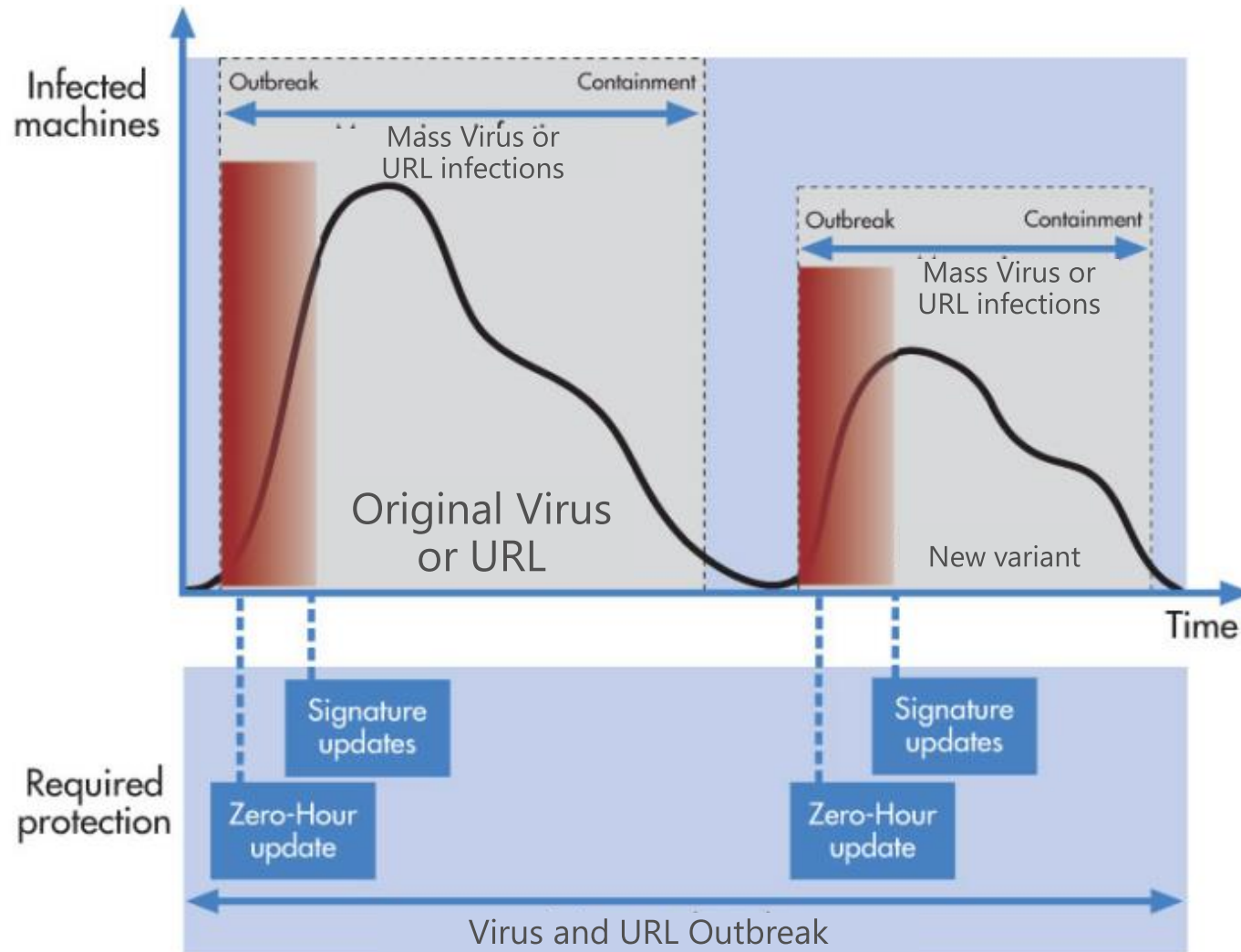


# Exchange Online Advanced Threat Protection

Benny Petrank



# Evolving threat space



Any new outbreak consists of two parts

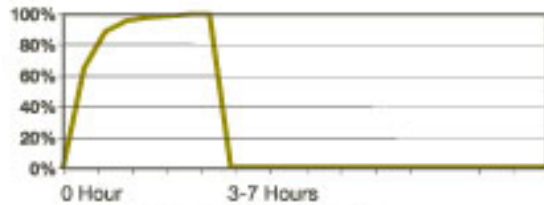
- A. Zero hour attack
- B. Elongated period of attack

Traditional AV/AS cannot protect against zero day attack comprehensibly

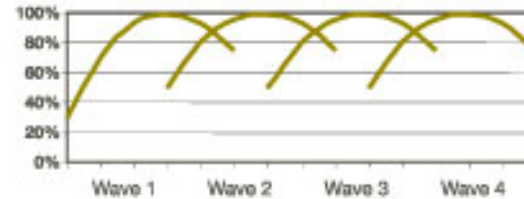
Attackers can go completely unnoticed during zero day attack

# Evolving threat space

Short-span attacks

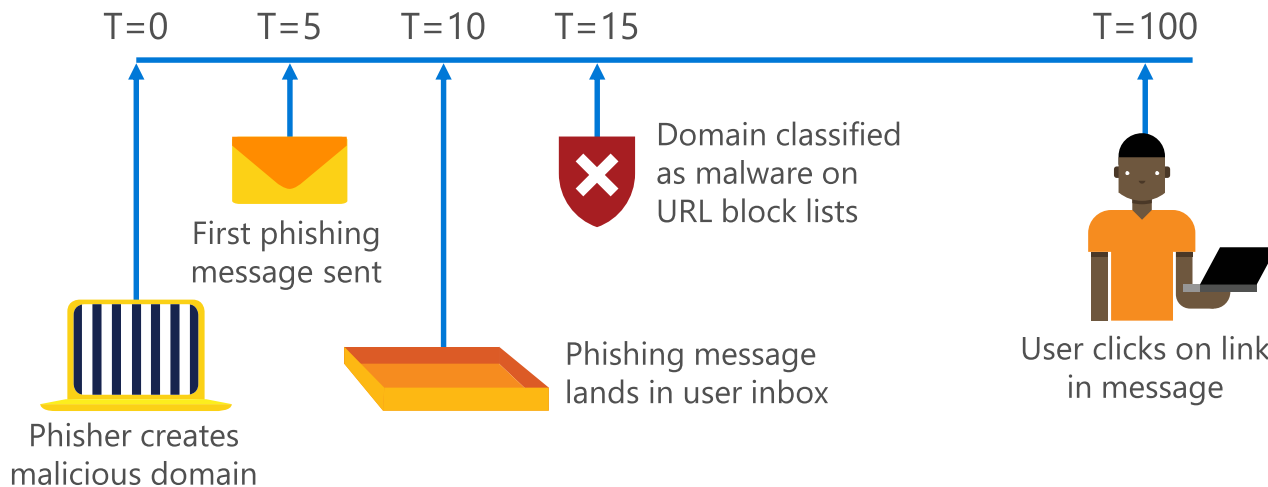


Serial variant attacks



Short-span attacks can be just minutes to hours

Serial variant attacks generally repeat pattern every few hours



Attacker can easily change the links in the message after mail is delivered

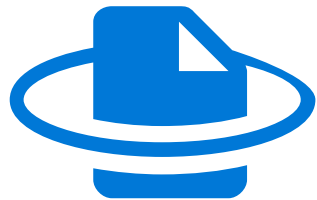
# Exchange Online advanced threat protection



---

Protection  
against unknown  
malware/virus

- Behavioral analysis with machine learning
- Admin alerts



---

Time of click  
protection

- Real time protection against Malicious URLs
- Growing URL coverage

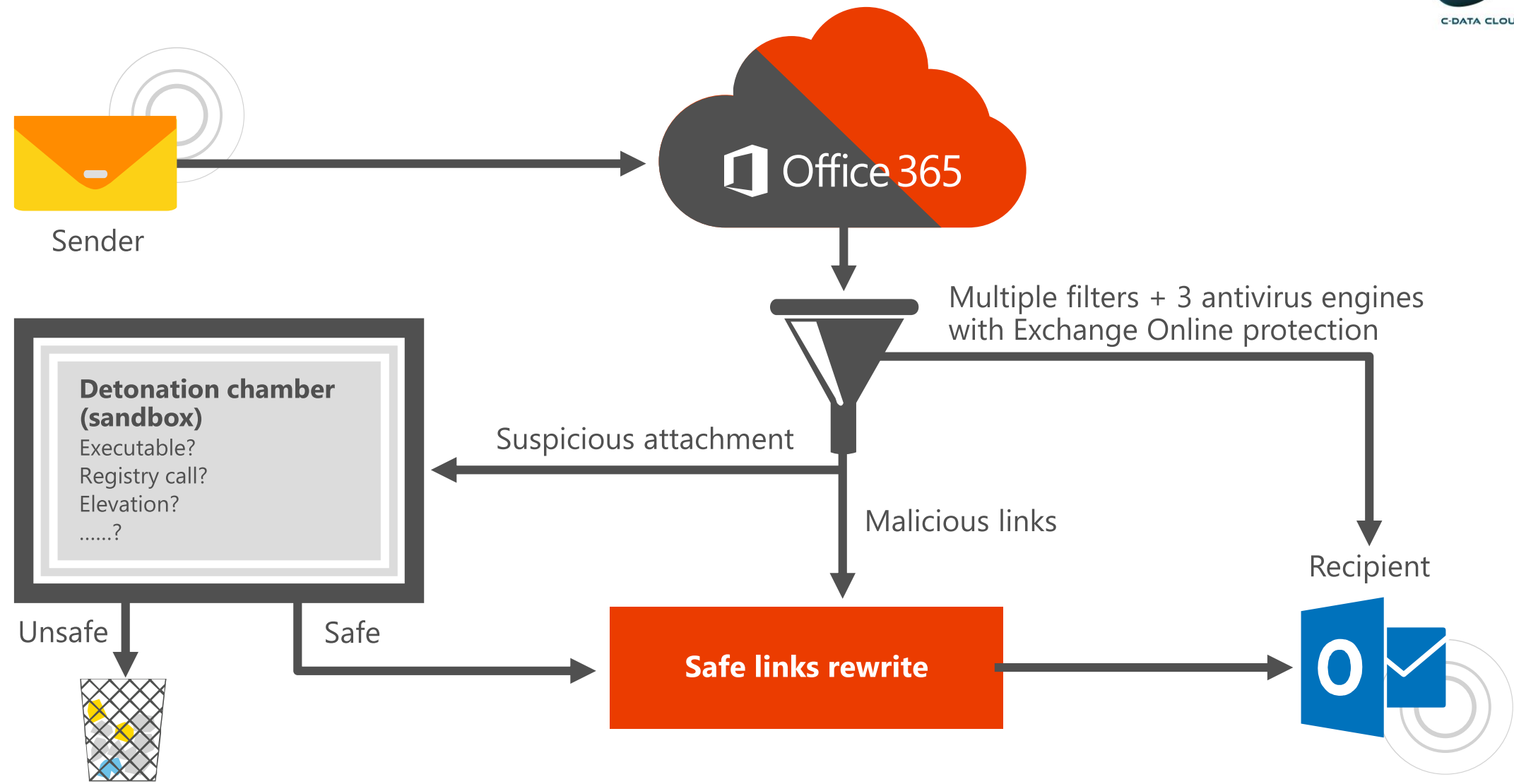


---

Rich reporting  
and tracing

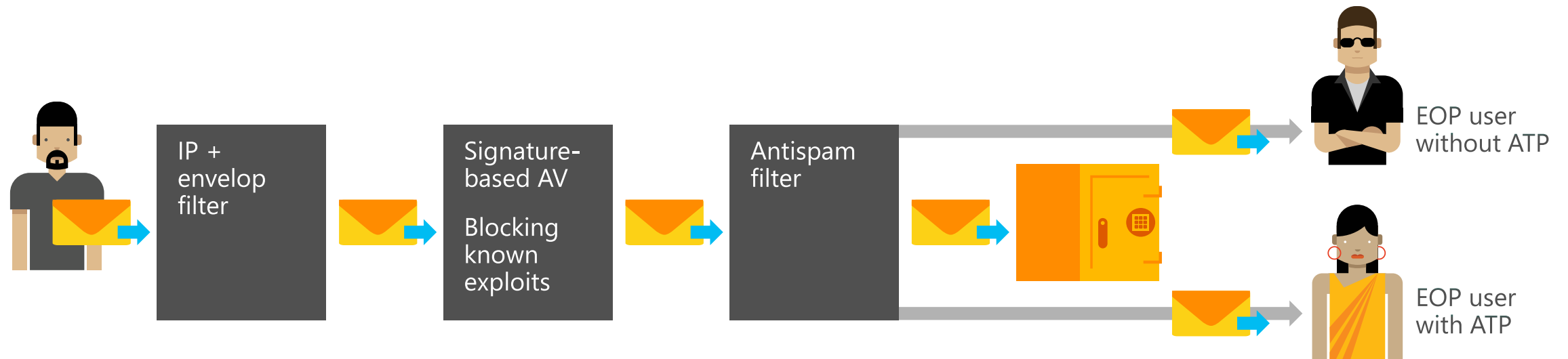
- Built-in URL trace
- Reports for advanced threats

# Service architecture



# Safe attachments

- Protect against zero day exploits in email attachments by blocking messages
- Provides admins visibility into compromised users
- Leverages sandboxing technology





# Safe attachment—experience



safe attachments

safe links

ENABLED

NAME

Safe Attachment Policy

Default

Safe attachments policy - Google Chrome

<https://outlook.office365.com/ecp/SafeAttachment/EditSafeAttachmentPolicy.aspx?reqId=1427150972917&pw>

Safe Attachment Policy - Block

general

settings

applied to

Safe attachments unknown malware response

Select the action for unknown malware in attachments.  
Warning: These actions may cause significant delay to email delivery. [Learn more](#)

☐ Off - Attachment will not be scanned for malware.

☐ Monitor - Continue delivering the message after malware is detected; track scan results.

☒ Block - Block the current and future emails and attachments with detected malware.

☐ Replace - Block the attachments with detected malware, continue to deliver the message.

Redirect attachment on detection

Send the blocked or replaced attachment to an email address.

☒ Enable redirect

Send the attachment to the following email address  
[admin@contosobankatp.onmicrosoft.com](mailto:admin@contosobankatp.onmicrosoft.com)

☒ Apply the above selection if malware scanning for at times out or error occurs.

Admin sets policy

Admin gets notification if message is blocked

INBOX

CONVERSATIONS BY DATE

All Unread To me Flagged

LAST WEEK

☒ Exchange Online Advanced Threat Protection <

Administrator Notification: Redirecting email with malware

Sat 3/21

Postmaster

Undeliverable message

Sat 3/21

Exchange Online Advanced Threat Protection <

Administrator Notification: Redirecting email with malware

Sat 3/21

Exchange Online Advanced Threat Protection <

Administrator Notification: Redirecting email with malware

Fri 3/20

Postmaster

Undeliverable message

Fri 3/20

Exchange Online Advanced Threat Protection <

Administrator Notification: Redirecting email with malware

Thu 3/19

Administrator Notification: Redirecting email with malware

Exchange Online Advanced Threat Protection <advanced-threat-protection@protection.outlook.com>

Sat 3/21/2015 2:31 PM

To: MOD Administrator;

112 KB

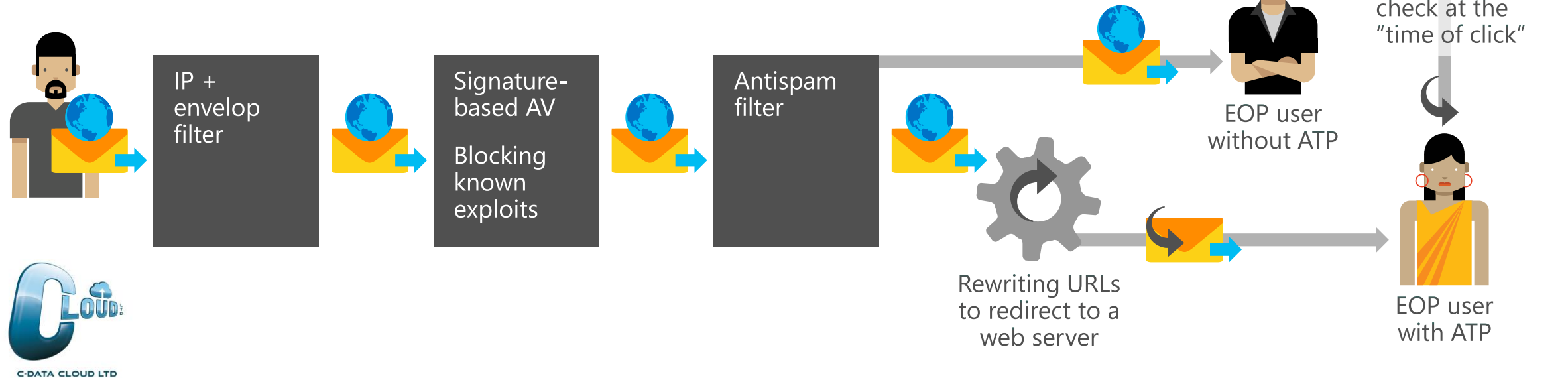
This message was created automatically by Exchange Online Advanced Threat Protection service  
Malware was detected in the email included with this message as an attachment

From:Jeremyc@contosobankatp.onmicrosoft.com  
To:shobhits@contosobankatp.onmicrosoft.com  
Subject:Limited time offering from Fabrikam  
Date:3/21/2015 9:31:03 PM

The attached email or the attachment has not been delivered to the intended recipient(s). If it is opened, it might infect the computer with malware. Please do not respond to this message, it is an unmonitored alias. For more information, please see <http://go.microsoft.com/fwlink/?LinkId=526076>.

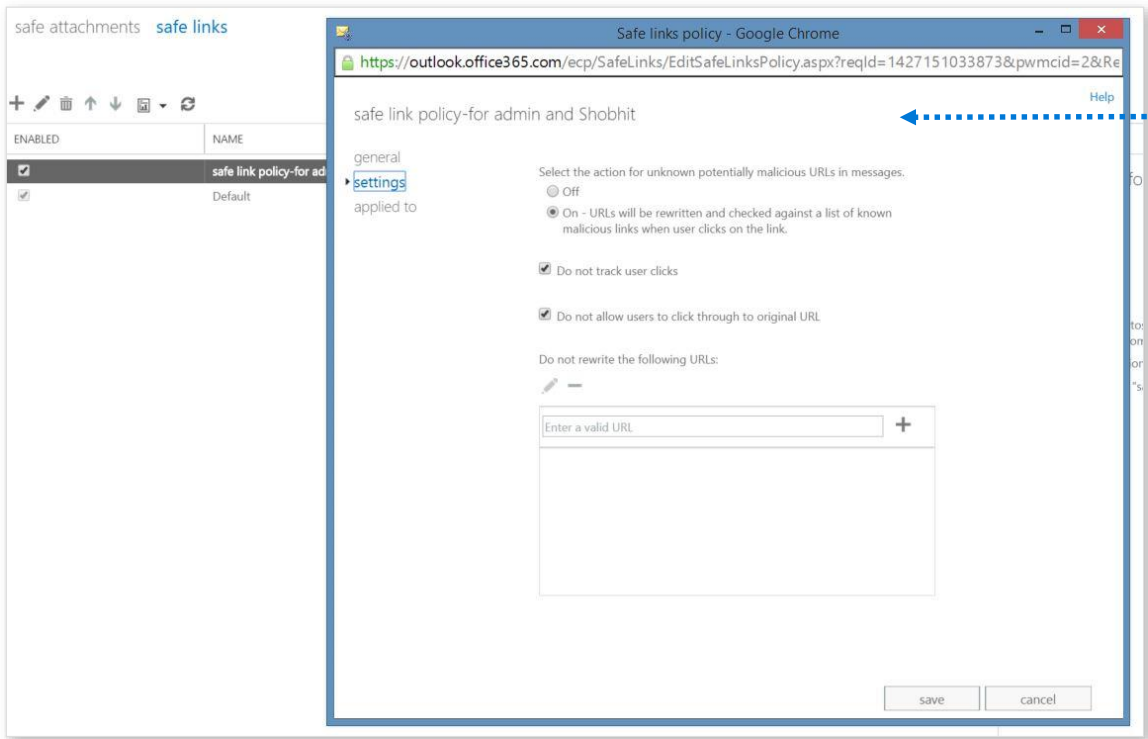
# Safe links

- Protect against sites with malicious content, phishing sites
- Provides admins visibility into compromised users
- Rewriting the URLs to proxy them through another server



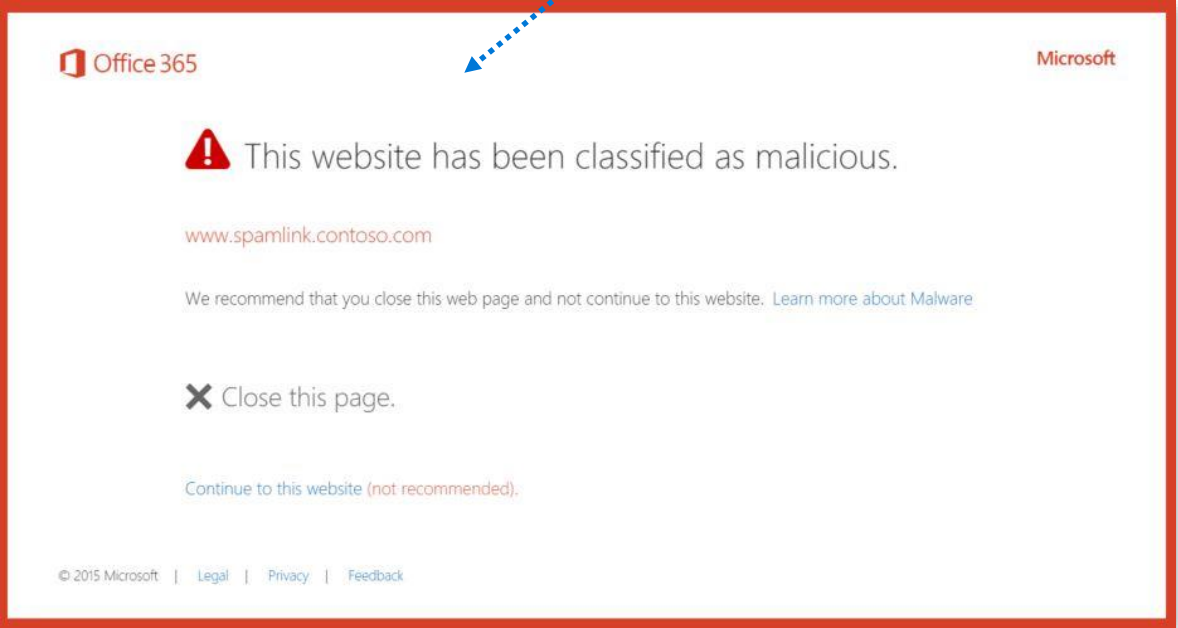


# Safe links—experience

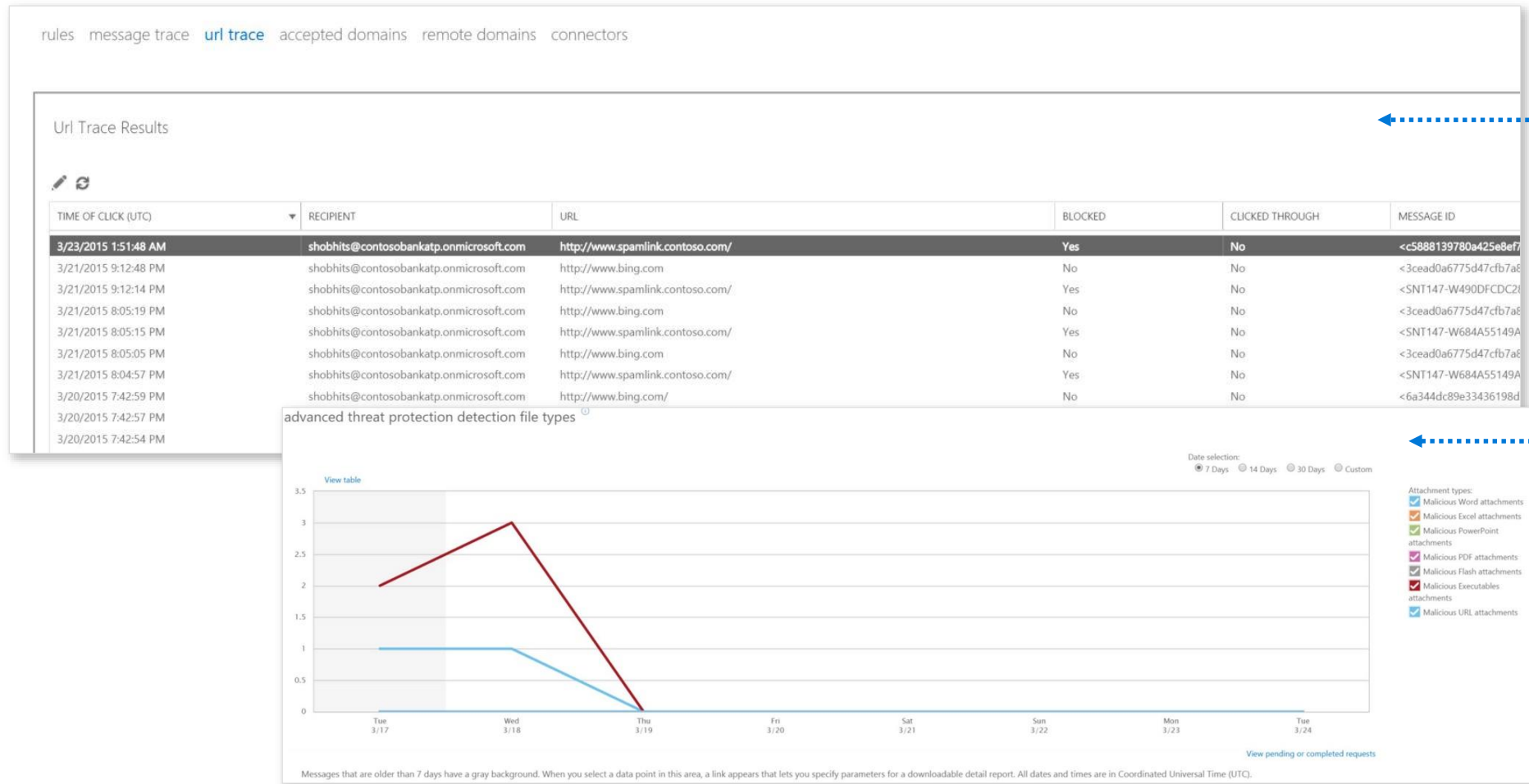


Admin sets policy

Users notified if  
a malicious link is  
clicked in email



# Rich reporting and click trace



Admins have complete visibility into who clicked on what links

Reporting by file types and disposition

# Purchasing Exchange Online ATP



Customer	Channel at launch	ERP at launch
All commercial customers	Direct, CSP, Open, MPSA, and EA channels	\$2 per user per month
Multi-tenant government customers	Direct, Open, MPSA, and EA channels at an ERP of \$1.75 per user per month at launch	\$1.75 per user per month
Office 365 Government Community Cloud (GCC), Office 365 Education, and Office 365 Nonprofit customers	Not available	Not available

