Steve Faehl
Microsoft Tools For Cyber Security

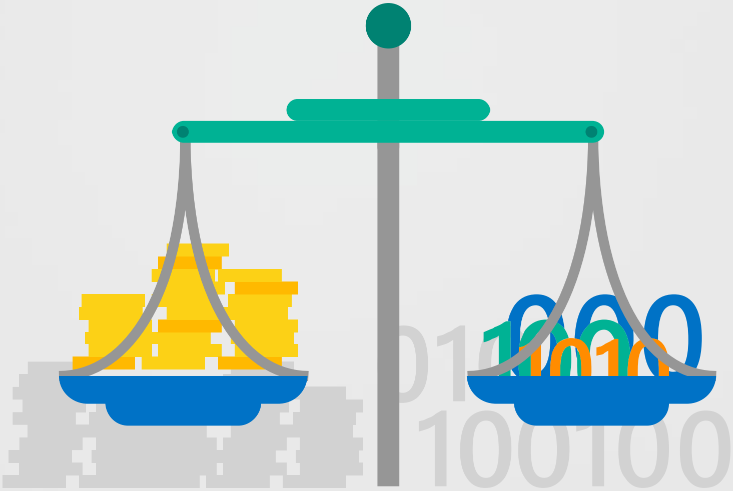
The world is changing . . .

. . . so are hackers

Cyber Security is the #1 concern of organizations and governments.

Cybercrime and cyber espionage are big business

$500 Billion in global impact



300 million new malware variants

Increased use of zero-days

Using legitimate IT tools

10% of breaches are in EDU

US Confirms BlackEnergy Malware Used In Ukrainian Power Plant Hack

http://www.ibtimes.com/us-confirms-blackenergy-malware-used-ukrainian-power-plant-hac-2263008

33% of organizations take 2+ years to discover breach

$5.9M Average cost of a breach in the United States

60% of data stolen in hours

65% of organizations say attacks evaded existing preventative security tools

Cost to **hire an outside firm** to audit level of breach

Costs to **remediate breach** like credit monitoring etc

Litigation costs arising from breach

Cost to **Brand Reputation**

A Layered security approach is necessary to safeguard productivity

Email Security

Application Security

Document Security

Device security

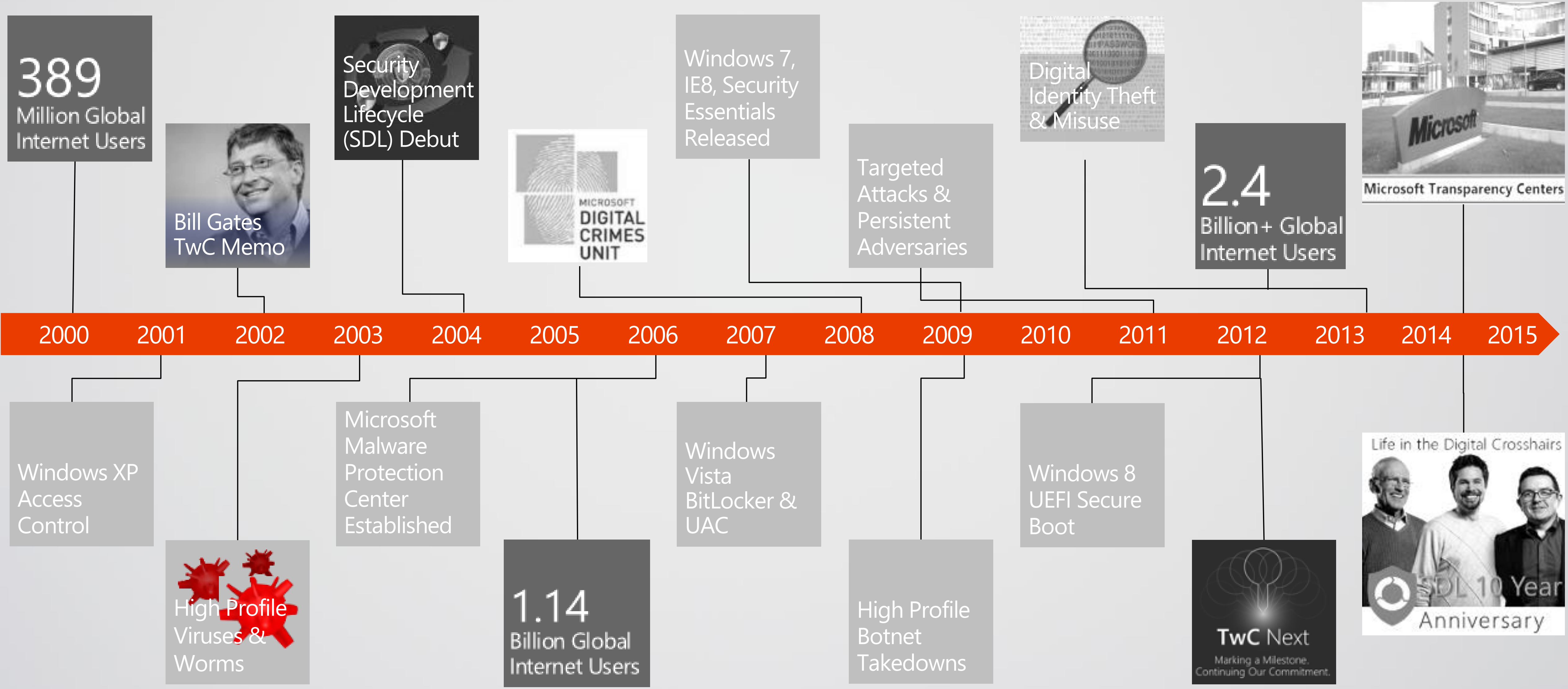
Network Security

Identity Security

THE MICROSOFT SECURITY STORY

Microsoft Experience & Credentials

Second decade of perspective & progress



2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
Microsoft Digital Crimes Unit
Microsoft
Life in the Digital Crosshairs
SDL 10 Year Anniversary
TwC Next
Marking a Milestone. Continuing Our Commitment.

389 Million Global Internet Users

Windows XP Access Control

Bill Gates TwC Memo

High Profile Viruses & Worms

Security Development Lifecycle (SDL) Debut

Microsoft Malware Protection Center Established

1.14 Billion Global Internet Users

Windows Vista BitLocker & UAC

Windows 7, IE8, Security Essentials Released

Targeted Attacks & Persistent Adversaries

High Profile Botnet Takedowns

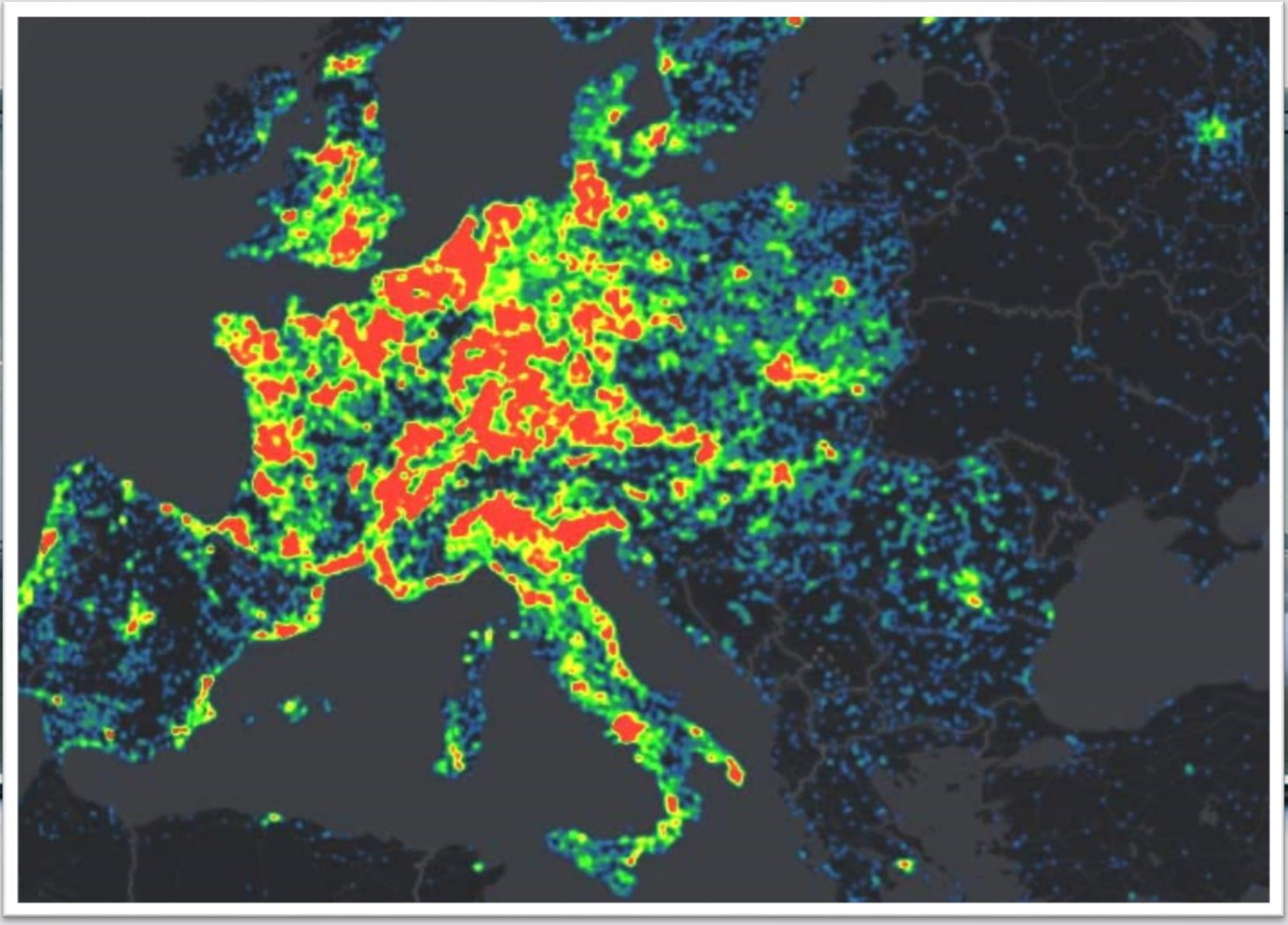
Digital Identity Theft & Misuse

Windows 8 UEFI Secure Boot

2.4 Billion+ Global Internet Users

Microsoft Transparency Centers

Big Data in the fight against cybercrime



Next-Gen Protection Benchmarks

Leverage big data and machine learning

Analyze signature and behavior for zero-day protection

Deep insights driving rapid iterative innovation

Actionable reporting that cuts through the noise

People-centric protection

A Layered security approach is necessary to safeguard productivity

Email Security

Application Security

Document Security

Enterprise Mobility Suite

Device security

Network Security

Identity Security

A Layered security approach is necessary to safeguard productivity

Azure AD Premium

Email Security

Application Security

Document Security

Device security

Network Security

Identity Security

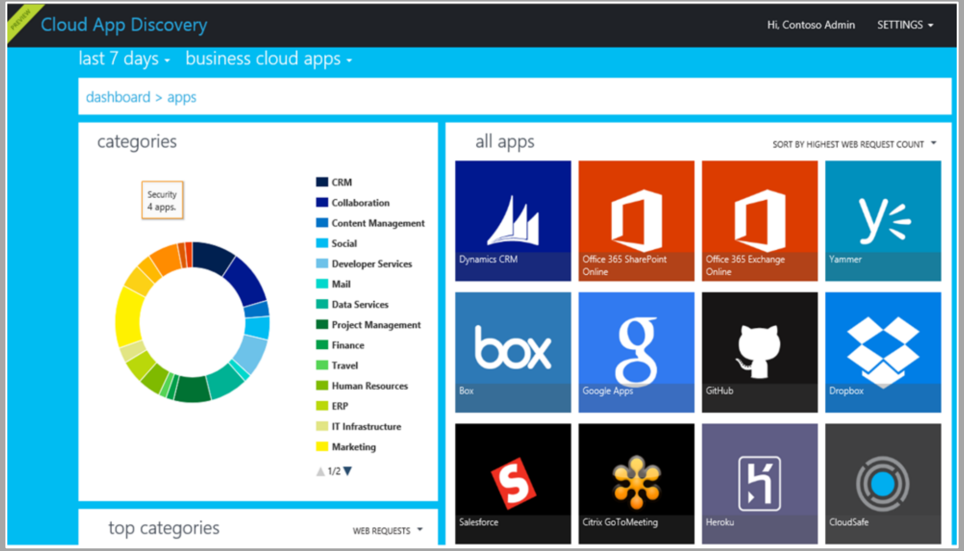
Simplify and Protect

Securing Identity with AADP

Enabling users and organizations with a common identity on-premises and in the cloud

Optionally add Multi-Factor Authentication per-app for additional user identity verification

Windows Azure
Active Directory



A Layered security approach is necessary to safeguard productivity

Intune + Azure RMS + DLP

Email Security

Application Security

Document Security

Device security

Network Security

Identity Security

PEOPLE CENTRIC PROTECTION

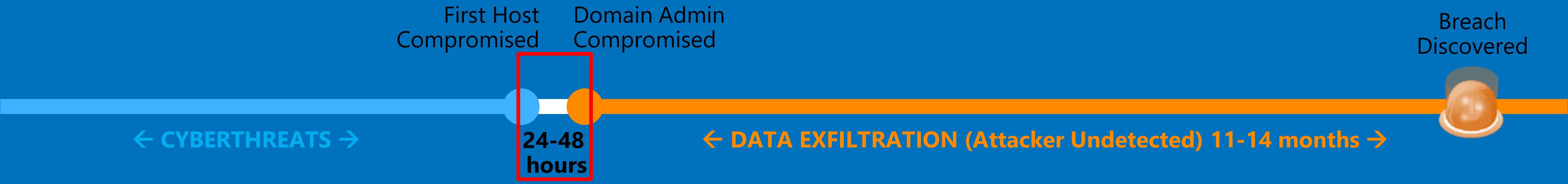
A Layered security approach is necessary to safeguard productivity

Advanced Threat Analytics

Email Security
Application Security
Document Security
Device security
Network Security
Identity Security

Typical Attack Profile

When you assume breach, you need to detect & respond ASAP



First Host Compromised

Domain Admin Compromised

Breach Discovered

← CYBERTHREATS →

24-48 hours

← DATA EXFILTRATION (Attacker Undetected) 11-14 months →

Target AD & Identities

- Active Directory controls access to business assets
- Attackers commonly target AD & IT Admins

Attacks not detected

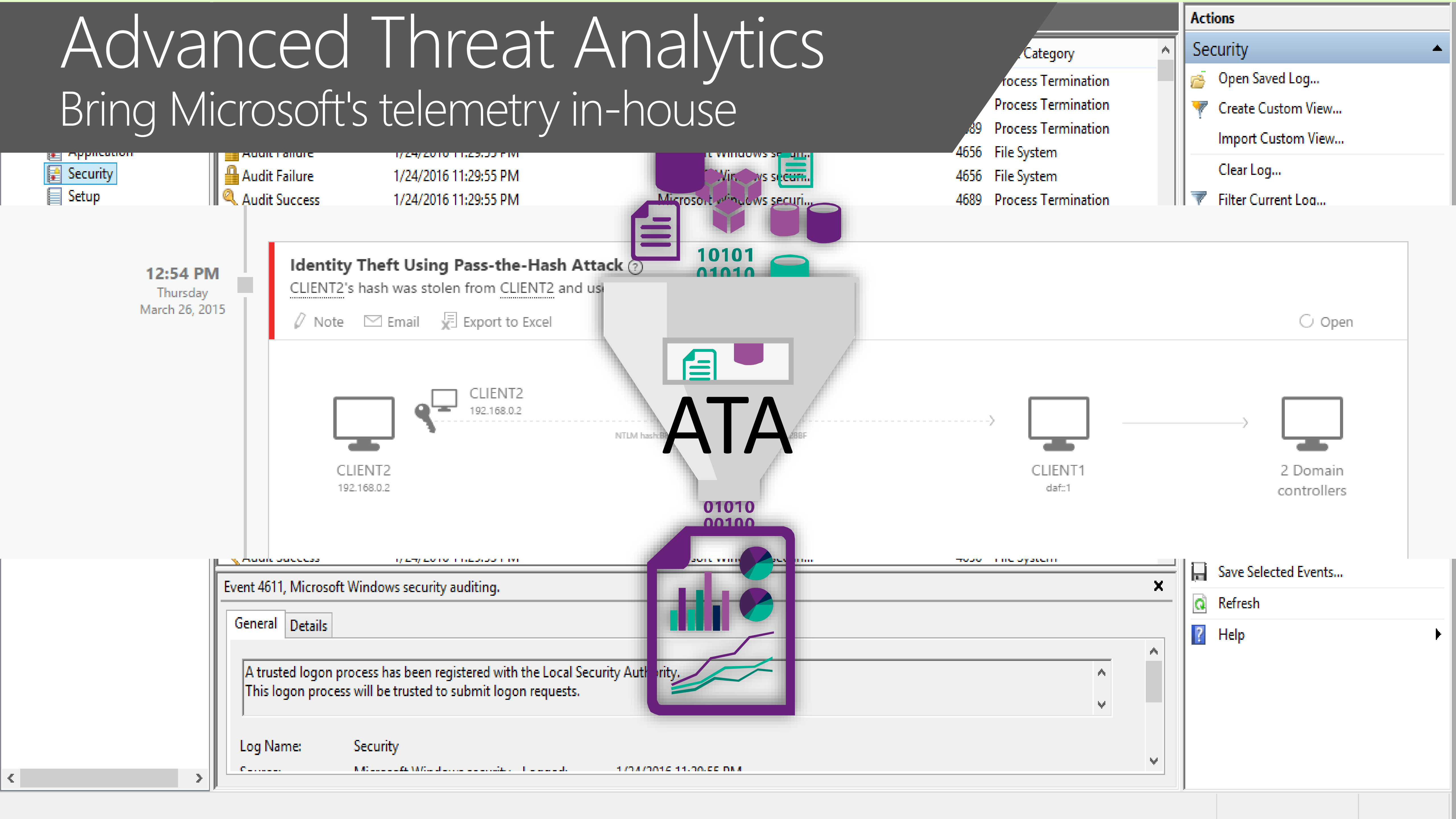
- Current detection tools miss most attacks
- You may be under attack (or compromised)

Response & Recovery

- Response requires advanced expertise & tools
- Expensive & challenging to successfully recover

Advanced Threat Analytics

Bring Microsoft's telemetry in-house



Level	Date and Time	Source	Event ID	Task Category
Audit Failure	1/24/2016 11:29:55 PM	Microsoft Windows securi...	4656	File System
Audit Success	1/24/2016 11:29:55 PM	Microsoft Windows securi...	4689	Process Termination

Identity Theft Using Pass-the-Hash Attack

CLIENT2's hash was stolen from CLIENT2 and us

12:54 PM
Thursday
March 26, 2015

CLIENT2
192.168.0.2

CLIENT1
daf::1

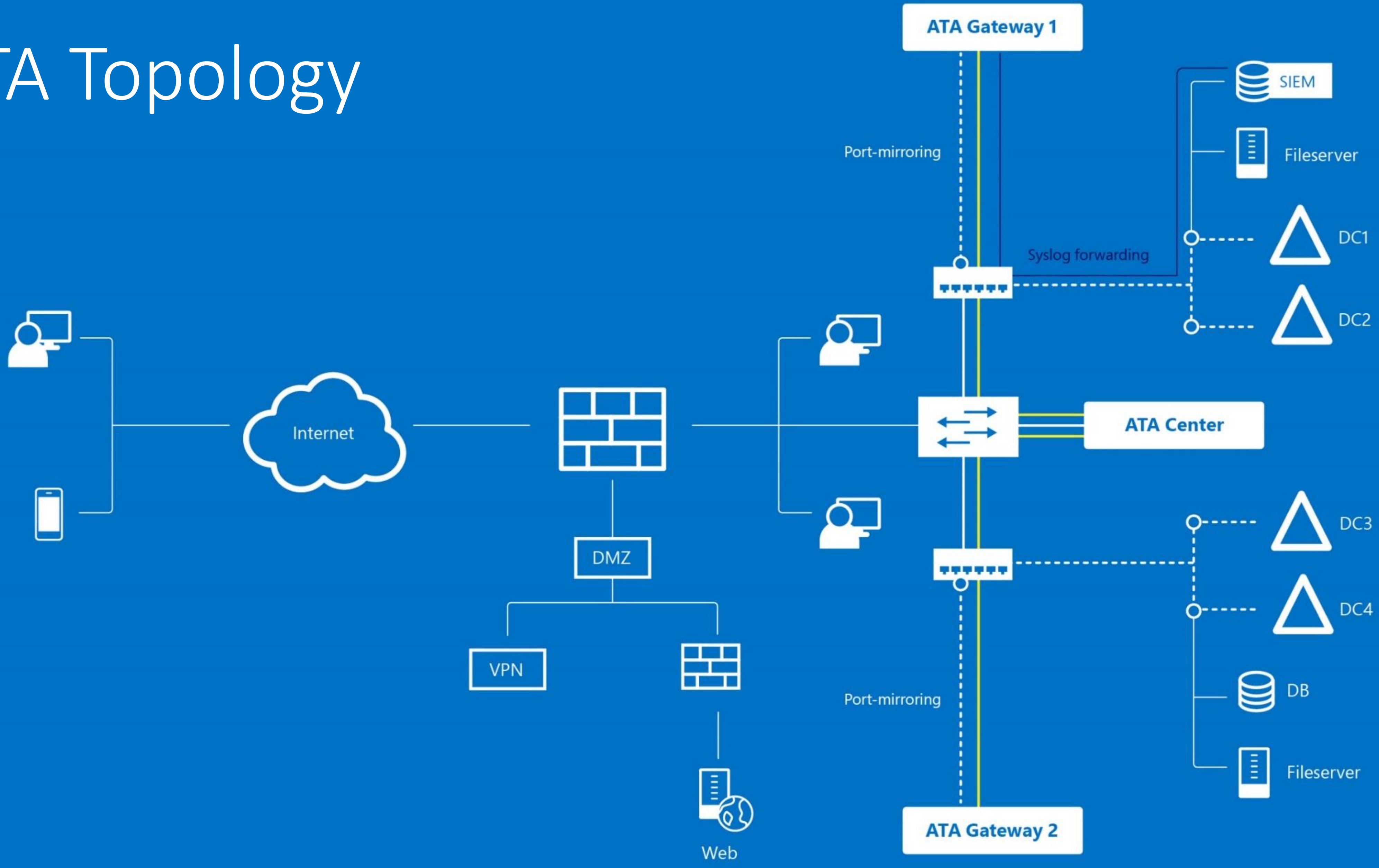
2 Domain controllers

Event 4611, Microsoft Windows security auditing.

A trusted logon process has been registered with the Local Security Authority.
This logon process will be trusted to submit logon requests.

Log Name: Security

ATA Topology



A Layered security approach is necessary to safeguard productivity

Advanced Threat Protection

Email Security

Application Security

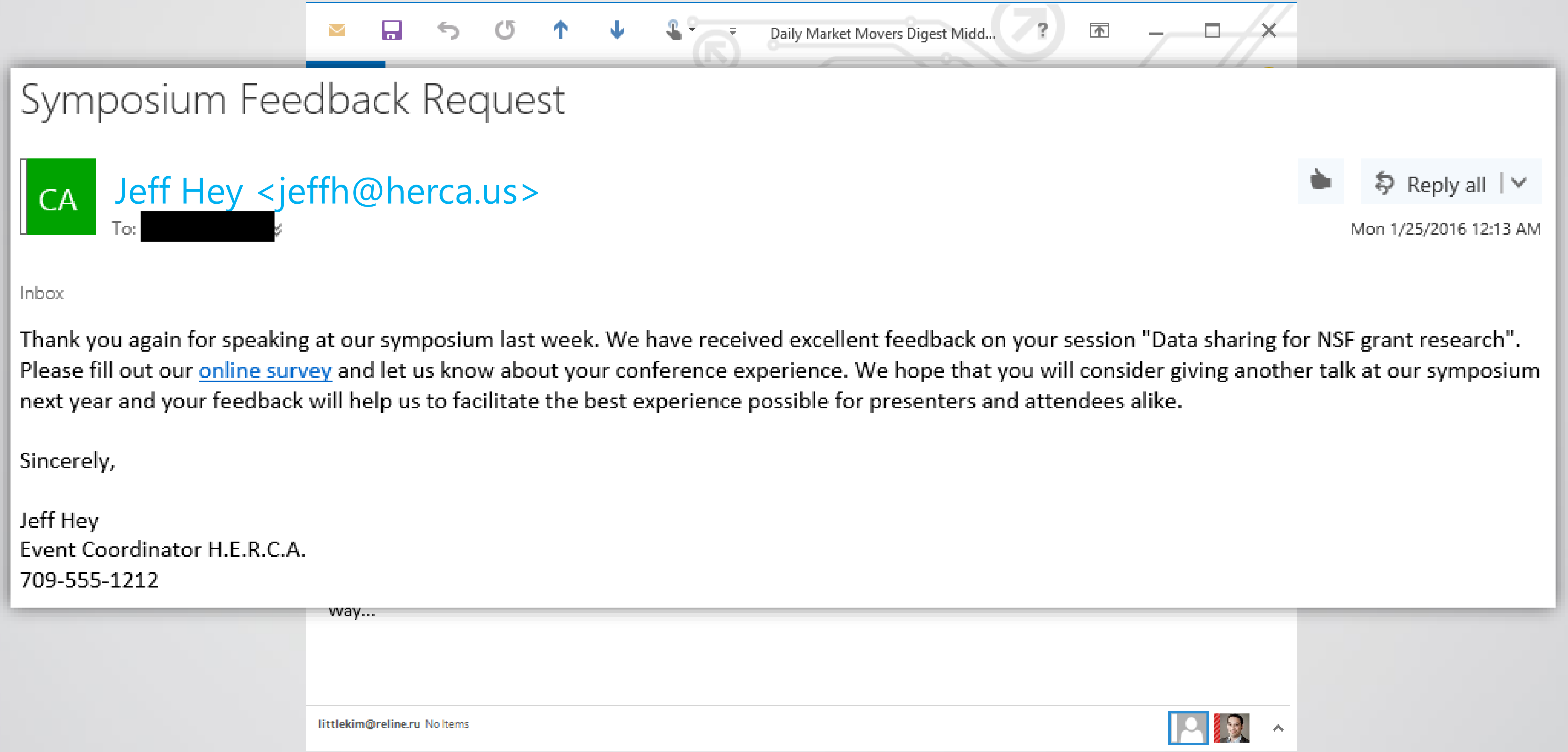
Document Security

Device security

Network Security

Identity Security

Phishing 101


Daily Market Movers Digest Midd...
CA
Reply all
Inbox
way...
littlekim@reline.ru No Items

Symposium Feedback Request

Jeff Hey <jeffh@herca.us>

To: [redacted]

Mon 1/25/2016 12:13 AM

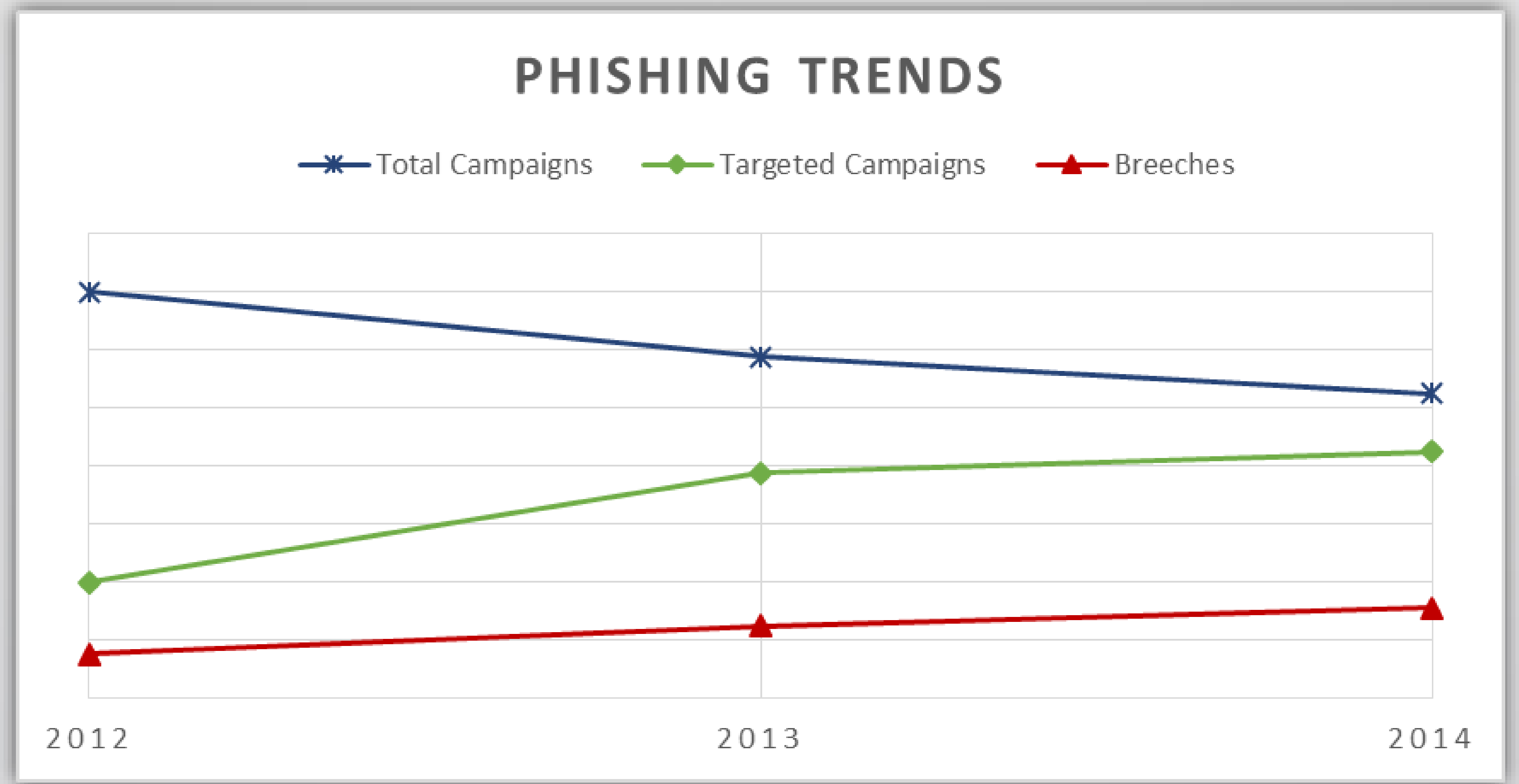
Thank you again for speaking at our symposium last week. We have received excellent feedback on your session "Data sharing for NSF grant research". Please fill out our online survey and let us know about your conference experience. We hope that you will consider giving another talk at our symposium next year and your feedback will help us to facilitate the best experience possible for presenters and attendees alike.

Sincerely,

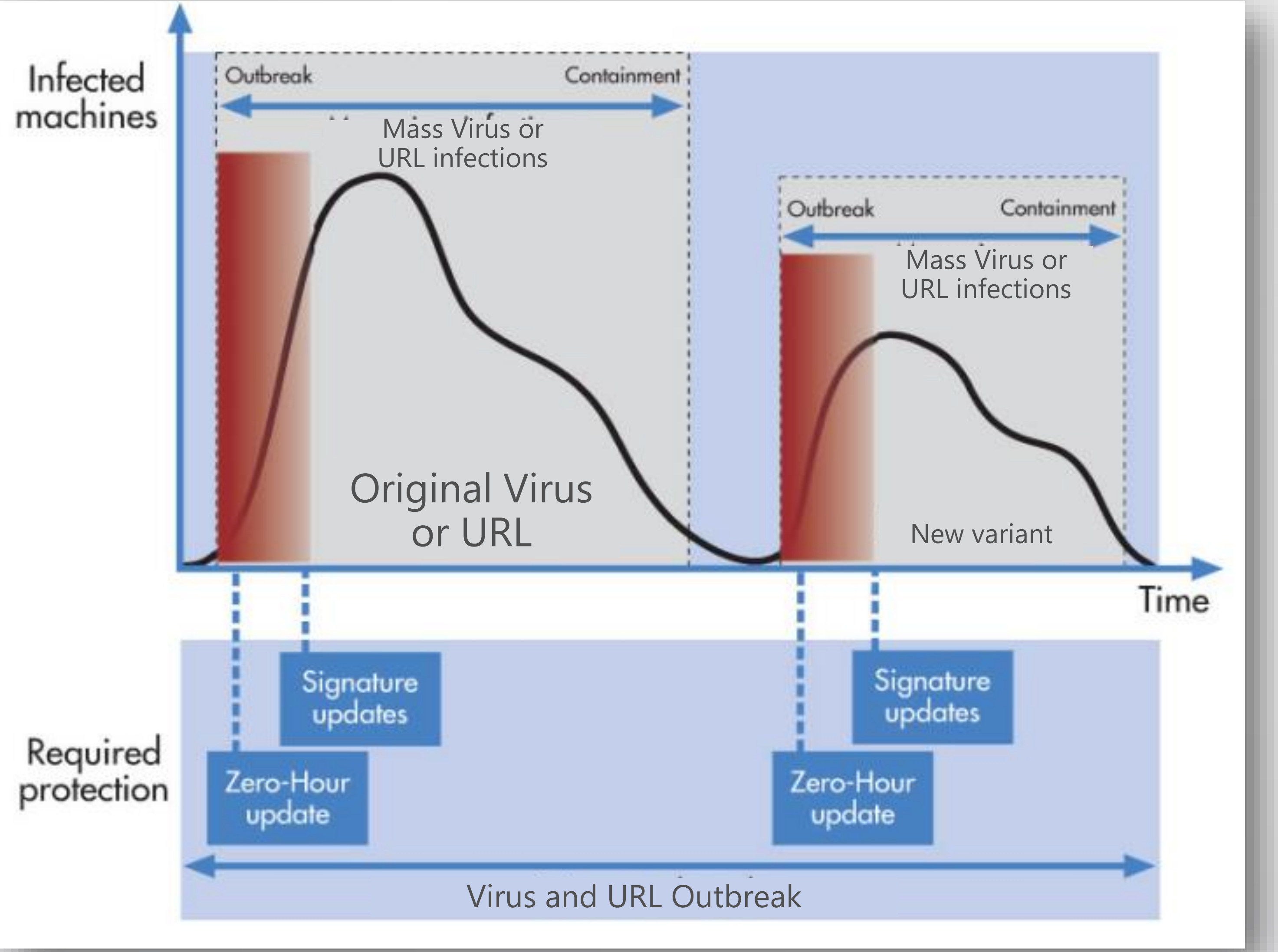
Jeff Hey
Event Coordinator H.E.R.C.A.
709-555-1212

Phishing Trends

By the numbers



Malware variant explosion



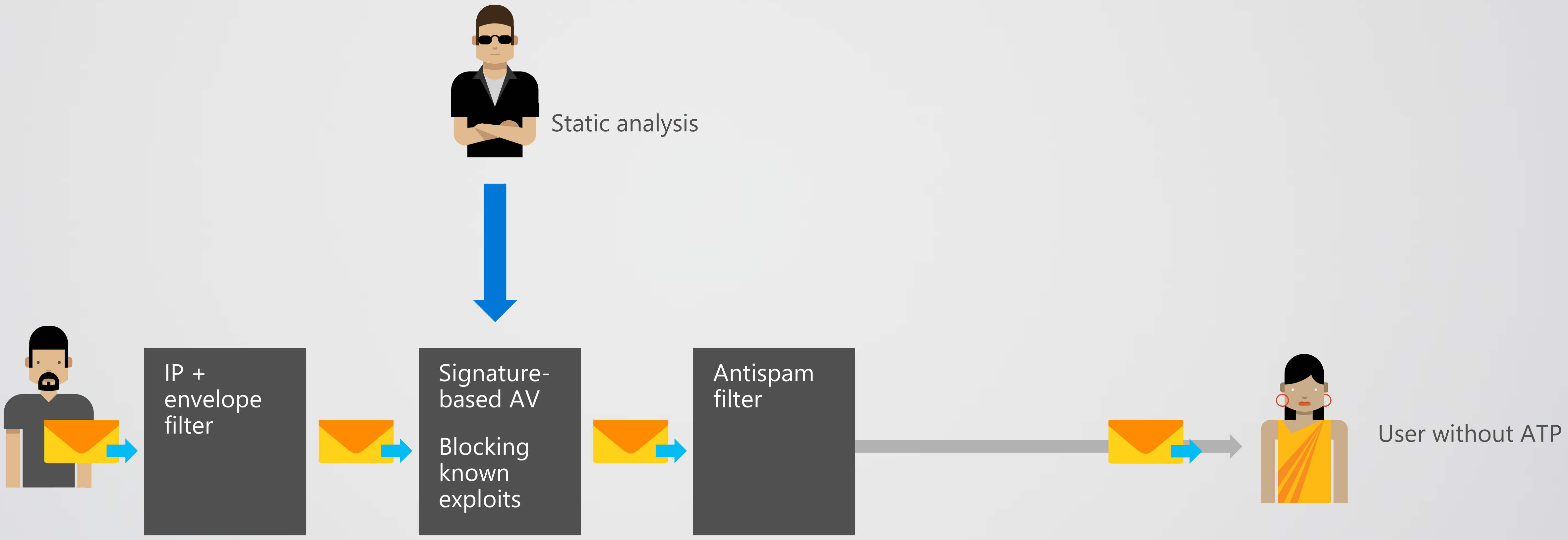
Any new outbreak consists of two parts

A. Zero hour attack
B. Elongated period of attack

Traditional signature-based AV/AS cannot provide comprehensive protection against zero day attack

Attackers can go completely unnoticed during zero day attack

Traditional Malware Detection



Static analysis

IP + envelope filter

Signature-based AV

Blocking known exploits

Antispam filter

User without ATP

Signature based Malware detection has a large latency due to static analysis

Exchange Online Advanced Threat Protection

Protection against unknown malware/virus

- Behavioral analysis with machine learning
- Dynamic Delivery
- Admin alerts

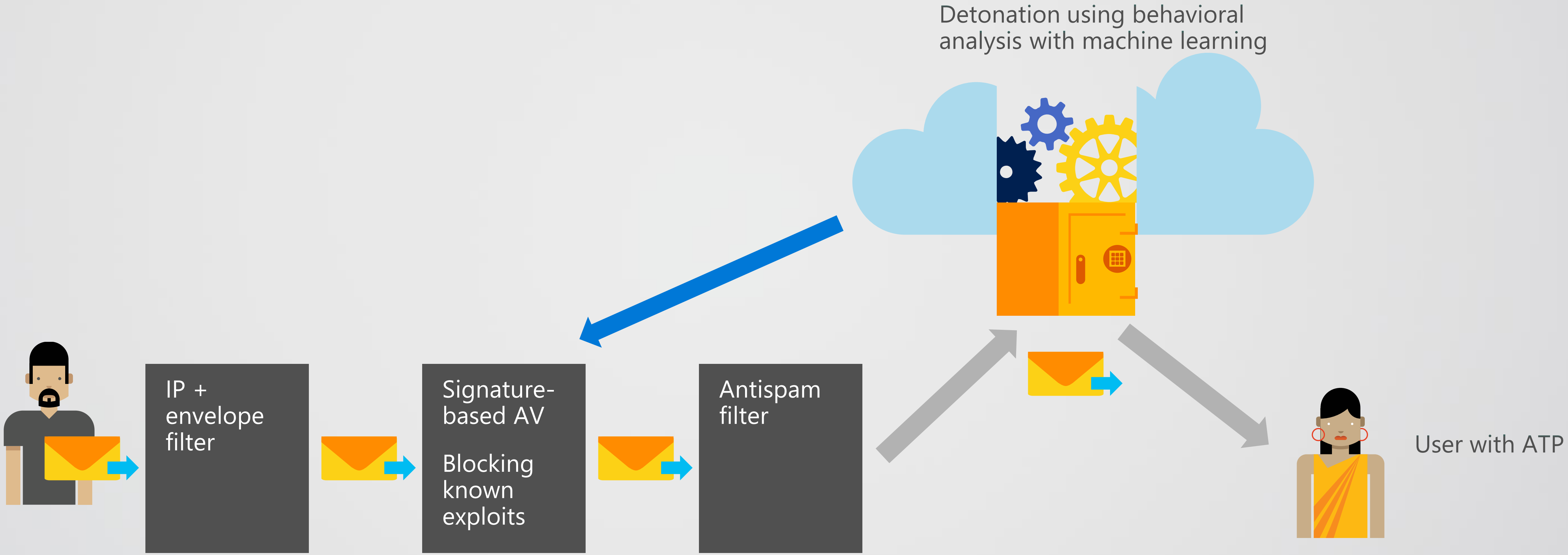
Time of click protection

- Real time protection against Malicious URLs
- Dynamic URL coverage
- Zero Hour Auto Purge

Rich reporting and tracing

- Built-in URL trace
- Reports for advanced threats

Next-Gen Malware Detection



Detonation using behavioral analysis with machine learning

IP + envelope filter

Signature-based AV

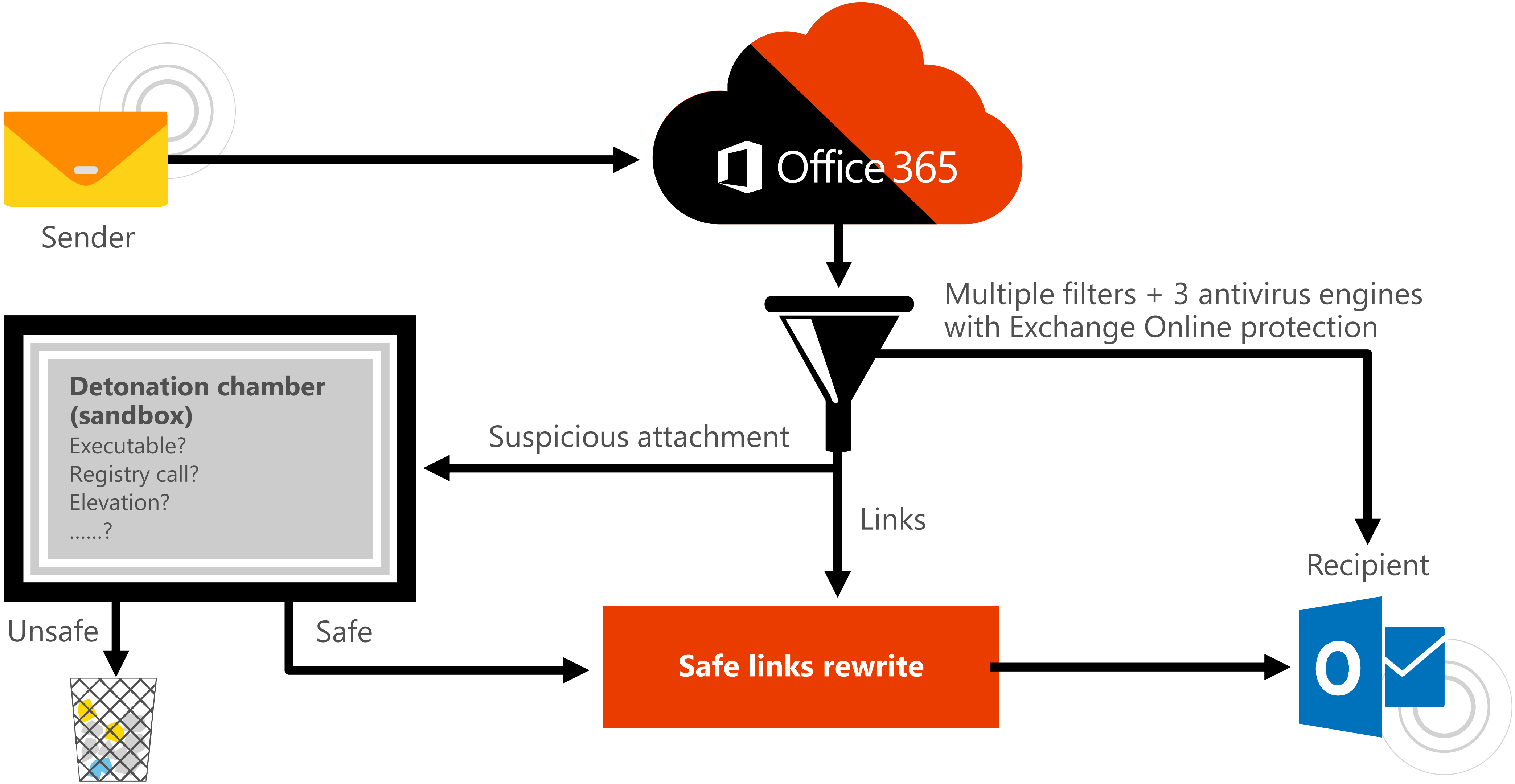
Blocking known exploits

Antispam filter

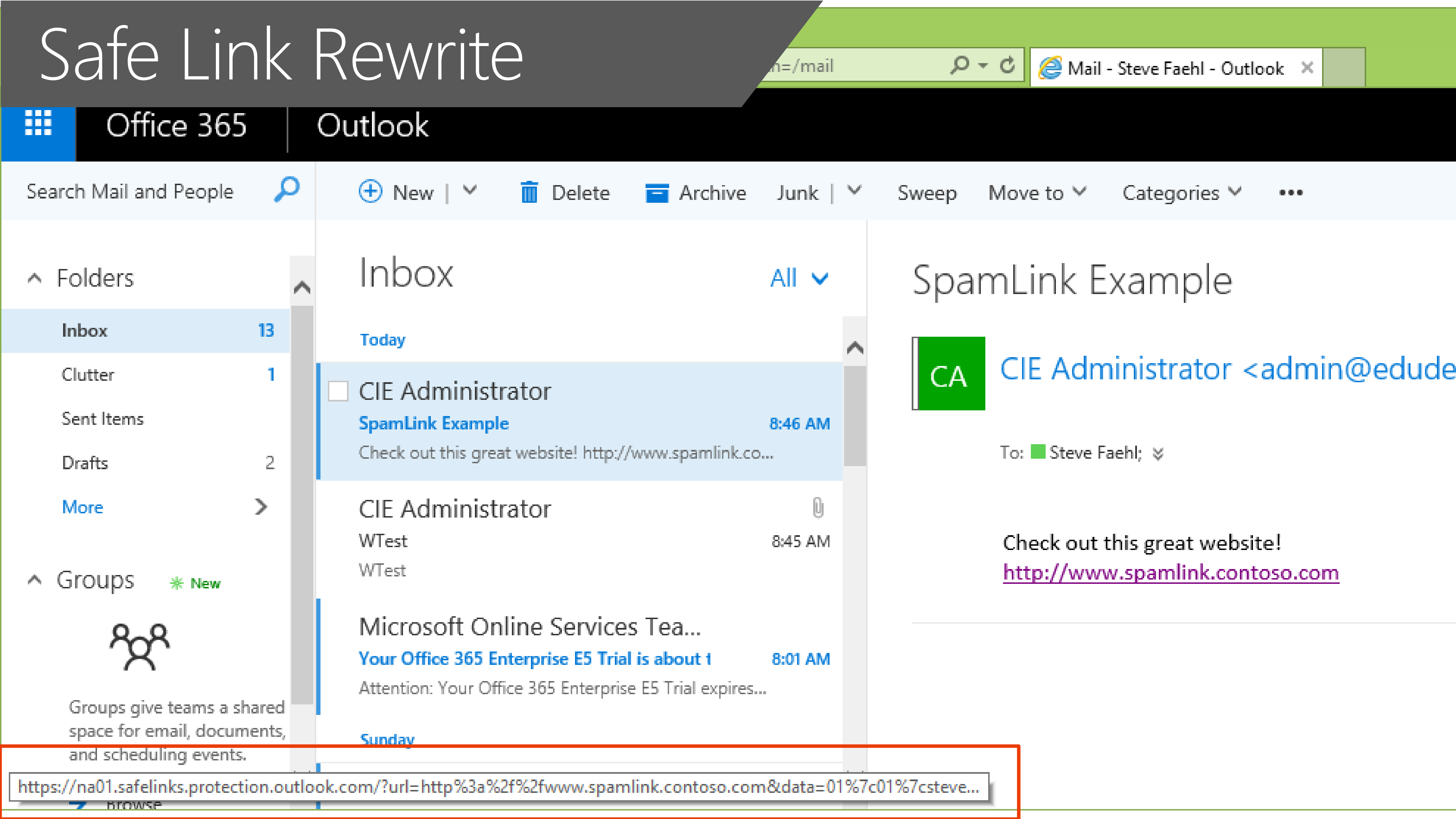
User with ATP

Behavior based Malware detection uses Machine Learning to flag Malware

ATP Service architecture



Safe Link Rewrite



Groups give teams a shared space for email, documents, and scheduling events.

CIE Administrator
SpamLink Example 8:46 AM
Check out this great website! http://www.spamlink.co...

CIE Administrator
WTest 8:45 AM
WTest

Microsoft Online Services Tea...
Your Office 365 Enterprise E5 Trial is about t 8:01 AM
Attention: Your Office 365 Enterprise E5 Trial expires...

SpamLink Example

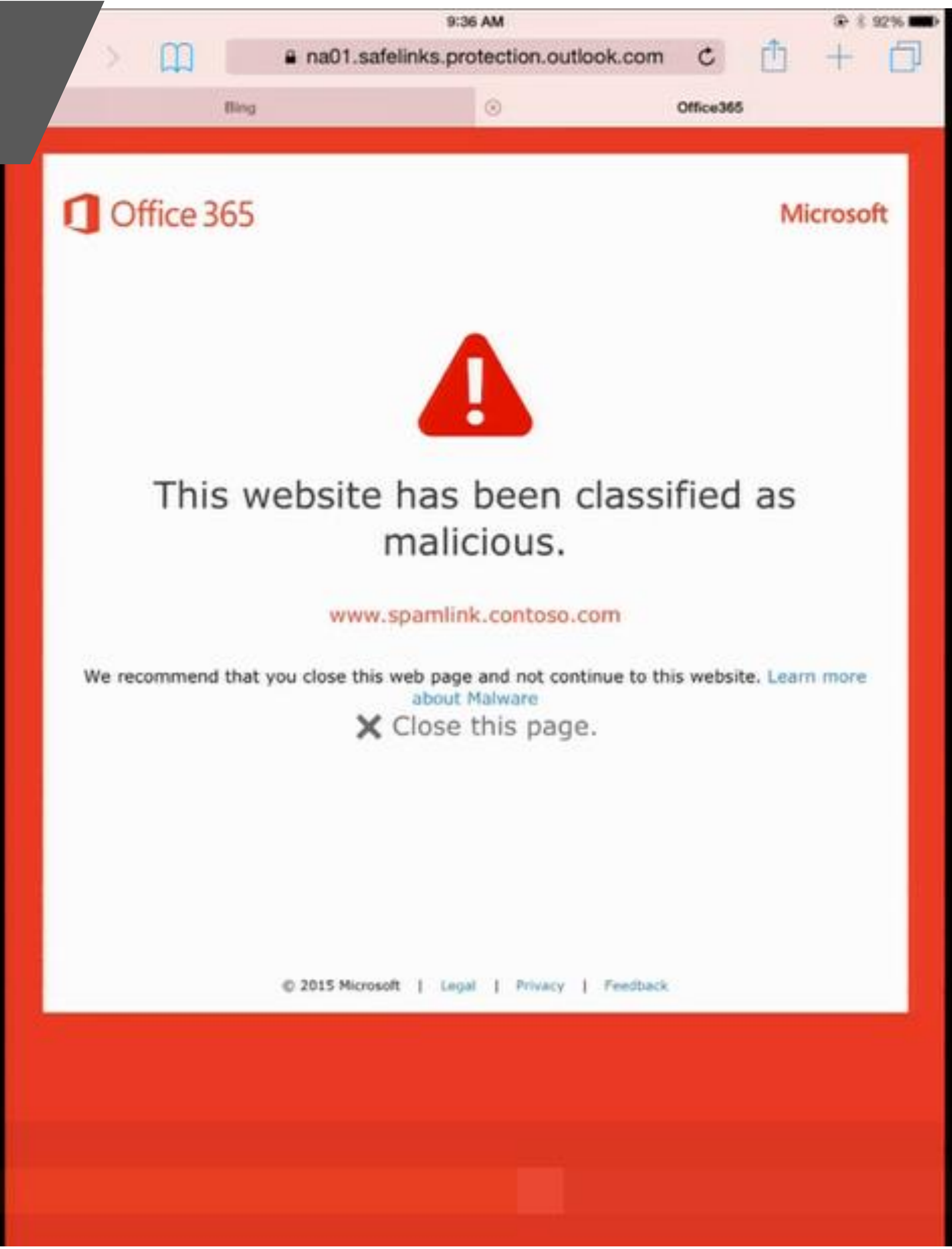
CA CIE Administrator <admin@edude

To: Steve Faehl;

Check out this great website!
http://www.spamlink.contoso.com

https://na01.safelinks.protection.outlook.com/?url=http%3a%2f%2fwww.spamlink.contoso.com&data=01%7c01%7csteve...

Blocked URL



Office 365 Microsoft

This website has been classified as malicious.

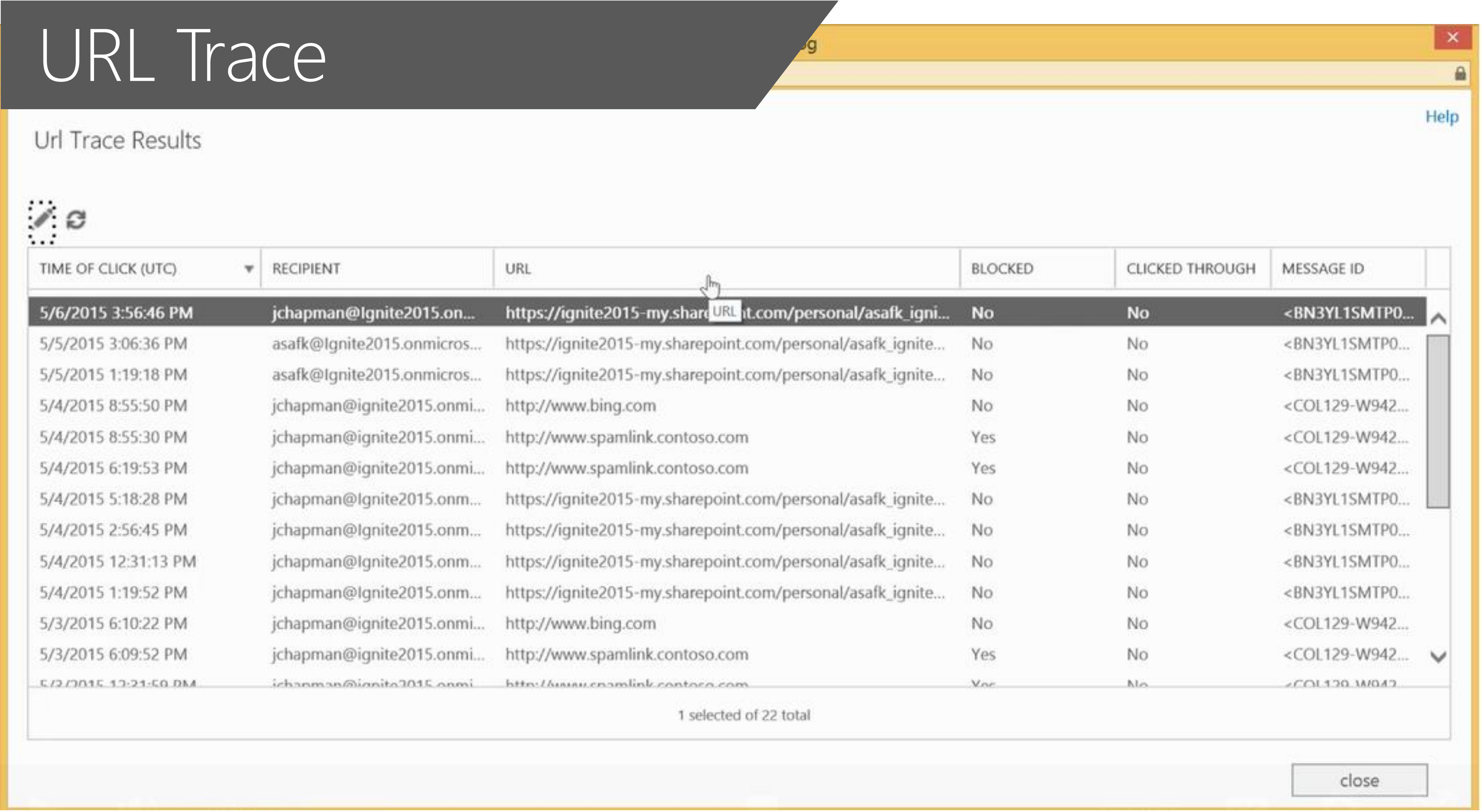
www.spamlink.contoso.com

We recommend that you close this web page and not continue to this website. Learn more about Malware

✕ Close this page.

© 2015 Microsoft | Legal | Privacy | Feedback

URL Trace

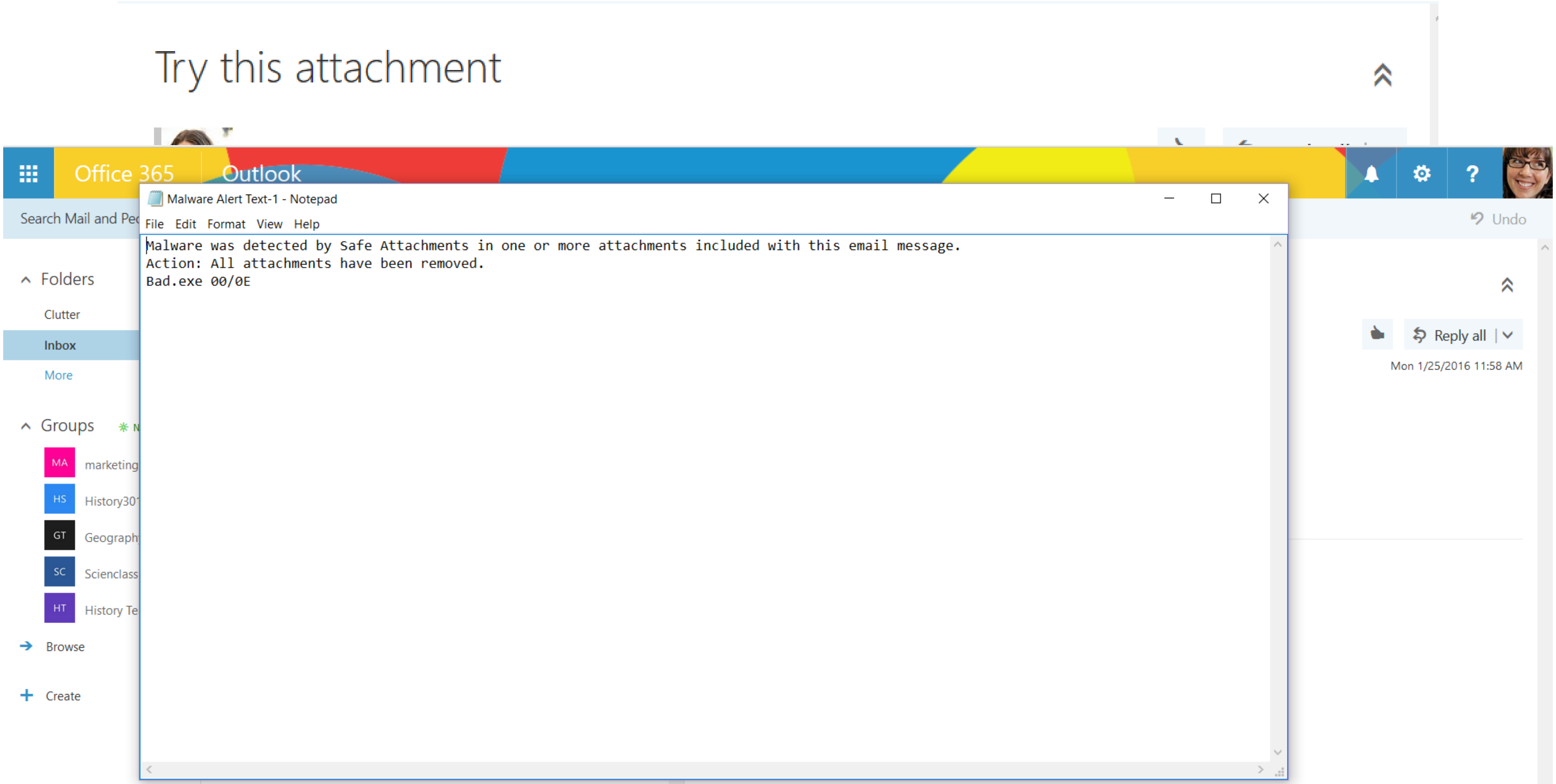


Url Trace Results

TIME OF CLICK (UTC)	RECIPIENT	URL	BLOCKED	CLICKED THROUGH	MESSAGE ID
5/6/2015 3:56:46 PM	jchapman@Ignite2015.on...	https://ignite2015-my.shar URL t.com/personal/asafk_igni...	No	No	<BN3YL1SMTP0...
5/5/2015 3:06:36 PM	asafk@Ignite2015.onmicros...	https://ignite2015-my.sharepoint.com/personal/asafk_ignite...	No	No	<BN3YL1SMTP0...
5/5/2015 1:19:18 PM	asafk@Ignite2015.onmicros...	https://ignite2015-my.sharepoint.com/personal/asafk_ignite...	No	No	<BN3YL1SMTP0...
5/4/2015 8:55:50 PM	jchapman@ignite2015.onmi...	http://www.bing.com	No	No	<COL129-W942...
5/4/2015 8:55:30 PM	jchapman@ignite2015.onmi...	http://www.spamlink.contoso.com	Yes	No	<COL129-W942...
5/4/2015 6:19:53 PM	jchapman@ignite2015.onmi...	http://www.spamlink.contoso.com	Yes	No	<COL129-W942...
5/4/2015 5:18:28 PM	jchapman@Ignite2015.onm...	https://ignite2015-my.sharepoint.com/personal/asafk_ignite...	No	No	<BN3YL1SMTP0...
5/4/2015 2:56:45 PM	jchapman@Ignite2015.onm...	https://ignite2015-my.sharepoint.com/personal/asafk_ignite...	No	No	<BN3YL1SMTP0...
5/4/2015 12:31:13 PM	jchapman@Ignite2015.onm...	https://ignite2015-my.sharepoint.com/personal/asafk_ignite...	No	No	<BN3YL1SMTP0...
5/4/2015 1:19:52 PM	jchapman@Ignite2015.onm...	https://ignite2015-my.sharepoint.com/personal/asafk_ignite...	No	No	<BN3YL1SMTP0...
5/3/2015 6:10:22 PM	jchapman@ignite2015.onmi...	http://www.bing.com	No	No	<COL129-W942...
5/3/2015 6:09:52 PM	jchapman@ignite2015.onmi...	http://www.spamlink.contoso.com	Yes	No	<COL129-W942...
5/3/2015 12:31:59 PM	jchapman@ignite2015.onmi...	http://www.spamlink.contoso.com	Yes	No	<COL129-W942...

1 selected of 22 total

Blocked Attachment



Try this attachment

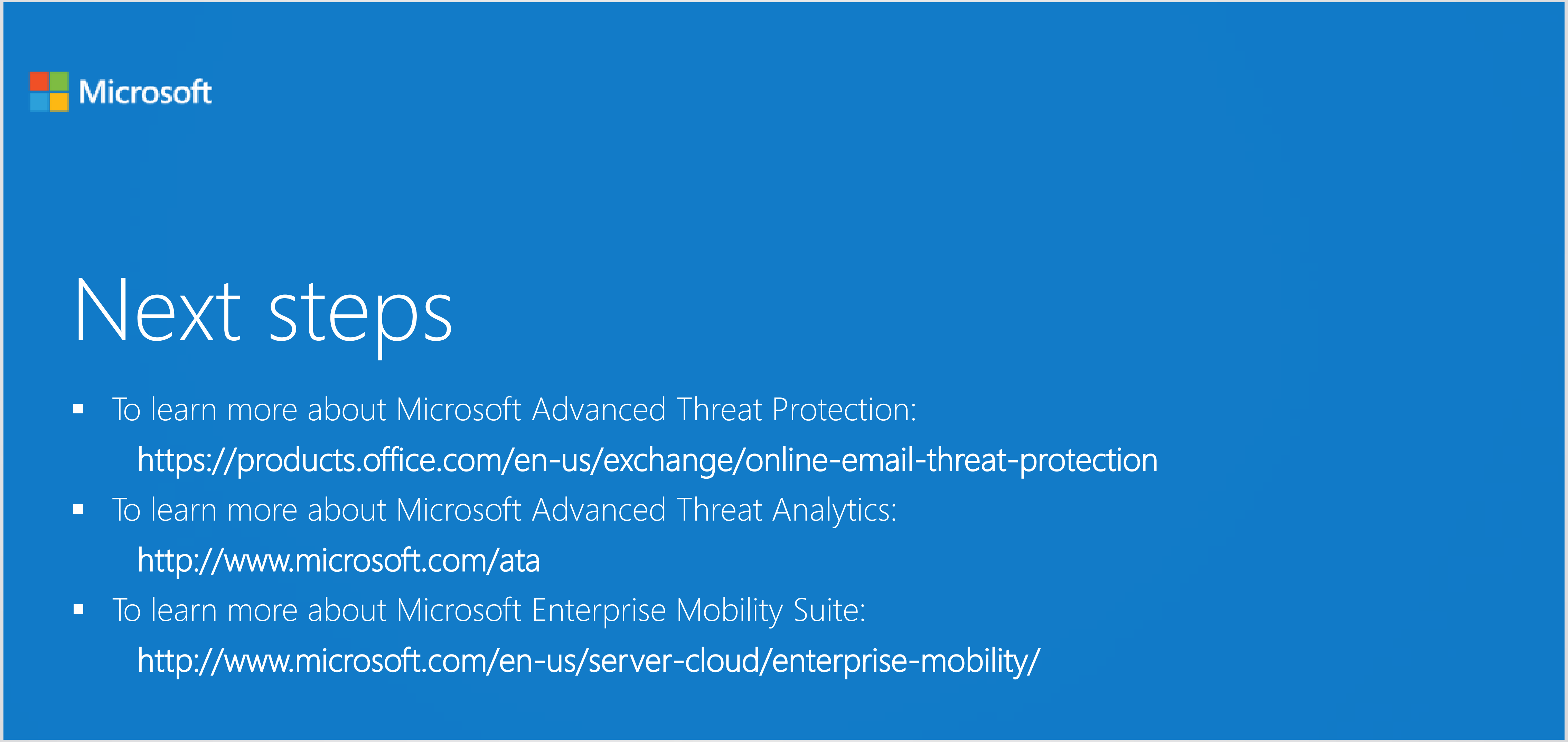
Malware Alert Text-1 - Notepad

```
Malware was detected by Safe Attachments in one or more attachments included with this email message.
Action: All attachments have been removed.
Bad.exe 00/0E
```

How to Purchase – Education Pricing

Product	Channel	ERP
Advanced Threat Protection	Direct, Open, and EES channels	$1.40/ Faculty/month $.70/Student/month
Advanced Threat Analytics	Direct, Open, and EES channels	Included with ECAL or EMS
Enterprise Mobility Suite (AADP+ Intune+ Azure RMS+ ATA)	Direct, Open, and EES channels	$1.07/ Faculty/month
Azure AD Premium (stand alone)	Direct, Open, and EES	$.55/ Faculty/month $.22/Student/Month

Thank you for attending!



Microsoft

Next steps

- To learn more about Microsoft Advanced Threat Protection:
  https://products.office.com/en-us/exchange/online-email-threat-protection
- To learn more about Microsoft Advanced Threat Analytics:
  http://www.microsoft.com/ata
- To learn more about Microsoft Enterprise Mobility Suite:
  http://www.microsoft.com/en-us/server-cloud/enterprise-mobility/

Who to contact for price details:

- Bryan Zatkulak - bzatkulak@belltechlogix.com - 888-989-8560
  USM Institutions and JHU Affiliates
- Dana McNeil - dmcneil@belltechlogix.com - 877-394-7900
  All K-12 Private Schools and K-12 Public Schools M-Z
- Lisa Goolsby - lgoolsby@belltechlogix.com - 877-213-5990
  Public Libraries, Community and Private Colleges,
  and K-12 Public Schools A-L
- Sarah Taggart - staggart@belltechlogix.com
- Click to view the Contract # N139976 Roadshow presentation

BELL Techlogix

Microsoft