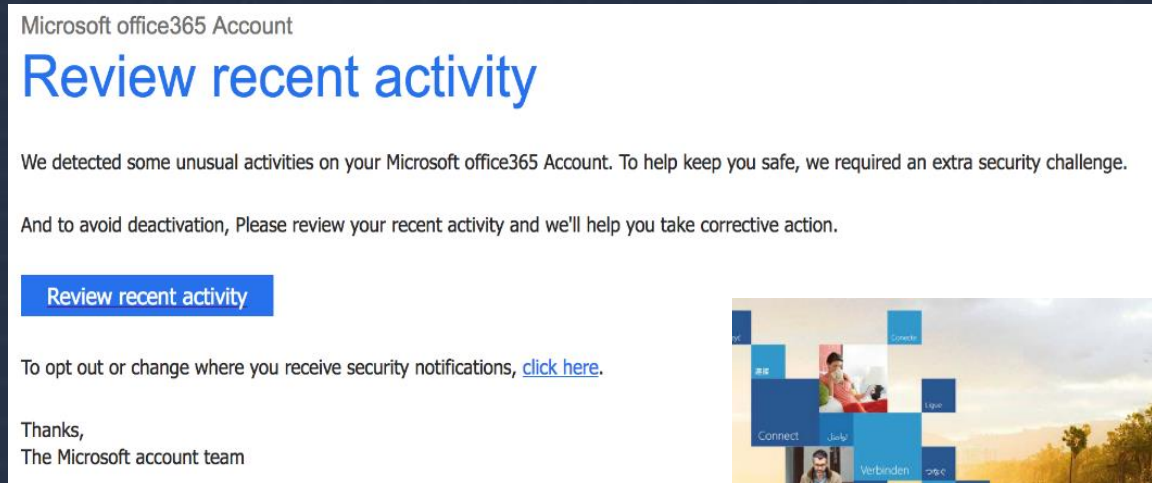
High reputation senders | No links | No attachments



Service Impersonation decoded

1. No malicious payload

2. Hosted on high reputation domain



3. Unusual email address and landing page



Account Takeover decoded

Compromised credentials through phishing attacks, malware or database breaches



Account Takeover

Threat type

Account
Takeover

Compromised credentials through phishing attacks, malware or database breaches

Watch, learn, collect information.
Compromise more accounts



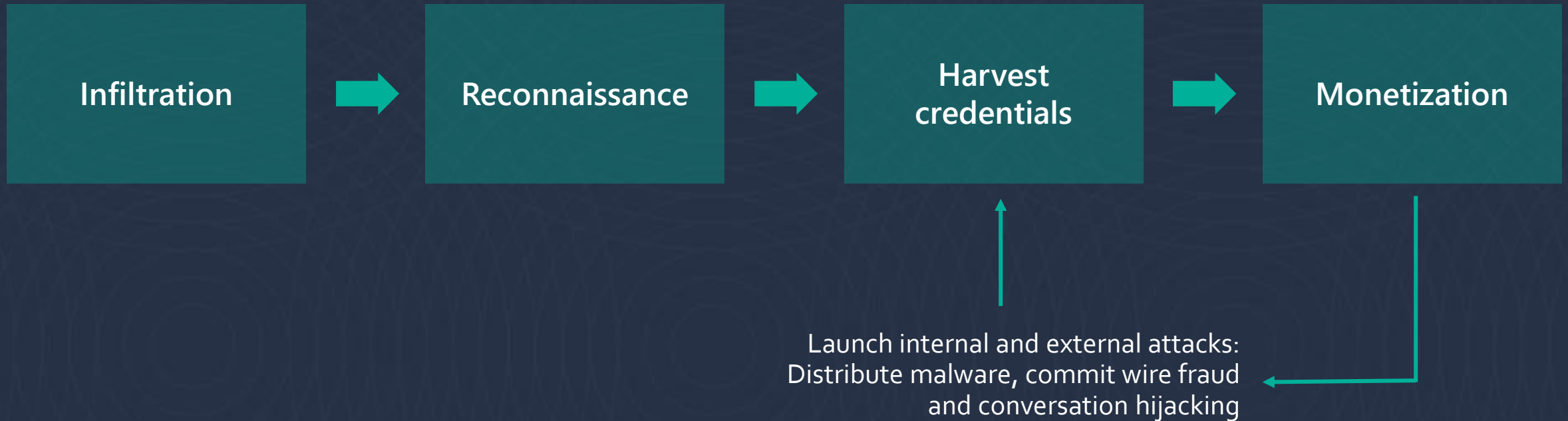
Account Takeover

Threat type

Account Takeover

Compromised credentials through phishing attacks, malware or database breaches

Watch, learn, collect information.
Compromise more accounts



Account Takeover: real-life example

From: Microsoft Outlook <ajohnson@school.k12.ga.us>
Reply to:
Date: Mar 27, 2018
Subject: Scanned Document Notification

This message is from a trusted sender.

OneDrive
You have a secured message

Some one uploaded a Pdf file on our secure server for your view only.

[View Now](#)

1. Email from a trusted sender

2. Link does not point to Microsoft



Beating threats with the right protection



Two forms of defense. You need both

THREAT TYPES	EMAIL GATEWAY	API-BASED INBOX DEFENSE
Spam	●	○
Malware	●	○
Data Exfiltration	●	○
URL Phishing	◐	●
Scamming	◐	●
Spear Phishing	○	●
Domain Impersonation	○	●
Service Impersonation	○	●
Blackmail	◐	◐
Business Email Compromise	○	●
Conversation Hijacking	○	●
Lateral Phishing	○	●
Account Takeover	○	●

○ Does not provide sufficient protection ◐ Provides some protection ● Provides best protection



Gateway based defenses work well for...

Spam, malware, data exfiltration



Inbox based defenses work well for....

Remaining 10 threat types



Gateway-based pros and cons



Gateway defense: great for high volume attacks

Spam

Gateway:

Blocked before it hits mail server or inbox

API Inbox defense:

Can overwhelm the server and impact inbox performance

Malware

Gateway:

Signature matching and sandboxing

API Inbox defense:

Large volume of malware can impact inbox performance

Data Exfiltration

Gateway:

DLP and encryption to protect sensitive data

API Inbox defense:

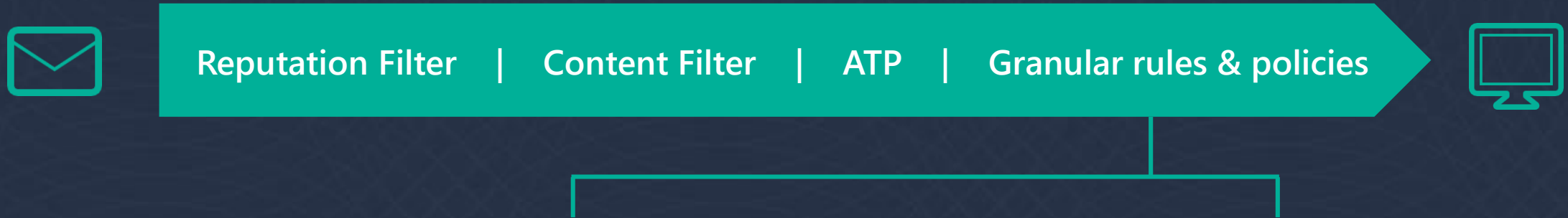
APIs can't remediate lost data post delivery



Limits of gateway approach

Threat type

Business Email
Compromise



Reputation Filter

Content Filter

ATP

Granular rules & policies

How it works?

- Configure unlimited number of policies
- Use LDAP
- Focus on highly targeted employees

Why not effective?

- Not scalable solution
- Use of LDAP has limits
- Does not take context into account



Impersonating Matthew Johnson

LDAP rules can miss

Threat type

Business Email
Compromise

To: Lauren Crawl
From: Matthew Johnson
Subject: Quick request



To: Lauren Crawl
From: Matthew R. Johnson
Subject: Quick request



To: Lauren Crawl
From: Johnson Matthew
Subject: Quick request



To: Lauren Crawl
From: Matt Johnson
Subject: Quick request



Deceptive language

Content filters can miss

Threat type

Business Email
Compromise

To: Lauren Crawl
From: Matthew Johnson
Subject: Quick request



... I need you to process a wire transfer?...

... funds transfer...



... money transfer...



... make a payment ...



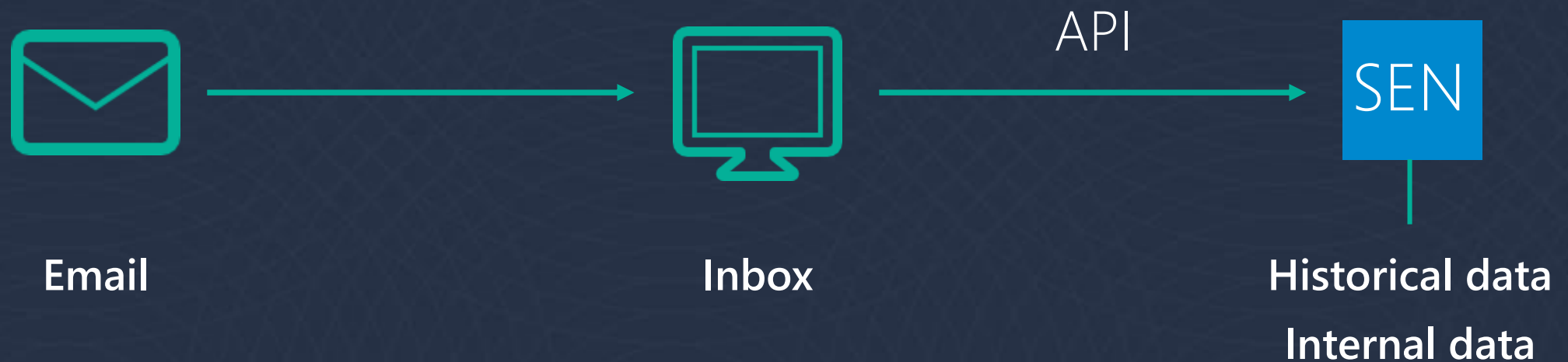
... process invoice...



API-based pros and cons



What is API-based Inbox Defense?



Inbox defense technology evaluates many factors



Inbox defense technology finds unique patterns



Understands abnormal behavior based on an **identity graph**

Gateways = 100s of rules for 1000s of individuals = **not scalable**



API defense: less effective for high volume attacks

Spam

Gateway:

Blocked before it hits mail server or inbox

API Inbox defense:

Can overwhelm the server and impact inbox performance

Malware

Gateway:

Signature matching and sandboxing

API Inbox defense:

Large volume of malware can impact inbox performance

Data Exfiltration

Gateway:

DLP and encryption to protect sensitive data

API Inbox defense:

APIs can't remediate lost data post delivery



Strategies to improve your email protection



Read the eBook



Next steps

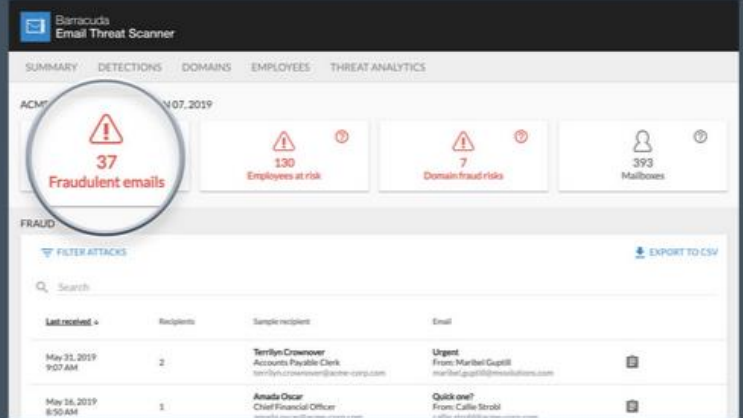
1. Protect against all 13 threats with Email gateway and API-based inbox defense
2. Educate your users on latest email threats
3. Automate & streamline incident response



Get started today

- Run free Email Threat Scan
- Identify gaps in your current email protection
- Easy to set up
- Fast results

Detect email threats that got past your email gateway.



The screenshot shows the Barracuda Email Threat Scanner dashboard. At the top, there are navigation tabs: SUMMARY, DETECTIONS, DOMAINS, EMPLOYEES, and THREAT ANALYTICS. Below these, there are four summary cards: '37 Fraudulent emails' (circled in red), '130 Employees at risk', '7 Domain fraud risks', and '393 Mailboxes'. A 'FRAUD' section is visible with a 'FILTER ATTACKS' button and an 'EXPORT TO CSV' link. Below this is a table of detected threats.

Last received	Recipients	Sample recipients	Email
May 31, 2019 9:07 AM	2	TerryJen.Crowner Accounts Payable Clerk terryjen.crowner@acmer.com	Urgent From: Maribel Cugat maribel.cugat@esocialhubs.com
May 16, 2019 8:50 AM	1	Amade Oscar Chief Financial Officer amadeoscar@acmer.com	Quick owl From: Celia Strobl celia.strobl@acmer.com

Fraud summary
Our artificial intelligence platform understands email sender intent to detect anomalies such as email impersonation and account takeover.

5,000+ organizations
have run this scan and discovered advanced threats in their Office 365 mailboxes.

8,000+ scans completed
since 2018

8.5 million mailboxes
have been scanned for threats

4 million spear phishing attacks
identified to date



Multi-layered email protection

Human Firewall

Security Awareness Training

Fraud Protection

AI-Based Spear Phishing Protection
DMARC to Prevent Brand Hijacking

Resiliency

Cloud Backup

Email Continuity

Gateway Defense

Inbound/Outbound
Security

Encryption and DLP for
Secure Messaging

Archiving for Compliance

O365 | G Suite | Exchange



<<MSP PARTNER>>Email Protection Suite

Awareness



API Inbox Defense



Resiliency



Gateway Defense



Thank You

