Protecting Your Email Perimeter

cStor
We look beyond IT

mimecast™

J. Peter Bruzzese
Mimecast Strategic
Technical Consultant

Andrew Roberts
Chief Cybersecurity Strategist
cStor

cStor: AN AWARD-WINNING PROVIDER

- Helps clients solve tough IT challenges with best-of-breed technology and expert consulting
- Creates and implements end-to-end solutions to fit your business needs
- Helps create a cost-effective architecture
- Displays a competitive advantage over other providers
- Creates flexibility by offering vendor agnostic solutions
- Always puts clients first

We look beyond IT

cStor

SOLUTION OFFERINGS

Professional Recommendations to Ensure Your Infrastructure
Evolves Alongside Your Business

DIGITAL TRANSFORMATION

CYBERSECURITY

DATA CENTER SOLUTIONS

OUR APPROACH

Our mission is to put people on a path to success

Clients First

Vendor Agnostic

Highly Specialized

cStor SERVICES

- CONSULTING AND OPTIMIZATION
- CLOUD
- STAFF AUGMENTATION
- CYBERSECURITY
- DATA MIGRATION
- DELIVERY
- MANAGED SERVICES

We look beyond IT

Protecting Your Email Perimeter

J. Peter Bruzzese

Mimecast Strategic
Technical Consultant

mimecast®

Protecting Your Email Perimeter

with J. Peter Bruzzese

MVP Microsoft Most Valuable Professional

CLIPTRAINING

ConversationalGeek

InfoWorld

PLURALSIGHT

J. Peter Bruzzese

- 8x awarded Microsoft MVP (2010-2019)
- Co-Founder of ClipTraining.com and ConversationalGeek.com
- Technical author with over a dozen books sold internationally
- Technical speaker for Techmentor, Connections, MEC and TechEd/Ignite
- Journalist for MSExchange.org, Redmond Magazine (and others)
- Journalist for InfoWorld (Enterprise Windows column) and Petri.com
- Instructor for Pluralsight on Exchange 2010/2013/2016/O365 courses
- Mimecast Strategic Technical Consultant and Techvangelist

No Silver Bullet

Colonial Pipeline ransomware attack highlights US vulnerability: Experts

Many American companies have not kept pace with the security threat, they say.

ZDNet

Ransomware: Meat firm JBS says it paid out $11m after attack

Liam Tung · 3 days ago

Like | 8

Global meatpacker JBS USA has paid $11 million in Bitcoin to cyberattackers that encrypted its files and disrupted operations in the US and Australia with ransomware, the company has said.

EDUCATION

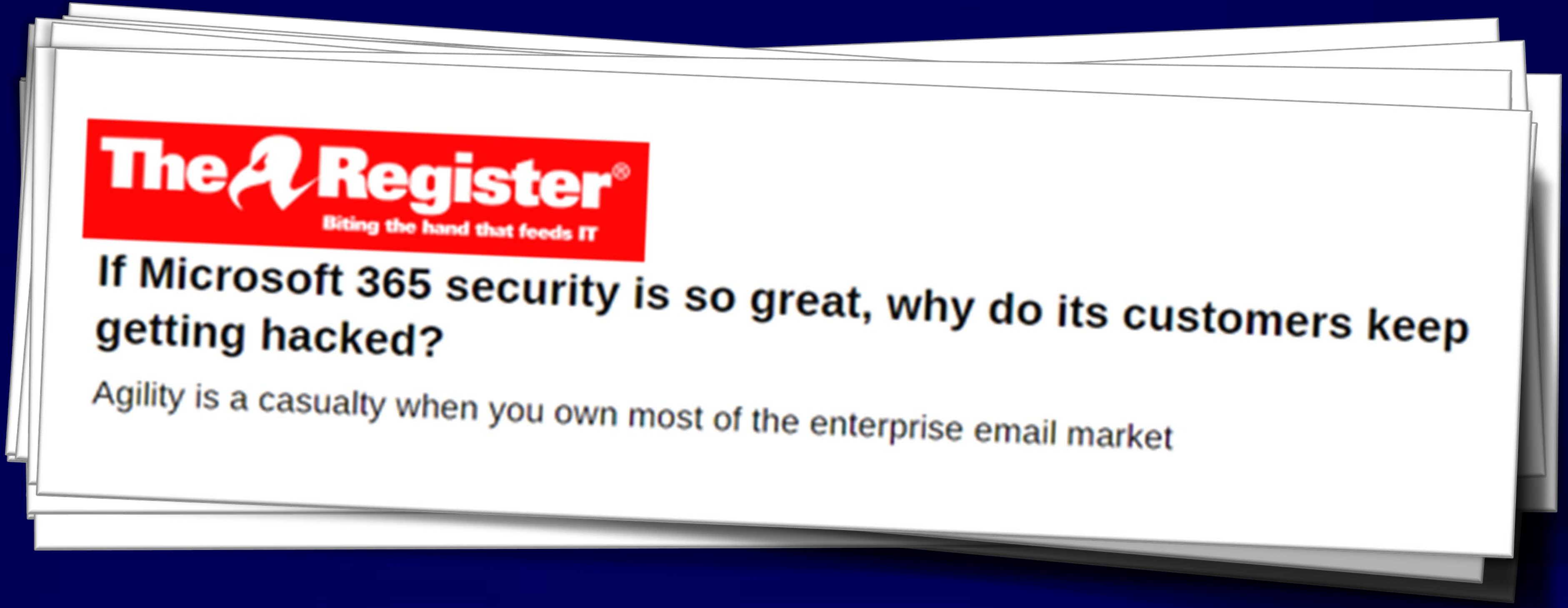
Ransomware attacks on the UK education sector

04TH JUNE 2021

The UK official National Cyber Security Centre (NCSC) says that it's investigating another increase in ransomware attacks against schools, colleges and universities in the UK.

The NCSC emphasises again the need for the sector to protect networks to prevent ransomware attacks. The NCSC urges all to follow guidance on 'Mitigating malware and ransomware.' This was updated in March and details steps to take to disrupt ransomware

Organizations are more vulnerable than ever…



The Register®

Biting the hand that feeds IT

If Microsoft 365 security is so great, why do its customers keep getting hacked?

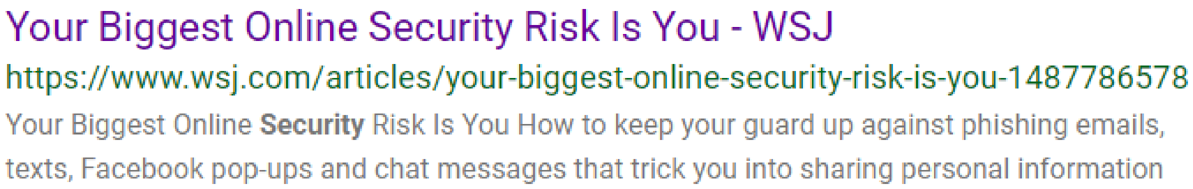
Agility is a casualty when you own most of the enterprise email market

Attacks are designed to succeed in today’s M365 dependent world…

Often… the Danger Starts with Email

90+% of all attacks start with some form of phish (some say it's higher)

- According to the Wall Street Journal "About 97% of all cyber attacks start with phishing"



Your Biggest Online Security Risk Is You - WSJ

https://www.wsj.com/articles/your-biggest-online-security-risk-is-you-1487786578

Your Biggest Online **Security** Risk Is You How to keep your guard up against phishing emails, texts, Facebook pop-ups and chat messages that trick you into sharing personal information

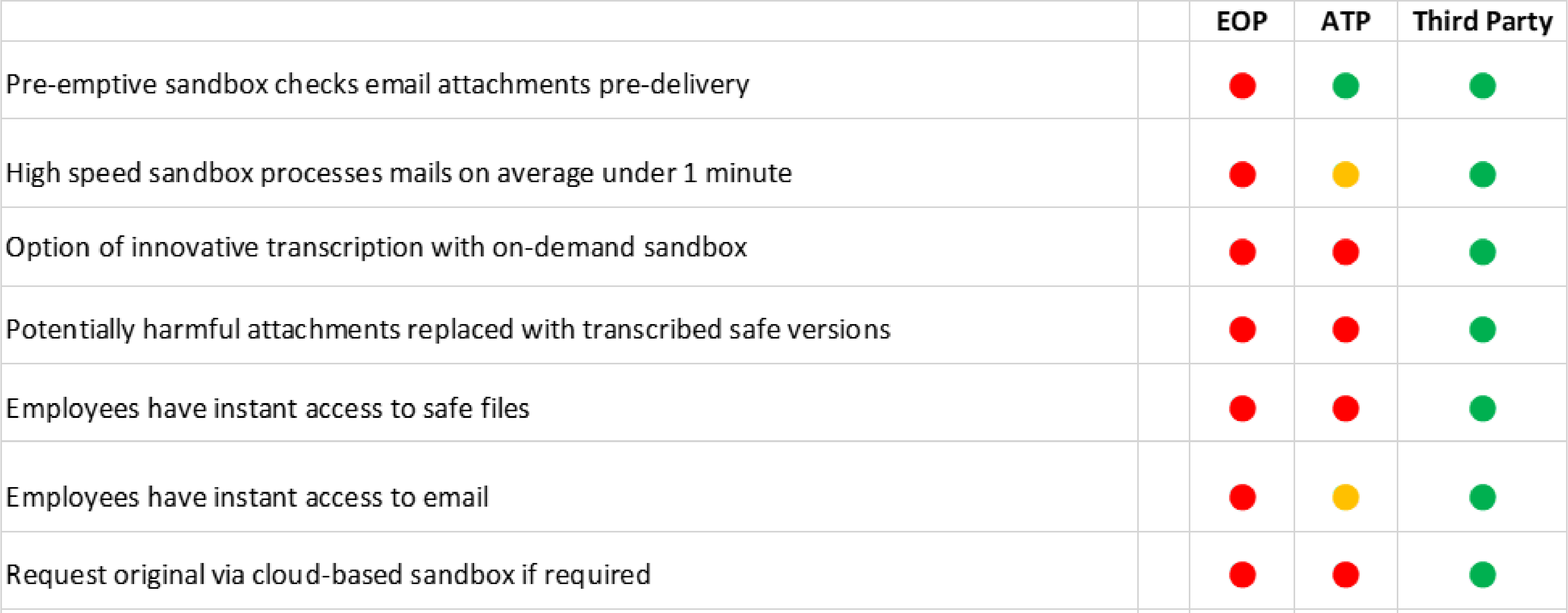
Security Risk

- Built-in (M365) vs Bolt-on
  - EOP/Defender for M365 vs. Third-party Solutions
  - Features and Efficacy
  - Primary focus points:
    - Attachment protection (ransomware, malware, etc.)
    - URL scanning (spear-phishing, etc.)
    - Impersonation protection
    - Internal email protection
    - Domain spoofing (SPF, DKIM, DMARC, etc.)

Microsoft 365 Efficacy

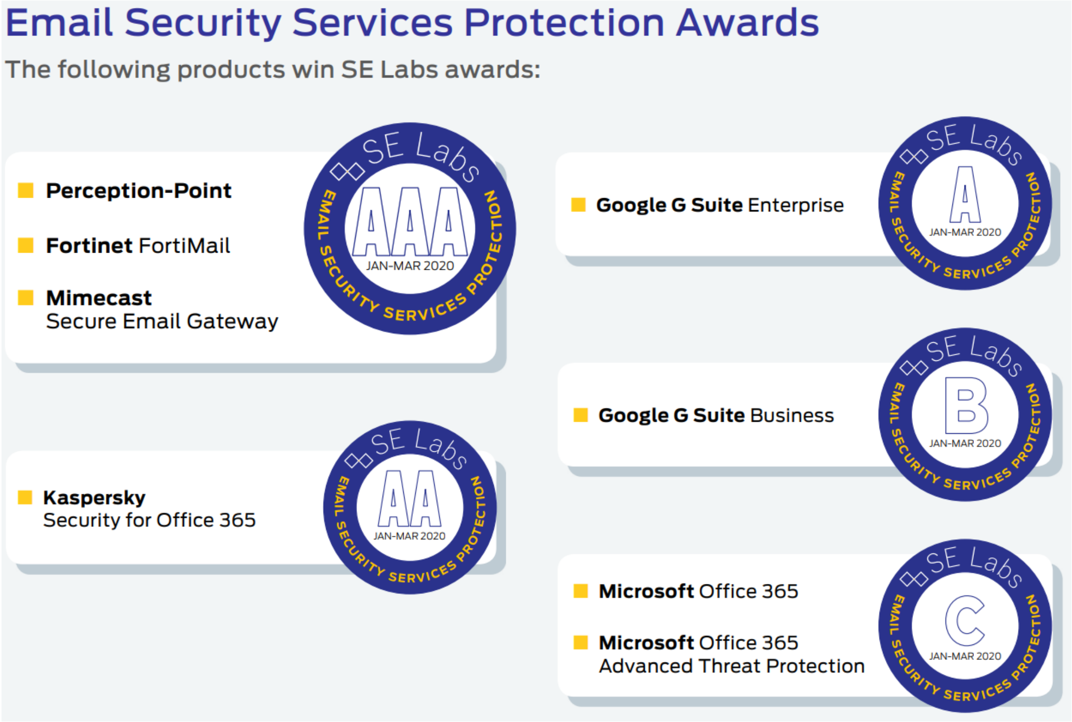
MICROSOFT 365
CLOUD
COMMUNITY

Feature/Efficacy Example: Attachments



		EOP	ATP	Third Party
Pre-emptive sandbox checks email attachments pre-delivery		🔴	🟢	🟢
High speed sandbox processes mails on average under 1 minute		🔴	🟡	🟢
Option of innovative transcription with on-demand sandbox		🔴	🔴	🟢
Potentially harmful attachments replaced with transcribed safe versions		🔴	🔴	🟢
Employees have instant access to safe files		🔴	🔴	🟢
Employees have instant access to email		🔴	🟡	🟢
Request original via cloud-based sandbox if required		🔴	🔴	🟢

SE Labs



Email Security Services Protection Awards

The following products win SE Labs awards:

- **Perception-Point**
- **Fortinet** FortiMail
- **Mimecast** Secure Email Gateway

SE Labs
AAA
JAN-MAR 2020
EMAIL SECURITY SERVICES PROTECTION

- **Google G Suite** Enterprise

SE Labs
A
JAN-MAR 2020
EMAIL SECURITY SERVICES PROTECTION

- **Google G Suite** Business

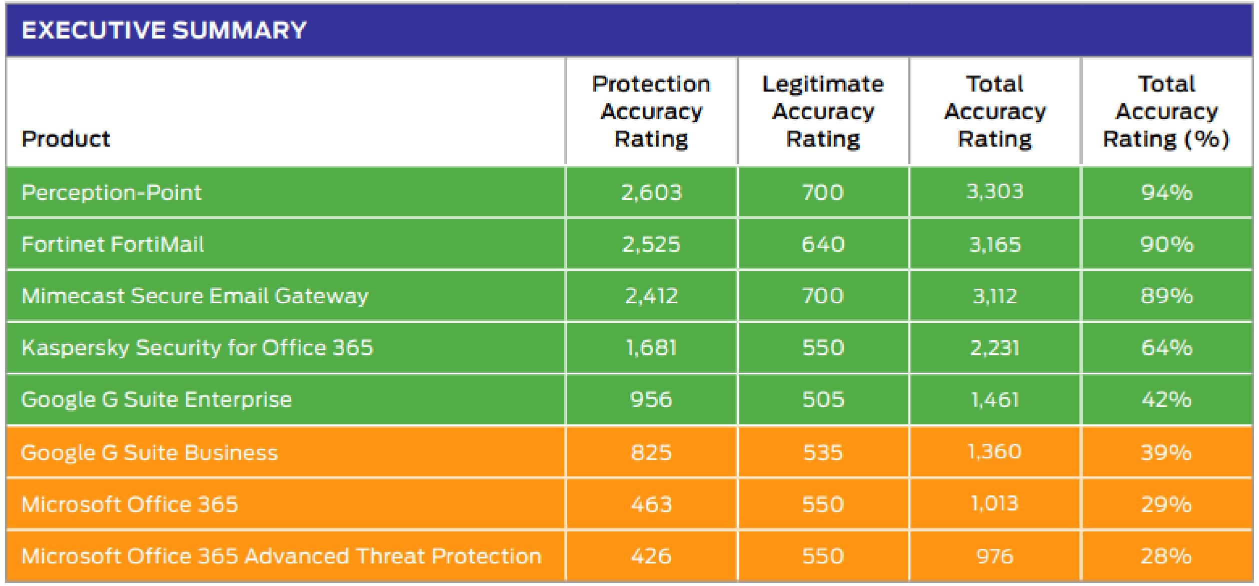
SE Labs
B
JAN-MAR 2020
EMAIL SECURITY SERVICES PROTECTION

- **Kaspersky** Security for Office 365

SE Labs
AA
JAN-MAR 2020
EMAIL SECURITY SERVICES PROTECTION

- **Microsoft** Office 365
- **Microsoft** Office 365 Advanced Threat Protection

SE Labs
C
JAN-MAR 2020
EMAIL SECURITY SERVICES PROTECTION



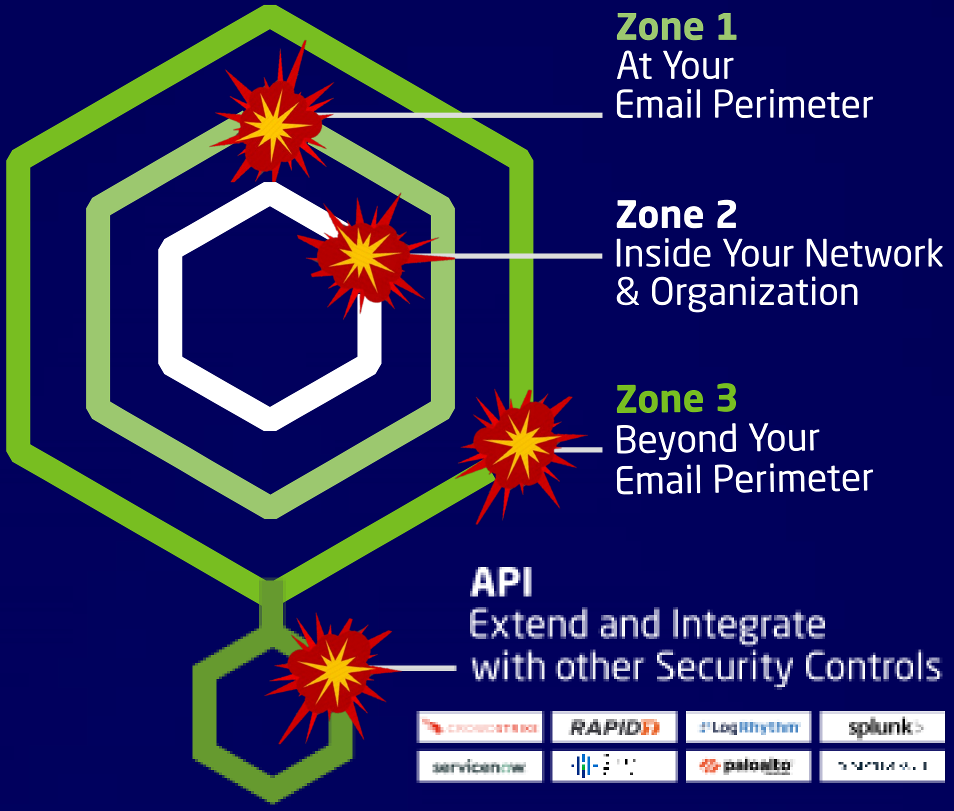
EXECUTIVE SUMMARY

Product	Protection Accuracy Rating	Legitimate Accuracy Rating	Total Accuracy Rating	Total Accuracy Rating (%)
Perception-Point	2,603	700	3,303	94%
Fortinet FortiMail	2,525	640	3,165	90%
Mimecast Secure Email Gateway	2,412	700	3,112	89%
Kaspersky Security for Office 365	1,681	550	2,231	64%
Google G Suite Enterprise	956	505	1,461	42%
Google G Suite Business	825	535	1,360	39%
Microsoft Office 365	463	550	1,013	29%
Microsoft Office 365 Advanced Threat Protection	426	550	976	28%

https://selabs.uk/wp-content/uploads/2020/04/enterprise-Email-Security-Services-ProtectionJANUARY-MARCH-2020.pdf

Holistic Security

Multidimensional problems…



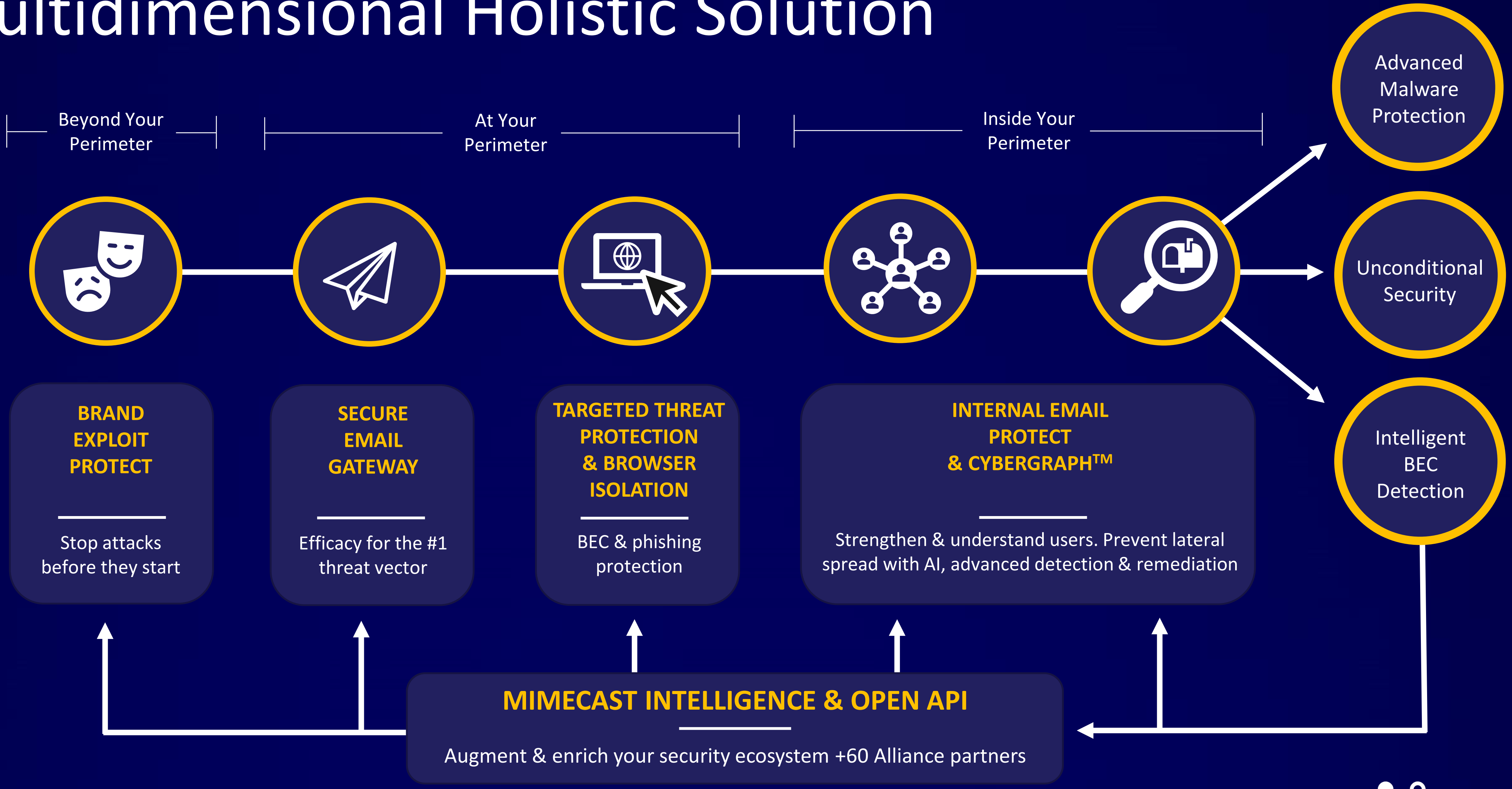
Zone 1
At Your
Email Perimeter

Zone 2
Inside Your Network
& Organization

Zone 3
Beyond Your
Email Perimeter

API
Extend and Integrate
with other Security Controls

Multidimensional Holistic Solution



Beyond Your Perimeter

At Your Perimeter

Inside Your Perimeter

Advanced Malware Protection

Unconditional Security

Intelligent BEC Detection

BRAND EXPLOIT PROTECT

Stop attacks before they start

SECURE EMAIL GATEWAY

Efficacy for the #1 threat vector

TARGETED THREAT PROTECTION & BROWSER ISOLATION

BEC & phishing protection

INTERNAL EMAIL PROTECT & CYBERGRAPH™

Strengthen & understand users. Prevent lateral spread with AI, advanced detection & remediation

MIMECAST INTELLIGENCE & OPEN API

Augment & enrich your security ecosystem +60 Alliance partners

Microsoft paloalto NETWORKS CROWDSTRIKE RAPID7 servicenow netskope

Microsoft 365 | Continuity

Built-in Availability/Resiliency

- Native Data Protection
- NO backup/recovery solution
- Result: Multiple long-term outages (whole/parts/pieces)

Solutions?

- Alternative approaches to provide cyber resilience
- People DO keep working (using Shadow IT) so you need to provide a way to avoid that

Shadow IT: Maintaining Your Protective “Bubble”

What REALLY happens when an email outage occurs?

- Some people stop working
- Others keep working… using Shadow IT (Gmail, Dropbox, etc.)

The result?

- Security “Bubble”? (Fingers crossed)
- Compliance “Bubble?” (No eDiscovery with Gmail)

The solution?

- An all-in-one, enterprise grade solution that provides continuity for working email, while also providing security and compliance through the cloud

Continuity Event Management

Monitor

Detect mail flow issues:

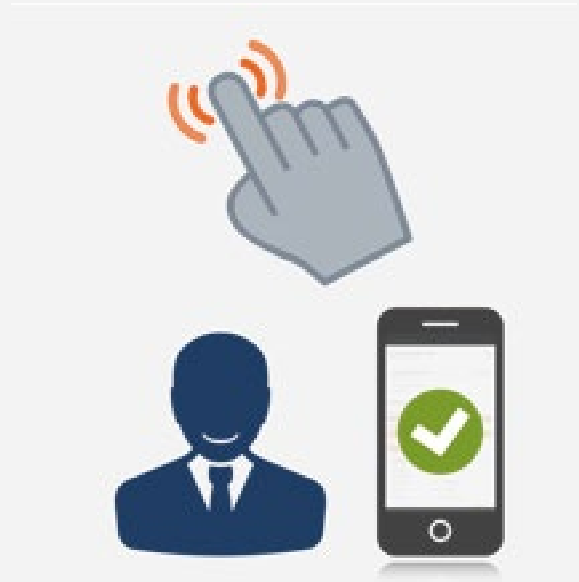
- On-premises
- Cloud
- Hybrid

Alert

Receive alerts:

- Delivered via SMS or an alternate email address.
- Continuity portal for quickly assessing the situation.

Respond



Respond:

- One click activation.
- Employees notified via a Mimecast for Outlook or SMS notification.

Stay Productive

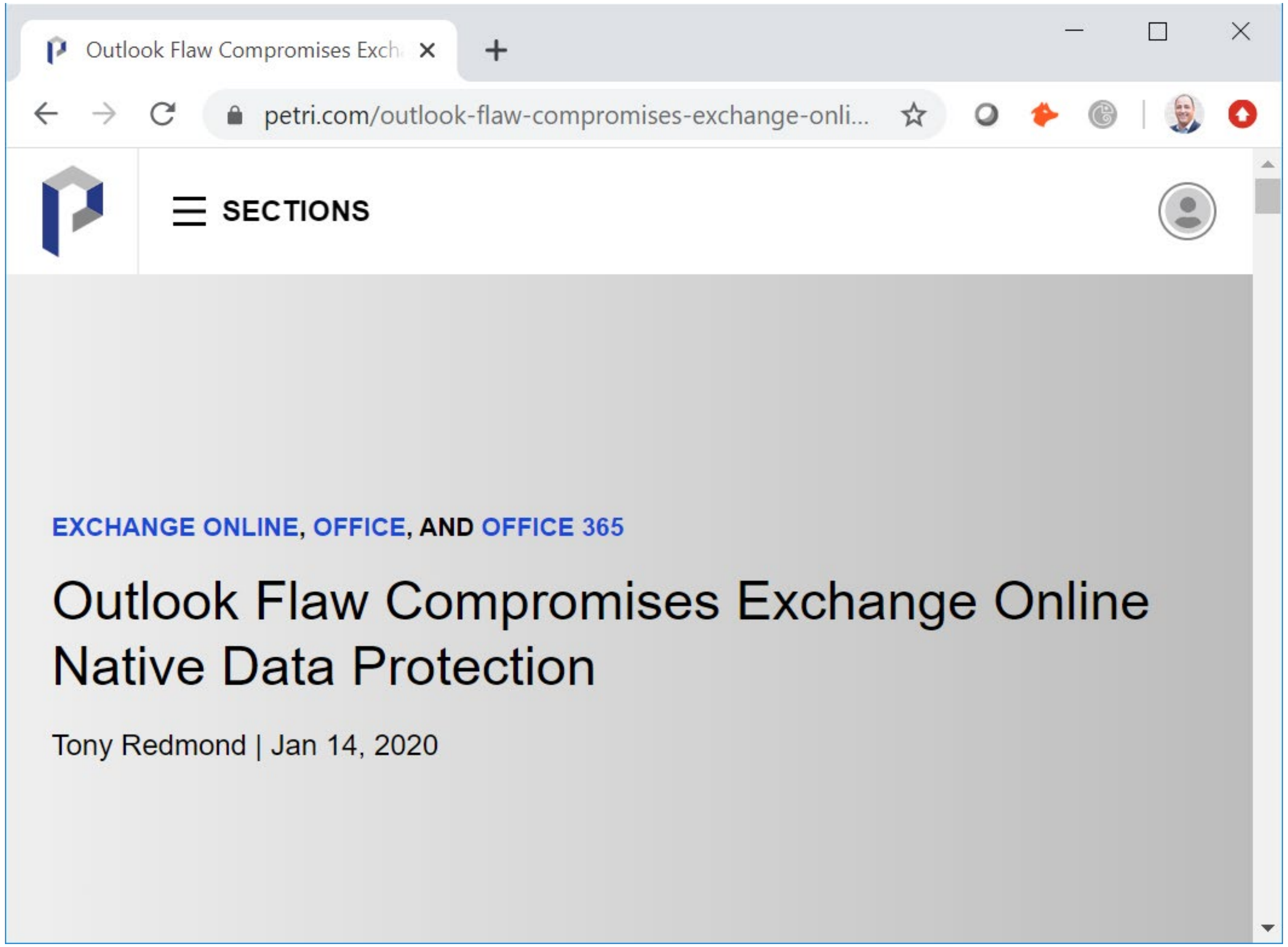
Stay Productive:

- Employees continue to send and receive email as well as access calendars via Outlook, mobile, web and Mac apps.

Expanding Resilience: Compliance/Discovery

- M365 retention (formerly Hold) retains email for discovery with the following drawbacks:
  - No interactive archive for end-users
  - Mailbox retains all mail (bloats) = app performance issues
  - Enterprise grade discovery requires upgrade (E5/a la carte)
  - Plagued by multiple flaw scandals
  - Side note: Lack of backup/recovery for point-in-time restoration

Expanding Resilience: Compliance/Discovery



Outlook Flaw Compromises Exch
petri.com/outlook-flaw-compromises-exchange-onli...
SECTIONS

EXCHANGE ONLINE, OFFICE, AND OFFICE 365

Outlook Flaw Compromises Exchange Online Native Data Protection

Tony Redmond | Jan 14, 2020

Point in time restoration of mailbox items is out of scope for the Exchange Online service, though there might be third-party solutions available that provide this functionality.

https://docs.microsoft.com/en-us/exchange/back-up-email

Conclusion

There may not be a silver bullet… but…

- Holistic thinking can help you to find gaps… do research into those “gaps” and find solutions that fill those “gaps”
- Areas that are currently worth investigating include security, compliance and continuity
- An all-in-one solution that hits all gaps and does it at a high level across the board is key

cStor

Questions?

mimecast®

cStor

We look beyond IT

Thank you!

J. Peter Bruzzese | jpbruzzese@mimecast.com