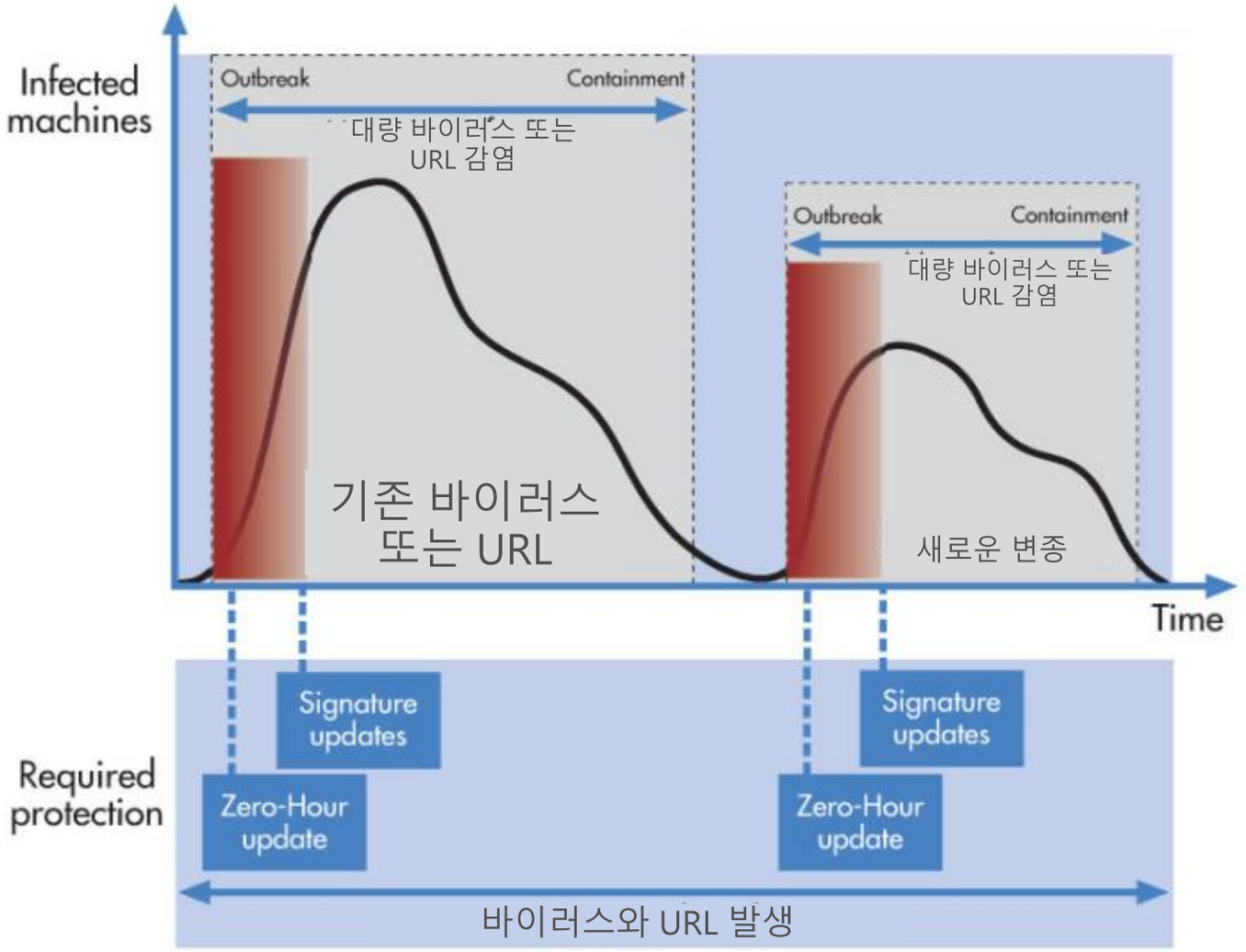
Exchange Online Advanced Threat Protection

Microsoft

진보하는 위협 요소



새롭게 발생되는 공격은 2개의 파트로 구성

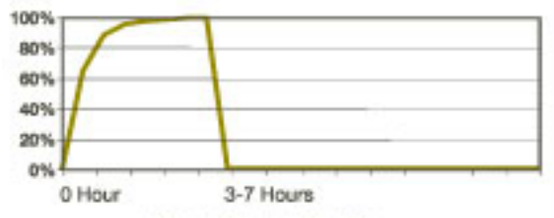
A. 제로 시간 공격
B. 공격 기간 연장

전통적인 AV/AS 제품은 제로 데이 공격으로부터 종합적으로 보호할 수 없습니다.

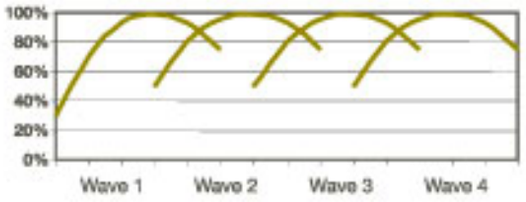
공격자는 제로 데이 공격 동안 완전이 들키지 않을 수 있습니다.

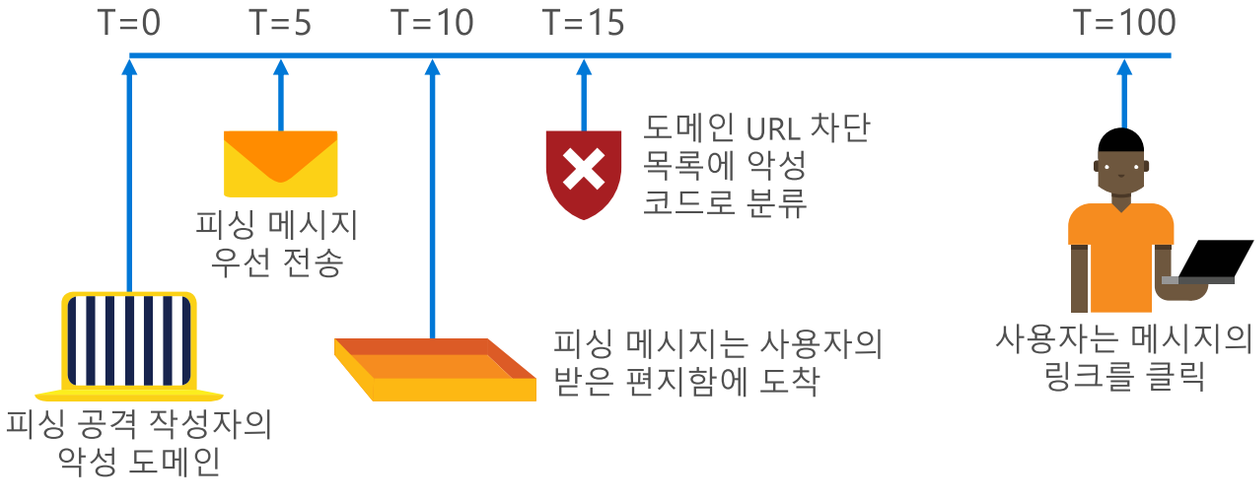
진보하는 위협 요소

Short-span attacks



Serial variant attacks





Short-span attacks은 몇 시간 동안 단지 몇 분

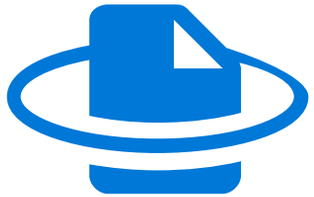
Serial variant attacks은 일반적으로 몇 시간마다 패턴을 반복

메일이 전달 된 후 공격자는 쉽게 메시지의 링크를 변경 가능

Exchange Online advanced threat protection

알려지지 않는 멜웨어/바이러스로부터 보호

- Behavioral analysis with machine learning
- Admin alerts



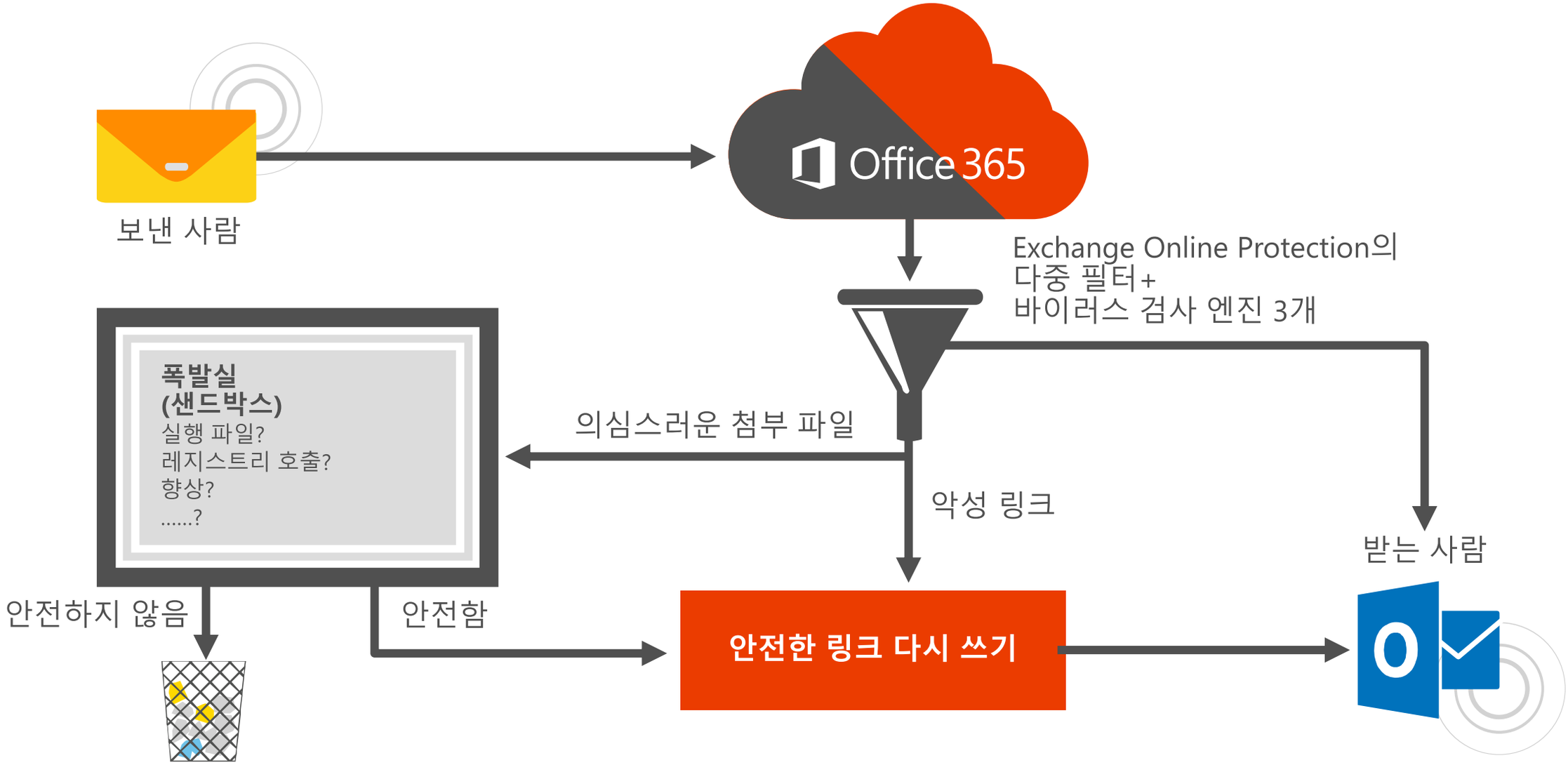
클릭 할 때의 보호

- 악성 URL에 대한 실시간 보호
- 증가하고 있는 URL 범위

유용한 보고 및 추적

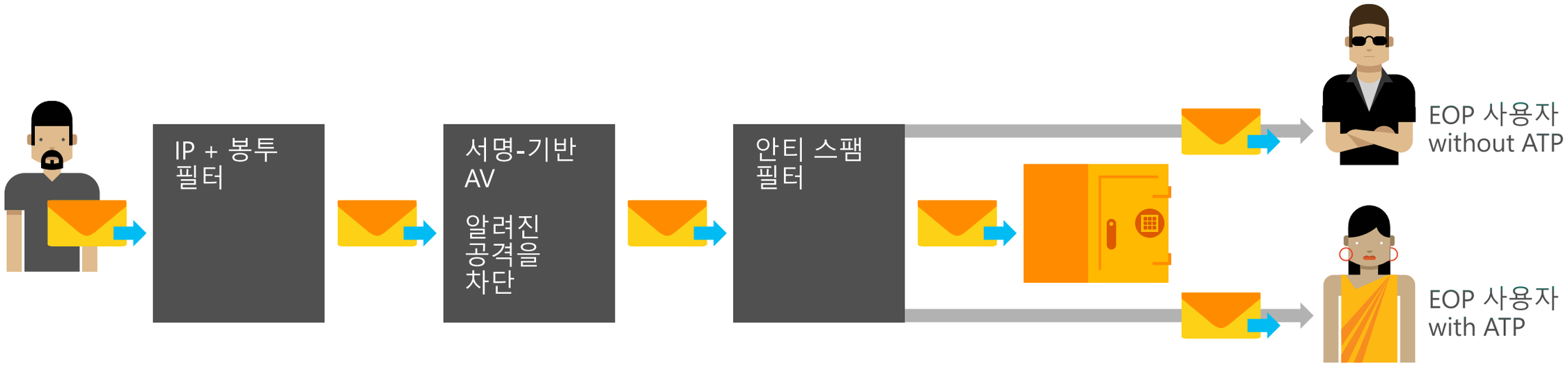
- URL 추적 내장
- 고급 위협 보고서

서비스 아키텍처

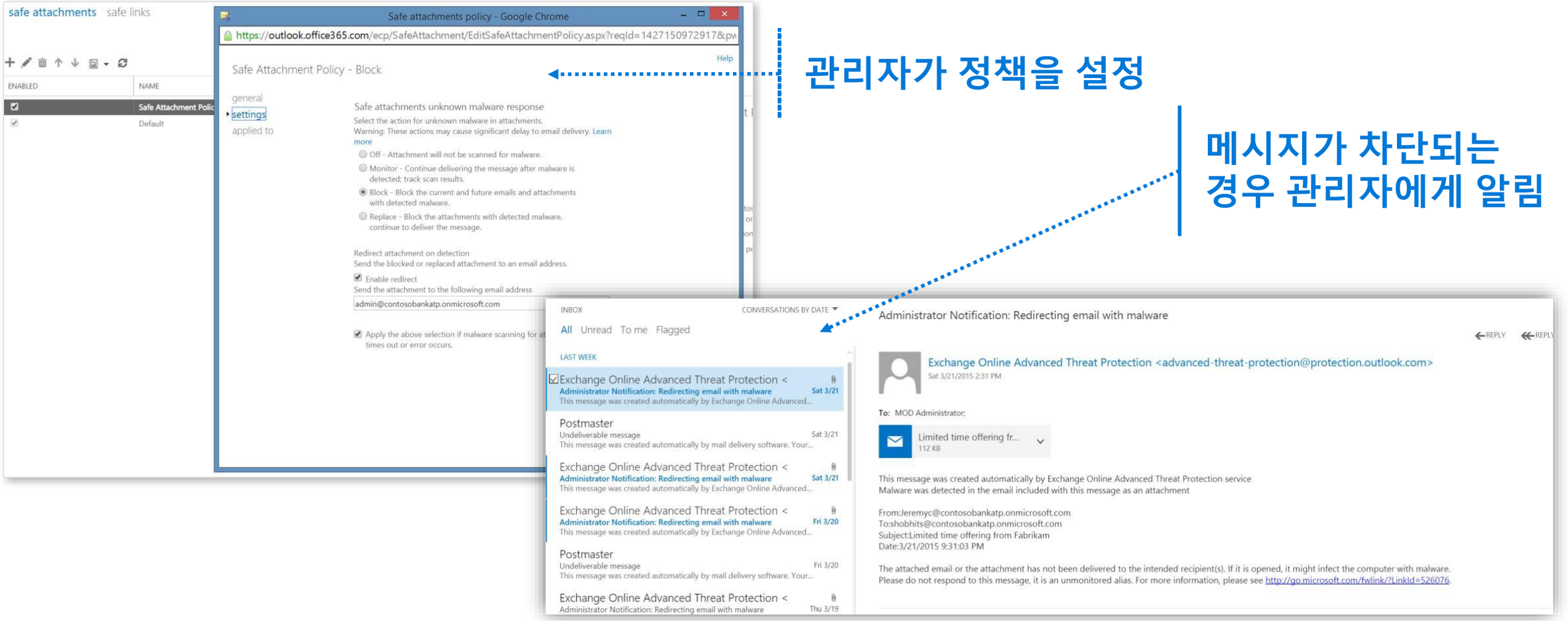

보낸 사람
Office 365
Exchange Online Protection의
다중 필터+
바이러스 검사 엔진 3개
폭발실
(샌드박스)
실행 파일?
레지스트리 호출?
향상?
.....?
의심스러운 첨부 파일
악성 링크
받는 사람
안전하지 않음
안전함
안전한 링크 다시 쓰기

안전한 첨부 파일

- 메시지 차단으로 전자 메일 첨부 파일에서의 제로 데이 공격으로부터 보호
- 감염된 사용자에 대한 관리자 가시성을 제공
- 샌드박스 기술을 활용

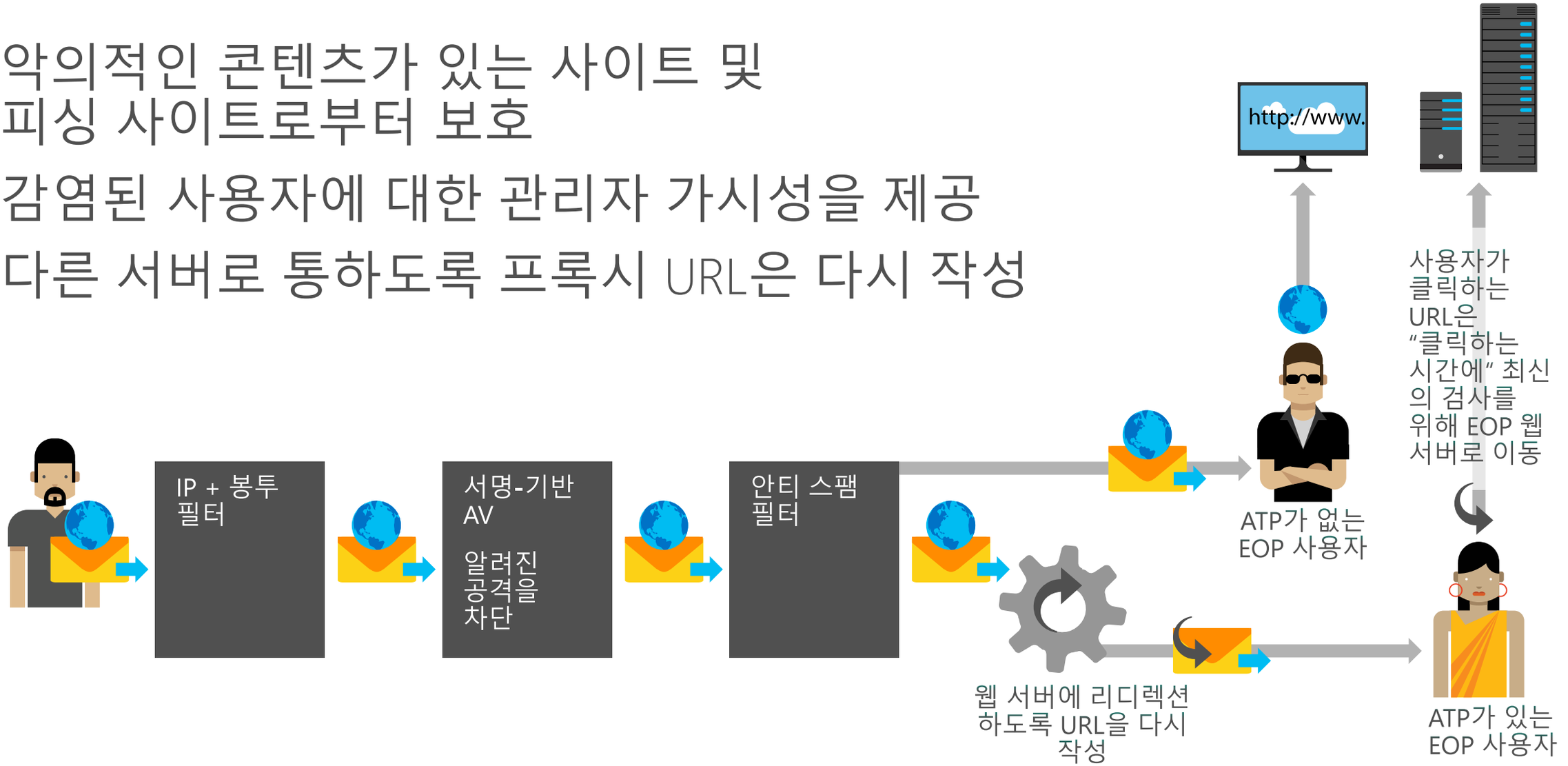


안전한 첨부 파일—체험

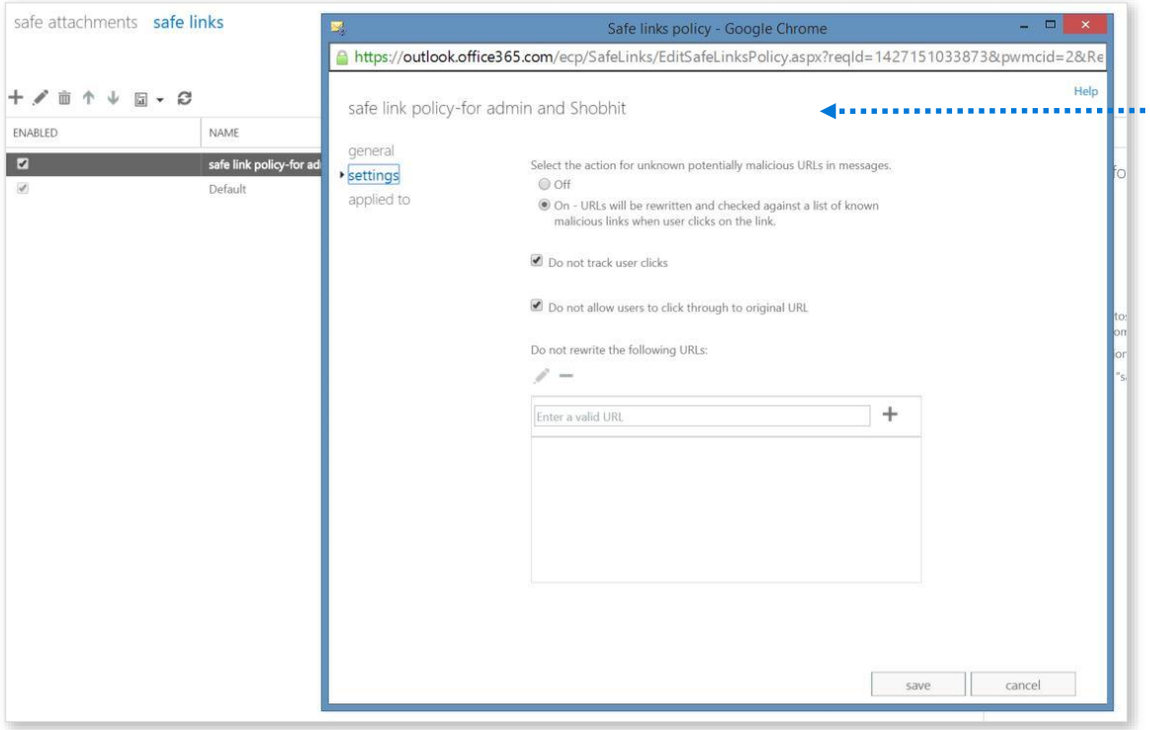

safe attachments
safe links
ENABLED
NAME
Safe Attachment Polic
Default
Safe attachments policy - Google Chrome
https://outlook.office365.com/ecp/SafeAttachment/EditSafeAttachmentPolicy.aspx?reqId=1427150972917&pw
Help
Safe Attachment Policy - Block
general
settings
applied to
Safe attachments unknown 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
Apply the above selection if malware scanning for at
times out or error occurs.
관리자가 정책을 설정
메시지가 차단되는
경우 관리자에게 알림
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
This message was created automatically by Exchange Online Advanced...
Postmaster
Undeliverable message
Sat 3/21
This message was created automatically by mail delivery software. Your...
Exchange Online Advanced Threat Protection <
Administrator Notification: Redirecting email with malware
Sat 3/21
This message was created automatically by Exchange Online Advanced...
Exchange Online Advanced Threat Protection <
Administrator Notification: Redirecting email with malware
Fri 3/20
This message was created automatically by Exchange Online Advanced...
Postmaster
Undeliverable message
Fri 3/20
This message was created automatically by mail delivery software. Your...
Exchange Online Advanced Threat Protection <
Administrator Notification: Redirecting email with malware
Thu 3/19
Administrator Notification: Redirecting email with malware
REPLY
Exchange Online Advanced Threat Protection <advanced-threat-protection@protection.outlook.com>
Sat 3/21/2015 2:31 PM
To: MOD Administrator;
Limited time offering fr...
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.

안전한 링크

- 악의적인 콘텐츠가 있는 사이트 및 피싱 사이트로부터 보호
- 감염된 사용자에 대한 관리자 가시성을 제공
- 다른 서버로 통하도록 프록시 URL은 다시 작성

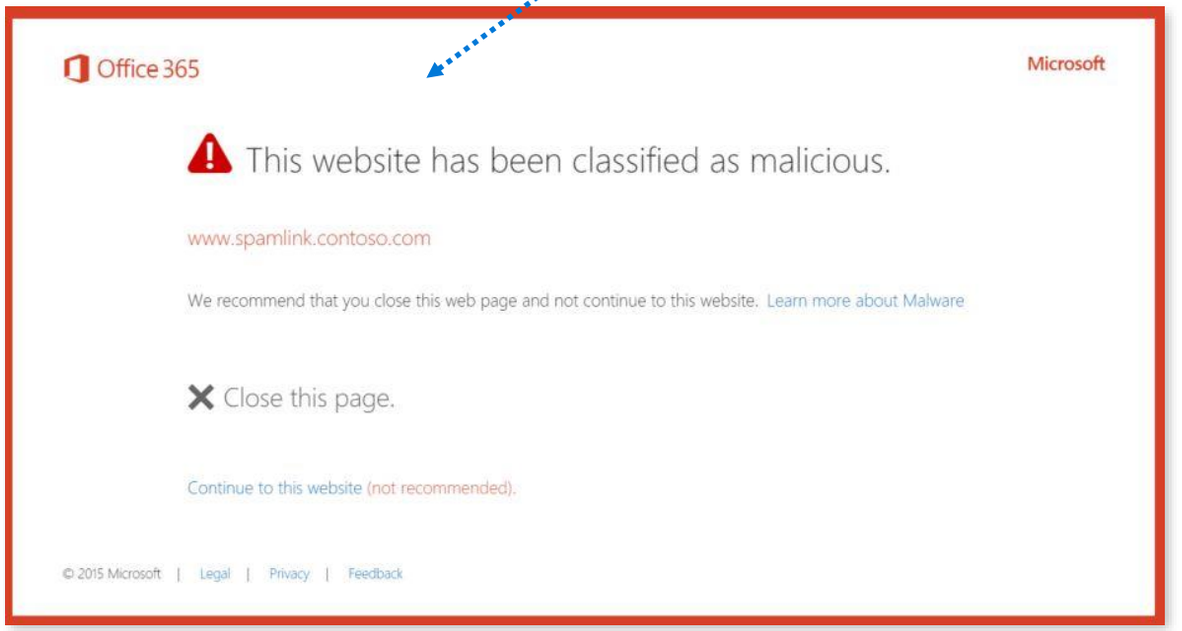


안전한 링크—체험

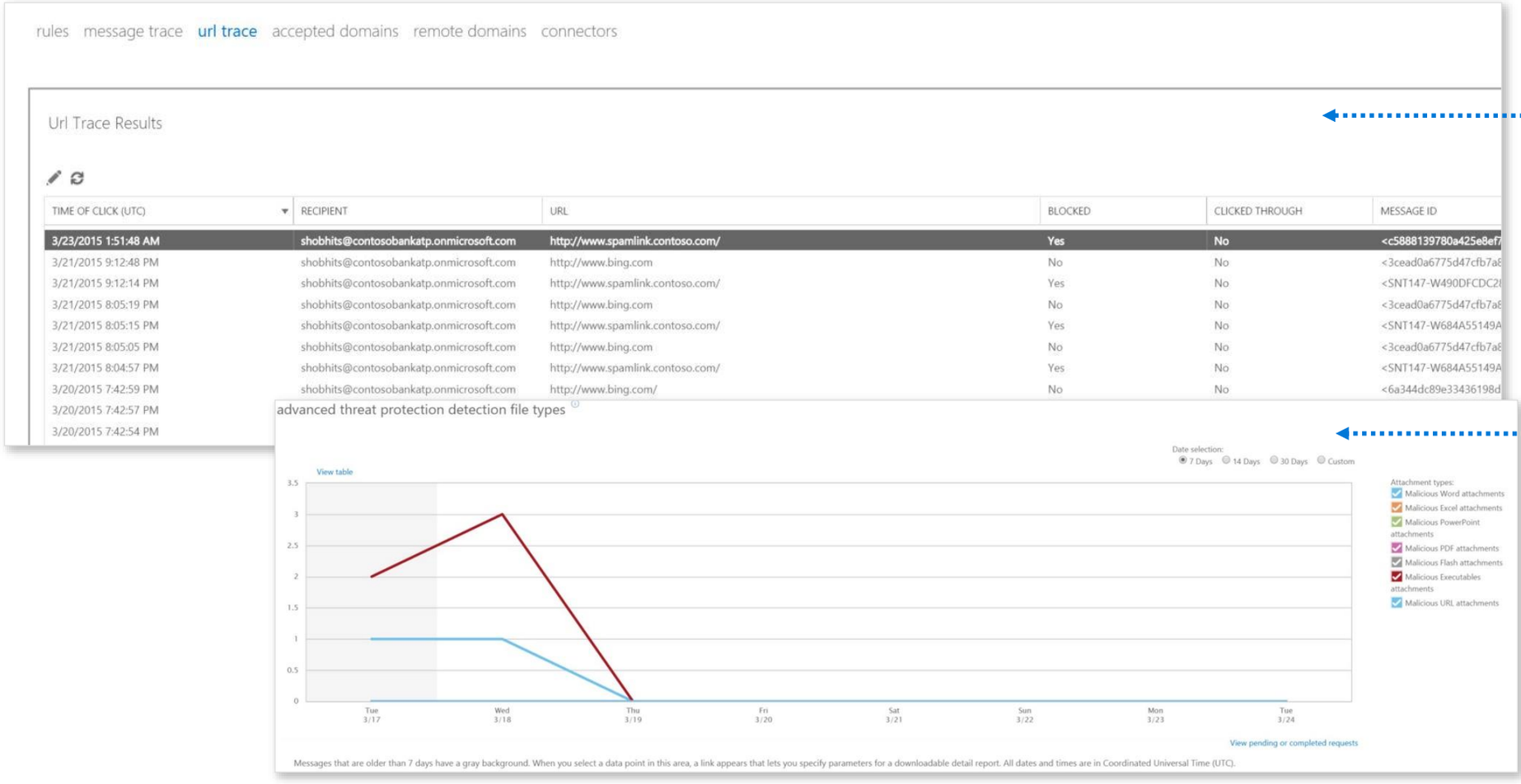


관리자가 정책을 설정

사용자가
이메일에 있는
악의적인 링크를
클릭하면
사용자에게 통지



풍부한 보고서 및 클릭 추적



관리자는 누가 어떤 링크를 클릭 한 것인지에 대한 완벽한 가시성 확보

파일 형식 및 성향에 대한 보고서

Exchange Online ATP 구입

고객	채널	ERP
모든 상용 고객	Direct, CSP, Open, MPSA, and EA channels	사용자당 $2 / 월
여러 테넌트(Multi-tenant) 정부 고객	Direct, Open, MPSA, and EA channels at an ERP of $1.75	사용자당 $1.75 / 월
Office 365 Government Community Cloud (GCC), Office 365 Education, and Office 365 Nonprofit customers	사용할 수 없음	사용할 수 없음