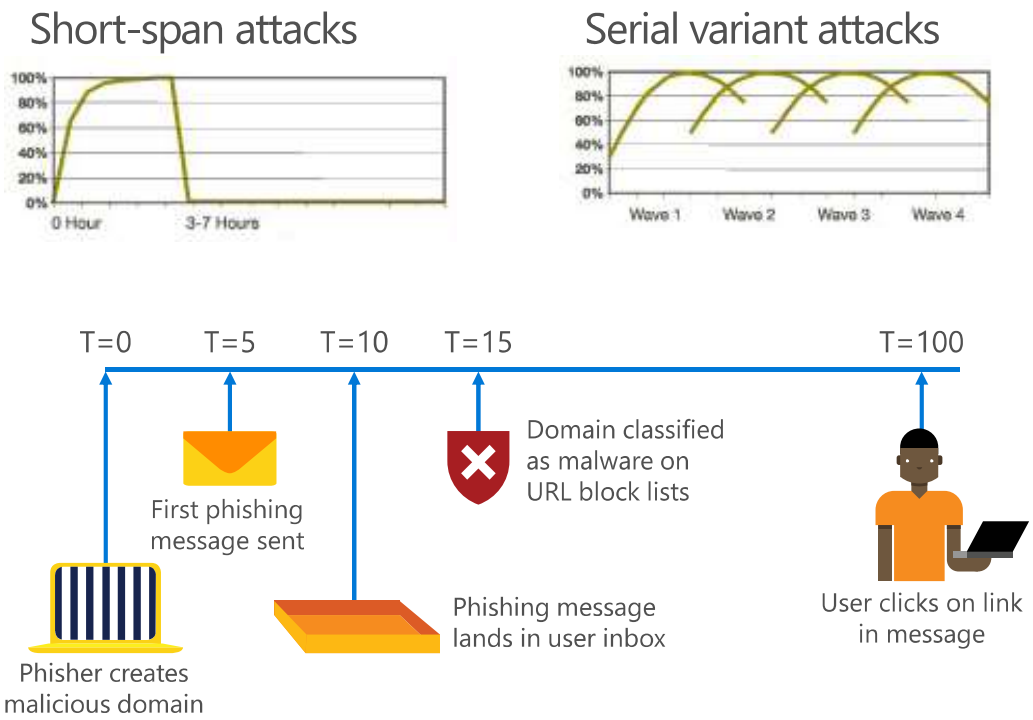
Exchange Online Advanced Threat Protection

Microsoft

Evolving threat space



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

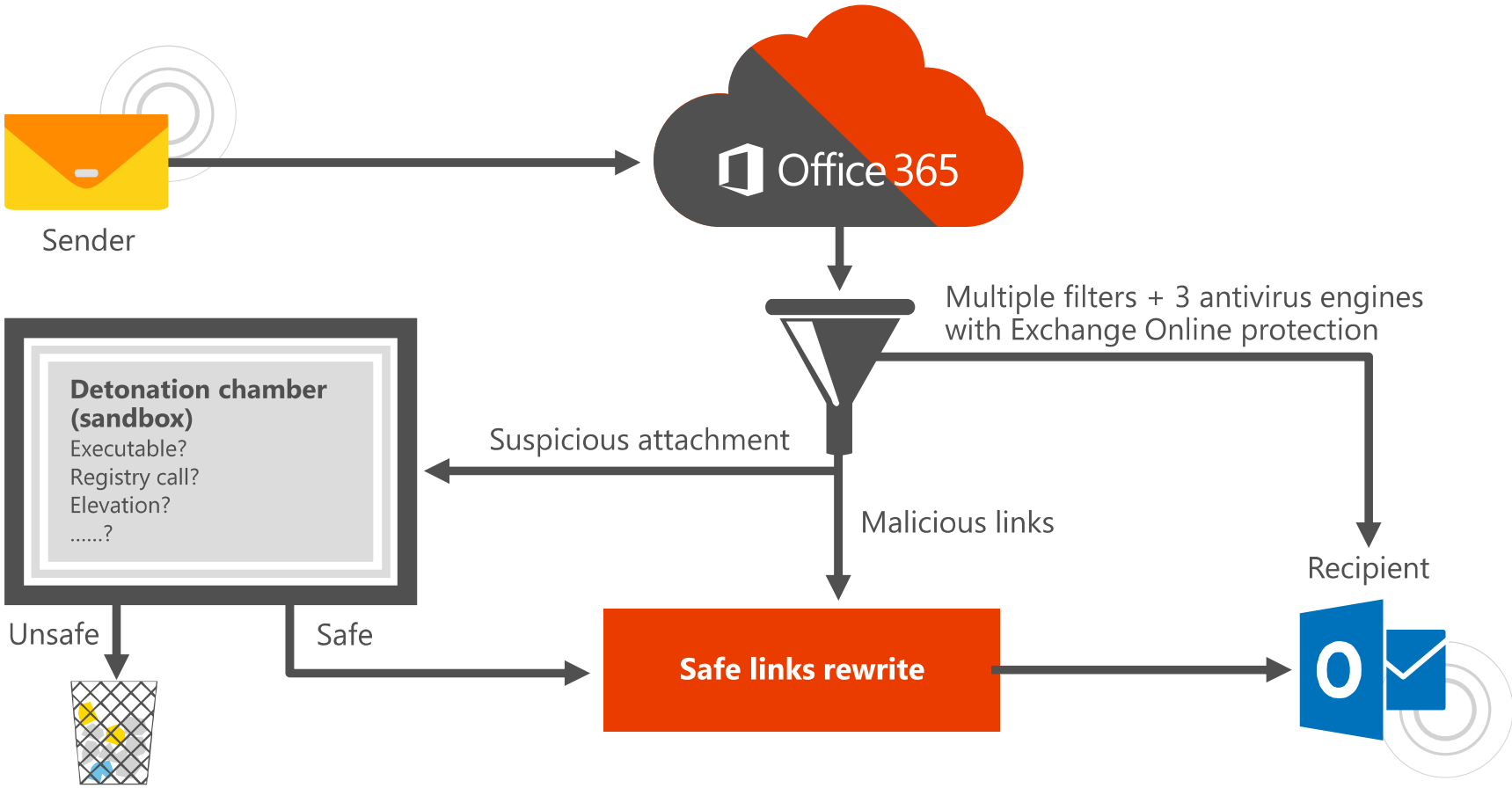
Time of click protection

- Real time protection against Malicious URLs
- Growing URL coverage

Rich reporting and tracing

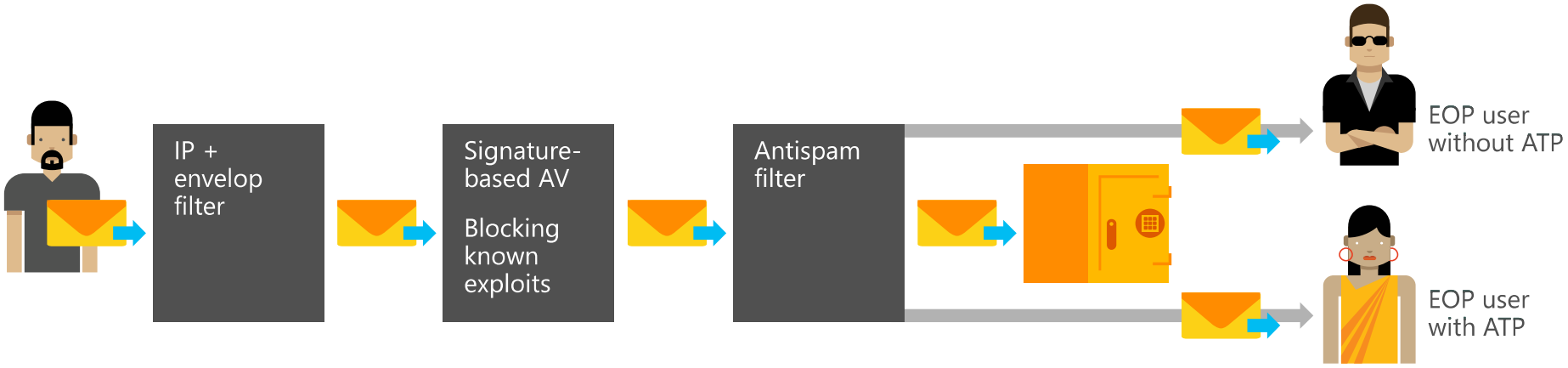
- Built-in URL trace
- Reports for advanced threats

Service architecture

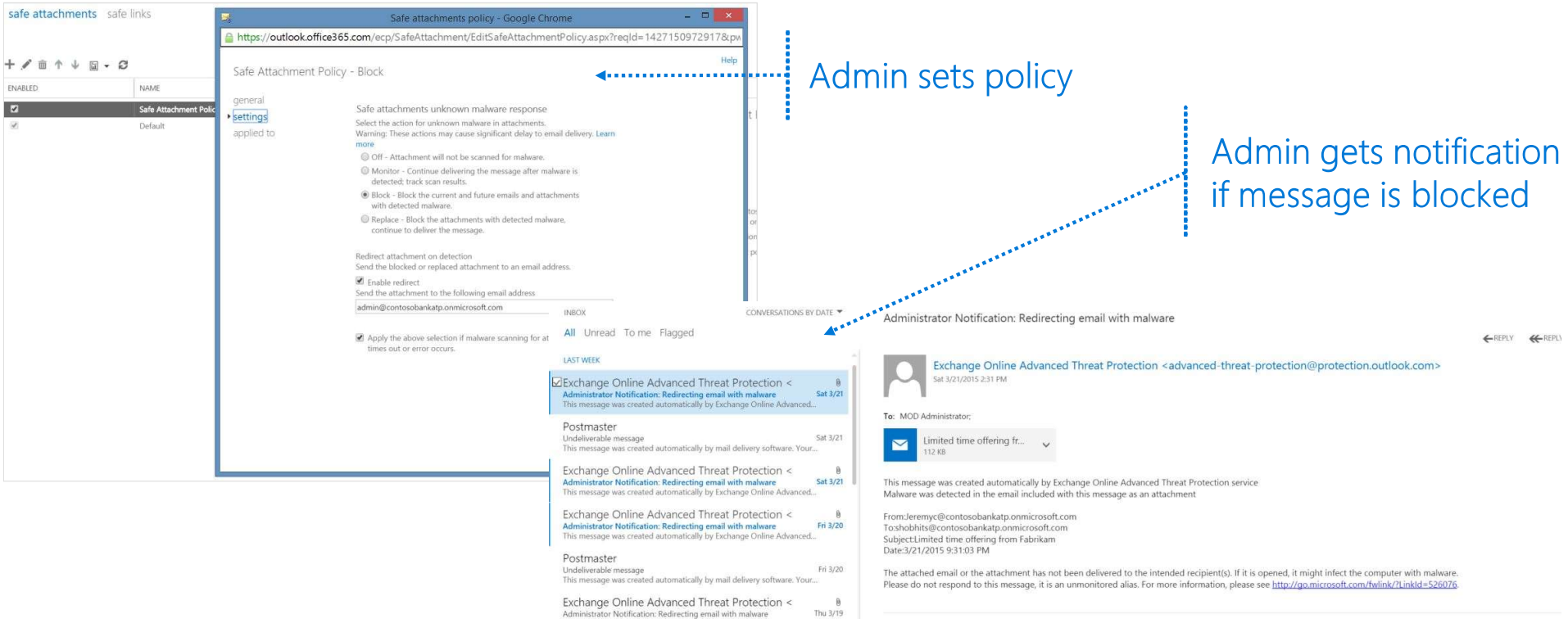


Safe attachments

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

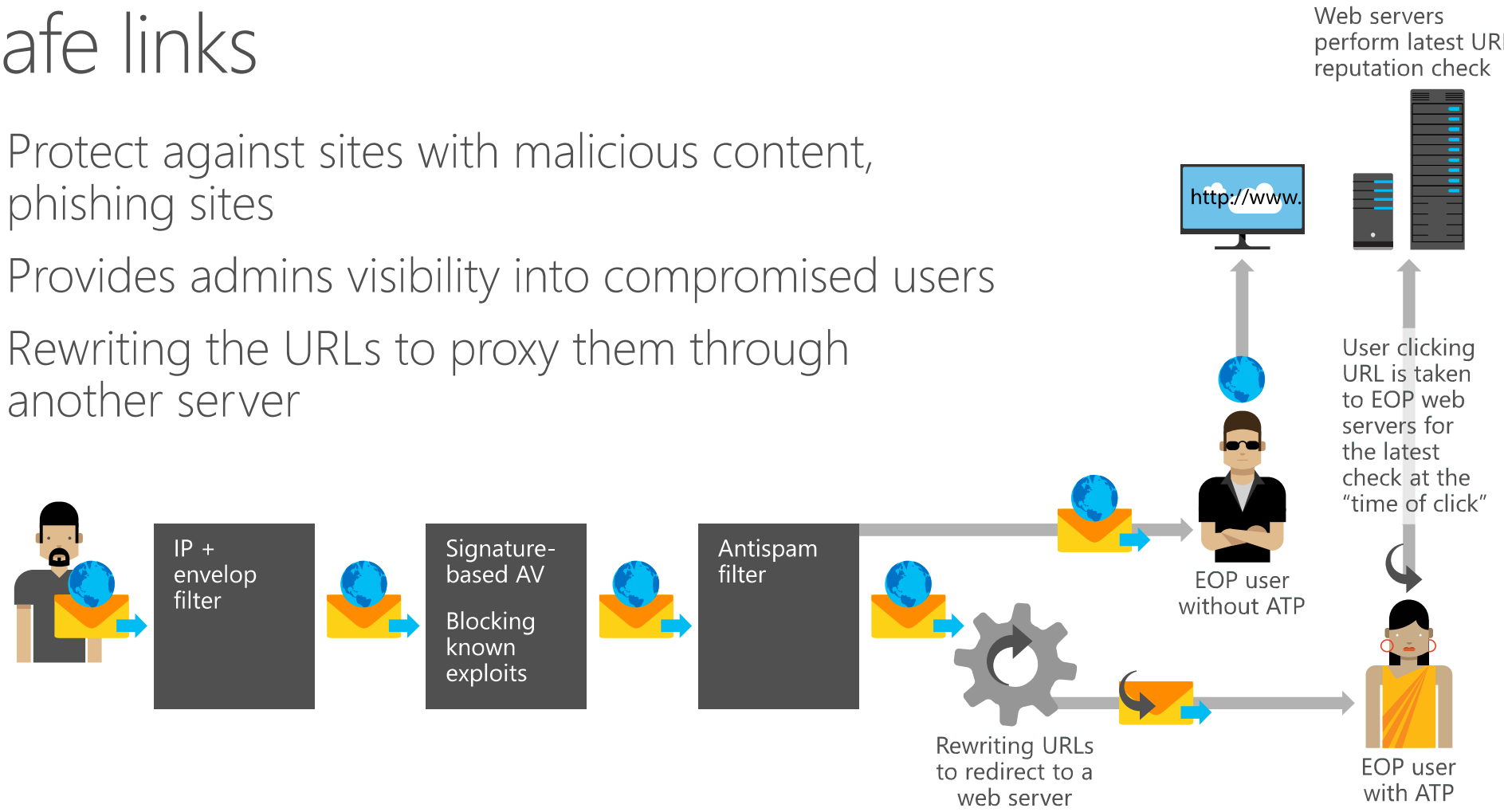


Safe attachment—experience

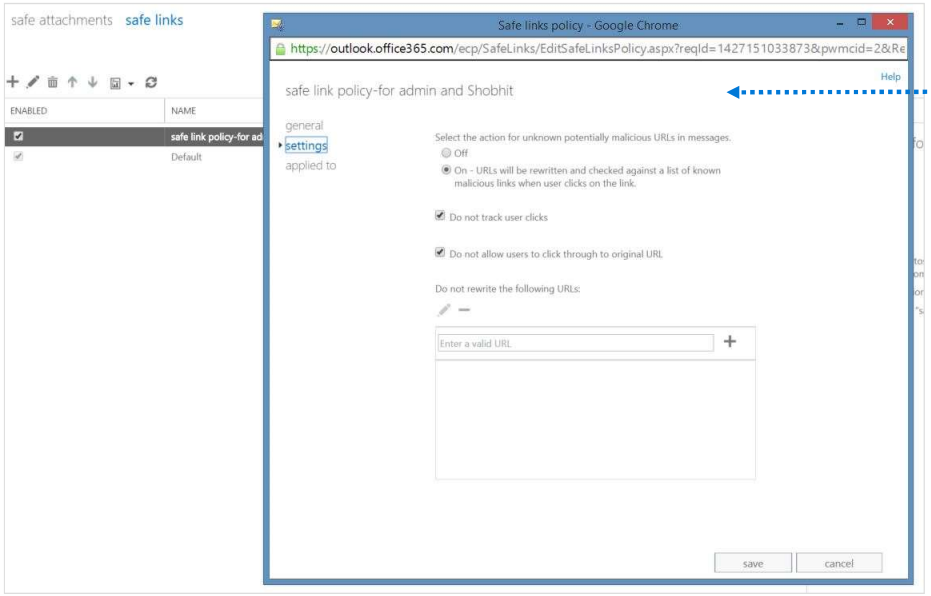


Safe links

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

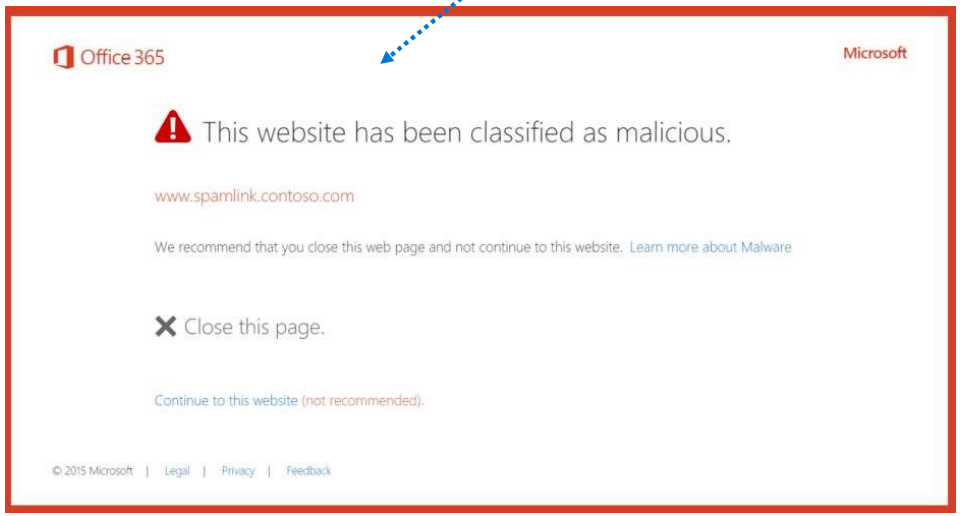


Safe links—experience

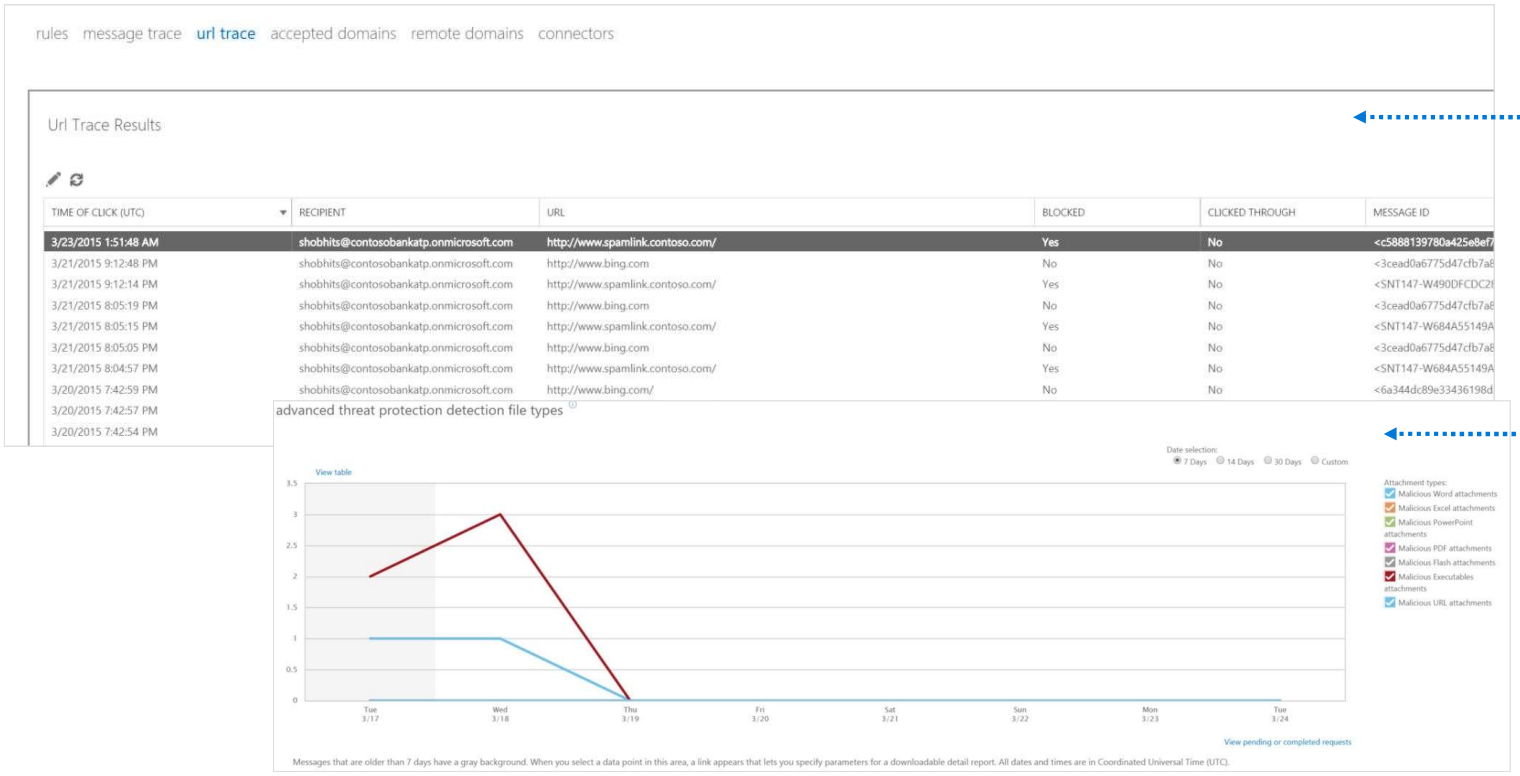


Admin sets policy

Users notified if a malicious link is clicked in email



Rich reporting and click trace

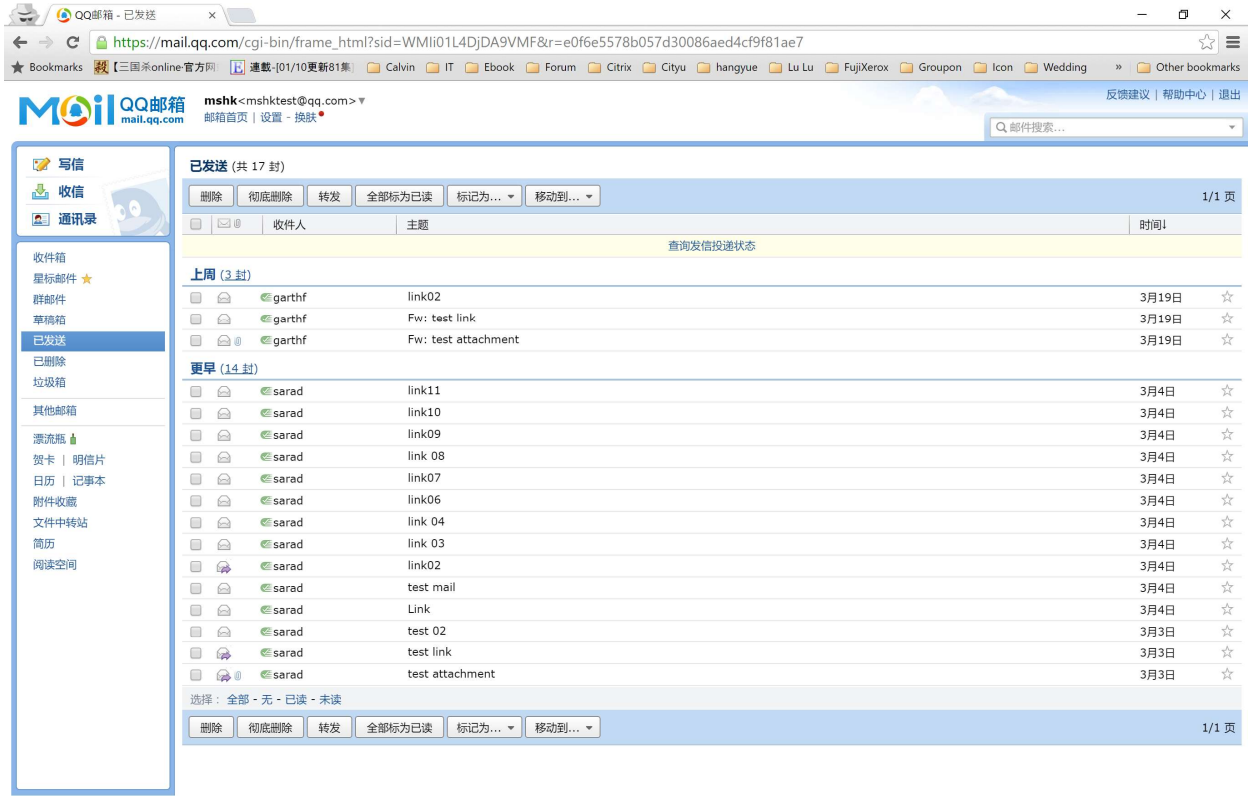


Admins have complete visibility into who clicked on what links

Reporting by file types and disposition

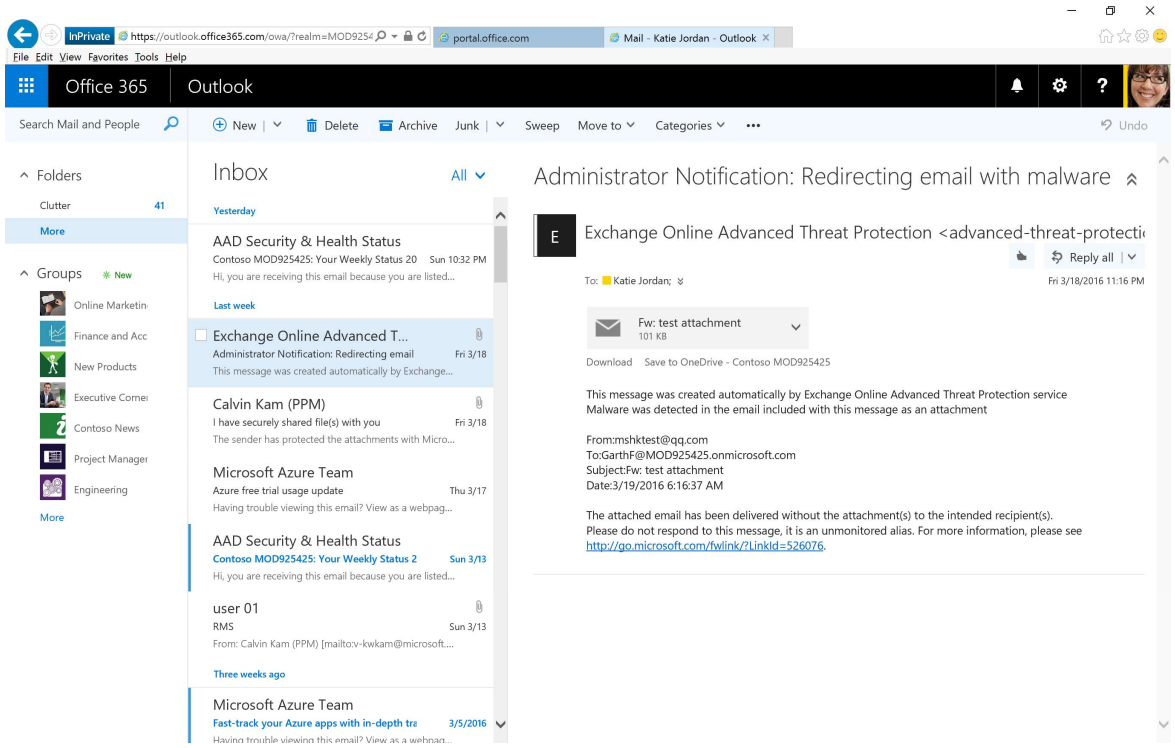
Demo

- Setup a less protect mail account (e.g. qq.com) to send out ransomware file and link



Demo - Attachment protect

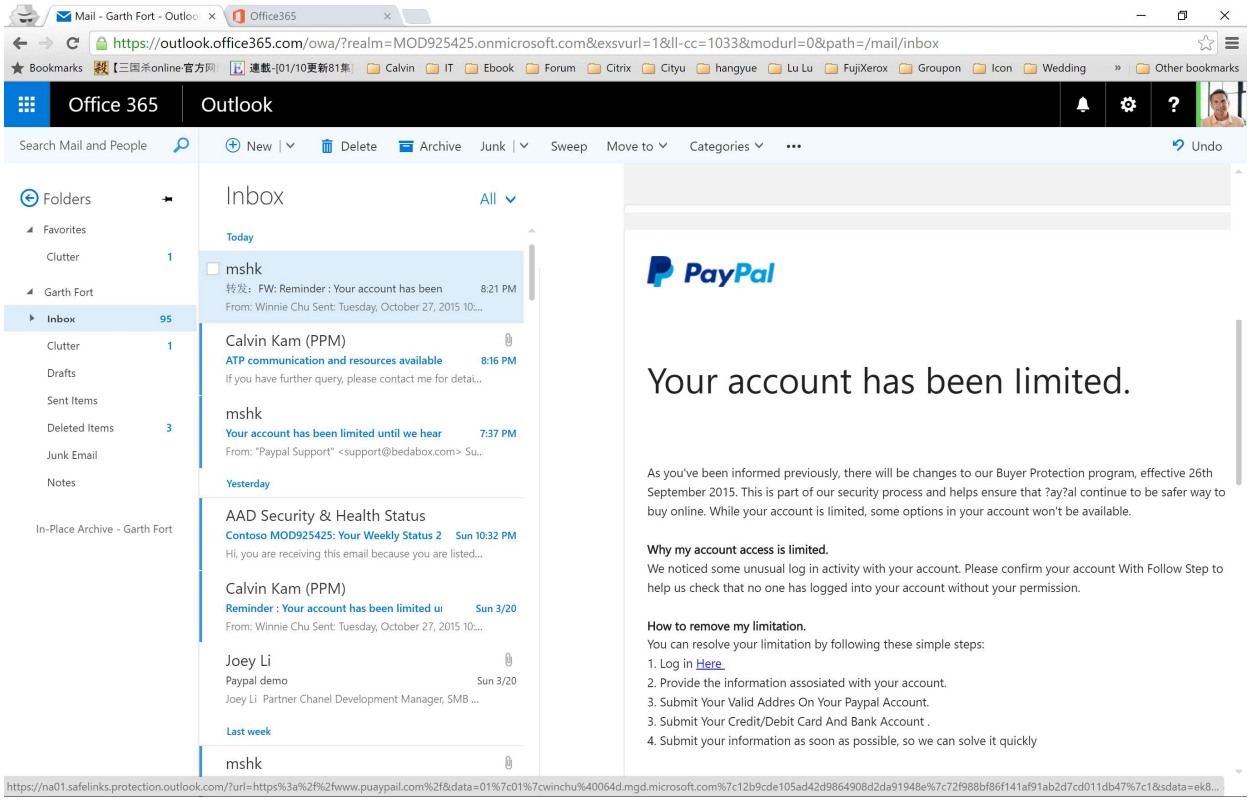
- Send a mail with ransomware to protected mailbox, (Block) the user won't receive the mail but the admin will receive a remind mail



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



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