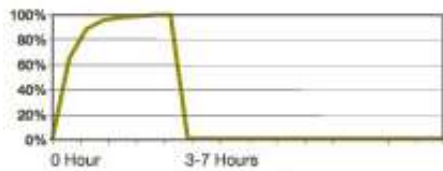


Exchange Online Advanced Threat Protection

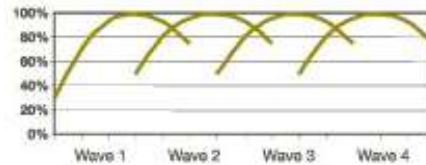


Evolving threat space

Short-span attacks



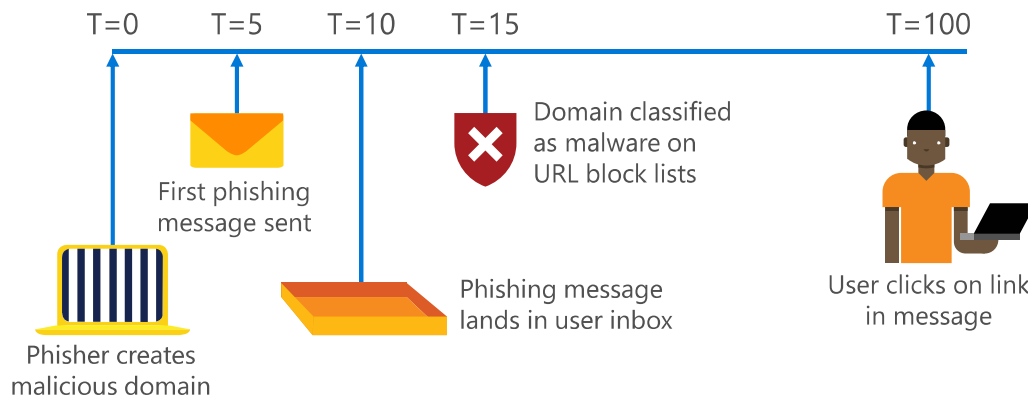
Serial variant attacks



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

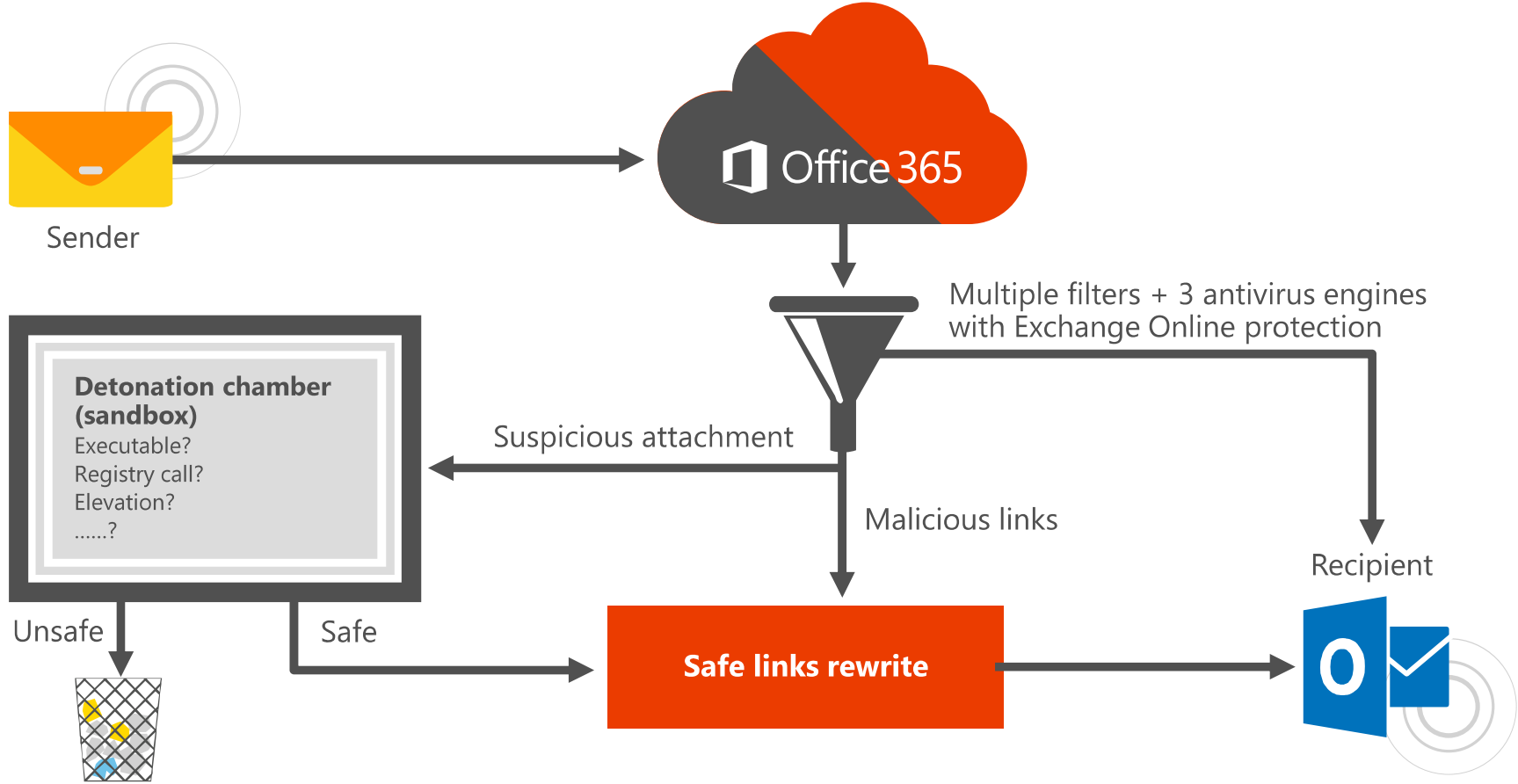
- Real time protection against Malicious URLs
- Growing URL coverage



Rich reporting and tracing

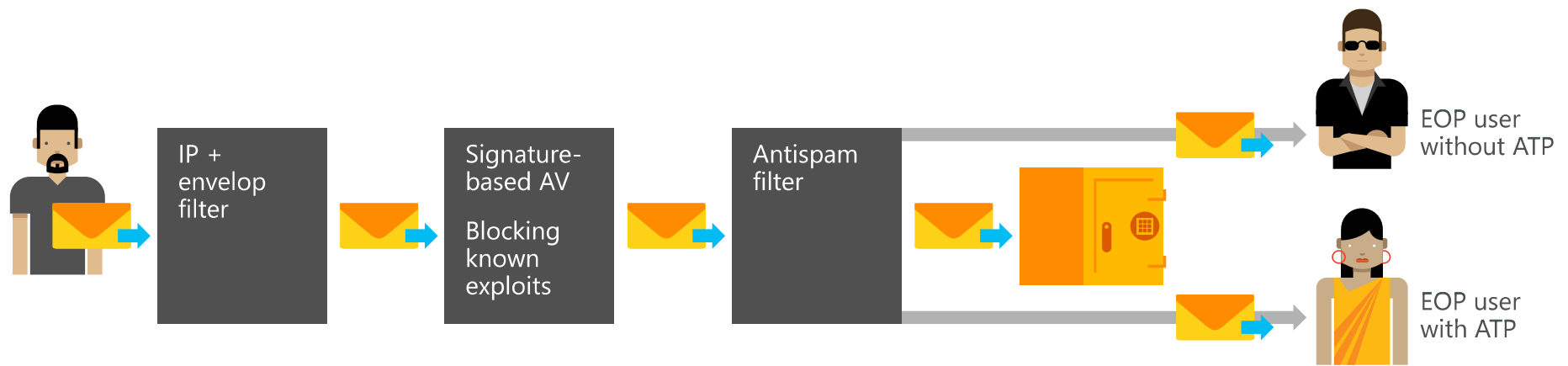
- Built-in URL trace
- Reports for advanced threats

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

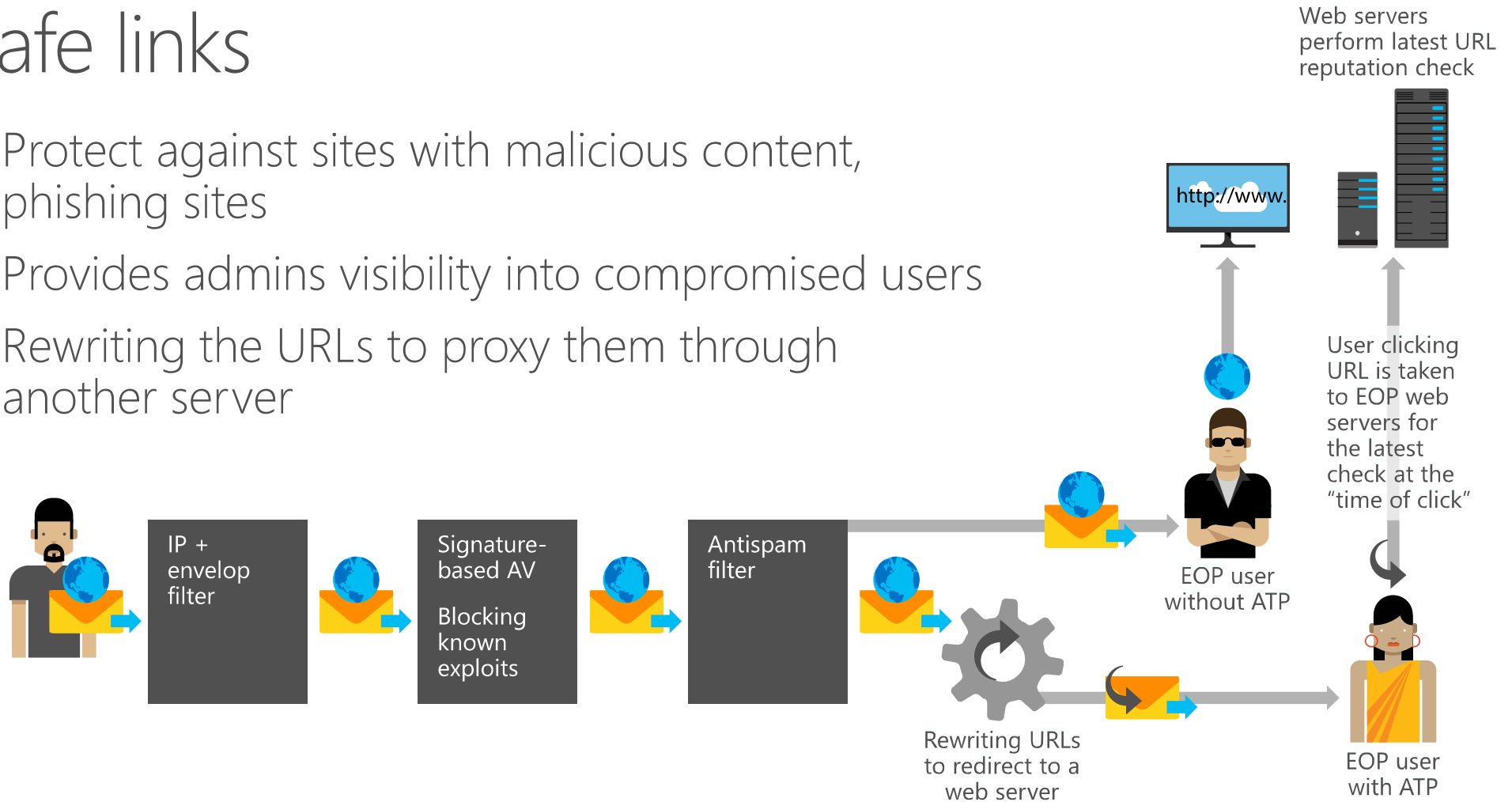
The screenshot illustrates the user experience for safe attachments in Outlook. It is divided into three main sections:

- Policy Configuration:** A browser window shows the "Safe Attachment Policy" settings page. The "Block" option is selected under "Safe attachments unknown malware response". A blue arrow points from the text "Admin sets policy" to this section.
- Notification Email:** An email from "Exchange Online Advanced Threat Protection" is shown. The subject is "Administrator Notification: Redirecting email with malware". A blue arrow points from the text "Admin gets notification if message is blocked" to this email.
- Message Content:** The email body contains a "Postmaster" message stating "Undeliverable message" and a notification from "Exchange Online Advanced Threat Protection" explaining that malware was detected in the email.

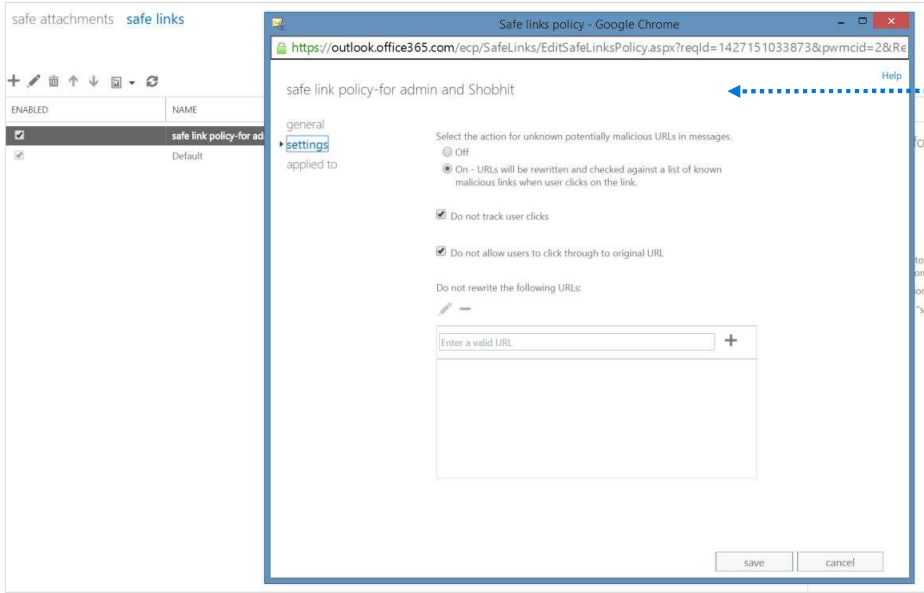
Additional interface elements include a "safe attachments" sidebar, a "Safe Attachment Policy" table, and a "CONVERSATIONS BY DATE" dropdown menu.

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

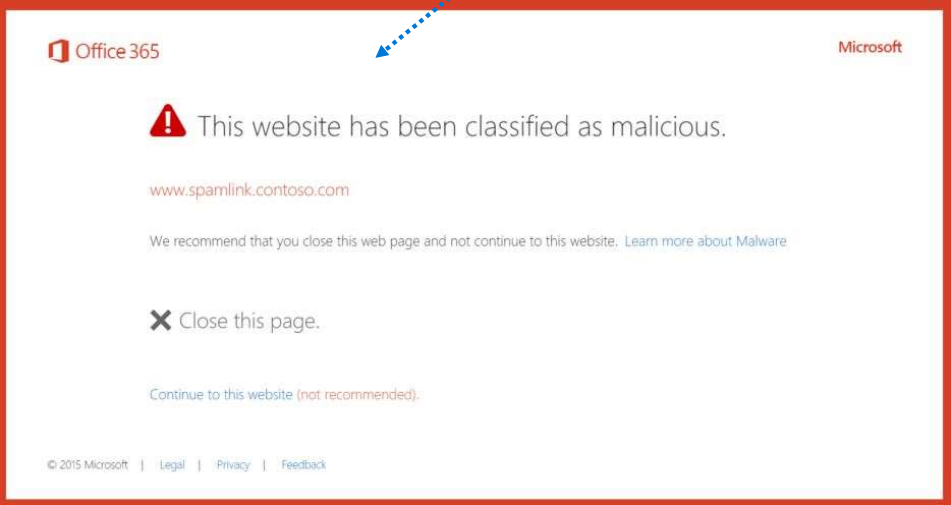


Safe links—experience

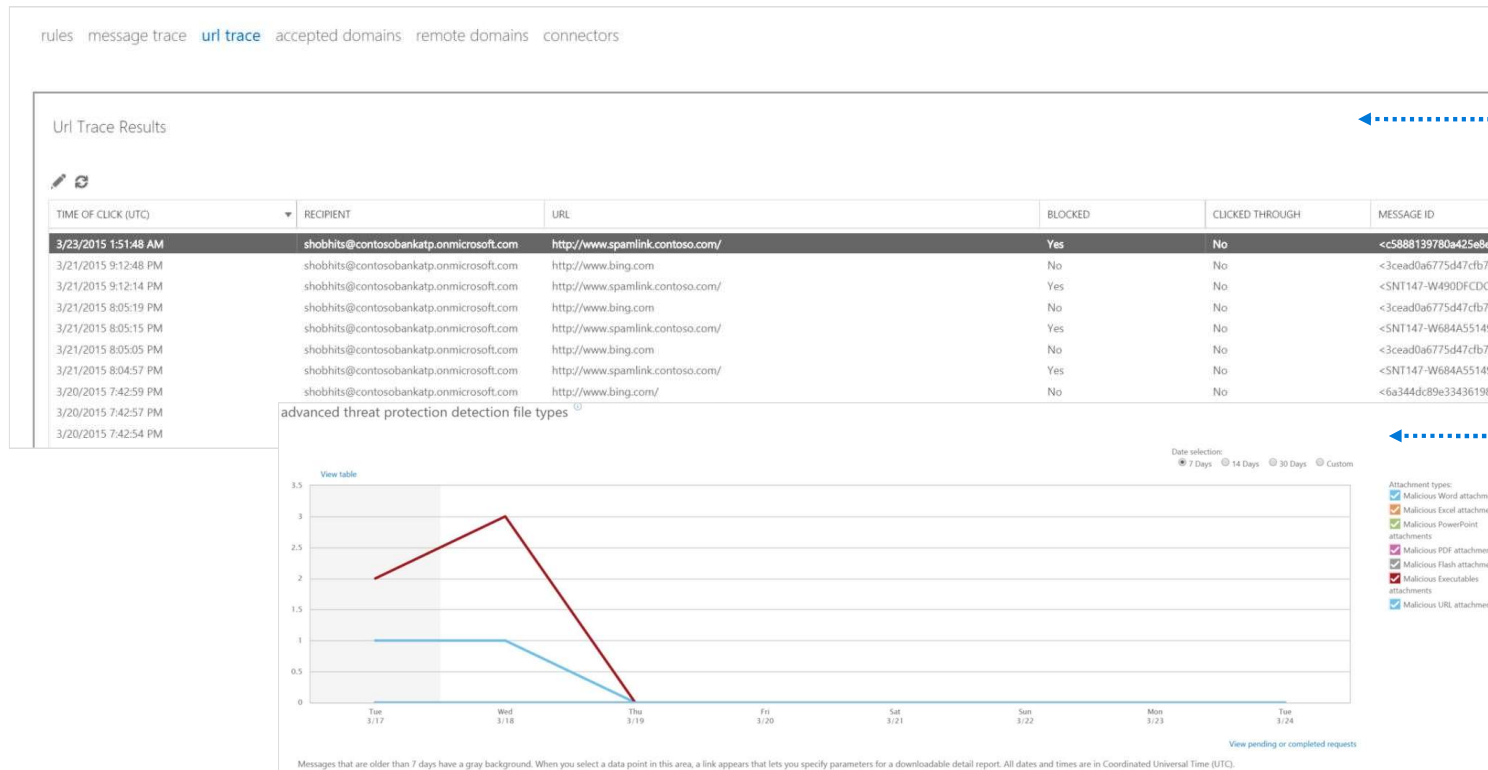


Admin sets policy

Users notified if a malicious link is clicked in email



Rich reporting and click trace

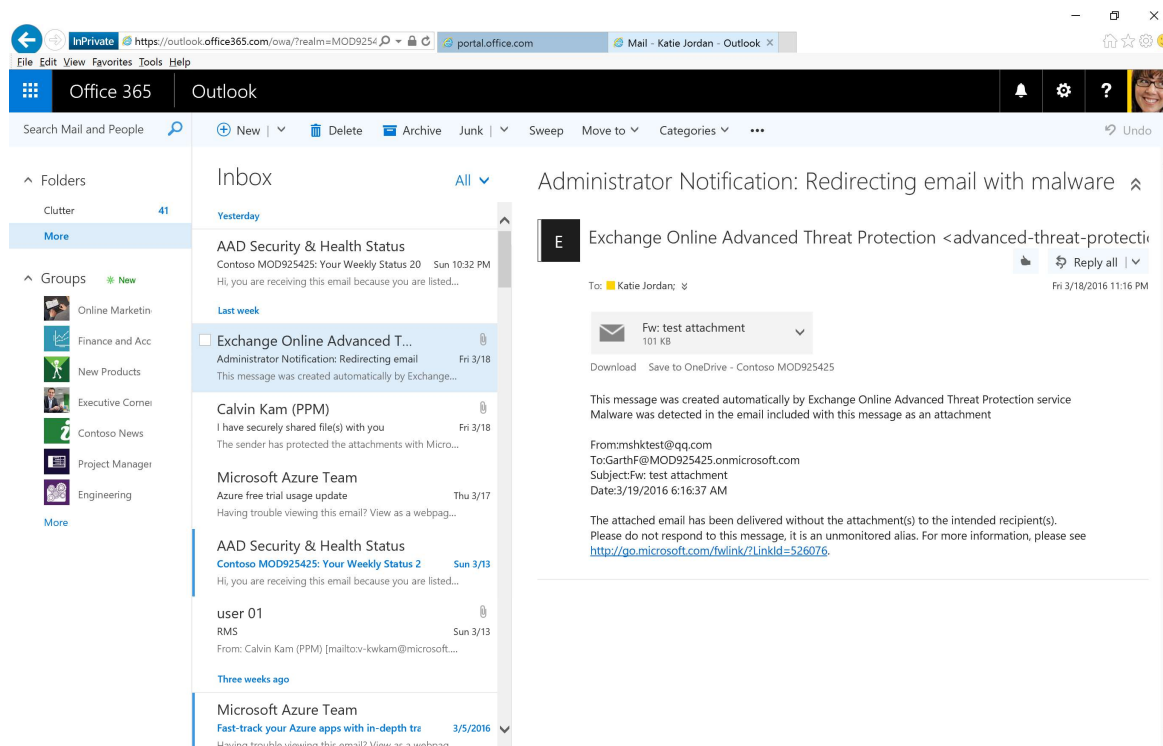


Admins have complete visibility into who clicked on what links

Reporting by file types and disposition

Demo - Attachment protect

- Send a mail with ransomware to protected mailbox, (Block) the user won't receive the mail but the admin will receive a remind mail



Demo - Link protect

- Via ATP services rewrite suspicious link in <https://na01.safelinks.protection.outlook.com/?url=https%3a%2f%2fwww.puaypail.com%2f&data=01%7c01>

The screenshot shows an Outlook inbox with several emails. The selected email is from 'mshk' with the subject 'Your account has been limited until we hear'. The main content of the email is a PayPal notice titled 'Your account has been limited.' The notice explains that the account is limited due to unusual login activity and provides instructions on how to remove the limitation. The URL in the browser's address bar is highlighted with a red circle, showing a safe link generated by Outlook's ATP service: <https://na01.safelinks.protection.outlook.com/?url=https%3a%2f%2fwww.puaypail.com%2f&data=01%7c01>

Demo - Access denied of malicious websites

- Each time access the link, Microsoft will pre-open the web site to protect the zero attack / delay attack

