



생산성을 확보한 Built-in 보안

EOP (Exchange Online Protection) & WDAV (Windows Defender AV)

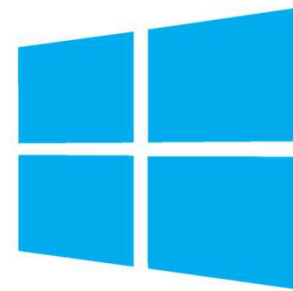
한국마이크로소프트
하석현 대리



임직원의 PC 업무 환경



Exchange Online

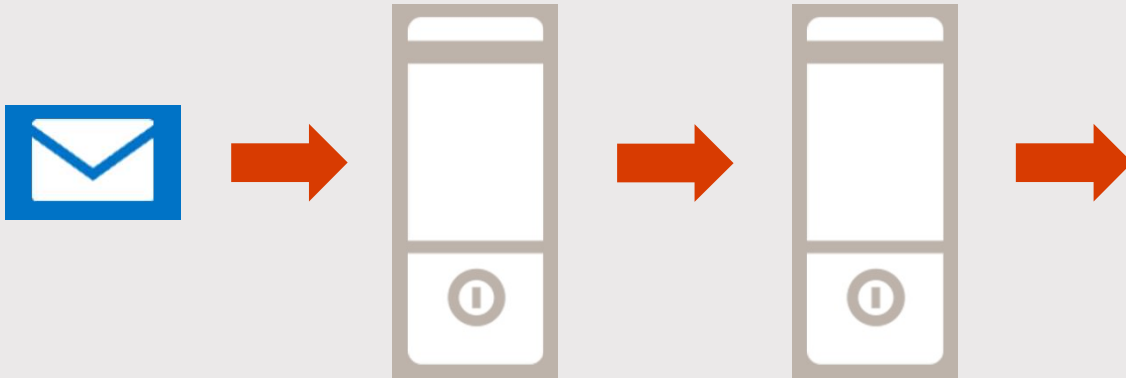


Windows 10

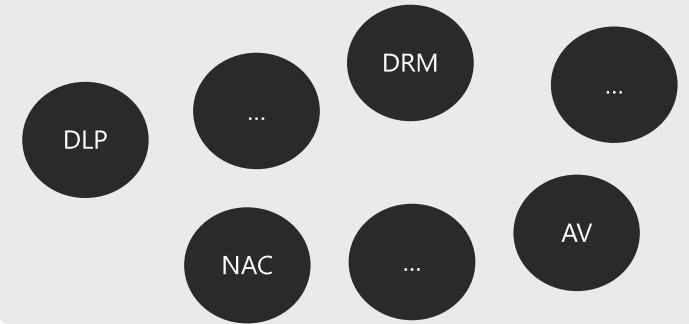
기존 환경의 문제점

“Built-in 보안으로 해결”

- 메일 수신까지 Delay 발생
- 메일 손실 가능성
- 메일 이슈 발생시, 어디서 발생한 문제인지 검토에 번거로움

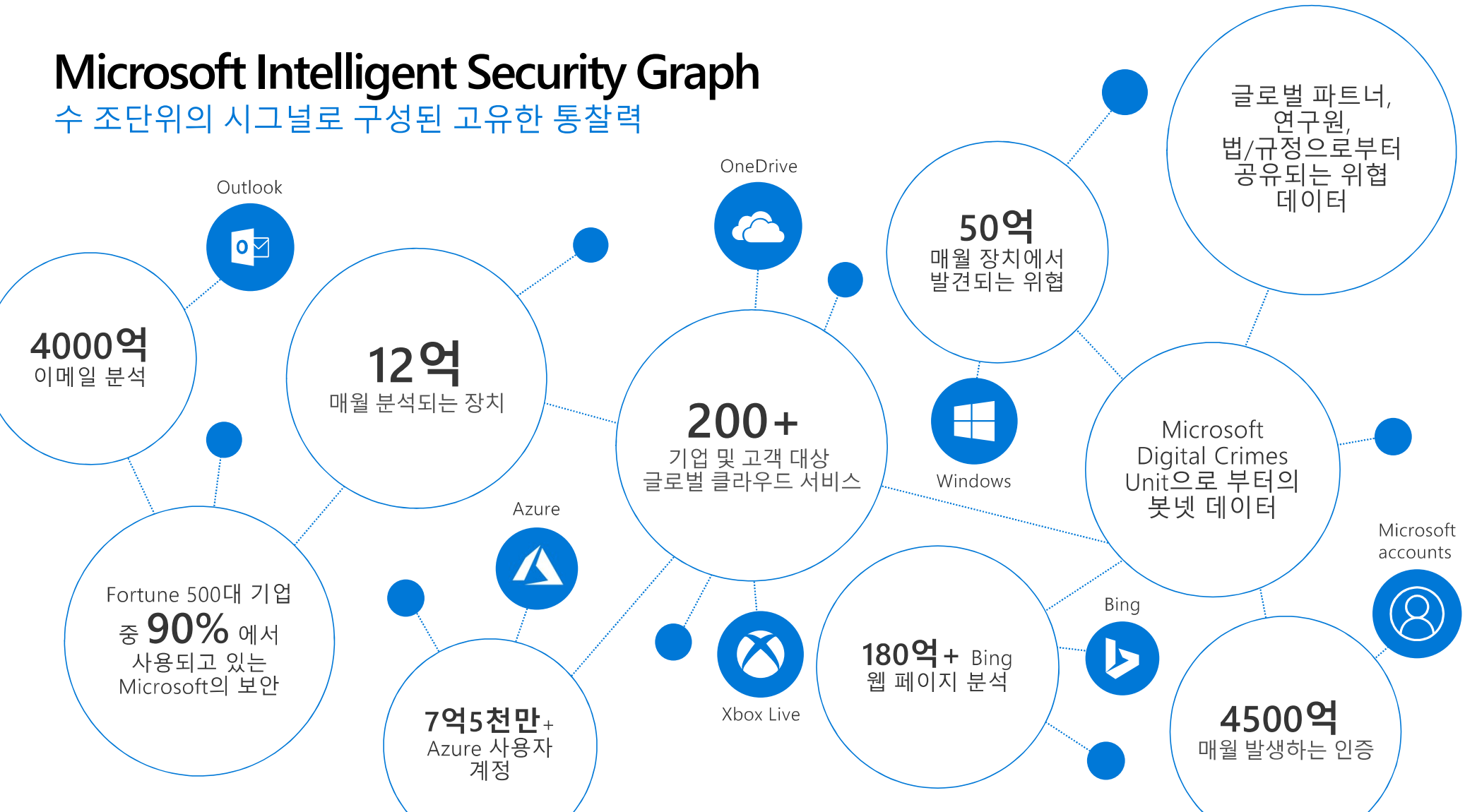


- PC 성능 저하
- 버전 업데이트시 호환성 검토의 불편함
- 직원들의 불만



Microsoft Intelligent Security Graph

수 조단위의 시그널로 구성된 고유한 통찰력



Exchange Online Protection

Exchange Online Protection (EOP)

바이러스 및 Malware 차단

다중 Anti-Virus 엔진 적용

지속적으로 Anti-Spam, Anti-Phishing, Anti-Spoofing 기능 향상

Seamless & User Friendly

EXO에 Built-in 되어있어 별도의 설치없이 설정 만으로 관리 가능

Office 365 관리 포탈에서 설정 및 보고서 확인 가능

Zero Hour Auto Purge

탐지 엔진 업데이트 후 이미 수신된 메일 중
스팸 또는 악성 메일이 있는 경우 처리

기업용 안정성

지역적으로 분산된 데이터 센터

메일 유실이 없도록 메일 큐잉

마이크로소프트 24시간 365일 운영

서비스 레벨 계약 (SLA) 제공



Office 365 Advanced Threat Protection (ATP)

해커들부터의 지능적인 공격에 대항하기 위한 Office365 ATP 기능은 지능적인 메일 위협에 대한 고급 방어 기능을 제공함

제로데이 공격 (Zero day Attack)

- 알려지지 않은 보안 취약점 및 보안패치가 개발/배포되지 않은 취약점을 집중 공격



알려지지 않은 Malware/Virus 차단 기능

- 머신 러닝 기법을 이용한 행위 기반의 분석
- 악성 **첨부파일** 차단

고도화된 피싱 기법

- 중요 업무 메일로 가장하여 클릭 유도



고도화된 피싱 탐지

- 악의적 **URL**에 대한 실시간 차단
- User/Domain Impersonation 형태 **피싱** 차단

집중 타겟 포함 전사 차원의 지능적 공격

- 웹으로 유출된 보안취약자에 대한 이메일 타게팅 공격 및 전사 레벨에 대한 지속적이고 지능적인 공격



풍부한 보고서 및 추적 기능

- Built-in URL 추적
- 위협에 대한 상세 보고서

Office 365 Threat Intelligence (1)

• 위협 메일 조사 및 대응

💡 보안 동향

Trojan Downloader Scripts
Trojan downloader scripts lev

Document Phishing
Phishing attempts to steal us

Malicious Macros
Macros are a feature of Micro

Microsoft
THREAT INTELLIGENCE

Have information on this threat or further questions? Email threat@microsoft.com

NOTE: This data is provided subject to the following conditions. Your organization may use the data solely for remediation and defensive purposes, and for no other purpose. The data may be inaccurate and/or may refer to legitimate but compromised properties. THIS INFORMATION IS PROVIDED AS-IS FOR INFORMATIONAL PURPOSES ONLY, WITH NO WARRANTY EXPRESSED OR IMPLIED.

Last update 2016-04-18

Summary

Win32/Locky is ransomware that, once installed on a victim computer, encrypts all personal files and demands a ransom payment of between 0.5 and 2 Bitcoins in order to receive the decryption key.

Locky is currently being distributed via spam email campaigns that have malicious Microsoft Office documents containing embedded VBA macros, or JavaScript files inside ZIP archives as attachments. The email attempts to convince recipients to open the attachment and, in the case of the Office documents, enable macros in order to

1. 보안 동향 보고서 제공

📄 대상 지정된 상위 사용자

	Debra Berger	6
	Debra Berger	2
	Lee Gu	2
	Diego Siciliani	1

2. 테넌트 내의 위협에 가장 많이 노출된 사용자 확인

admin@M365x123923.onmicrosoft.com 2
자 메일

🗑️ 제출 삭제 + 작업

날짜	제목
2018-05-25	23923.OnMicros... SA & SL test2
2018-05-25	23923.OnMicros... SA & SL test2
2018-05-29 09:49:06	GradyA@M365x123923.OnMicr... SA & SL test2
2018-05-29 09:49:11	DiegoS@M365x123923.OnMicr... SA & SL test2

정크로 이동
지운 편지함으로 이동
일시 삭제
영구 삭제
받은 편지함으로 이동
첨부 파일 삭제

선택한 메시지에서 첨부 파일을 삭제합니다.

3. 테넌트 내의 메일들에 대해 이동/삭제 등 제어 가능

🌐 맬웨어가 포함된 메시지...

아시아 북아메리카 태평양

Bing


4. 공격 메시지의 근원지를 맵으로 제공

Office 365 Threat Intelligence (2)

- 위협 추적기 - 당사 테넌트에 영향을 줄 수 있는 이메일 관련 위협 인텔리전스 제공

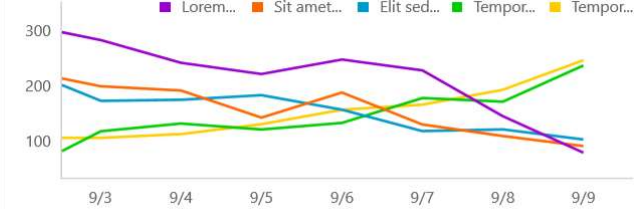
Home > Threat management: Threat explorer

Noteworthy



Petya Ransomware
The newest Petya malware variant, known as "NotPetya," surfaced on June 27, 2017.
[Learn more](#)

Trending



Clustering

8

campaigns targeting similar users

21

campaigns targeting users by groups

5

campaigns targeting users by location

The targeted campaigns display threats that appear to be targeting certain segments of your organization. We evaluate the malware and phish attacks on your users based on titles, groups, and locations we derive from Active Directory data to find cases where attacks seem to cluster. Since targeted attacks can be short-lived, the attacks in this list will typically drop off of this list after a few days.

Noteworthy campaigns ▾

Export

Date	Malware Family	Today's count	Prior day message count	Target	Target category	Top Targeted Users	Actions
11/1/2017	Malware - San Diego	423	223	San Diego	Location	Mike Morrissey, Bella Cho, Tomer Asimov	Explore
11/1/2017	Phish - Operations	23	24	Operations	Department	Tim Davis	Explore
11/1/2017	Malware/Phish - Beirut	8	128	Beirut	Location	Samuel Swari	Explore
11/1/2017	Malware - Executives	17	8	Executives	Classification/tag	Alexi Paterov, Tim Davis	Explore
10/31/2017	Phish - Vice President	44	63	Vice President	Title	Gopi Patlela, Alexis Li, Jim Smith	Explore
10/31/2017	Malware/Phish - Product Marketing	93	73	Product Marketing	Department	Taylor Nguyen, Lexi Llewelyn, Bill Taylor	Explore

Office 365 Threat Intelligence (3)

- 공격 시뮬레이터 – 사내 직원 대상으로 가상의 무해한 공격을 시도할 수 있는 기능

The screenshot shows the Office 365 Threat Intelligence Attack Simulator interface. The left sidebar contains navigation options: 홈, 알림, 사용 권한, 분류, 데이터 손실 방지, 데이터 거버넌스, 위협 관리, 대시보드, 탐색기, 공격 시뮬레이터 (highlighted), 검토, 정책, 위협 추적기, 메일 흐름, 데이터 개인 정보 보호, and 검색 및 조사. The main content area is titled '공격 시뮬레이션' and includes a shield icon with a red 'X' and an exclamation mark. The text reads: '공격을 시뮬레이션하여 방어를 테스트합니다. 스피어 피싱 및 암호 공격과 같은 현실적인 피싱 공격을 실행하여 조직 내 취약한 사용자들 확인합니다.' Below this, it shows '3 공격' with a '새로 고침' button. A yellow warning box states: '▲ 공격 시뮬레이션을 실행하려면 몇 가지 설정이 필요하며, 완료하는 데 보통 몇 시간 정도 소요됩니다. 지금 설치' and '▲ 공격을 예약하거나 종료하려면 MFA(다단계 인증)를 사용하도록 설정해야 합니다. MFA 사용 설정에 대해 자세히 알아보세요.' The interface also displays details for a '스피어 피싱(자격 증명 수락) Account Breach' attack, including a '공격 시작' button and a '공격 정보' link. At the bottom, it shows '무작위 암호 대입(사전 공격) Account Breach' and a '피드백' button.

The banner features an illustration of a laptop, a tablet, and a smartphone displaying various data. Below the illustration, the text reads: '\$(username), Your payroll details need updating, please click below to start the update.' A prominent red button with white text says 'UPDATE YOUR ACCOUNT DETAILS'.

Dear, \$(username)

We have recently upgraded our payroll system, as a security measure we need you to confirm your bank routing number details for your account nominated to receive your salary.

Please review and enter your routing number details at the link above \$(username) - by clicking on the "Update Your Account Details" button above.

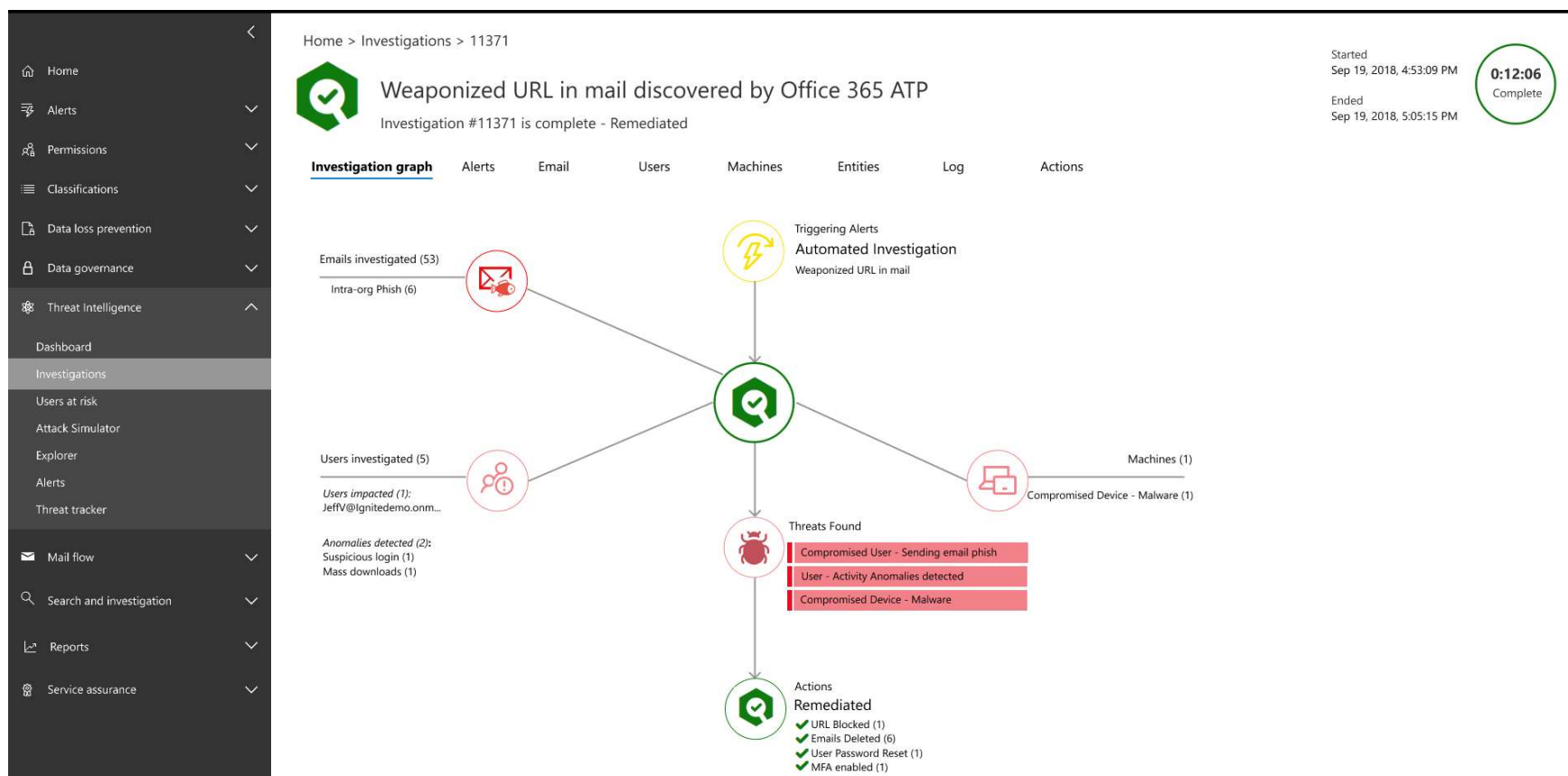
Failure to update your account details will result in delays with your salary being processed. Please make sure to update the details at least 5 days before the next Payroll cycle to avoid an unnecessary delay in processing.

Please let us know if you have any questions.

Thank you.

Office 365 Threat Intelligence (4)

- 자동 대응 (예정) – 취약한 부분 발생시 자동 대응하여 추가 피해 방지 또는 치료



Office 365 위협 보호

보호

탐지

대응

Powered by the:

Microsoft Intelligent security graph

In-depth, integrated, intelligent



Exchange Online
Protection

시그니처 기반의 맬웨어
탐지



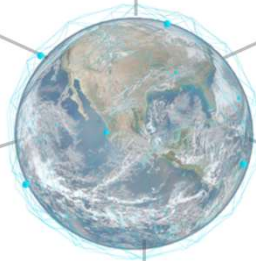
Advanced Threat
Protection

알려지지 않은 위협 탐지



Threat
Intelligence

선제적인 보안 전략 수립



인바운드



Email is routed to EOP DC based on MX record resolution
(Contoso-com.mail.protection.outlook.com)

Perimeter Protection

- IP-based edge blocks
- Directory based edge blocks
- Envelope blocks

Virus Scanning

- AV Engine 1
- AV Engine 2
- AV Engine 3



Policy Enforcement

- Custom transport rules

Quarantine

Spam Analysts

Spam Protection

- Safe Sender/Recipient
- Content scanning and heuristics
- SPF & Sender ID filter
- Bulk mail filtering
- International spam
- Advanced Spam management

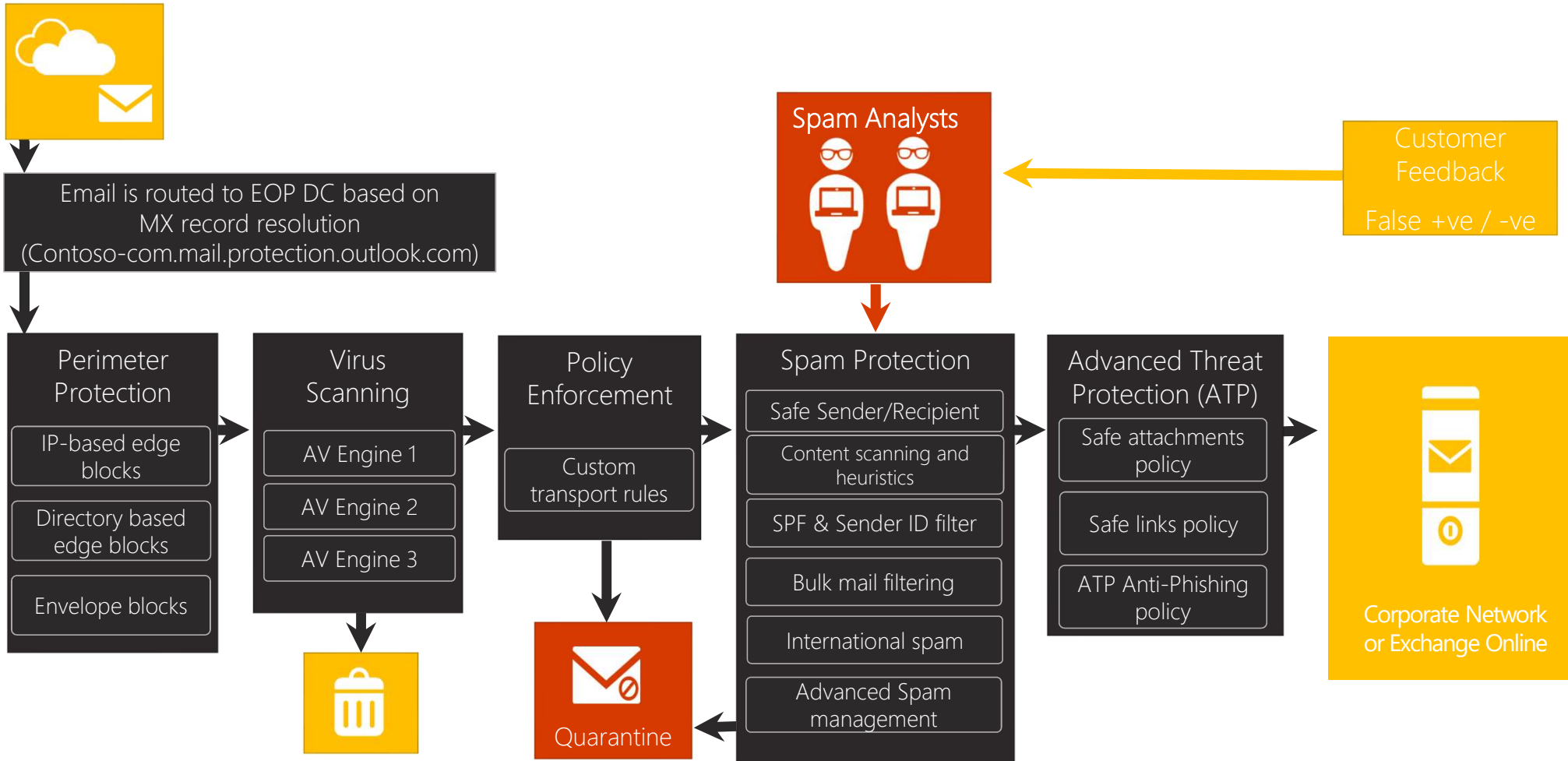
Advanced Threat Protection (ATP)

- Safe attachments policy
- Safe links policy
- ATP Anti-Phishing policy

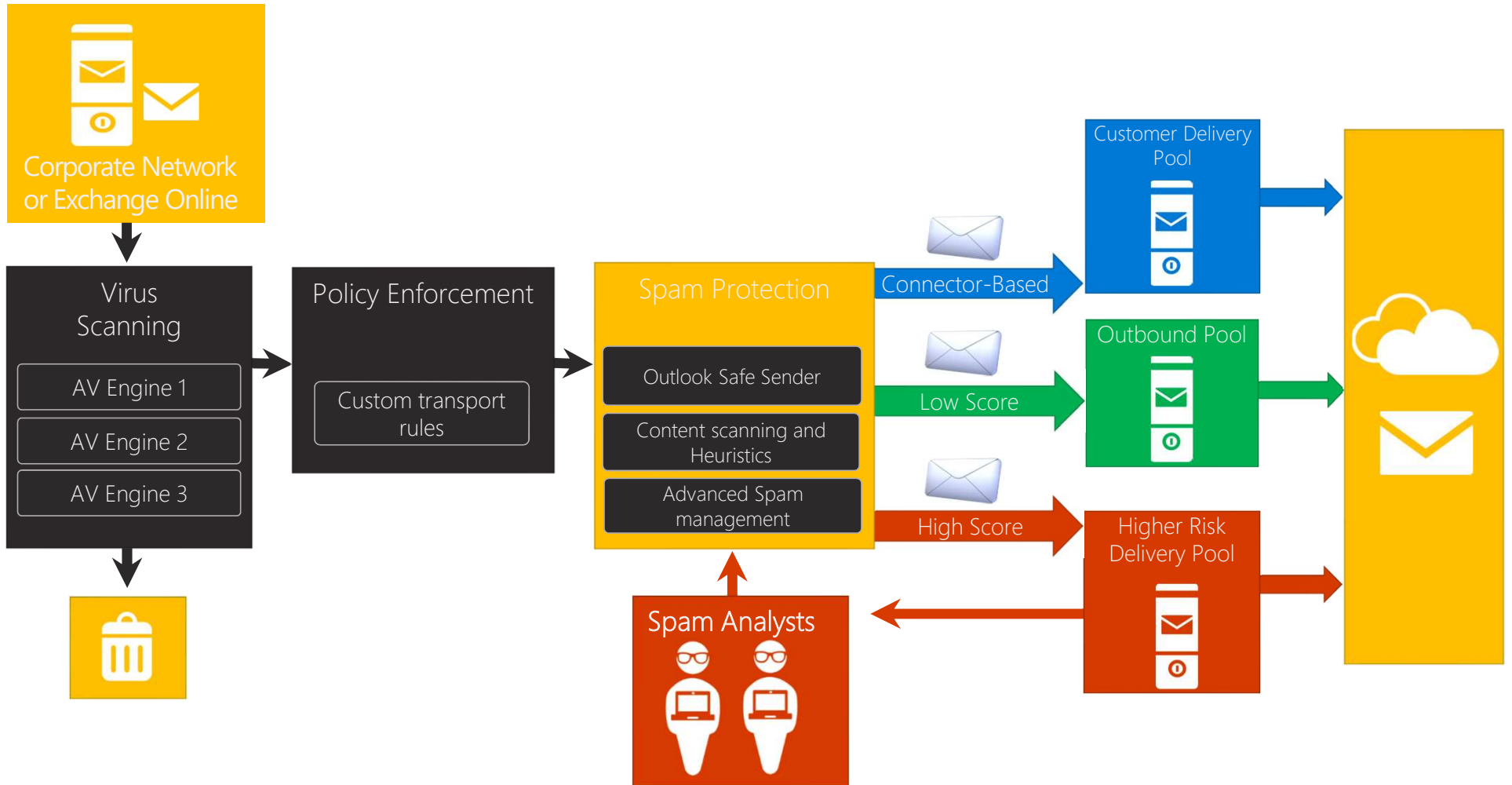
Corporate Network or Exchange Online

Customer Feedback

False +ve / -ve



아웃바운드



Exchange 관리 센터

- 대시보드
- 받는 사람
- 사용 권한
- 주소 관리
- 조직
- 보호**
- 고급 위협
- 메일 흐름
- 모바일
- 공용 폴더
- 통합 메시징
- 하이브리드

맬웨어 필터 연결 필터 스팸 필터 아웃바운드 스팸 격리 작업 센터 dkim

+ ✎ 🗑 ↑ ↓ ↻

사용

Default

일반

▶ 설정

맬웨어 검색 반응

전자 메일 첨부 파일에서 맬웨어가 발견되면 메시지가 격리되며 관리자만 해제할 수 있습니다. 메시지가 격리된 경우 받는 사람에게 알리시겠습니까?

아니요
 기본 알림 텍스트 사용
 사용자 지정 알림 텍스트 사용

*사용자 지정 알림 텍스트:

Yo! it's Malware

일반 첨부 파일 형식 필터

이 기능을 설정하면 컴퓨터를 손상시킬 수 있는 첨부 파일 형식을 차단합니다.

해제
 설정 - 필터링된 파일 형식의 첨부 파일이 포함된 전자 메일에서 맬웨어 검색 응답을 트리거합니다(권장).

+ -

파일 형식

- .ace**
- .ani
- .app
- .docm

저장 취소

Exchange 관리 센터

- 대시보드
- 받는 사람
- 사용 권한
- 주소 관리
- 조직
- 보호**
- 고급 위협
- 메일 흐름
- 모바일
- 공용 폴더
- 통합 메시징
- 하이브리드

메일웨어 필터 **연결 필터** 스팸 필터 아웃바운드 스팸 격리 작업 센터 dkim

- 이름
- Default**

스팸 필터 정책 편집 - Chrome

https://outlook.office365.com/ecp/Antispam/EditConnectionFilter.aspx?ActivityCorrelationID=e64951f0-931b-e883-c8d2-bdee00e26...

Default

일반

▶ **연결 필터링**

연결 필터링
IP 허용 목록
다음 IP 주소에서 보낸 메시지를 항상 수락합니다.

+ ✎ -

허용된 IP 주소

IP 차단 목록
다음 IP 주소에서 보낸 메시지를 항상 차단합니다.

+ ✎ -

차단된 IP 주소

수신 허용 목록 사용

세요

Exchange 관리 센터

- 대시보드
- 받는 사람
- 사용 권한
- 준수 관리
- 조직
- 보호**
- 고급 위협
- 메일 흐름
- 모바일
- 공용 폴더
- 통합 메시징
- 하이브리드

메일웨어 필터 연결 필터 스팸 필터 아웃바운드 스팸 격리 작업 센터 dkim

+ ✎ 🗑 ↑ ↓ ↻

사용	이름	
<input checked="" type="checkbox"/>	Default	<div style="border: 1px solid #ccc; padding: 5px;"> <h4 style="margin: 0;">Default</h4> <p>일반</p> <p>스팸 및 대량 전자 메일 작업</p> <p>받은 스팸 메일과 대량 전자 메일에 대해 수행할 동작을 선택합니다. 자세한 정보</p> <p>스팸:</p> <p>차단 목록: 정크 메일 폴더로 메시지 이동</p> <p>허용 목록: 높은 스팸 지수:</p> <p>국가별 스팸: 정크 메일 폴더로 메시지 이동</p> <p>고급 옵션</p> <p>대량 전자 메일:</p> <p><input checked="" type="checkbox"/> 대량 전자 메일을 스팸으로 표시</p> <p>임계값을 선택하세요. 1은 대부분의 대량 전자 메일을 스팸으로 표시하며 9는 대부분의 대량 전자 메일이 배달 되도록 허용합니다.</p> <p>7(기본값)</p> <p>격리</p> <p>스팸 보존 기간(일): 15</p> <p>*이 X-헤더 텍스트 추가:</p> <p>*제목 줄 앞에 다음 텍스트 추가:</p> <p>*이 전자 메일 주소로 리디렉션:</p> </div>

Exchange 관리 센터

- 대시보드
- 받는 사람
- 사용 권한
- 주소 관리
- 조직
- 보호**
- 고급 위협
- 메일 흐름
- 모바일
- 공용 폴더
- 통합 메시징
- 하이브리드

맬웨어 필터 연결 필터 **스팸 필터** 아웃바운드 스팸 격리 작업 센터 dkim

+ ✎ 🗑️ ↑ ↓ ↻

사용	이름
<input checked="" type="checkbox"/>	Default

스팸 필터 정책 편집 - Chrome

https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=85dd209b-3aa0-4fcc-0cf9-48f10a52...

Default

일반
스팸 및 대량 전자 메일 작업

- 차단 목록
 - 보낸 사람 차단 목록
 - 다음 보낸 사람의 전자 메일을 항상 스팸으로 표시합니다.
 - + ✎ -
 - 차단된 보낸 사람
- 허용 목록
- 국가별 스팸
- 고급 옵션

도메인 차단 목록
다음 도메인의 전자 메일을 항상 스팸으로 표시합니다.

- + ✎ -
- 차단된 도메인

Exchange 관리 센터

- 대시보드
- 받는 사람
- 사용 권한
- 준수 관리
- 조직
- 보호**
- 고급 위협
- 메일 흐름
- 모바일
- 공용 폴더
- 통합 메시징
- 하이브리드

맬웨어 필터 연결 필터 스팸 필터 아웃바운드 스팸 격리 작업 센터 dkim

+ ✎ 🗑 ↑ ↓ ↻

사용	이름
<input checked="" type="checkbox"/>	Default

스팸 필터 정책 편집 - Chrome

https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=85dd209b-3aa0-4fcc-0cf9-48f10a52...

Default

일반

스팸 및 대량 전자 메일 작업

차단 목록

허용 목록

국가별 스팸

고급 옵션

허용 목록

보낸 사람 허용 목록
다음 보낸 사람의 전자 메일을 항상 받은 편지함으로 배달합니다.

+ ✎ -

허용된 보낸 사람

도메인 허용 목록
다음 도메인의 전자 메일을 항상 받은 편지함으로 배달합니다.

+ ✎ -

허용된 도메인

Exchange 관리 센터

- 대시보드
- 받는 사람
- 사용 권한
- 주소 관리
- 조직
- 보호**
- 고급 위협
- 메일 흐름
- 모바일
- 공용 폴더
- 통합 메시징
- 하이브리드

메일웨어 필터 연결 필터 스팸 필터 아웃바운드 스팸 격리 작업 센터 dkim

+ ✎ 🗑 ↑ ↓ ↻

사용	이름
<input checked="" type="checkbox"/>	Default

Default

일반

스팸 및 대량 전자 메일 작업

차단 목록

허용 목록

▶ **국가별 스팸**

고급 옵션

국가별 스팸

다음 언어로 된 전자 메일 메시지 필터링

+ -

코드	언어
GU	구자라트어

다음 국가/지역에서 전송된 전자 메일 메시지 필터링

+ -

코드	지역
----	----

Exchange 관리 센터

- 대시보드
- 받는 사람
- 사용 권한
- 준수 관리
- 조직
- 보호**
- 고급 위협
- 메일 흐름
- 모바일
- 공용 폴더
- 통합 메시징
- 하이브리드

맬웨어 필터 연결 필터 **스팸 필터** 아웃바운드 스팸 격리 작업 센터 dkim

사용 이름

사용	이름
<input checked="" type="checkbox"/>	Def

Default

일반

스팸 및 대량 전자 메일 작업

해제

URL이 다른 포트로 리디렉션됨:

해제

차단 목록

.biz 또는 .info 웹 사이트에 대한 URL:

해제

허용 목록

국가별 스팸

고급 옵션

스팸으로 표시

이러한 속성이 포함된 메시지를 스팸으로 표시할 것인지 여부를 지정합니다.

빈 메시지:

해제

HTML의 JavaScript 또는 VBScript:

해제

HTML의 Frame 또는 IFrame 태그:

해제

HTML의 Object 태그:

해제

HTML의 Embed 태그:

해제

HTML의 Form 태그:

해제

HTML의 웹 버그:

해제

중요한 단어 목록 적용:

해제

SPF 레코드: 실패:

해제

조건부 보낸 사람 ID 필터링: 실패:

해제

NDR 후방 산란:

해제

이 설정을 활성화하면 본문과 제목 줄이 모두 비어 있고 첨부 파일도 없는 모든 메시지가 스팸으로 표시됩니다.

Exchange 관리 센터

- 대시보드
- 받는 사람
- 사용 권한
- 준수 관리
- 조직
- 보호
- 고급 위협
- 메일 흐름**
- 모바일
- 공용 폴더
- 통합 메시징
- 하이브리드

규칙 메시지 추적 URL 추적 허용 도메인 원격 도메인 커넥터

- 설정
- -
 -
 -
 -
 -
 -
 -

새 규칙 - Chrome

https://outlook.office365.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=1b941b...

새 규칙

이름:

*다음의 경우 이 규칙 적용...

보낸 사람 위치... [조직 내부](#)

및

받는 사람 위치... [조직 외부](#)

및

메시지 유형... [자동 전달](#)

* 다음 작업을 수행...

[메시지 차단](#)

다음의 경우 제외...

이 규칙 속성:

다음 심각도 수준을 사용하여 이 규칙 감사:

이 규칙의 모드 선택:

적용

정책 설명이 있는 테스트

도움이 필요하세요

홈

알림

데이터 손실 방지

데이터 거버넌스

위험 관리

대시보드

탐색기

검토

정책

메일 흐름

데이터 개인 정보 보호

검색 및 조사

보고서

홈 > 검토 > 격리

표시 **모두** 전자 메일 다음 이유로 인해 격리됨 **스팸**

여기의 전자 메일 메시지는 맬웨어, 스팸, 피싱 또는 대량 전자 메일로 분류되었기 때문에 격리되었습니다. 메시지를 검토하고 이를 한 명 이상의 원래 의도된 받는 사람에게 해제할지 여부를 결정하세요. 격리된 전자 메일

결과 정렬 기준

메시지 ID 정확한 ID, 주소 또는 제목을 입력한 다음 [새로 고침]을 클릭하세요

00:00 고급 필터

- 정책
- 대량
- 피싱
- 맬웨어
- 스팸

2019-01-07 00:00 2019-02-08

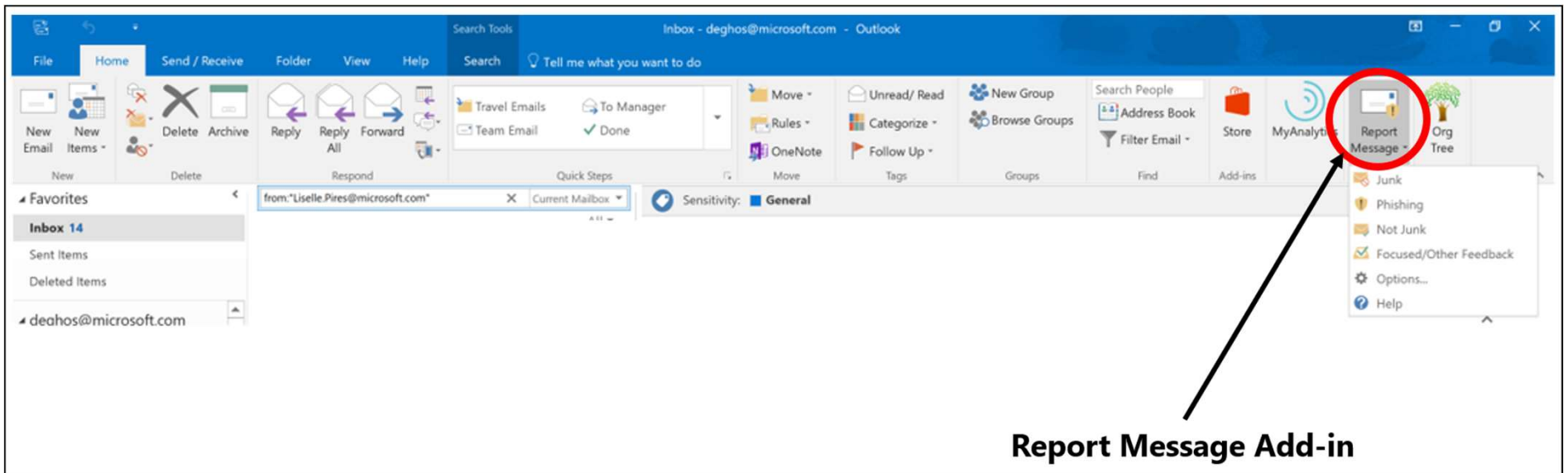
수신됨 보낸 사람 제목 만료

사용할 수 있는 데이터 없음

0개 항목이 로드되었습니다.

도움이 필요하세요? 피드백

- **Protect** users by enabling message reporting of potential phish



- 관리자가 Outlook 2016에 'Report Message' add-in 활성화
- 버튼 클릭시, 사용자는 Microsoft에 의심스러운 메일에 대한 분석 요청 가능
- 선택 가능한 옵션:
 - Phish – phish@office365.microsoft.com
 - Junk – junk@office365.microsoft.com
 - Not Junk – not_junk@office365.microsoft.com

- 홈
- 알림
- 분류
- 데이터 손실 방지
- 데이터 거버넌스
- 위협 관리
- 대시보드
- 탐색기
- 검토
- 정책
- 메일 흐름
- 데이터 개인 정보 보호
- 검색 및 조사
- 보고서

보기 사용자 보고한 메시지

- 전자 메일
- 피싱
- 사용자가 보고한 메시지
- 콘텐츠
- 멀웨어

2019-02-02 2019-02-08

선택된 필터에 대한 결과가 없습니다. 필터를 업데이트하고 다시 시도하세요.

사용자 보고

날짜	보고자	제목	보낸 사람	보낸 사람 IP	보고서 종류
----	-----	----	-------	----------	--------

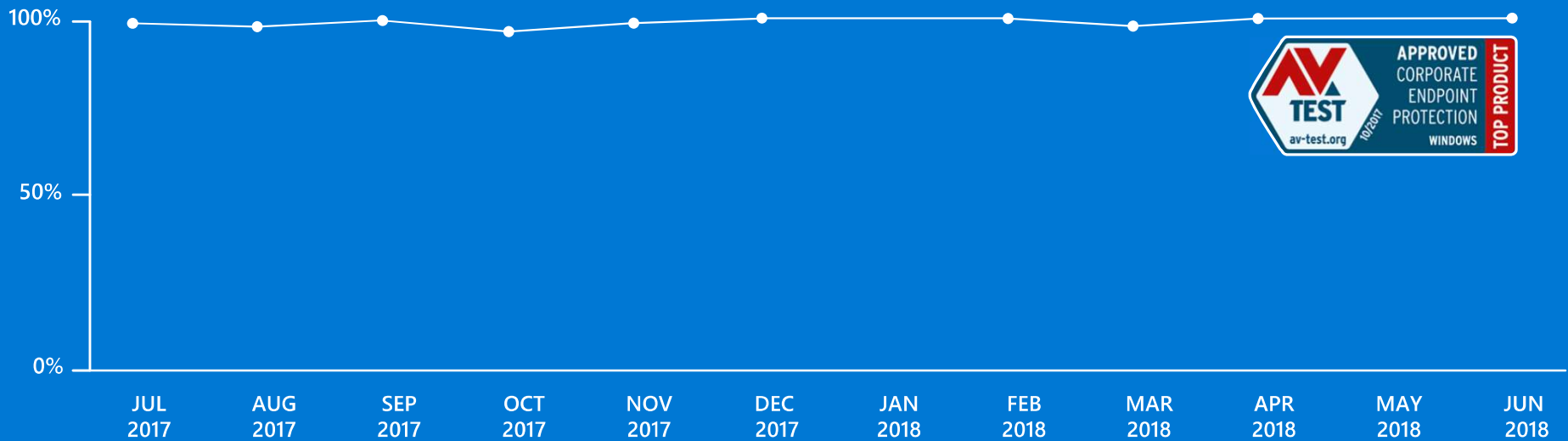
선택된 필터에 대한 결과가 없습니다. 필터를 업데이트하고 다시 시도하세요.

Windows Defender Antivirus

Windows 10 Edition Security differences



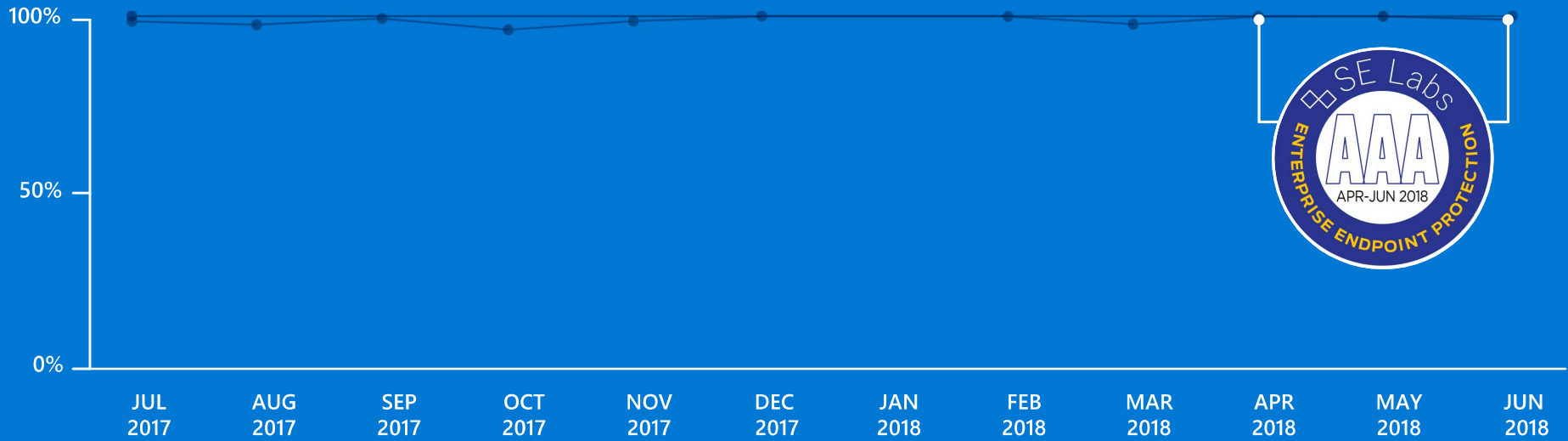
	<p>For consumers</p>	<p>Basic security</p>	<ul style="list-style-type: none"> ■ Windows Defender Antivirus ■ Windows Defender Smart Screen ■ Windows Defender Firewall ■ Windows Defender Exploit Guard <ul style="list-style-type: none"> ■ Windows Trusted Boot ■ Trusted Platform Module ■ Windows Hello ■ Windows Update ■ Universal Windows Platform
	<p>For small Businesses</p>	<p>Increase convenience Security</p>	<ul style="list-style-type: none"> ■ Group Policy ■ BitLocker ■ Windows Hello for Business ■ Windows information Protection <ul style="list-style-type: none"> ■ Including above all
	<p>For medium and large enterprises</p>	<p>Effective for targeted attacks Virtualization-Based Security</p>	<ul style="list-style-type: none"> ■ Windows Defender Device Guard ■ Windows Defender Application Control ■ Windows Defender Credential Guard ■ Windows Defender Application Guard <ul style="list-style-type: none"> ■ Including above all
	<p>For medium and large enterprises</p>	<p>Cloud based EDR Security</p>	<ul style="list-style-type: none"> ■ Windows Defender Advanced Threat Protection (ATP) <ul style="list-style-type: none"> ■ Including above all



안티바이러스와 엔드포인트 보안의 실제 환경 성능 평가 주요 기관으로부터 획득한 점수



안티바이러스와 엔드포인트 보안의 실제 환경 성능 평가 주요 기관으로부터 획득한 점수

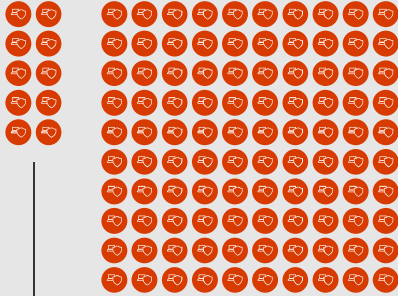


안티바이러스와 엔드포인트 보안의 실제 환경 성능 평가 주요 기관으로부터 획득한 점수



Polymorphism

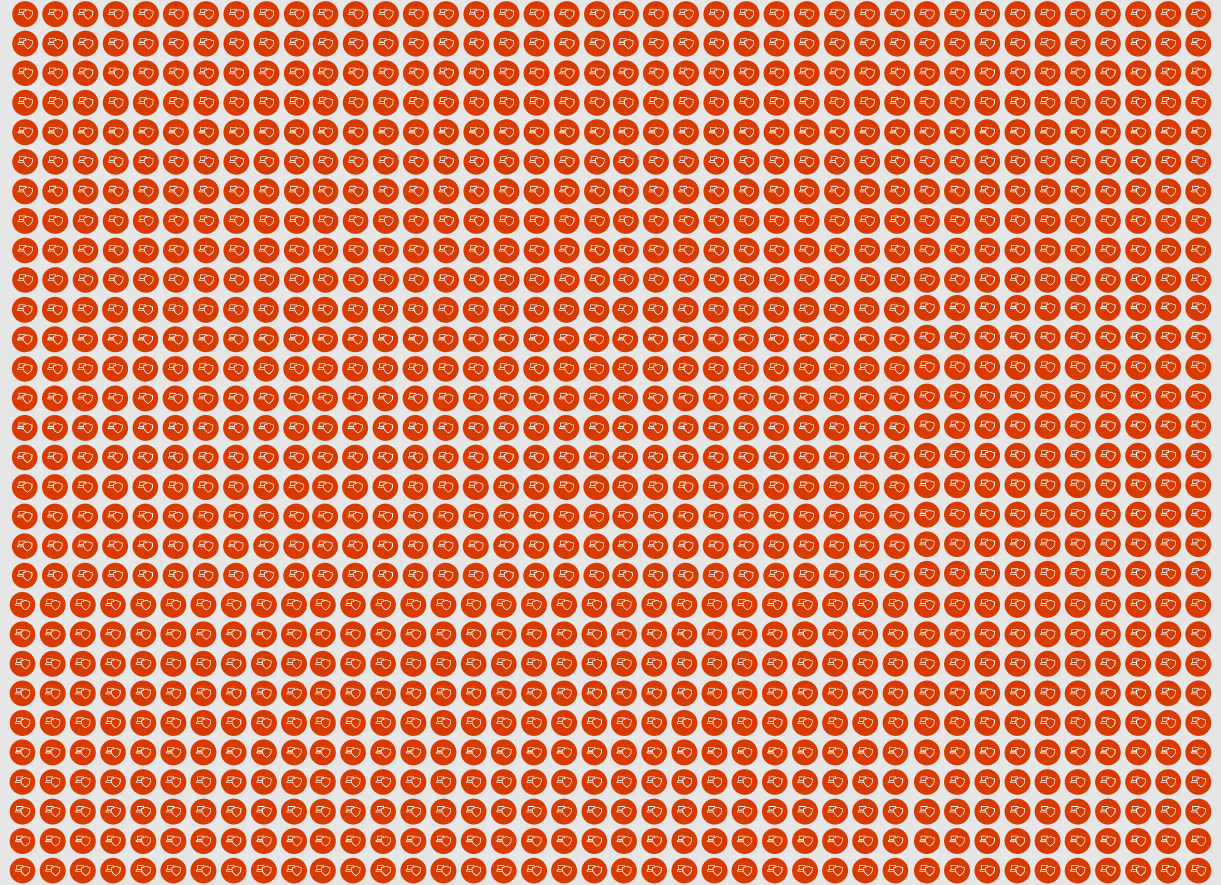
96% malware seen once and never again



3% seen 2–10

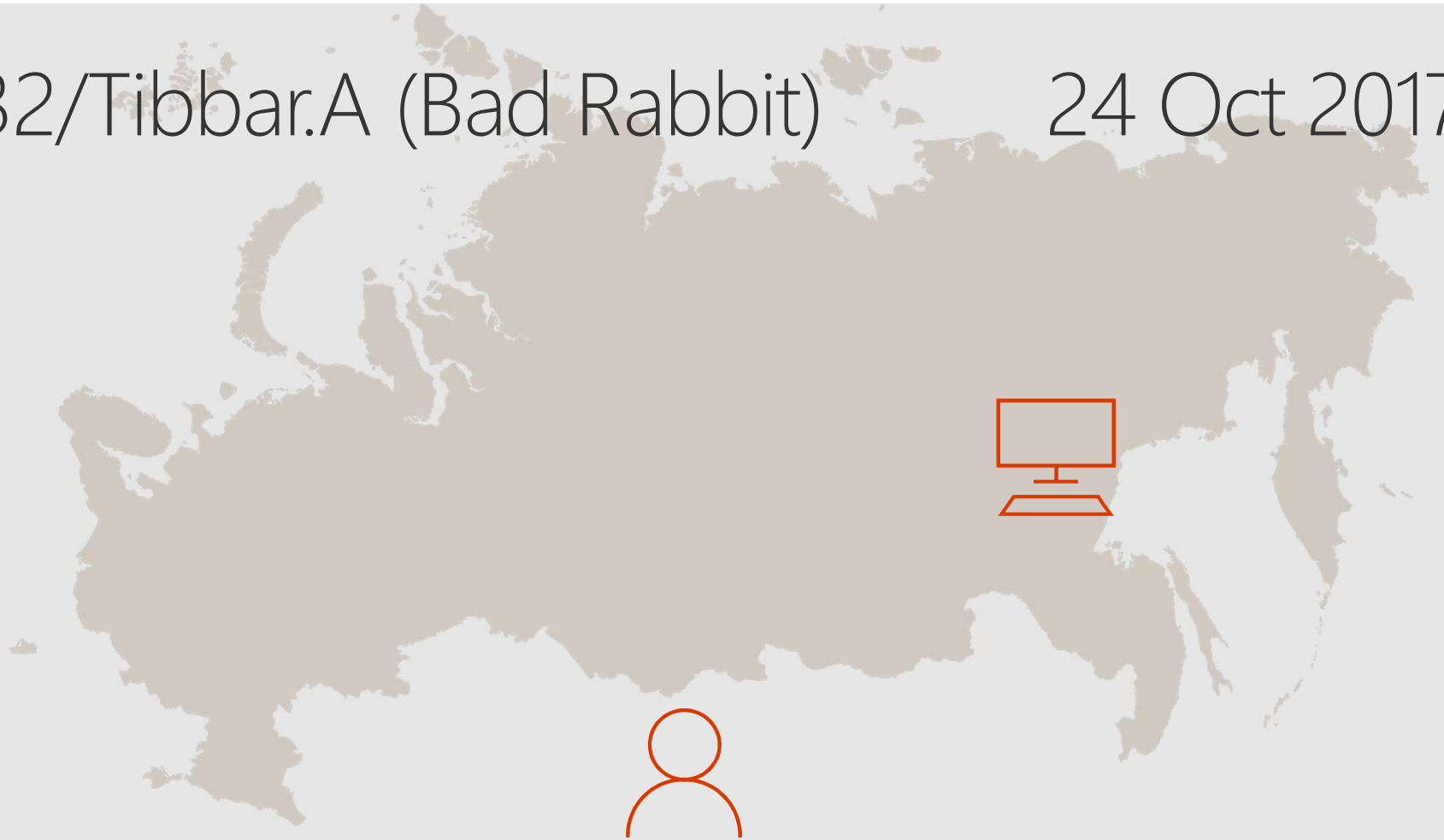
0.4% seen 11–100

0.01% seen on 1001+

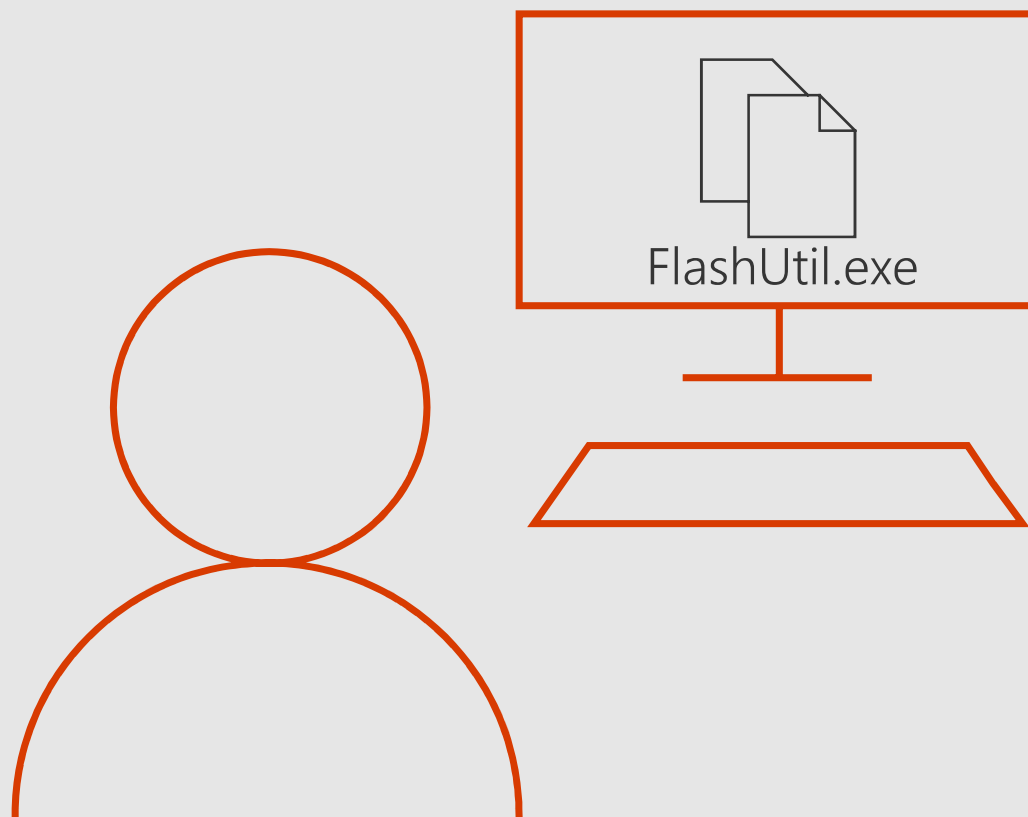


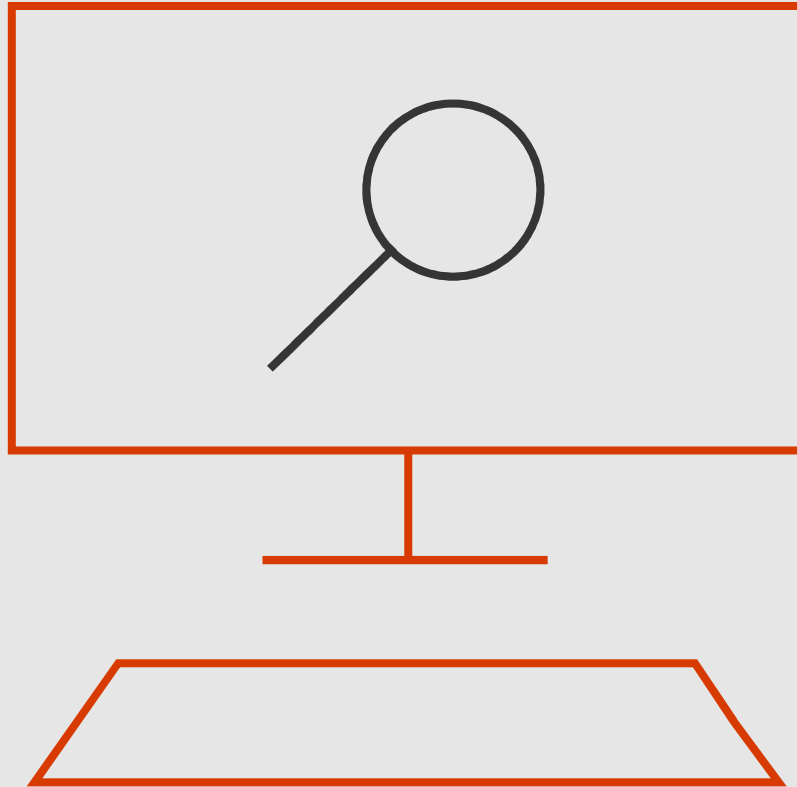
Win32/Tibbar.A (Bad Rabbit)

24 Oct 2017

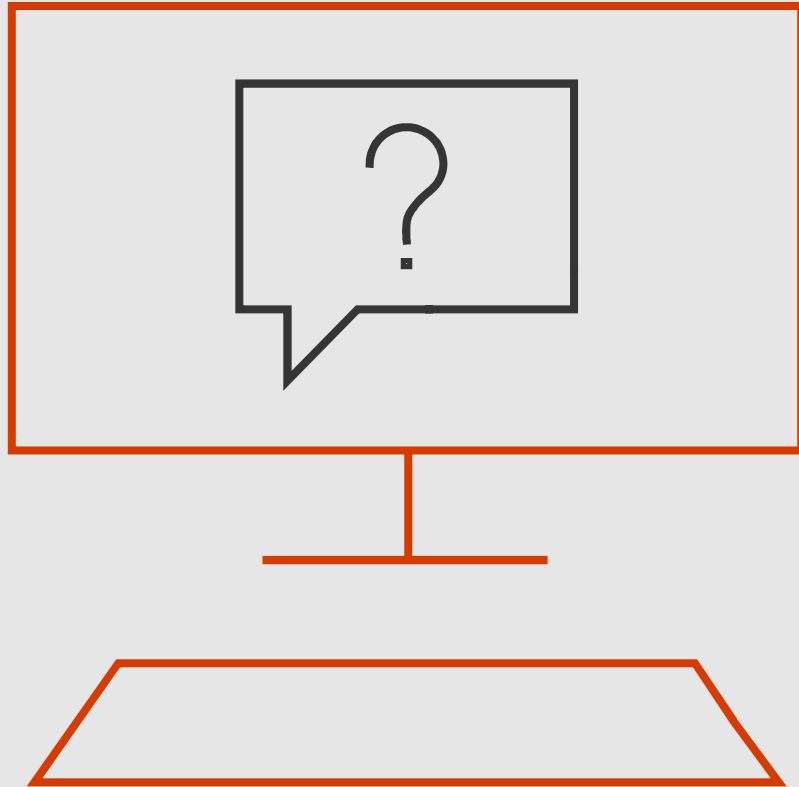


2017-10-24
11:17am

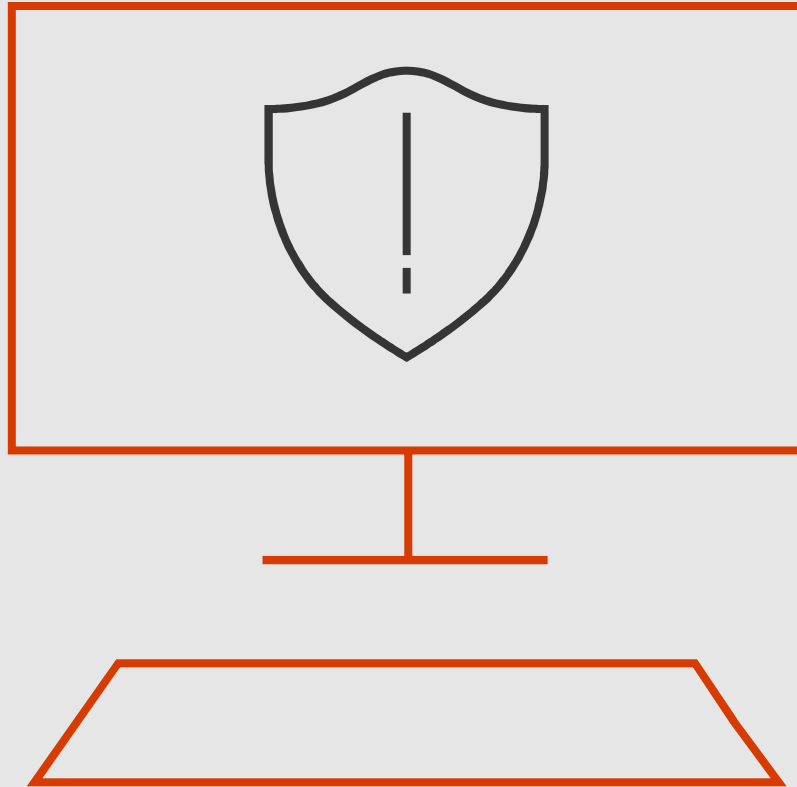




Windows Defender AV, 파일
스캔 및 악성으로 의심



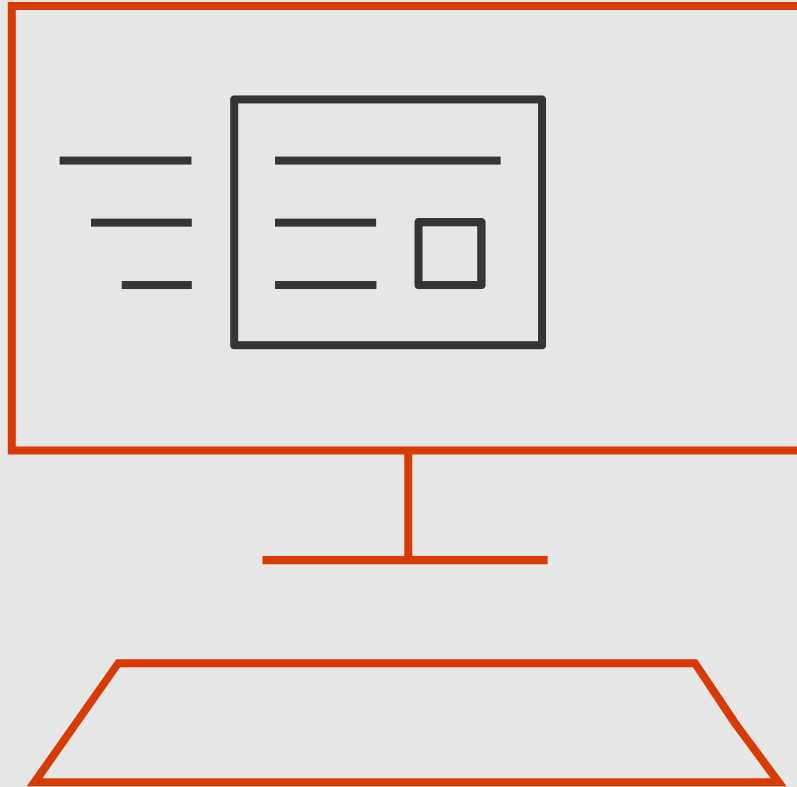
추가 검토를 위해
클라우드로 신호 전달



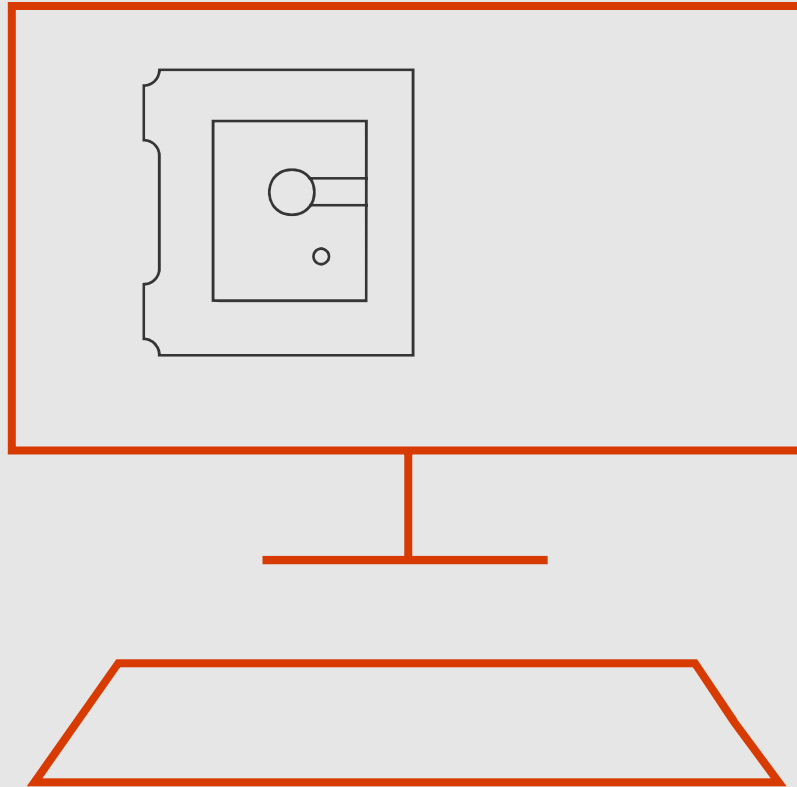
여전히 의심스러워
클라이언트에 샘플 요청



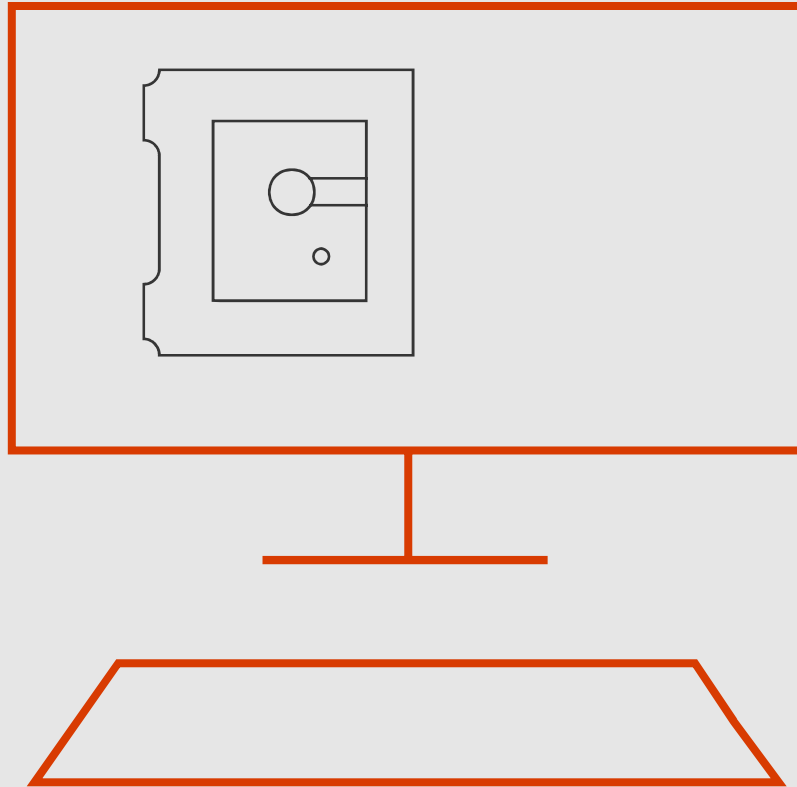
샘플 업로드



81.6%로 악성으로
판단했으나 False Positive
방지를 위해 추가 검토

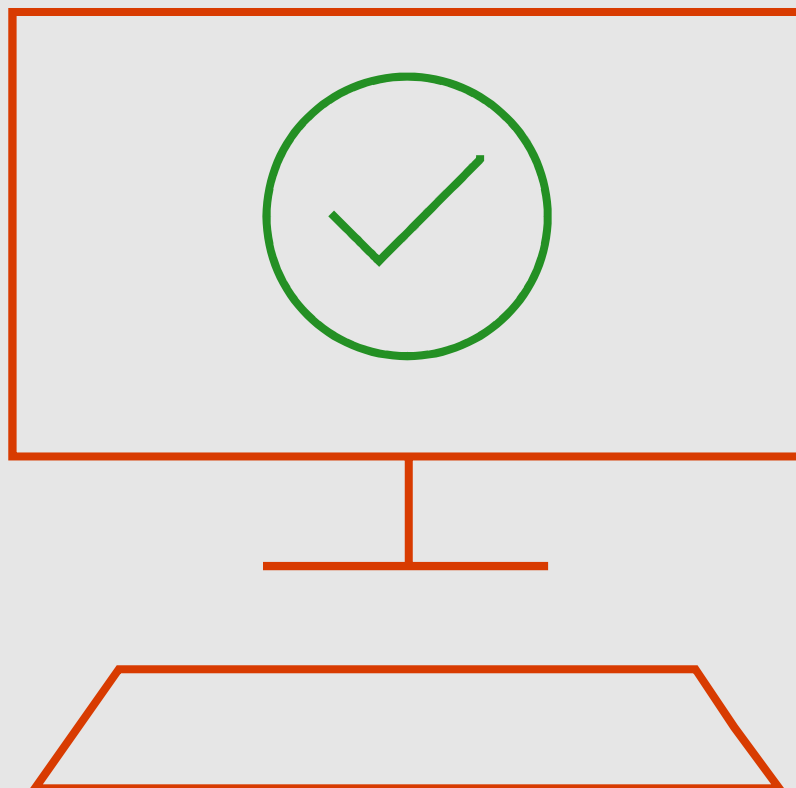


그 사이 우크라이나, 이스라엘,
불가리아 지역 포함 추가 8명의
감염자 발생



샌드박스 분석 결과 90.7%의
확신으로 악성 판단

2017-10-24
11:31am






총 14분 소요 및 해당 파일의 Hash를 글로벌의 모든 Windows Defender AV 사용자에게 배포하여 추가 확산 방지

Windows Defender Antivirus Cloud Protection: Real-time defense

Client 



Cloud 

Milliseconds 단위 보호

대부분의 일반적인 맬웨어는 Windows Defender AV의 높은 정확도의 탐지에 의해 차단

Milliseconds 단위 보호

머신러닝이 적용된 클라우드는 클라이언트의 Windows Defender AV에서 보내진 의심스러운 파일의 메타데이터를 평가하고 악성 여부 판단

Seconds 단위 보호

필요할 경우, 의심스러운 파일의 복사본이 업로드되어 여러 단계의 머신러닝 분류체계에 의해 검사

Minutes 단위 보호

추가 검사가 필요할 경우, 의심스러운 파일을 샌드박스를 통해 동적 분석 실행

Hours 단위 보호

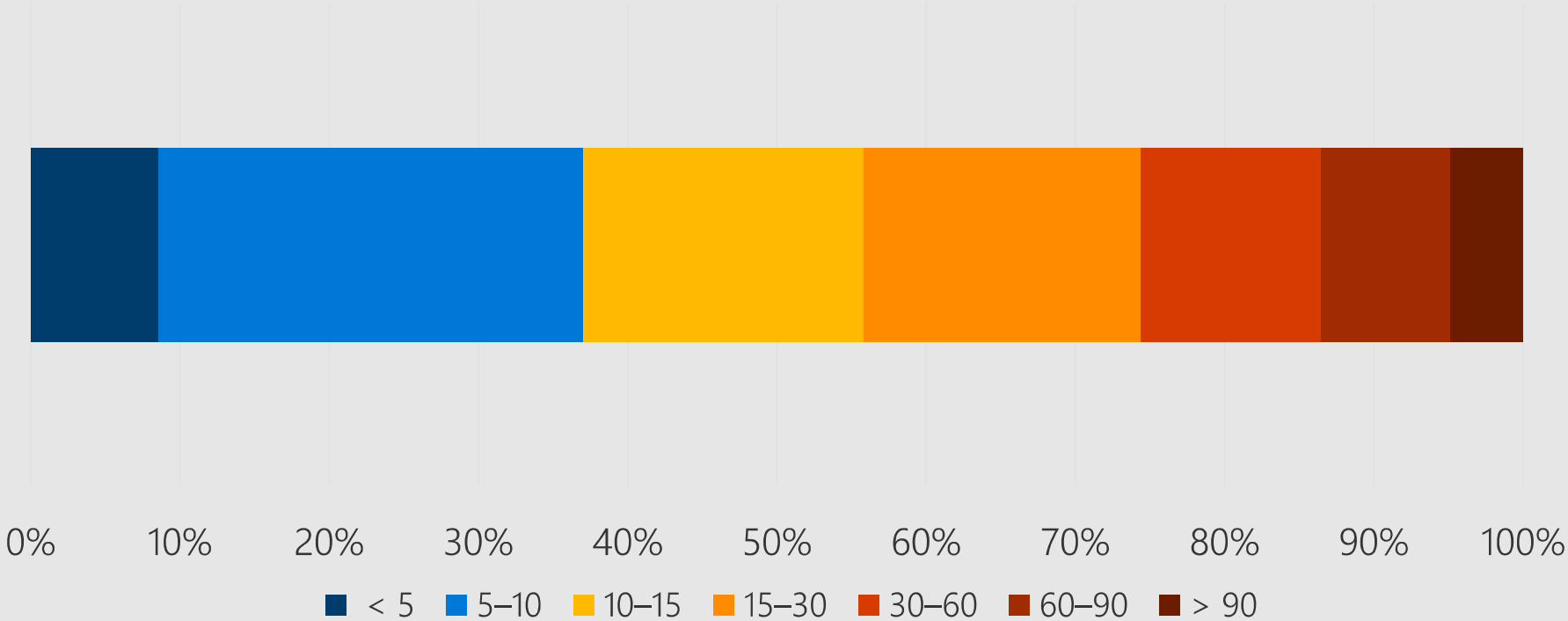
이전 단계에서 해결되지 않은 경우, 방대한 센서들의 네트워크로부터 발생하는 연관된 시그널을 추가 머신러닝 모델과 전문가 룰에 의해 검사하고 자동 분류 실행



- Component 1
- Component 2



End-to-end latency

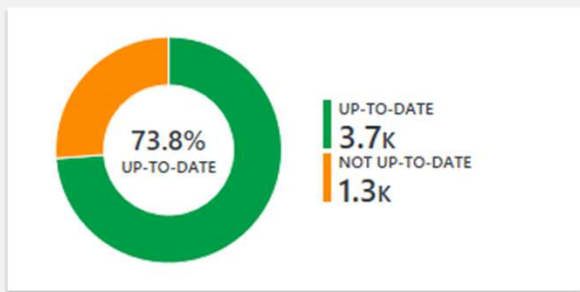


Windows Defender Antivirus 관리 방안



배포	Intune	PowerShell/ Group Policy	SCCM
시그니처 업데이트	Windows Update	WSUS	SCCM
리포트	Windows Defender ATP	Windows Analytics Update Compliance	SCCM
원격 스캔	Windows Defender ATP	Intune	SCCM

OVERALL SECURITY UPDATE STATUS



OS VERSION	UP-TO-DATE	NOT UP-TO-DATE [UPDATE ISSUES]
Preview build	133	0 [0]
1803	3,292	918 [0]
1709	262	356 [0]
1703	4	35 [0]

LATEST SECURITY UPDATE DEPLOYMENT STATUS



OS BUILD	VERSION	INSTALLED	IN PROGRESS OR DEFERRED	UPDATE ISSUES	STATUS UNKNOWN
17134.285	1803	3,292	653	161	102
16299.665	1709	262	236	83	37
15063.1324	1703	4	23	8	4

PREVIOUS SECURITY UPDATE DEPLOYMENT STATUS

OS BUILD	VERSION	INSTALLED	IN PROGRESS OR DEFERRED	UPDATE ISSUES	STATUS UNKNOWN
17134.228	1803	4,172	30	8	0
16299.611	1709	495	86	25	12
15063.1266	1703	27	8	2	2



Home

Virus & threat protection

Account protection

Firewall & network protection

App & browser control

Device security

Device performance & health

Family options

Settings

Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.



Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.



[Privacy Statement](#)

This setting is managed by your administrator.

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.



[Privacy Statement](#)

Have a question?

[Get help](#)

Help improve Windows Security

[Give us feedback](#)

Change your privacy settings

View and change privacy settings for your Windows 10 device.

[Privacy settings](#)

[Privacy dashboard](#)

[Privacy Statement](#)



Home

Virus & threat protection

Account protection

Firewall & network protection

App & browser control

Device security

Device performance & health

Family options

Settings



This setting is managed by your administrator.

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.



[Privacy Statement](#)

[Submit a sample manually](#)

Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.

[Manage Controlled folder access](#)

Exclusions

Windows Defender Antivirus won't scan items that you've excluded. Excluded items could contain threats that make your device vulnerable.

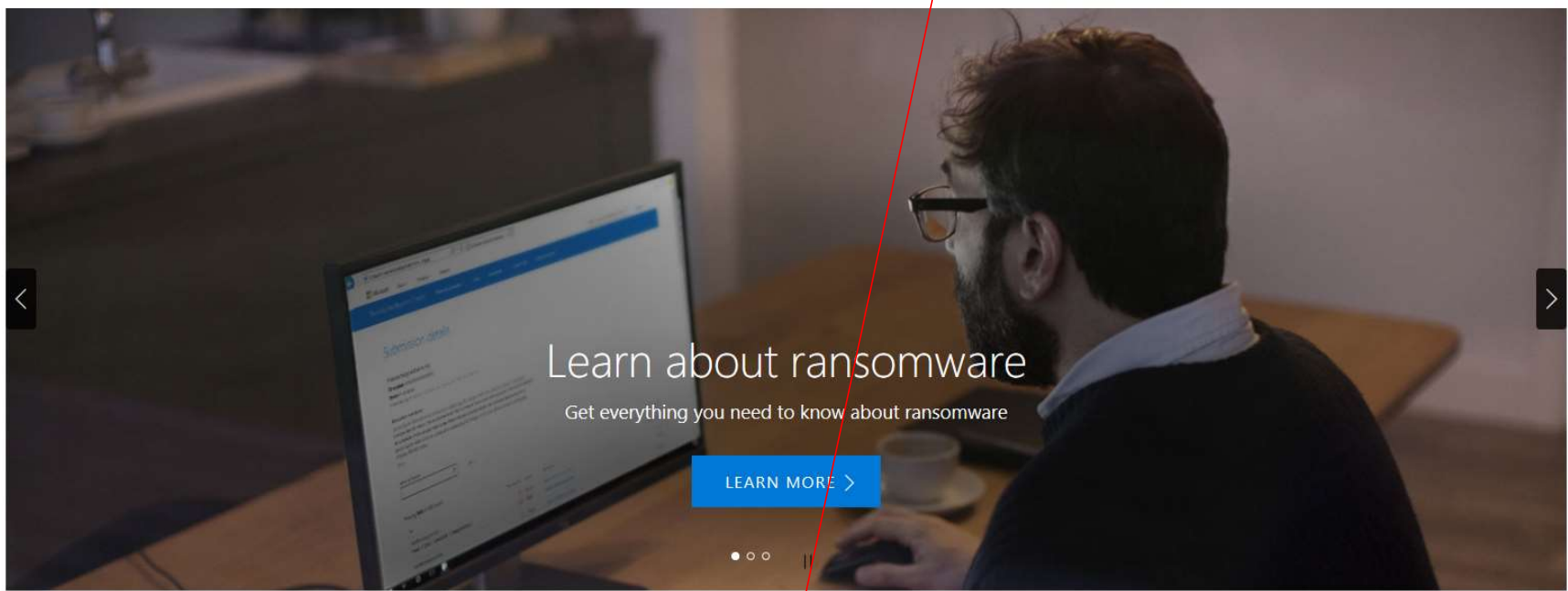
[Add or remove exclusions](#)

Notifications

Windows Defender Antivirus will send notifications with critical information about the health and security of your device. You can specify which non-critical notifications you would like.

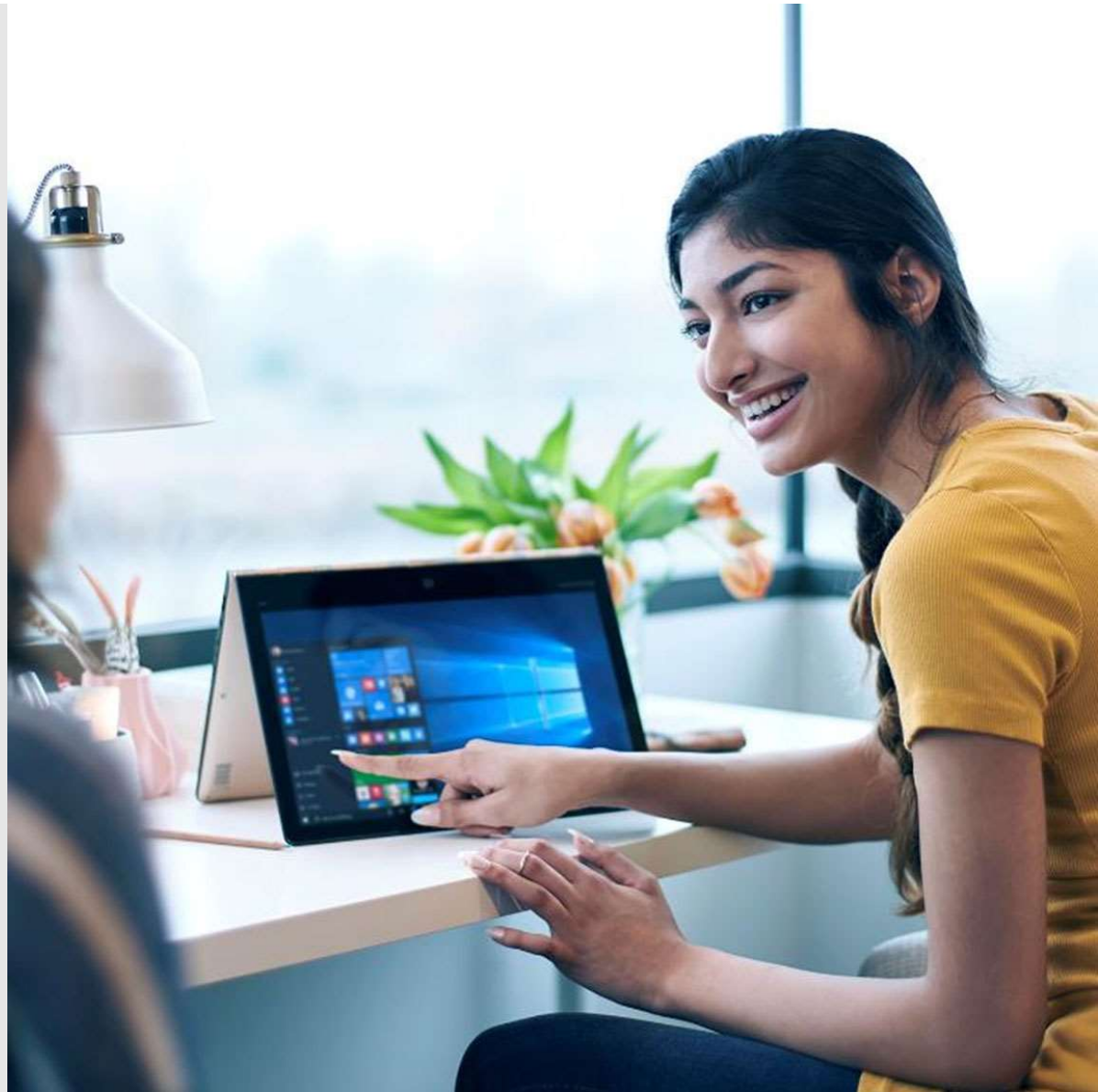
[Change notification settings](#)

📘 Microsoft Malware Protection Center (MPPC) is now Windows Defender Security Intelligence (WDSI). Watch out for even more info about threats and protecting you and your Windows computer. ✕



Submit a file for malware analysis

Summary



라이선스



Exchange Online Protection

Exchange Online Plan 1/2
Office 365 Business Premium/Essential
Office 365 F1/E1/E3/E5
Microsoft 365 E3/E5

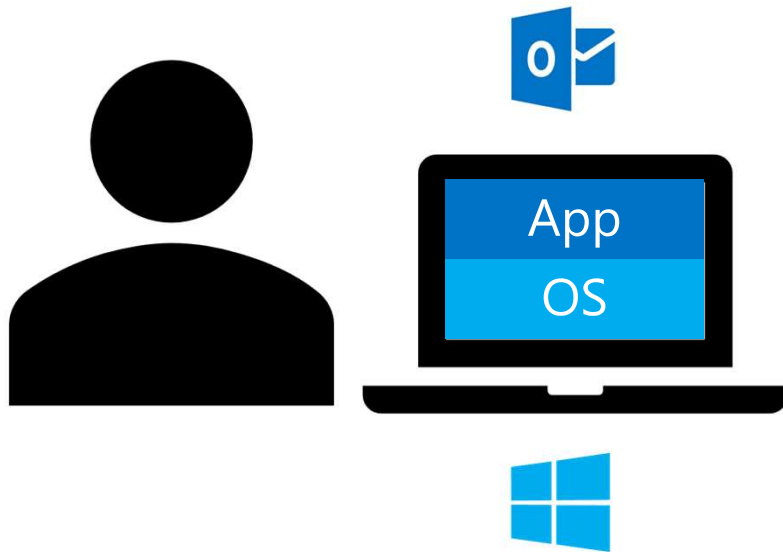


Windows Defender AV

Windows 10 Home
Windows 10 Pro
Windows 10 E3/E5
Microsoft 365 E3/E5

*Windows Server 2016도 Anti-virus가 Built in 되어 있음

Key Takeaways



- 직원들의 업무와 직결된 환경에서는 생산성을 해치지 않는 보안이 필요
- Windows 10과 EXO는 Built-in 보안 솔루션을 지원하여 설치 및 주기적인 관리가 필요 없으며, 직원들의 생산성을 최대한 보장
- 테스트 또는 PoC 진행

