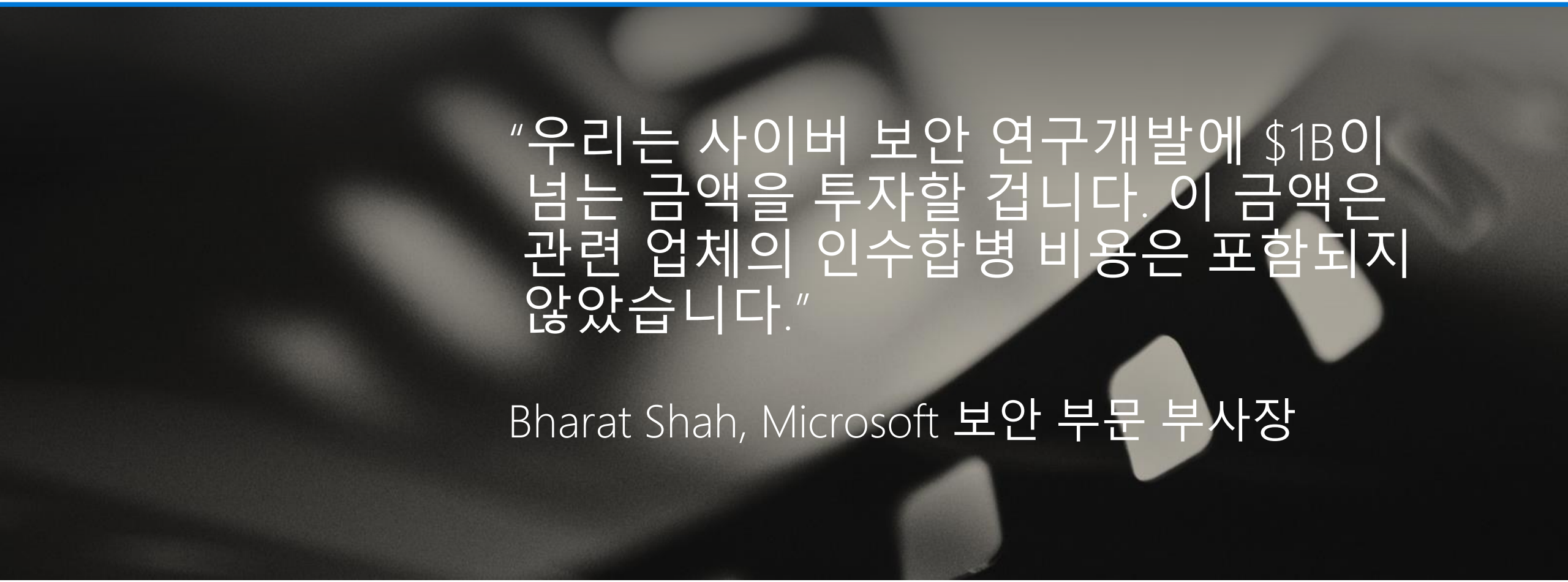
# 디지털 업무 환경의 미래, M365의 인텔리전트 보안

한국마이크로소프트

Microsoft 365 비즈니스 그룹 박상준 부장

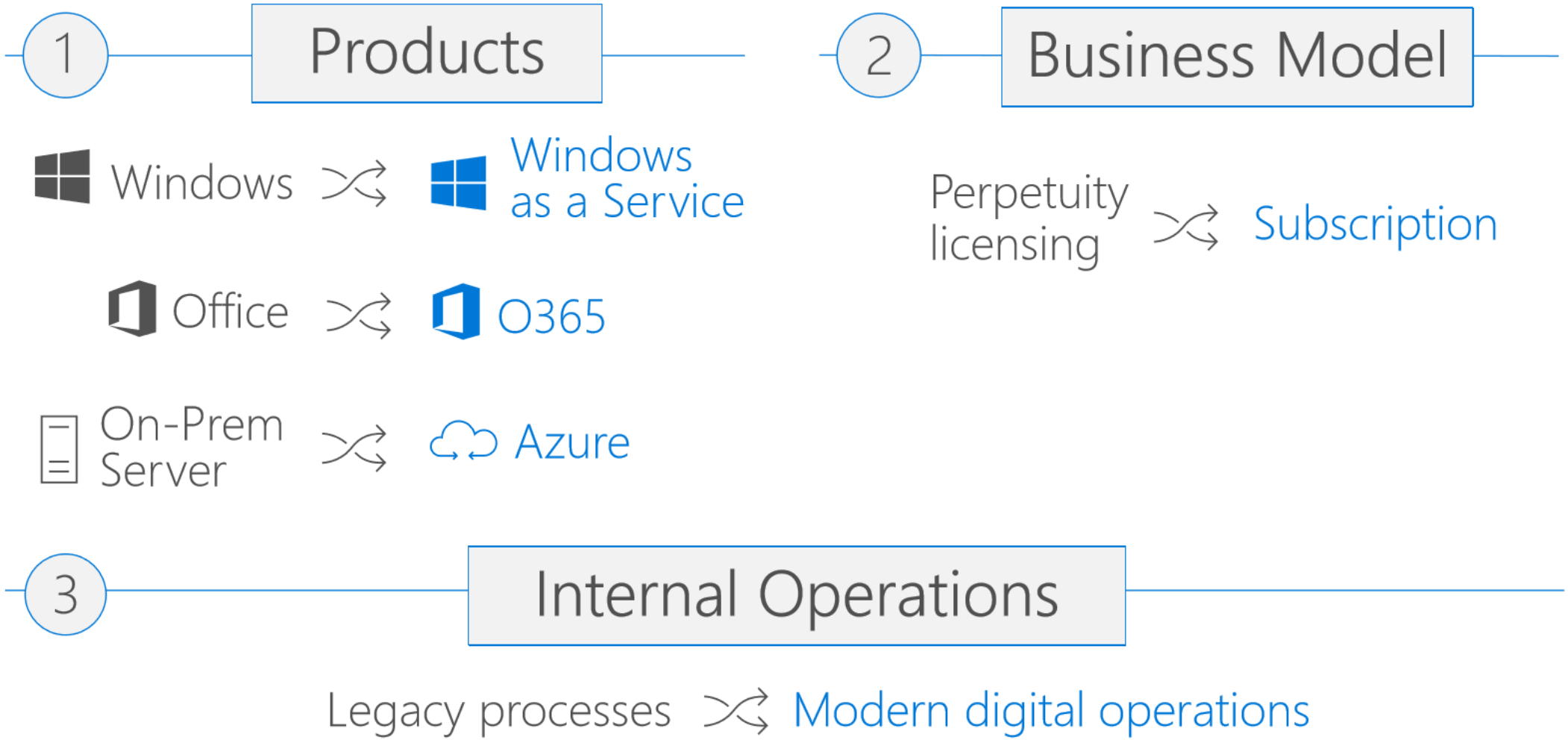
Microsoft

# 마이크로소프트는 보안 회사입니다.




Source: Zero Day Auction for the Masses

# 클라우드 기업으로의 전환

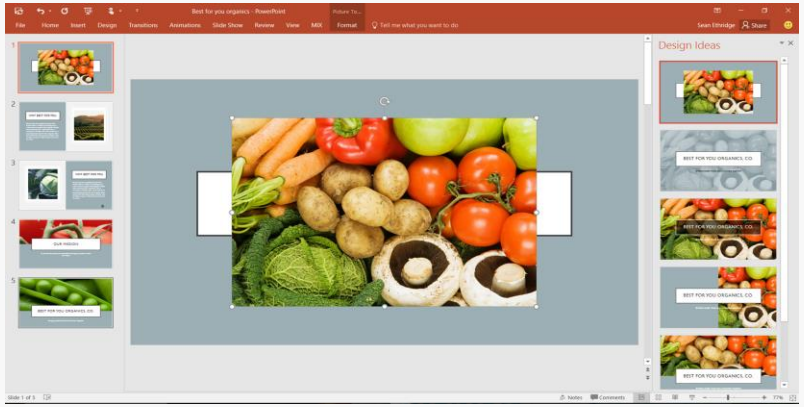


# 새로운 일하는 방식

더 진화하는 비즈니스 환경, 더 확장된 팀, 그리고 더 복잡해진 보안 환경을 위해 새로운 업무 환경 필요

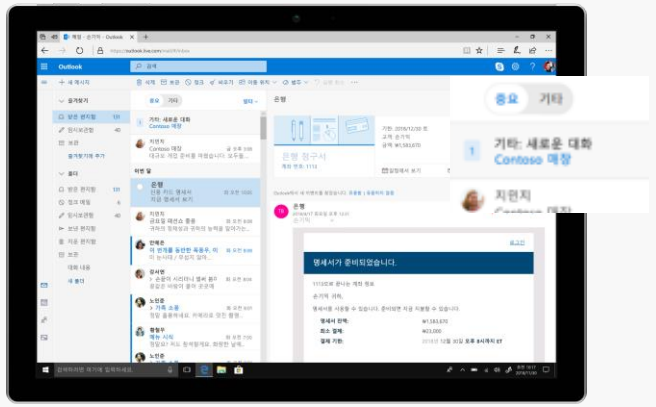
# 새로운 일하는 방식을 위한 생산성

## AI 기반의 더 지능적이고 더 생산적인 새로운 일하는 방식



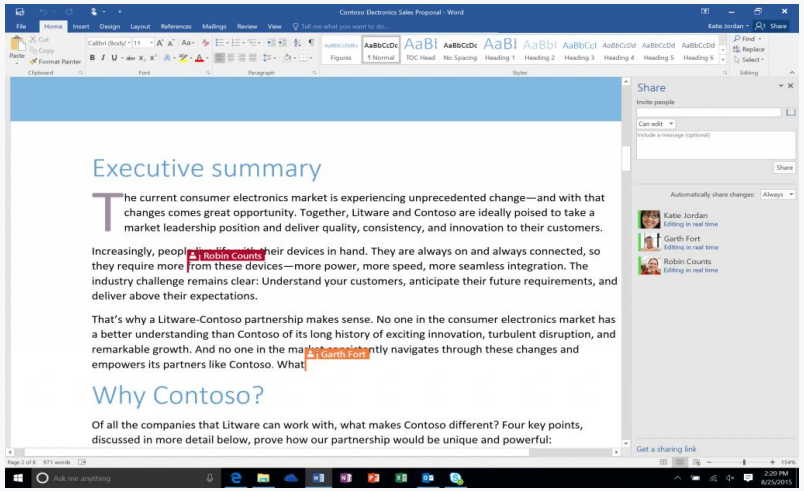

### 디자인 비서: POWERPOINT 디자인 아이디어

*파워포인트 디자인의 품질을 한번의 클릭으로 올려줍니다.*



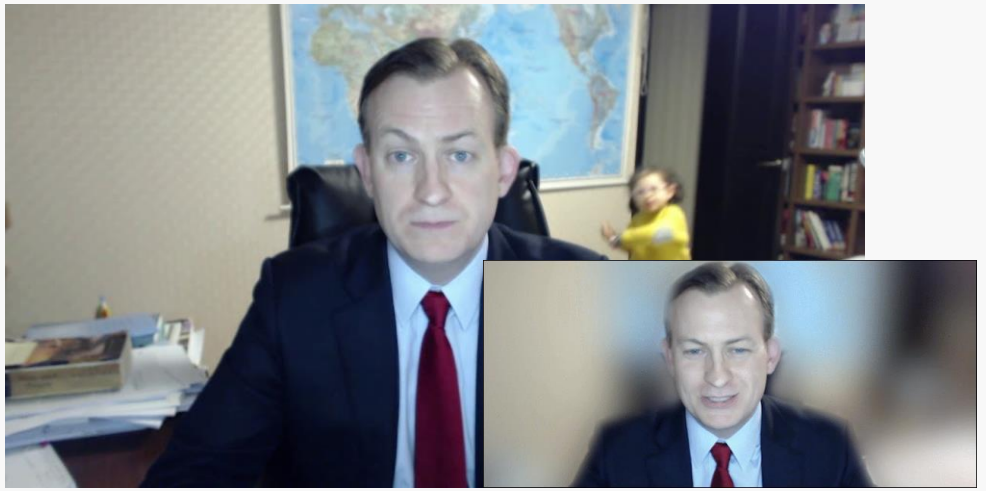

### 업무 비서: Outlook 중요 메일 구분

*AI 비서가 알아서 중요한 메일과 중요하지 않은 메일을 구분해줍니다.*




### 업무 비서: Office 동시 편집

*하나의 문서에 여러명이 동시에 접근하여 동시 편집을 가능하게 해줌으로써, 시간을 절감해드립니다.*

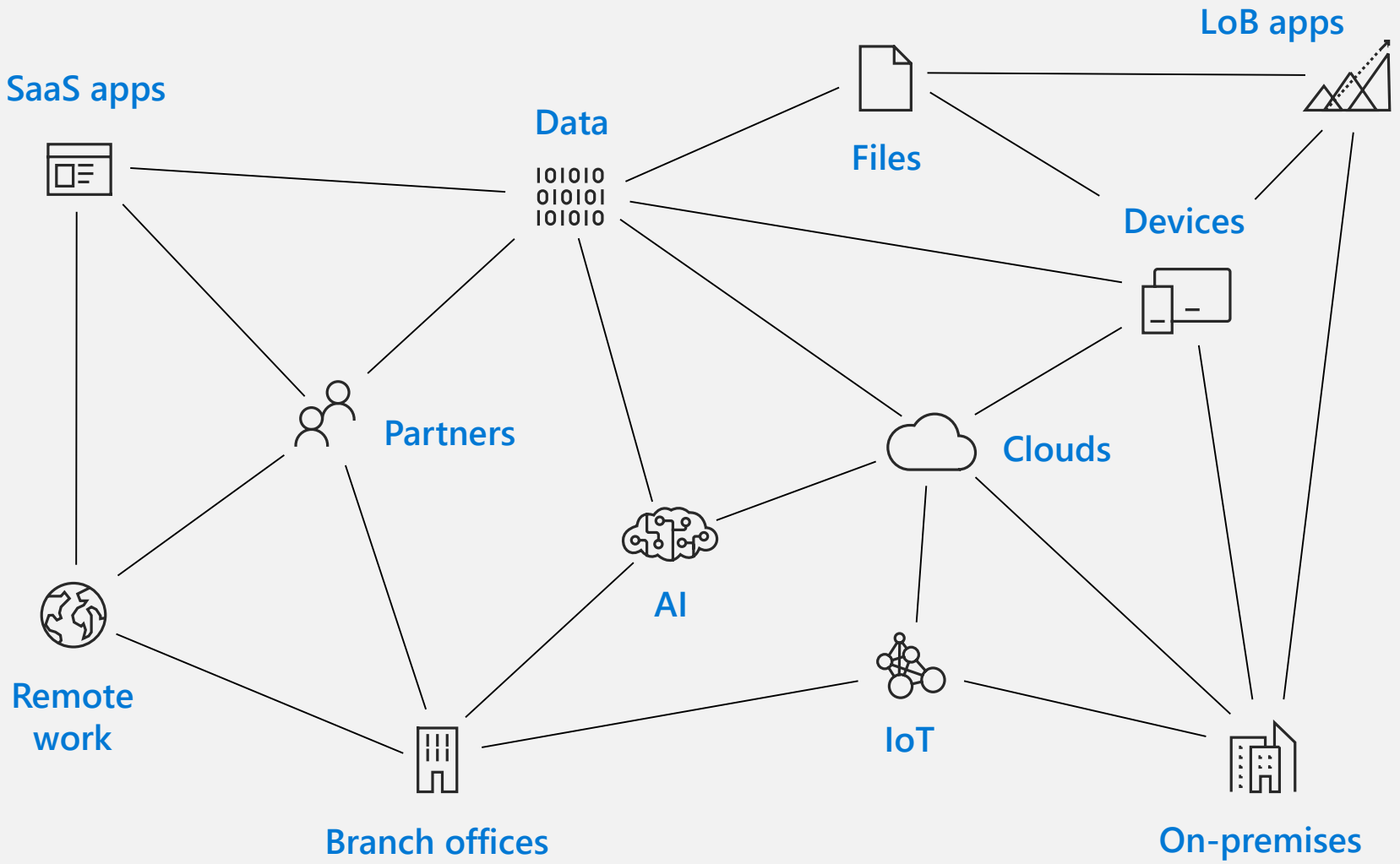


### 회의 비서: TEAMS 화상회의 blur 기능

*언제 어디서 화상회의를 하더라도, 민감한 정보를 AI가 자동으로 차단*

# 그런데 보안은...?

# 디지털 트랜스포메이션으로 인한 경계의 확장



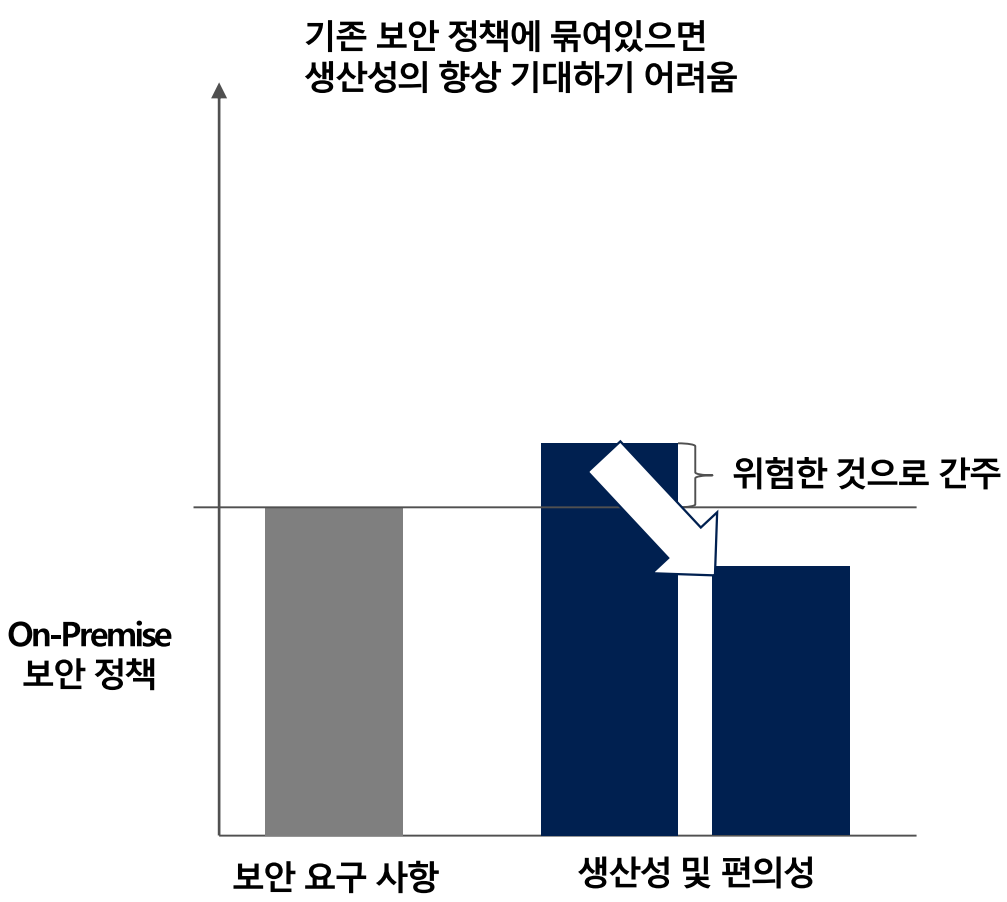
# 현재의 보안 인식 범위

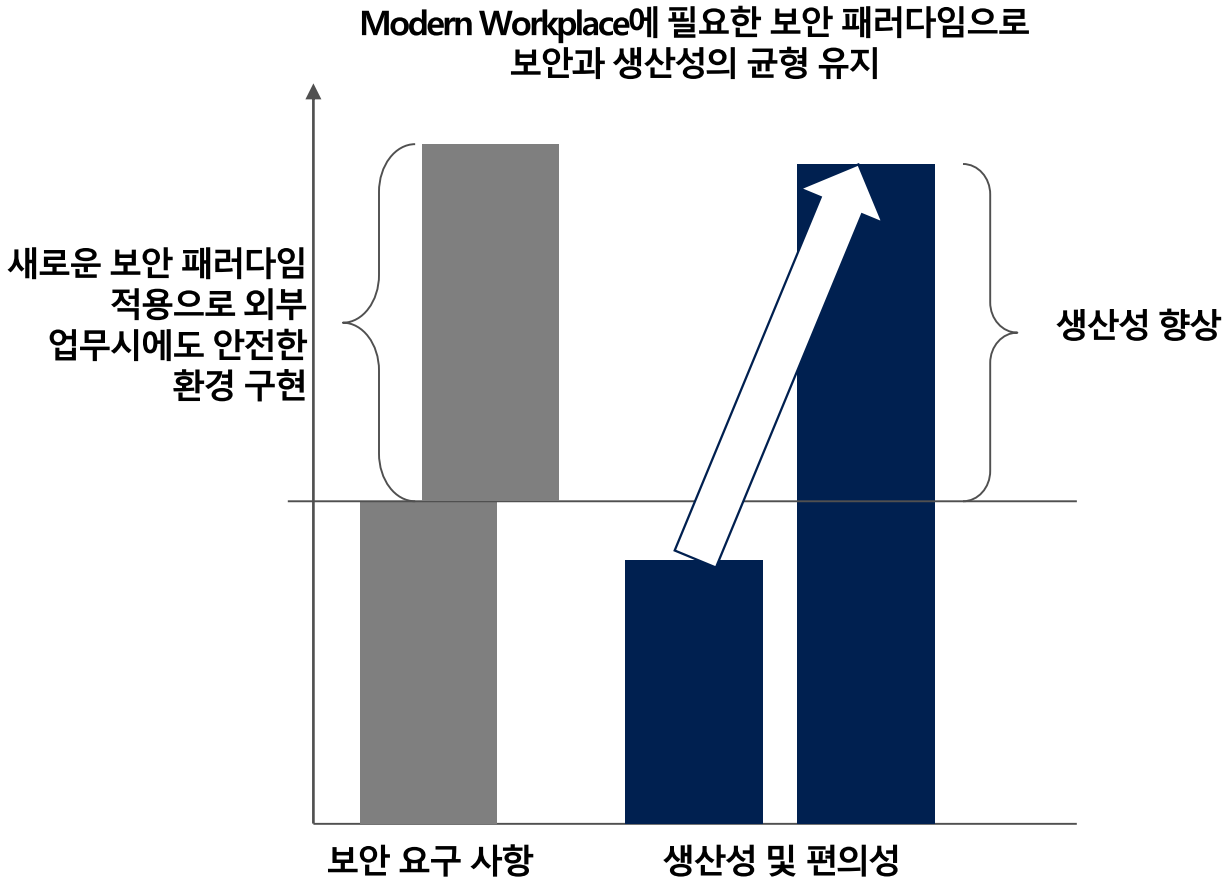
**사내에서만 활용하는 것을 목표로 구축 및 운영되는 IT 환경**

# 생산성 혁신을 위해서는 보안 경계도 확산되어야

# 보안과 생산성 모두의 혁신, 가능하다

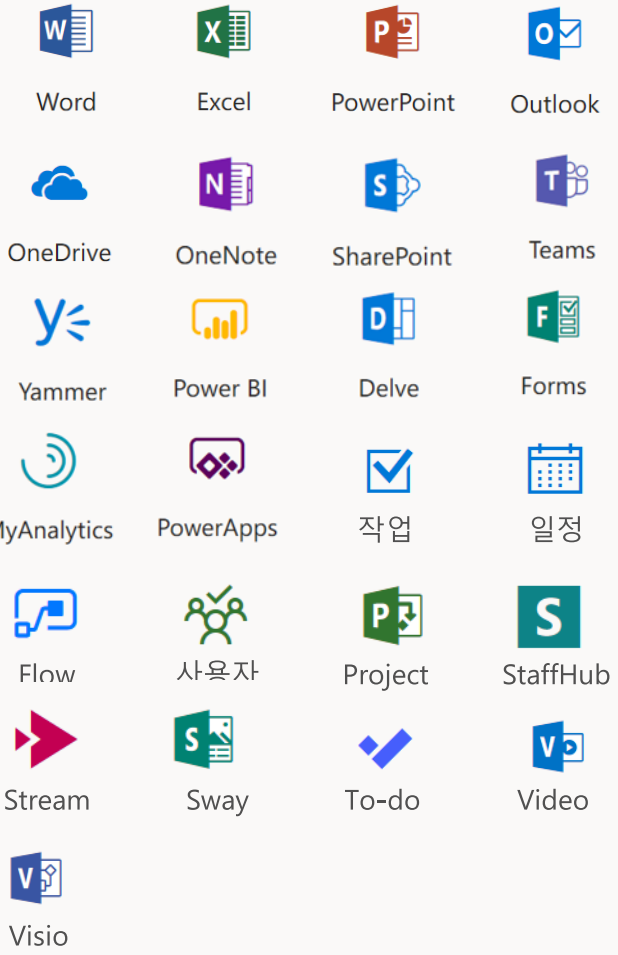
**비즈니스 성과를 높이는 것과 동시에,**
**<u>보안과 생산성의 균형</u>을 유지하는 것이 무엇보다도 중요**




Office 365
Microsoft 365
Windows 10
Enterprise Mobility + Security

## Office 365

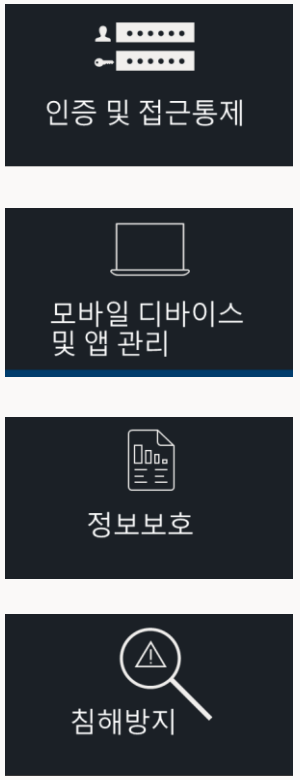



## Windows 10

OS

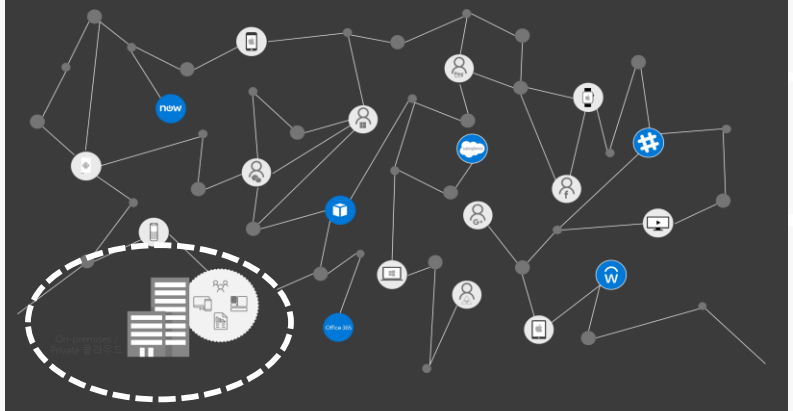
- Windows Defender System Guard
- Windows Defender Application Guard
- Windows Defender Exploit Guard
- Windows Defender Anti-virus
- Windows Defender Application Control
- SmartScreen
- Hello for Business
- Windows Defender Credential Guard
- Windows Information Protection
- Bitlocker
- Windows Defender ATP
- Windows Defender System Center

## Enterprise Mobility + Security



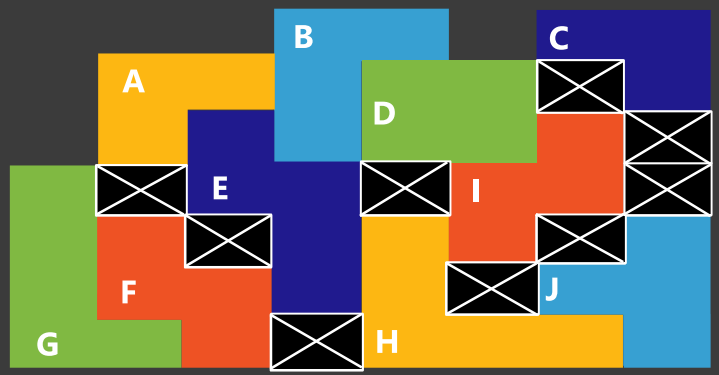
# Microsoft 365 보안

# 디지털 시대의 보안, 사람의 능력을 넘어서는 경지

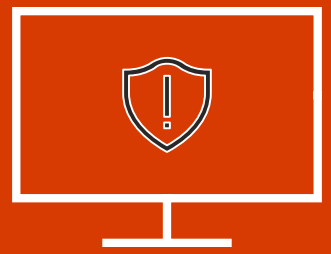


회사 내만 집중보호

도입하는 보안솔루션이 너무 많음




여전히 완벽하지 못한 보안



매월 50억개의 새로운 위협*

처리 가능한 보안경고: 10개/일/전문가


긍정오류를 범하기 쉬움

*The Microsoft Intelligent Security Graph data

# 보안은 변화해야 합니다.

**75**

한 기업당 사용하는 보안 솔루션 갯수[1]

**70%**

10개 중 7개의 기업은 **endpoint**에 대해서 위협을 느끼고 있습니다.[2]

**56%**

하루에 **IT** 관리자가 처리할 수 있는 평균 경고 비율[3]

1. CSO. "Defense in depth: Stop spending, start consolidating." Mar 2016.
2. Barkly. "3 Key Findings from the Upcoming 2017 State of Endpoint Security Risk Report." Nov 2017.
3. Cisco. "Annual Cybersecurity Report." 2017.

# Microsoft 365 보안 영역 및 차별점

## 인증 및 접근 통제

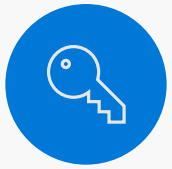
사용자 인증 체계 및 사용자별 자원 접근에 대한 통제

## 침해 방지

지능화된 침해 방지 및 빠른 대응

## 정보 보호

문서 및 이메일이 사전에 인가된 사용자에게만 허용하도록 통제



## 보안 관리

통합 보안 툴을 이용하여 보안 상황에 대한 가시성을 제공하고 통제권을 유지

Security Platform

Built-in, not Bolt-on

Microsoft Intelligent Security Graph

# Microsoft Intelligent Security Graph

마이크로소프트 클라우드 서비스 및 윈도우 업데이트로부터 공격 징후 감지

매월 50억 개의 위협 차단

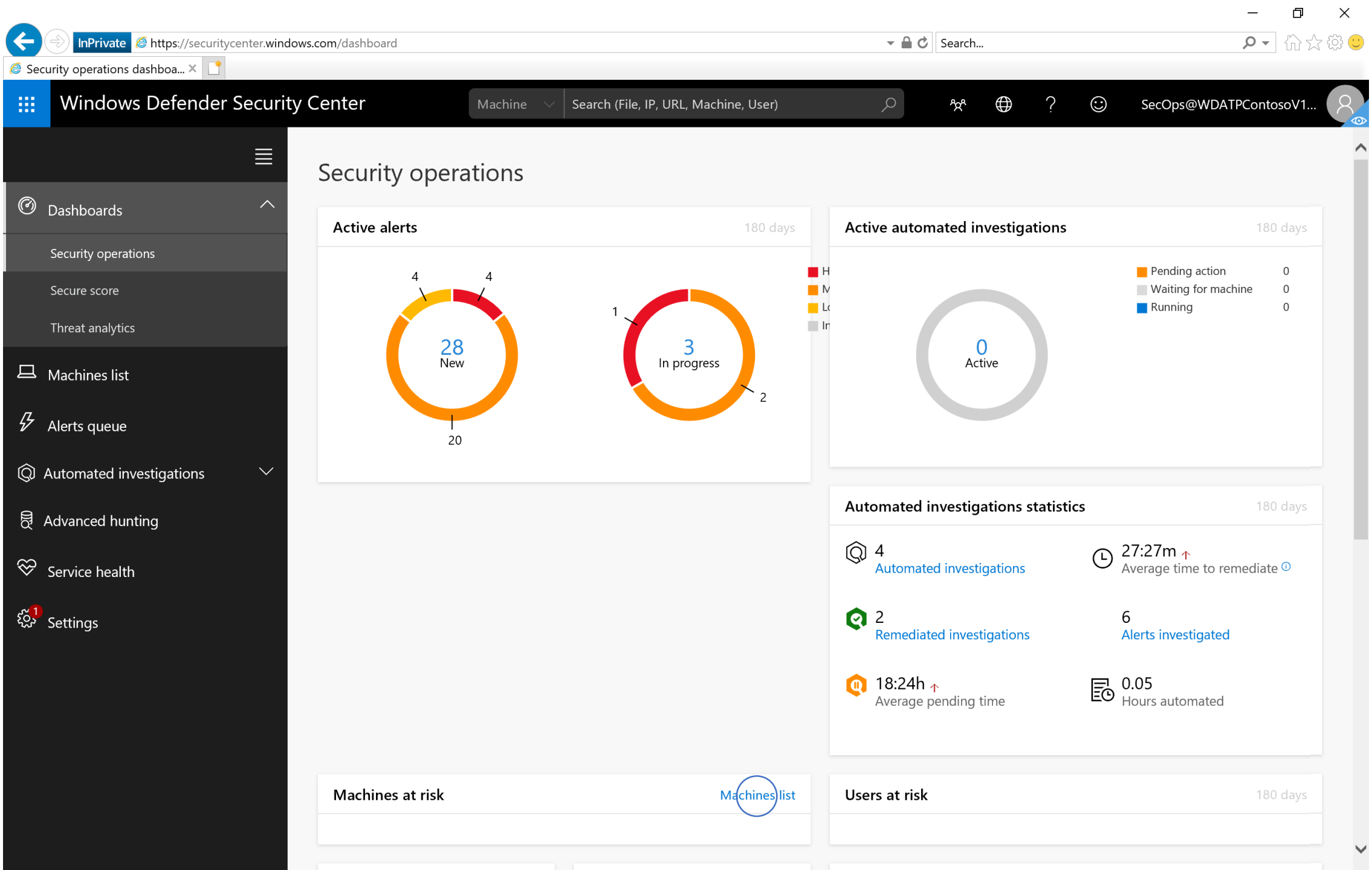
매월 4천억 개의 이메일 패턴 분석

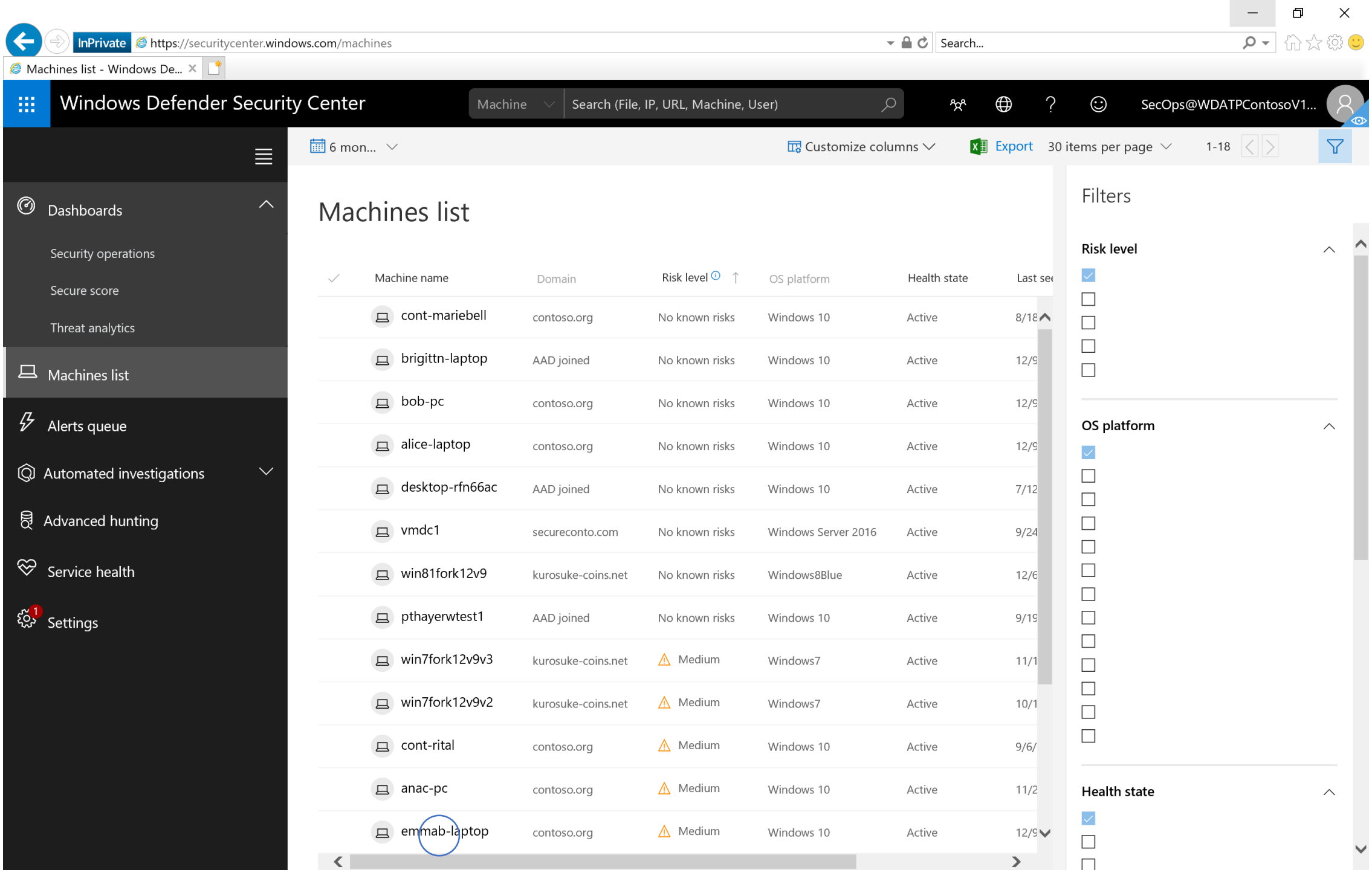
매월 4,500억 개 인증 처리

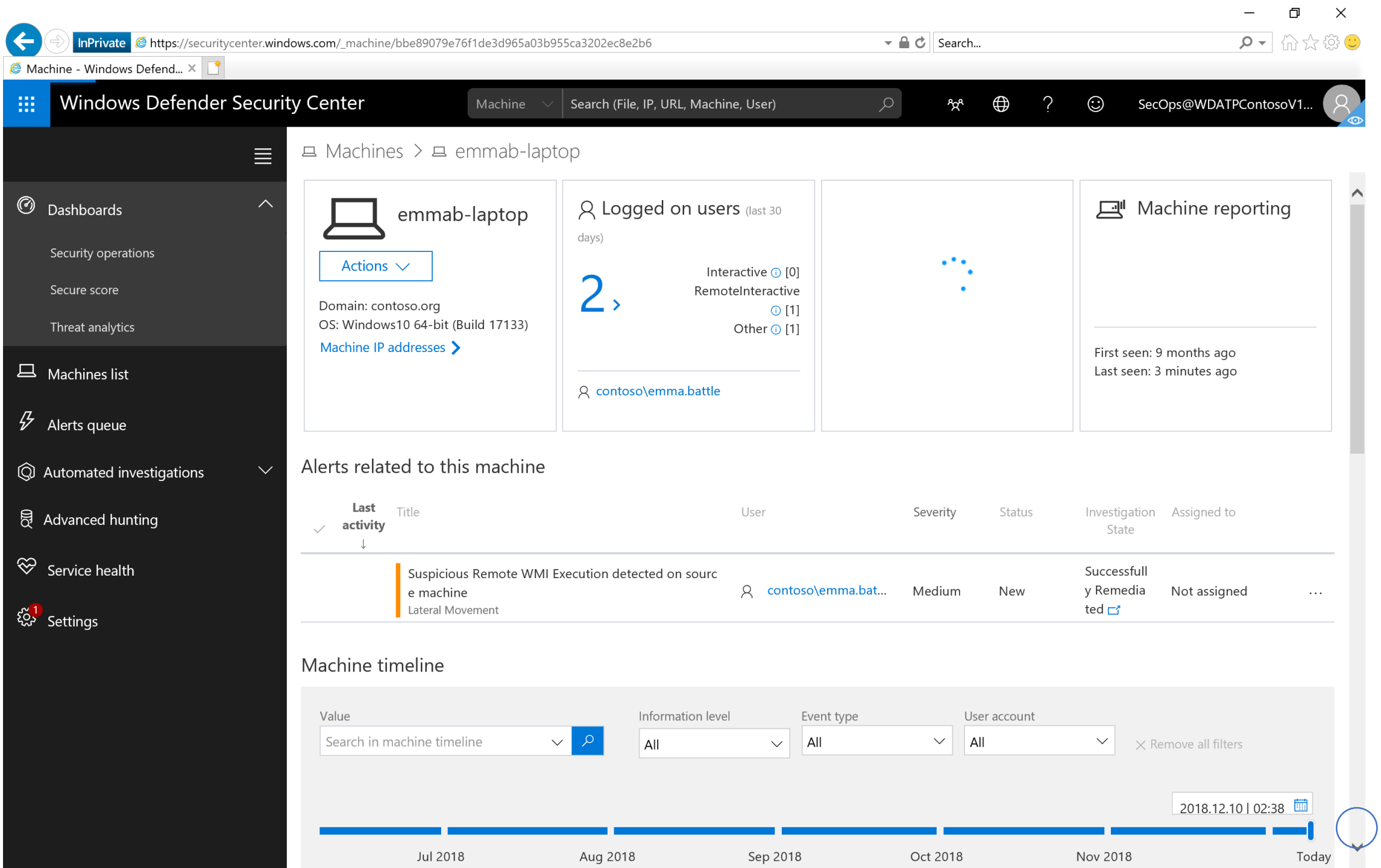
매월 12억 대의 디바이스 업데이트

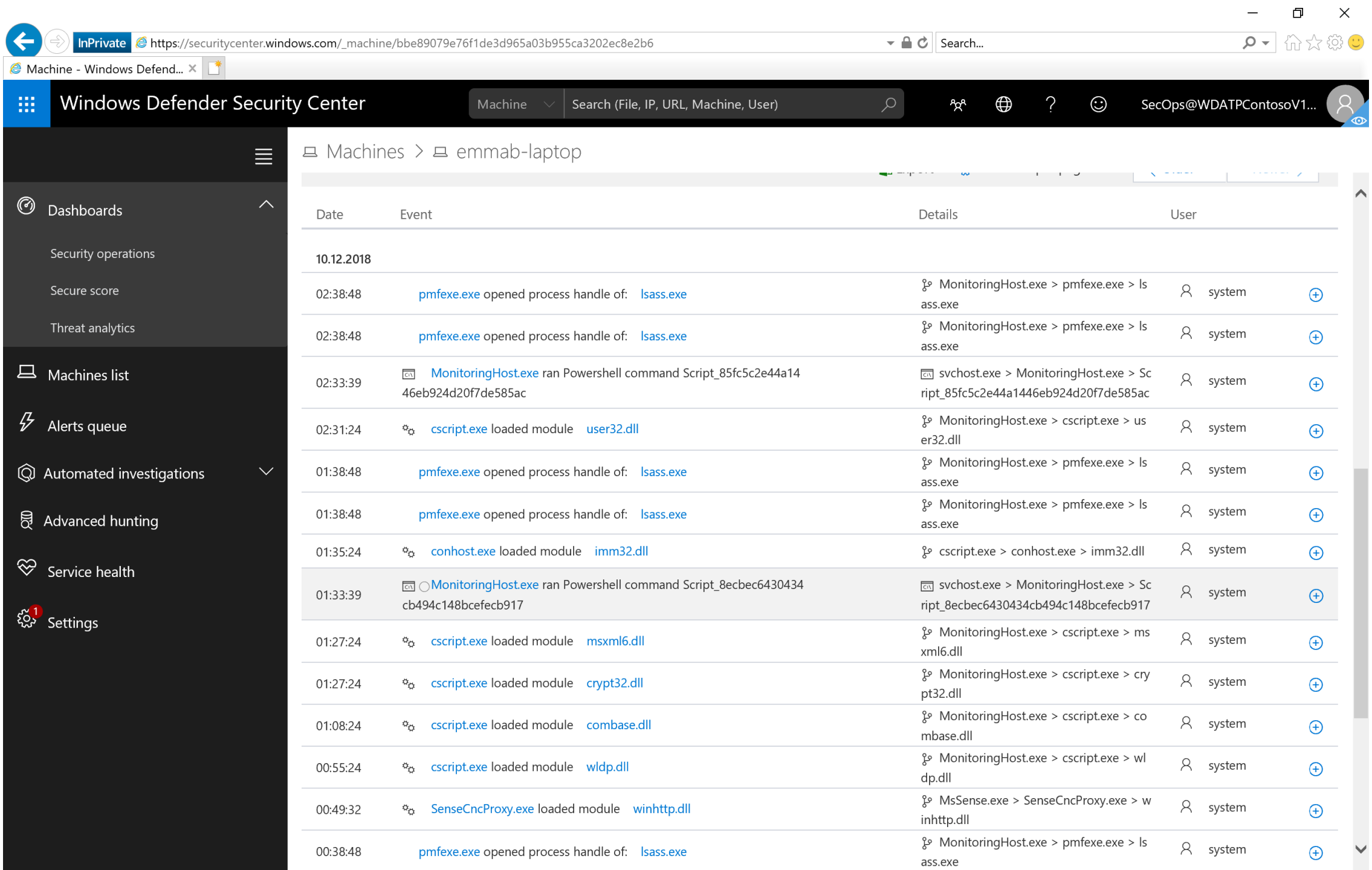
매월 180억 이상의 페이지 검사

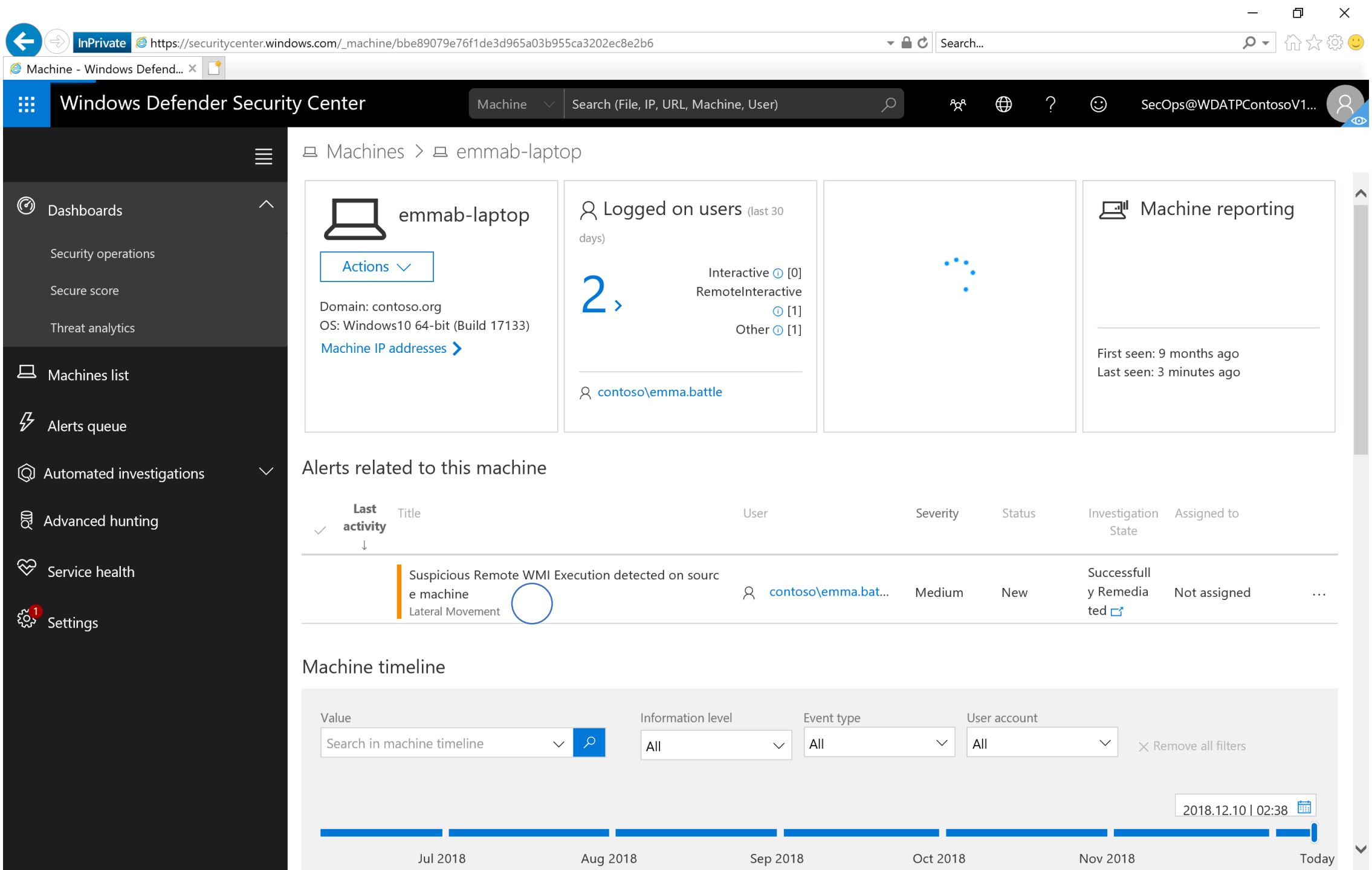
3,500명 이상의 보안 전문가

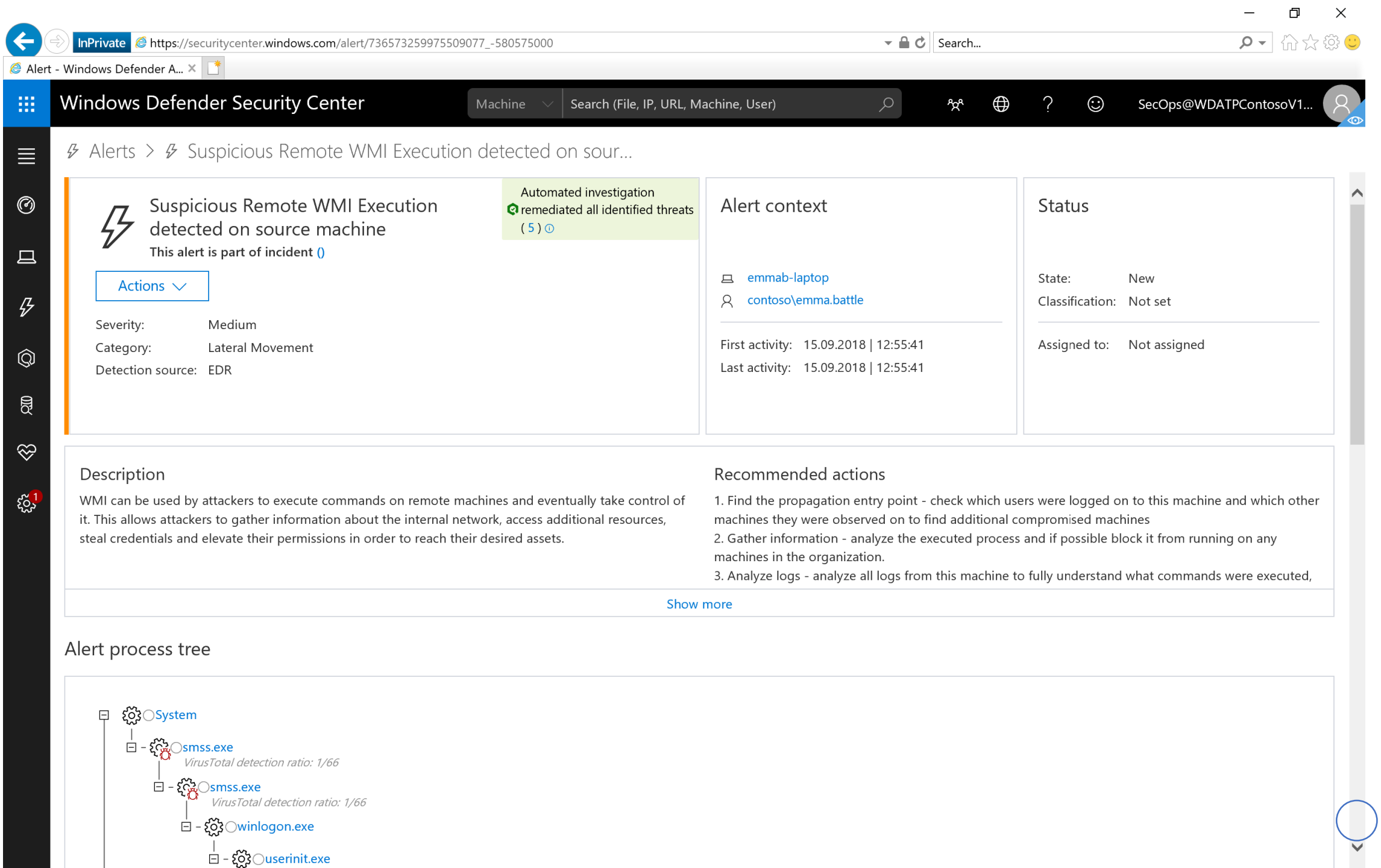

InPrivate
https://securitycenter.windows.com/dashboard
Search...
Security operations dashboa...
Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
Dashboards
Security operations
Secure score
Threat analytics
Machines list
Alerts queue
Automated investigations
Advanced hunting
Service health
Settings
Security operations
Active alerts
180 days
4
4
28
New
20
1
3
In progress
2
Active automated investigations
180 days
0
Active
Pending action 0
Waiting for machine 0
Running 0
Automated investigations statistics
180 days
4
Automated investigations
27:27m
Average time to remediate
2
Remediated investigations
6
Alerts investigated
18:24h
Average pending time
0.05
Hours automated
Machines at risk
Machines list
Users at risk
180 days

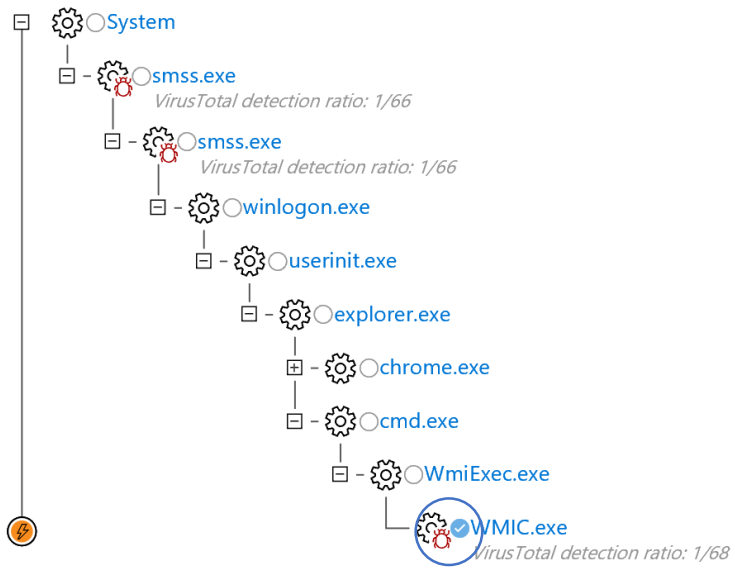

InPrivate
https://securitycenter.windows.com/machines
Search...
Machines list - Windows De...
Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
6 mon...
Customize columns
Export
30 items per page
1-18
Dashboards
Security operations
Secure score
Threat analytics
Machines list
Alerts queue
Automated investigations
Advanced hunting
Service health
Settings
Machines list
Machine name
Domain
Risk level
OS platform
Health state
Last se
cont-mariebell contoso.org No known risks Windows 10 Active 8/18
brigittn-laptop AAD joined No known risks Windows 10 Active 12/9
bob-pc contoso.org No known risks Windows 10 Active 12/9
alice-laptop contoso.org No known risks Windows 10 Active 12/9
desktop-rfn66ac AAD joined No known risks Windows 10 Active 7/12
vmdc1 secureconto.com No known risks Windows Server 2016 Active 9/24
win81fork12v9 kurosuke-coins.net No known risks Windows8Blue Active 12/6
pthayerwtest1 AAD joined No known risks Windows 10 Active 9/19
win7fork12v9v3 kurosuke-coins.net Medium Windows7 Active 11/1
win7fork12v9v2 kurosuke-coins.net Medium Windows7 Active 10/1
cont-rital contoso.org Medium Windows 10 Active 9/6/
anac-pc contoso.org Medium Windows 10 Active 11/2
emmab-laptop contoso.org Medium Windows 10 Active 12/9
Filters
Risk level
OS platform
Health state


InPrivate
https://securitycenter.windows.com/_machine/bbe89079e76f1de3d965a03b955ca3202ec8e2b6
Search...
Machine - Windows Defend...
Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
Dashboards
Security operations
Secure score
Threat analytics
Machines list
Alerts queue
Automated investigations
Advanced hunting
Service health
Settings
Machines > emmab-laptop
emmab-laptop
Actions
Domain: contoso.org
OS: Windows10 64-bit (Build 17133)
Machine IP addresses
Logged on users (last 30 days)
2
Interactive [0]
RemoteInteractive [1]
Other [1]
contoso\emma.battle
Machine reporting
First seen: 9 months ago
Last seen: 3 minutes ago
Alerts related to this machine
Last activity
Title
User
Severity
Status
Investigation State
Assigned to
Suspicious Remote WMI Execution detected on source machine
Lateral Movement
contoso\emma.bat...
Medium
New
Successfully Remediated
Not assigned
Machine timeline
Value
Search in machine timeline
Information level
All
Event type
All
User account
All
Remove all filters
2018.12.10 | 02:38
Jul 2018
Aug 2018
Sep 2018
Oct 2018
Nov 2018
Today


InPrivate
https://securitycenter.windows.com/_machine/bbe89079e76f1de3d965a03b955ca3202ec8e2b6
Search...
Machine - Windows Defend...
Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
Machines > emmab-laptop
Dashboards
Security operations
Secure score
Threat analytics
Machines list
Alerts queue
Automated investigations
Advanced hunting
Service health
Settings
Date
Event
Details
User
10.12.2018
02:38:48 pmfexe.exe opened process handle of: lsass.exe MonitoringHost.exe > pmfexe.exe > lsass.exe system
02:38:48 pmfexe.exe opened process handle of: lsass.exe MonitoringHost.exe > pmfexe.exe > lsass.exe system
02:33:39 MonitoringHost.exe ran Powershell command Script_85fc5c2e44a1446eb924d20f7de585ac svchost.exe > MonitoringHost.exe > Script_85fc5c2e44a1446eb924d20f7de585ac system
02:31:24 cscript.exe loaded module user32.dll MonitoringHost.exe > cscript.exe > user32.dll system
01:38:48 pmfexe.exe opened process handle of: lsass.exe MonitoringHost.exe > pmfexe.exe > lsass.exe system
01:38:48 pmfexe.exe opened process handle of: lsass.exe MonitoringHost.exe > pmfexe.exe > lsass.exe system
01:35:24 conhost.exe loaded module imm32.dll cscript.exe > conhost.exe > imm32.dll system
01:33:39 MonitoringHost.exe ran Powershell command Script_8ecbec6430434cb494c148bcefecb917 svchost.exe > MonitoringHost.exe > Script_8ecbec6430434cb494c148bcefecb917 system
01:27:24 cscript.exe loaded module msxml6.dll MonitoringHost.exe > cscript.exe > msxml6.dll system
01:27:24 cscript.exe loaded module crypt32.dll MonitoringHost.exe > cscript.exe > crypt32.dll system
01:08:24 cscript.exe loaded module combase.dll MonitoringHost.exe > cscript.exe > combase.dll system
00:55:24 cscript.exe loaded module wldp.dll MonitoringHost.exe > cscript.exe > wldp.dll system
00:49:32 SenseCncProxy.exe loaded module winhttp.dll MsSense.exe > SenseCncProxy.exe > winhttp.dll system
00:38:48 pmfexe.exe opened process handle of: lsass.exe MonitoringHost.exe > pmfexe.exe > lsass.exe system


InPrivate
https://securitycenter.windows.com/_machine/bbe89079e76f1de3d965a03b955ca3202ec8e2b6
Search...
Machine - Windows Defend...
Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
Dashboards
Security operations
Secure score
Threat analytics
Machines list
Alerts queue
Automated investigations
Advanced hunting
Service health
Settings
Machines > emmab-laptop
emmab-laptop
Actions
Domain: contoso.org
OS: Windows10 64-bit (Build 17133)
Machine IP addresses
Logged on users (last 30 days)
2
Interactive [0]
RemoteInteractive [1]
Other [1]
contoso\emma.battle
Machine reporting
First seen: 9 months ago
Last seen: 3 minutes ago
Alerts related to this machine
Last activity
Title
User
Severity
Status
Investigation State
Assigned to
Suspicious Remote WMI Execution detected on source machine
Lateral Movement
contoso\emma.bat...
Medium
New
Successfully Remediated
Not assigned
Machine timeline
Value
Search in machine timeline
Information level
All
Event type
All
User account
All
Remove all filters
2018.12.10 | 02:38
Jul 2018
Aug 2018
Sep 2018
Oct 2018
Nov 2018
Today


InPrivate
https://securitycenter.windows.com/alert/736573259975509077_-580575000
Search...
Alert - Windows Defender A...
Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
Alerts
Suspicious Remote WMI Execution detected on sour...
Suspicious Remote WMI Execution detected on source machine
This alert is part of incident ()
Actions
Severity: Medium
Category: Lateral Movement
Detection source: EDR
Automated investigation remediated all identified threats ( 5 )
Alert context
emmab-laptop
contoso\emma.battle
First activity: 15.09.2018 | 12:55:41
Last activity: 15.09.2018 | 12:55:41
Status
State: New
Classification: Not set
Assigned to: Not assigned
Description
WMI can be used by attackers to execute commands on remote machines and eventually take control of it. This allows attackers to gather information about the internal network, access additional resources, steal credentials and elevate their permissions in order to reach their desired assets.
Recommended actions
1. Find the propagation entry point - check which users were logged on to this machine and which other machines they were observed on to find additional compromised machines
2. Gather information - analyze the executed process and if possible block it from running on any machines in the organization.
3. Analyze logs - analyze all logs from this machine to fully understand what commands were executed,
Show more
Alert process tree
System
smss.exe
VirusTotal detection ratio: 1/66
smss.exe
VirusTotal detection ratio: 1/66
winlogon.exe
userinit.exe




This alert is also related to 1 process creation event not displayed here.
Last event time is 15.09.2018 | 12:55:41.
Click here to see all related events in the machine timeline.

## Incident graph

## WMIC.exe

### Execution details

Execution time: 15.09.2018 | 12:55:40
Path: C:\Windows\SysWOW64\wbem
User: CONTOSO\Emma.Battle
Access privileges (UAC): Restricted
Integrity level: Medium
Process ID: 5460
Command line:

```
"WMIC.exe" /node:"SummerB-PC"
process call create
"c:\windows\system32\rundll32.exe
C:\\windows\\Service.dll M10"
```

### File details

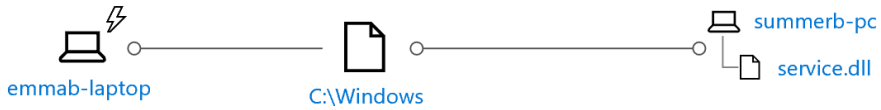
SHA1: c902cef254ed2423bc2
SHA256: c4639422cf50ee039dc
MD5: 08bae6a2086c7c99397
Signer: INVALID: Microsoft Windows
Issuer: INVALID: Microsoft Development PCA 2014

### Detections

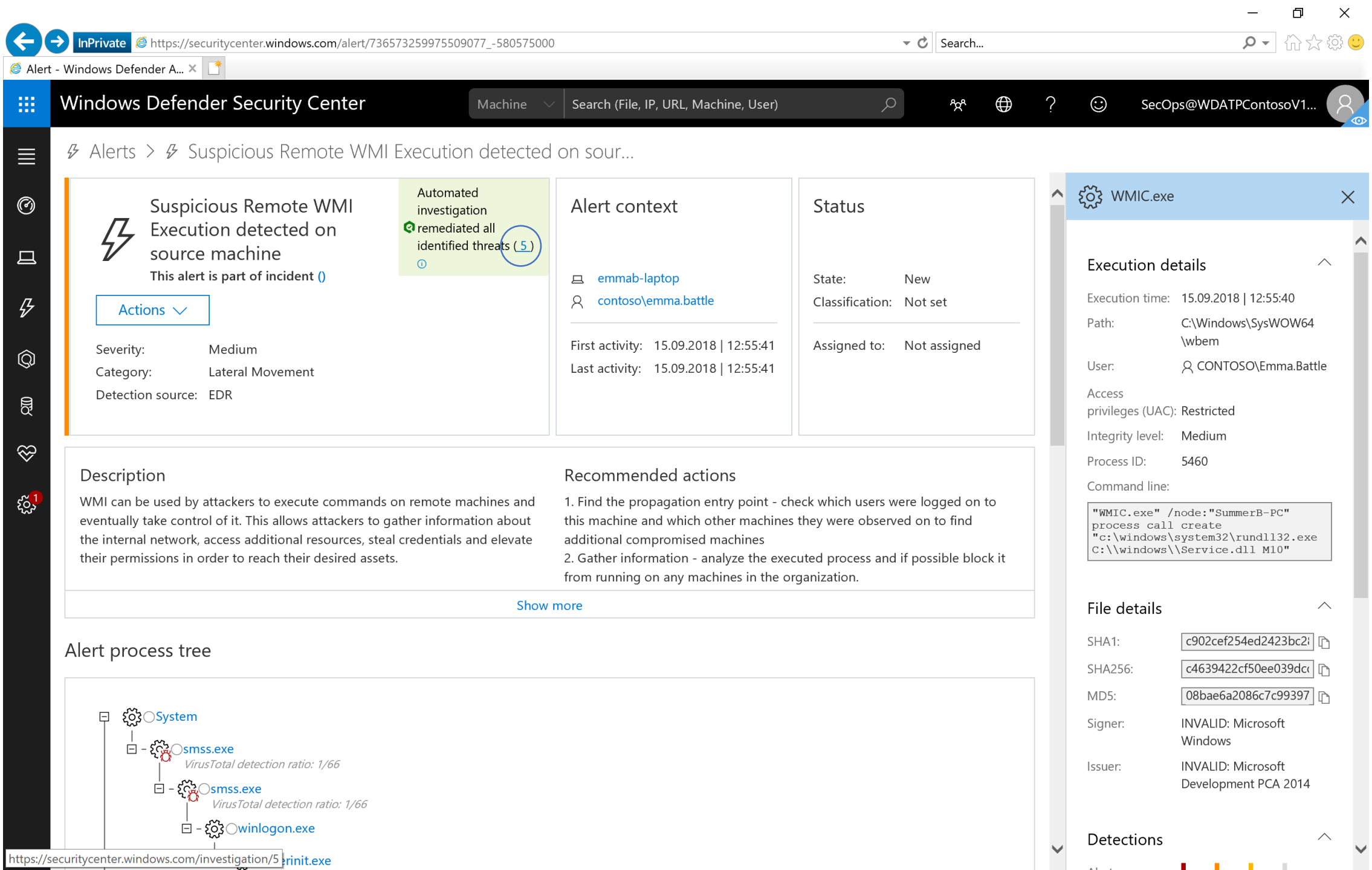
WMIC.exe
*VirusTotal detection ratio: 1/68*

This alert is also related to 1 process creation event not displayed here.
Last event time is 15.09.2018 | 12:55:41.
Click here to see all related events in the machine timeline.

## Incident graph




## Artifact timeline


InPrivate
https://securitycenter.windows.com/alert/736573259975509077_-580575000
Search...
Alert - Windows Defender A...
Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
Alerts > Suspicious Remote WMI Execution detected on sour...
Suspicious Remote WMI Execution detected on source machine
This alert is part of incident ()
Actions
Severity: Medium
Category: Lateral Movement
Detection source: EDR
Automated investigation remediated all identified threats ( 5 )
Alert context
emmab-laptop
contoso\emma.battle
First activity: 15.09.2018 | 12:55:41
Last activity: 15.09.2018 | 12:55:41
Status
State: New
Classification: Not set
Assigned to: Not assigned
Description
WMI can be used by attackers to execute commands on remote machines and eventually take control of it. This allows attackers to gather information about the internal network, access additional resources, steal credentials and elevate their permissions in order to reach their desired assets.
Recommended actions
1. Find the propagation entry point - check which users were logged on to this machine and which other machines they were observed on to find additional compromised machines
2. Gather information - analyze the executed process and if possible block it from running on any machines in the organization.
Show more
Alert process tree
System
smss.exe
VirusTotal detection ratio: 1/66
smss.exe
VirusTotal detection ratio: 1/66
winlogon.exe
https://securitycenter.windows.com/investigation/5
WMIC.exe
Execution details
Execution time: 15.09.2018 | 12:55:40
Path: C:\Windows\SysWOW64\wbem
User: CONTOSO\Emma.Battle
Access privileges (UAC): Restricted
Integrity level: Medium
Process ID: 5460
Command line:
"WMIC.exe" /node:"SummerB-PC" process call create "c:\windows\system32\rundll32.exe C:\\windows\\Service.dll M10"
File details
SHA1: c902cef254ed2423bc2
SHA256: c4639422cf50ee039dc
MD5: 08bae6a2086c7c99397
Signer: INVALID: Microsoft Windows
Issuer: INVALID: Microsoft Development PCA 2014
Detections

# Suspicious Remote WMI Execution

Investigation #5 is complete - Remediated

Started
Sep 15, 20
18, 2:33:1
9 PM

Ended
Sep 1 20
18, 3:3 :5
0 PM

Complete

Total pending time: 44:17m

Comments (2)

## Investigation details

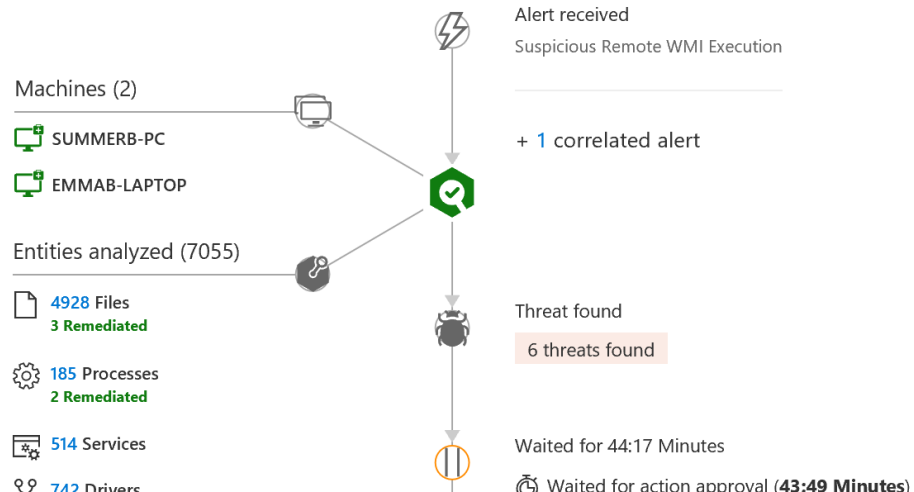
Status
Remediated
Malicious entities found were succe ssfully remediated.

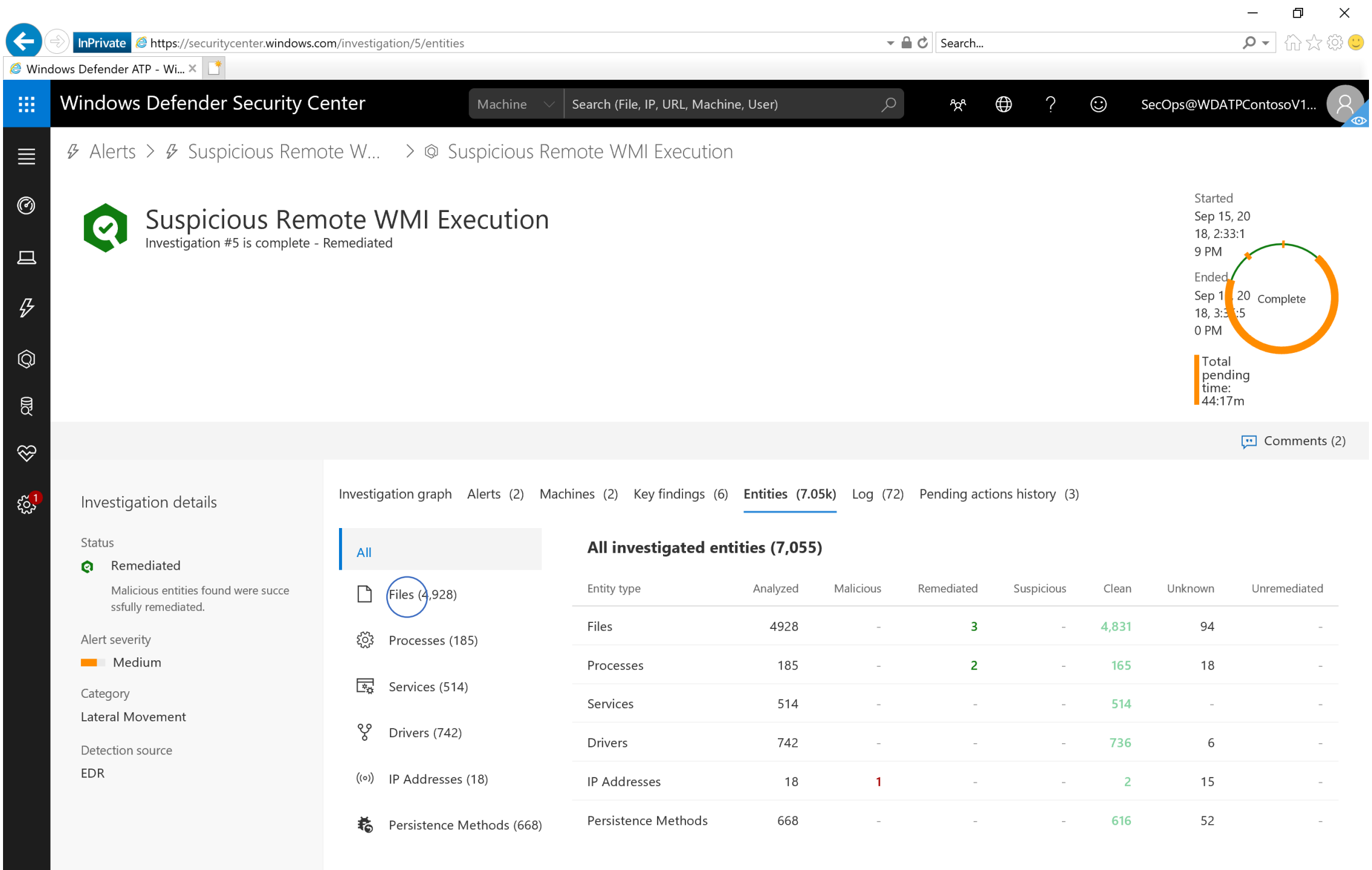
Alert severity
Medium

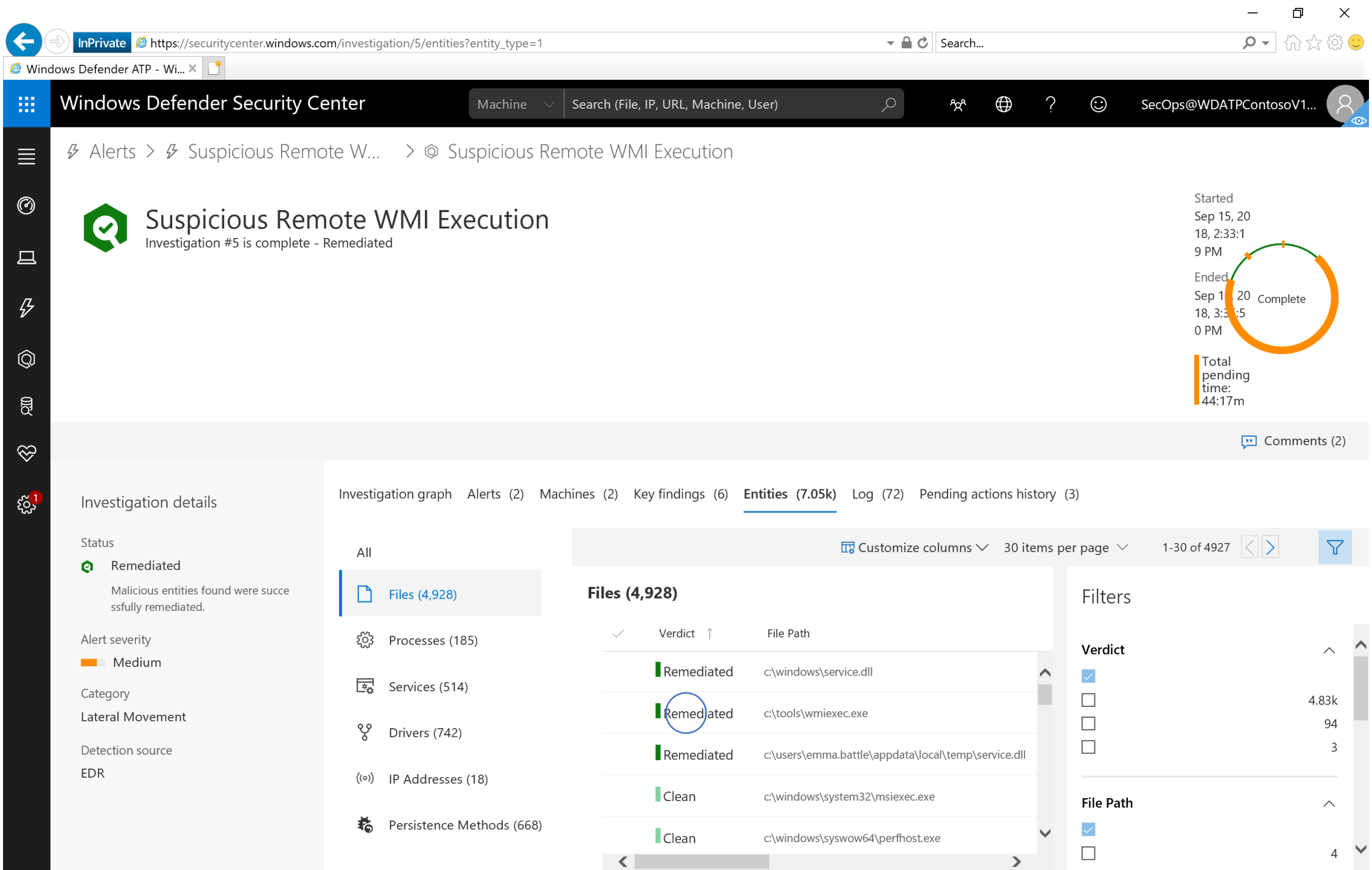
Category
Lateral Movement

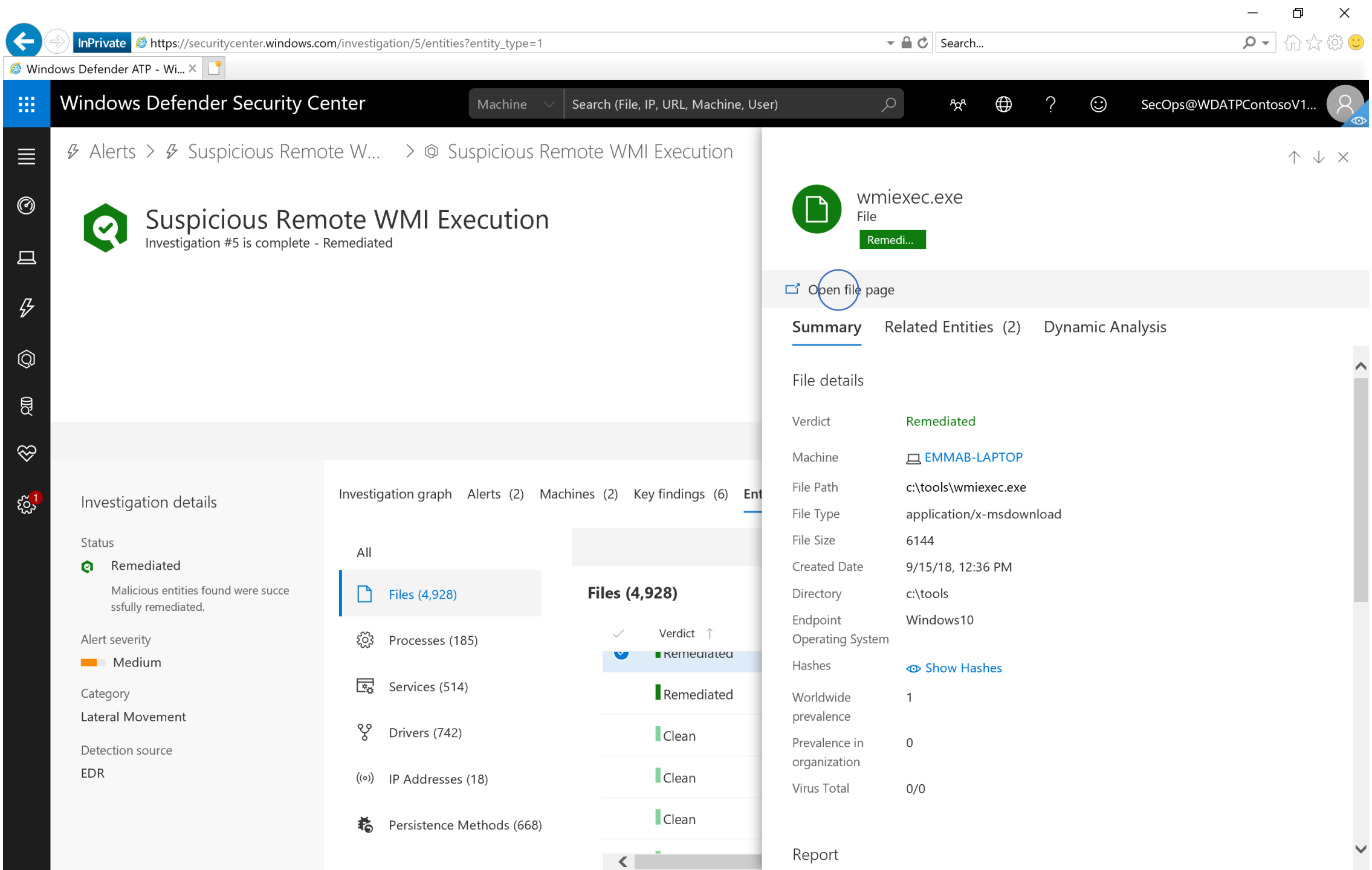
Detection source
EDR

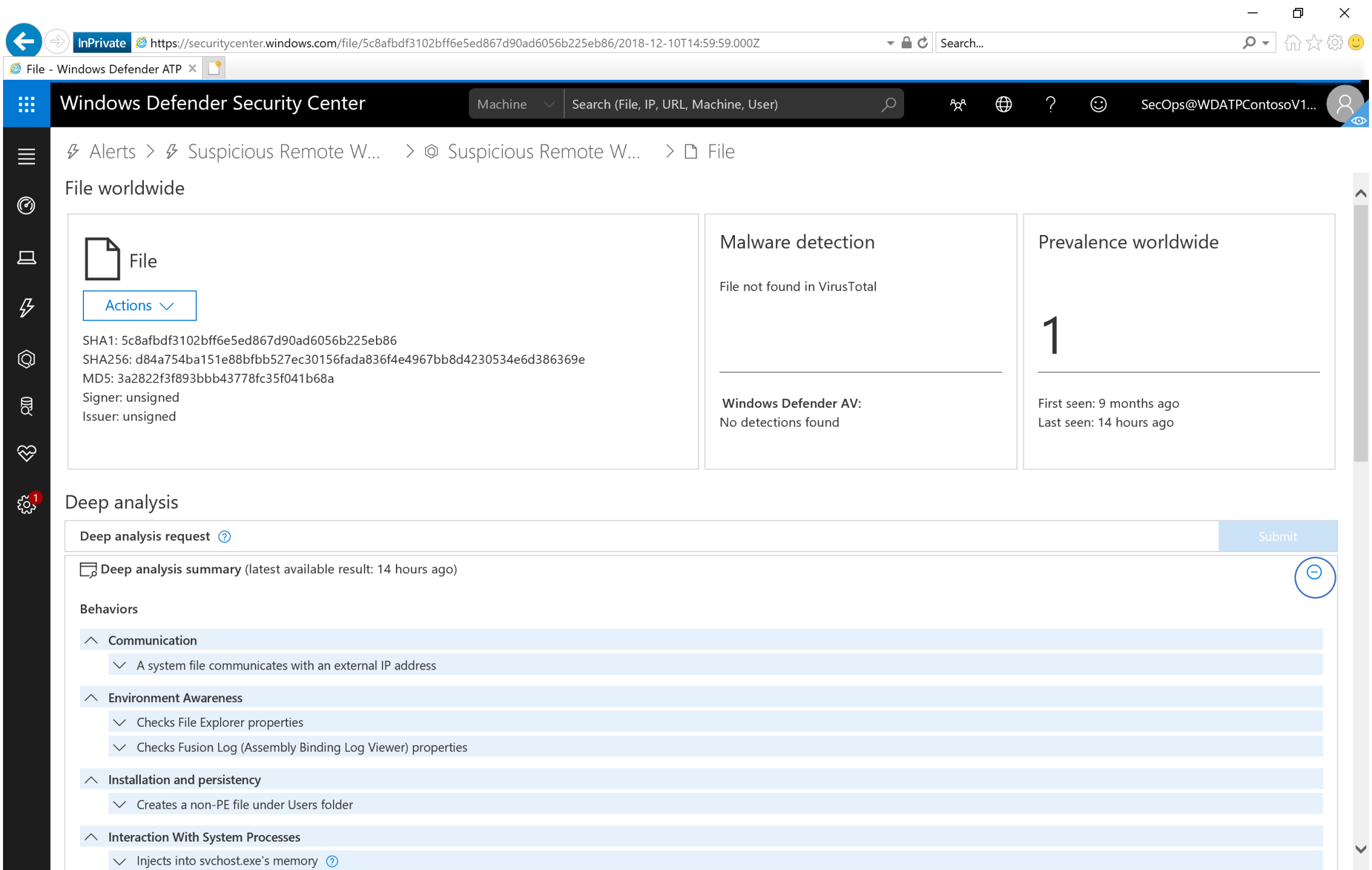
Investigation graph | Alerts (2) | Machines (2) | Key findings (6) | Ent .05k) | Log (72) | Pending actions history (3)




InPrivate
https://securitycenter.windows.com/investigation/5/entities
Search...
Windows Defender ATP - Wi...
Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
Alerts > Suspicious Remote W... > Suspicious Remote WMI Execution
Suspicious Remote WMI Execution
Investigation #5 is complete - Remediated
Started
Sep 15, 20
18, 2:33:1
9 PM
Ended
Sep 1 20
18, 3:
0 PM
Complete
Total pending time: 44:17m
Comments (2)
Investigation details
Status
Remediated
Malicious entities found were succe ssfully remediated.
Alert severity
Medium
Category
Lateral Movement
Detection source
EDR
Investigation graph
Alerts (2)
Machines (2)
Key findings (6)
Entities (7.05k)
Log (72)
Pending actions history (3)
All
Files (4,928)
Processes (185)
Services (514)
Drivers (742)
IP Addresses (18)
Persistence Methods (668)
All investigated entities (7,055)
Entity type
Analyzed
Malicious
Remediated
Suspicious
Clean
Unknown
Unremediated
Files 4928 - 3 - 4,831 94 -
Processes 185 - 2 - 165 18 -
Services 514 - - - 514 - -
Drivers 742 - - - 736 6 -
IP Addresses 18 1 - - 2 15 -
Persistence Methods 668 - - - 616 52 -


InPrivate
https://securitycenter.windows.com/investigation/5/entities?entity_type=1
Search...
Windows Defender ATP - Wi...
Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
Alerts > Suspicious Remote W... > Suspicious Remote WMI Execution
Suspicious Remote WMI Execution
Investigation #5 is complete - Remediated
Started
Sep 15, 20
18, 2:33:1
9 PM
Ended
Sep 1 20
18, 3:
0 PM
Complete
Total pending time: 44:17m
Comments (2)
Investigation details
Status
Remediated
Malicious entities found were succe ssfully remediated.
Alert severity
Medium
Category
Lateral Movement
Detection source
EDR
Investigation graph
Alerts (2)
Machines (2)
Key findings (6)
Entities (7.05k)
Log (72)
Pending actions history (3)
All
Files (4,928)
Processes (185)
Services (514)
Drivers (742)
IP Addresses (18)
Persistence Methods (668)
Customize columns
30 items per page
1-30 of 4927
Files (4,928)
Verdict
File Path
Remediated
c:\windows\service.dll
Remediated
c:\tools\wmiexec.exe
Remediated
c:\users\emma.battle\appdata\local\temp\service.dll
Clean
c:\windows\system32\msiexec.exe
Clean
c:\windows\syswow64\perfhost.exe
Filters
Verdict
4.83k
94
3
File Path
4


InPrivate
https://securitycenter.windows.com/investigation/5/entities?entity_type=1
Search...
Windows Defender ATP - Wi...
Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
Alerts
Suspicious Remote W...
Suspicious Remote WMI Execution
Suspicious Remote WMI Execution
Investigation #5 is complete - Remediated
wmiexec.exe
File
Remedi...
Open file page
Summary
Related Entities (2)
Dynamic Analysis
File details
Verdict
Remediated
Machine
EMMAB-LAPTOP
File Path
c:\tools\wmiexec.exe
File Type
application/x-msdownload
File Size
6144
Created Date
9/15/18, 12:36 PM
Directory
c:\tools
Endpoint Operating System
Windows10
Hashes
Show Hashes
Worldwide prevalence
1
Prevalence in organization
0
Virus Total
0/0
Report
Investigation details
Status
Remediated
Malicious entities found were succe ssfully remediated.
Alert severity
Medium
Category
Lateral Movement
Detection source
EDR
Investigation graph
Alerts (2)
Machines (2)
Key findings (6)
All
Files (4,928)
Processes (185)
Services (514)
Drivers (742)
IP Addresses (18)
Persistence Methods (668)
Files (4,928)
Verdict
Remediated
Remediated
Clean
Clean
Clean


InPrivate
https://securitycenter.windows.com/file/5c8afbdf3102bff6e5ed867d90ad6056b225eb86/2018-12-10T14:59:59.000Z
Search...
File - Windows Defender ATP
Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
SecOps@WDATPContosoV1...
Alerts
Suspicious Remote W...
Suspicious Remote W...
File
File worldwide
File
Actions
SHA1: 5c8afbdf3102bff6e5ed867d90ad6056b225eb86
SHA256: d84a754ba151e88bfbb527ec30156fada836f4e4967bb8d4230534e6d386369e
MD5: 3a2822f3f893bbb43778fc35f041b68a
Signer: unsigned
Issuer: unsigned
Malware detection
File not found in VirusTotal
Windows Defender AV:
No detections found
Prevalence worldwide
1
First seen: 9 months ago
Last seen: 14 hours ago
Deep analysis
Deep analysis request
Submit
Deep analysis summary (latest available result: 14 hours ago)
Behaviors
Communication
A system file communicates with an external IP address
Environment Awareness
Checks File Explorer properties
Checks Fusion Log (Assembly Binding Log Viewer) properties
Installation and persistency
Creates a non-PE file under Users folder
Interaction With System Processes
Injects into svchost.exe's memory

Windows Defender ATP가 여타 EDR 도구에 비해 **1.7배 더 많은 위협 감지**

Windows Defender ATP 덕분에 데이터 유출 위험 감소:
**40% 감소**

Windows Defender ATP가 최종 사용자에게 미치는 영향:
**위협 한 건당 4시간 절약**

# 인텔리전트 보안 기능을 활용한 사례

- Windows 10, Windows Defender ATP (Advanced Threat Protection) 도입
- 침해 위협 및 대응에 걸렸던 시간을 수 일에서 수 시간 이내로 줄임
- 수동적인 보안 대응에서 AI 기반의 능동적 대응으로 전환


Windows Defender ATP를 도입해,
PC에서의 공격 탐지 및 대응시간
현격히 감소

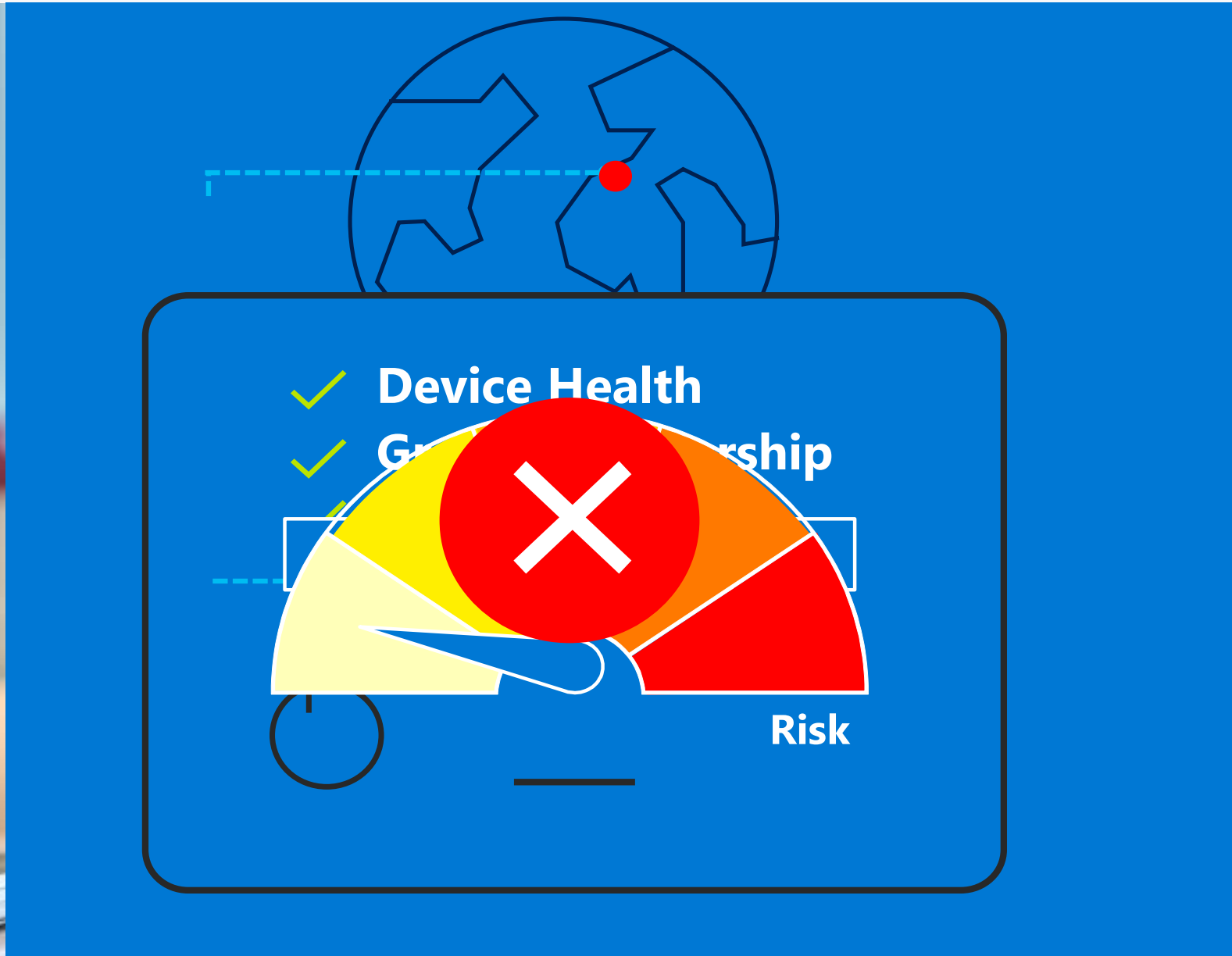
# Microsoft Intelligent Security Graph를 이용한 서비스

# 인증 및 접근통제 : 생체정보를 통한 보안

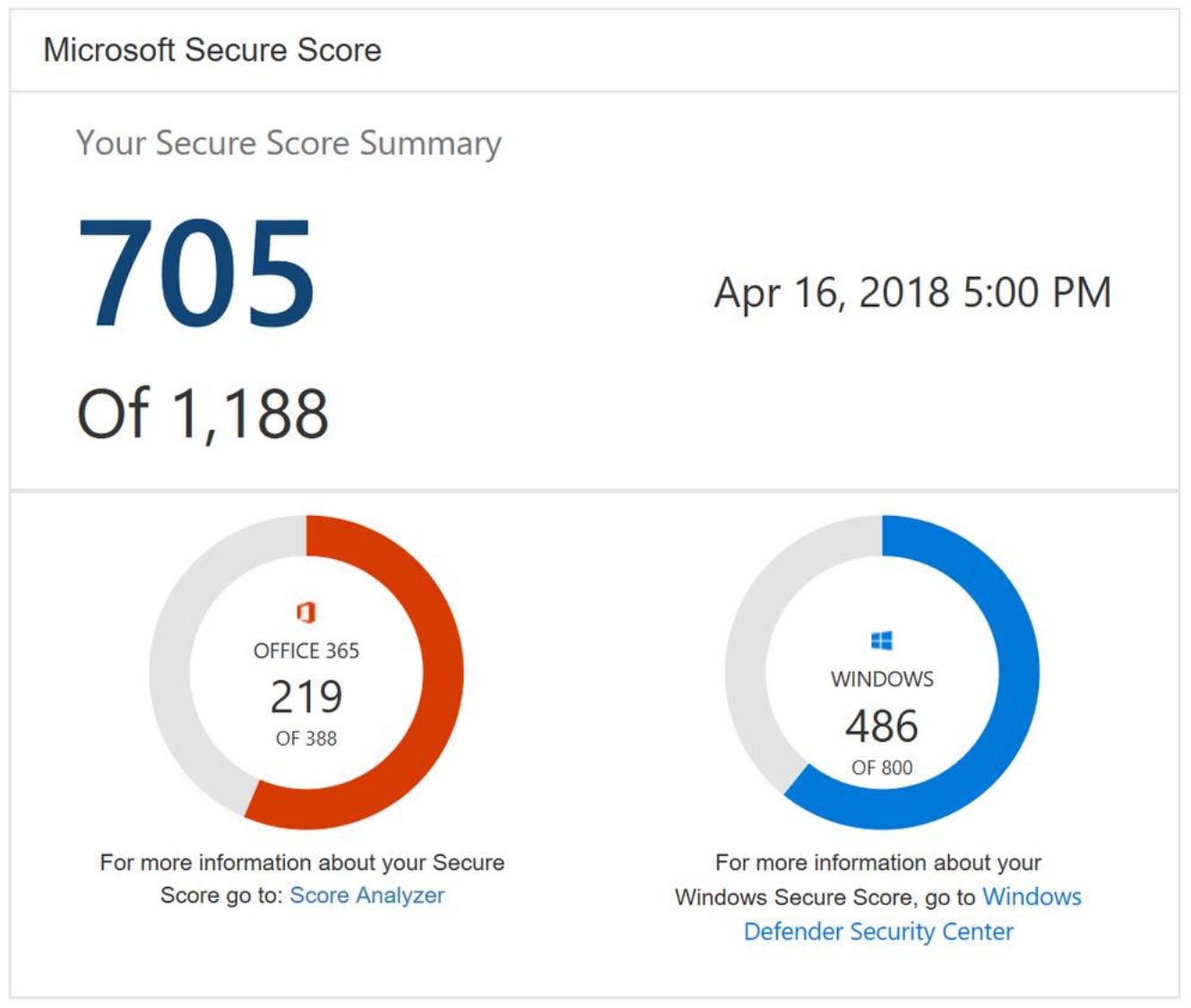





# 인증 및 접근통제 : Conditional Access

# Secure Score



# Built-in, not Bolt on

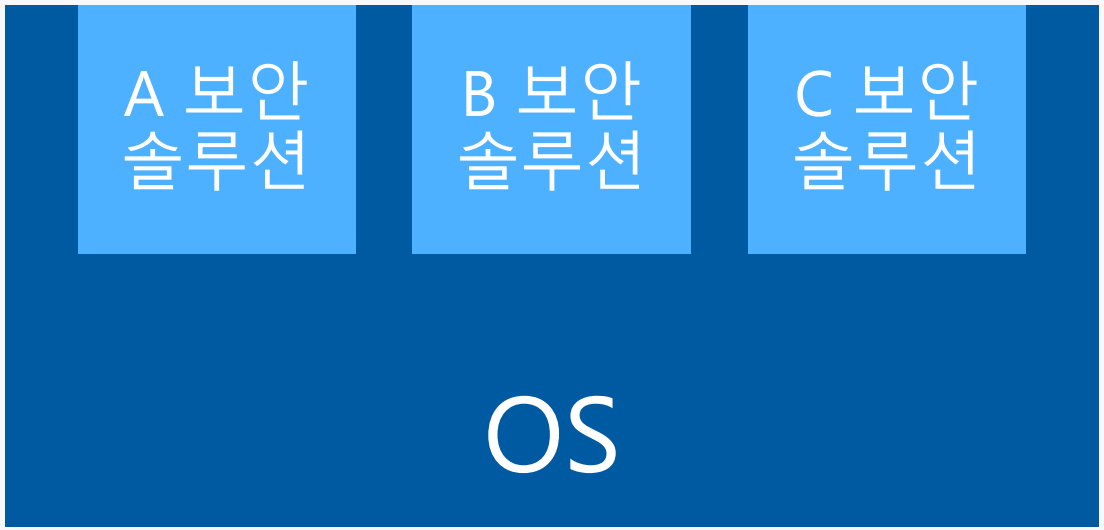

추가 보안 솔루션 구매

늦어지는 업데이트. 이로 인한 보안 위협 증가

수많은 보안 솔루션

새로운 보안 공격에 대한 취약

# Built-in, not Bolt on



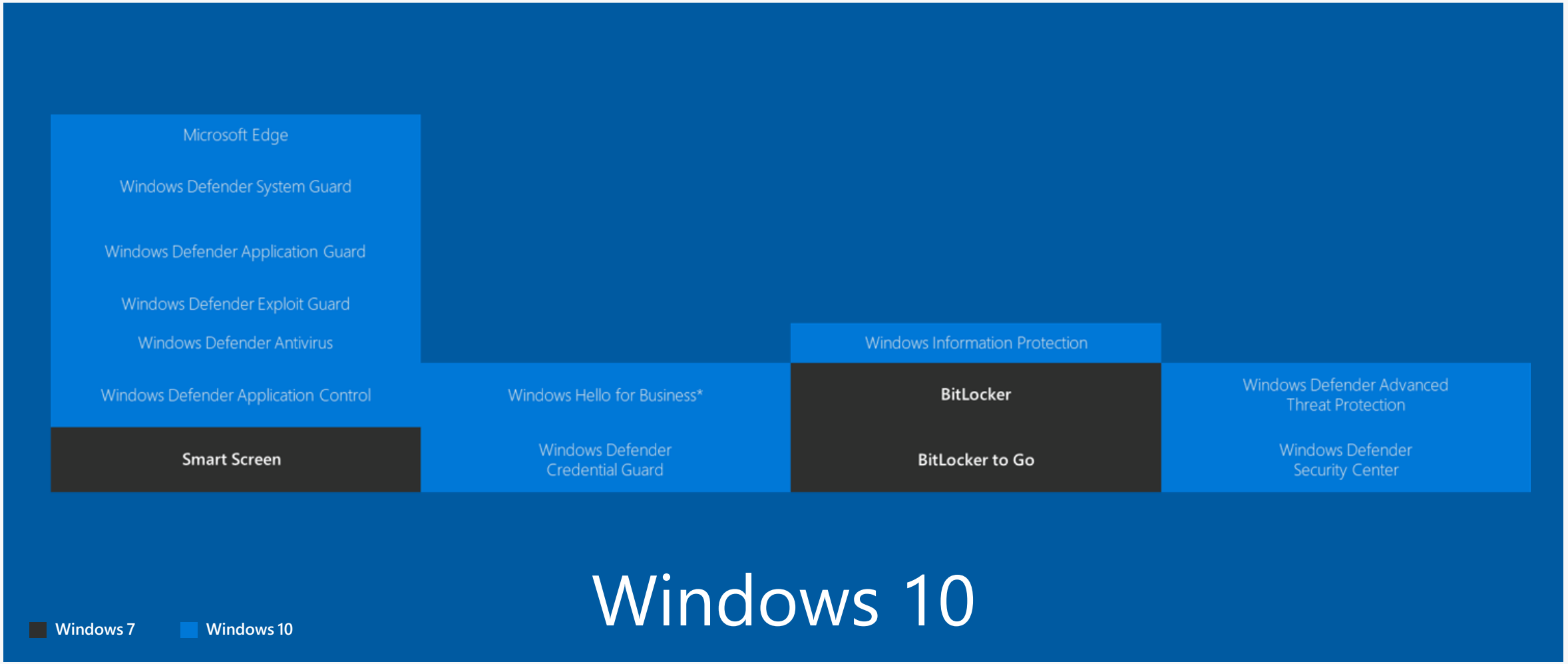

**추가 보안 솔루션의 구축 불필요**
End point 보안을 위한 추가 구축 또는 인프라가 필요 없음

**클라우드 기반의 업데이트**
Windows 10의 업데이트를 실시간 클라우드 기반으로 진행

**신경 써야 할 범위를 상당 줄임**
시스템 hardening을 통해서 보안위협을 상당 부분 없앰

**새로운 보안 플랫폼**
지능화 다양화해지는 공격에 대해 선제 대응

# Built-in, not Bolt on



# 보안 플랫폼 (Platform)

인증 및 접근보호

정보 보호

침해 방지

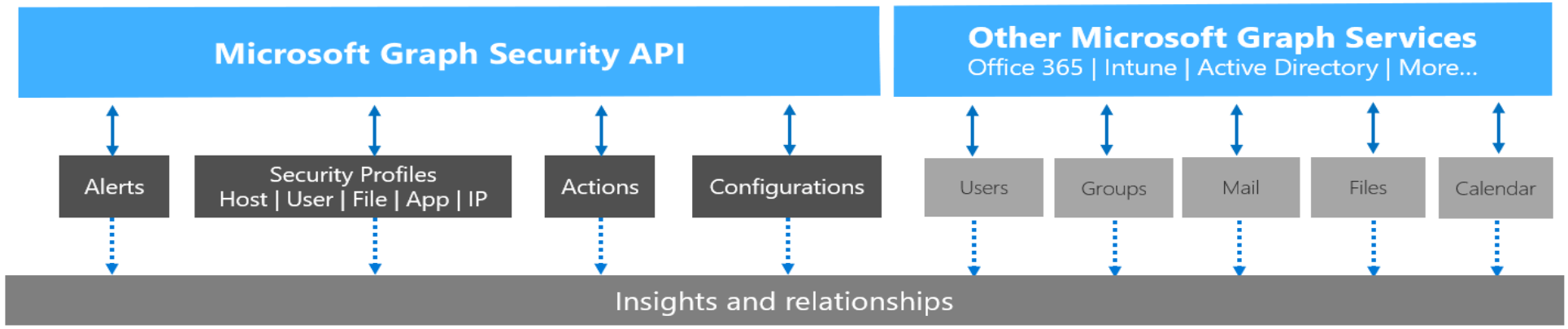
보안 관리

# 보안 플랫폼 (Platform)

**Security Providers**

Azure ATP | Azure AD Identity Protection | Windows Defender ATP | Azure Security Center | Office 365 ATP | Cloud Application Security | Azure Information Protection | Intune | Ecosystem Partners

**Data and Actions**




**Authentication & Authorization**

OAuth 2.0 and OpenID Connect 1.0

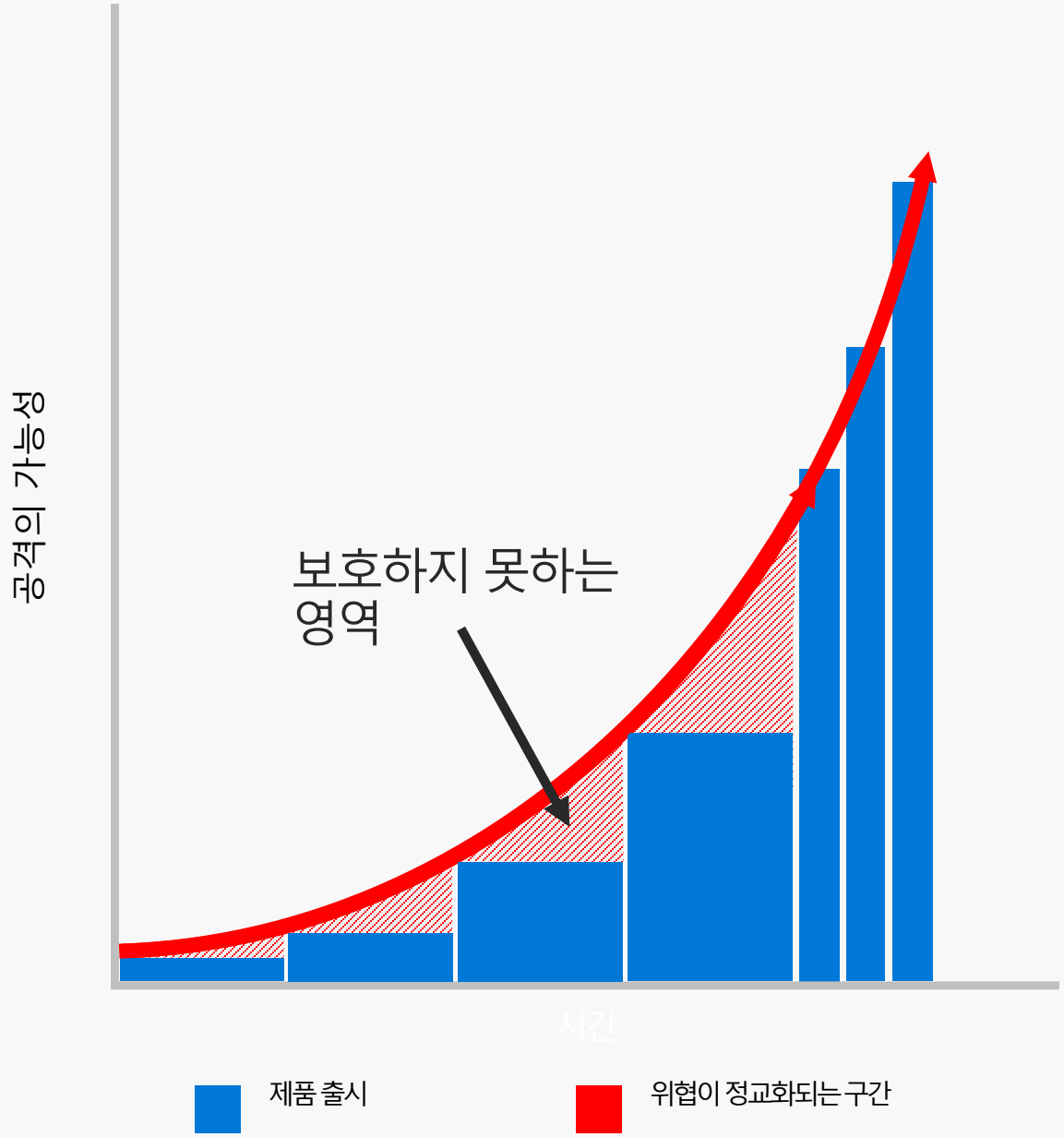
**Supported SDKs and Sample Code**

ASP.NET MVC | Xamarin | UWP | JavaScript | Angular | PHP | Android | iOS | Ruby | Python

# 안전한 보안의 시작은 안전한 OS로부터

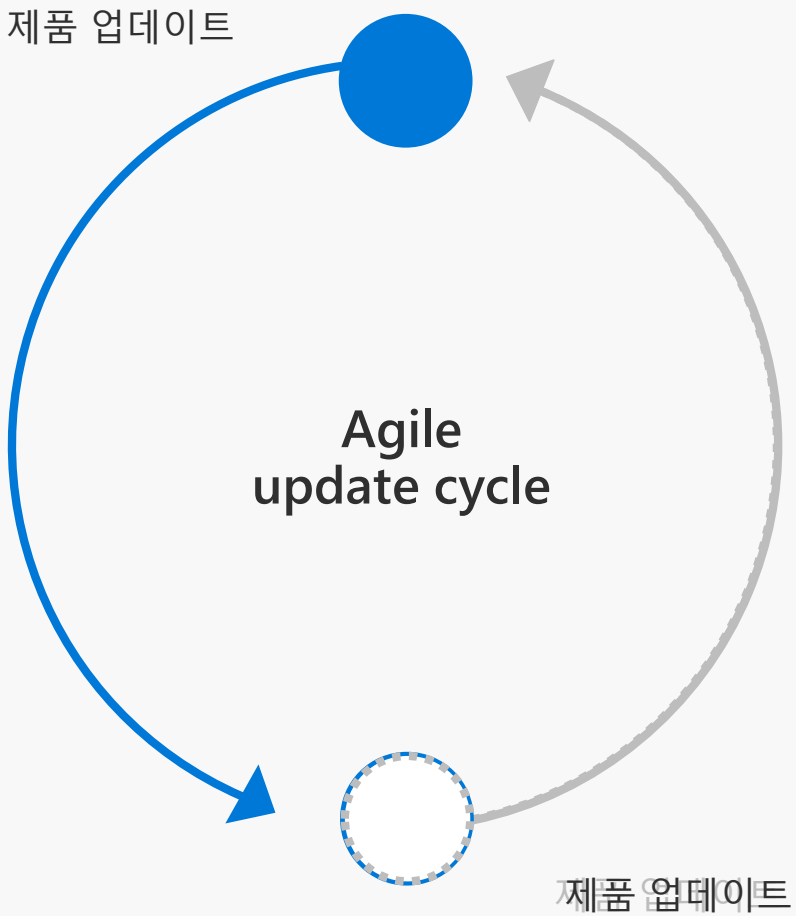
# 시간차를 두고 위협으로부터 보호

출시간격이 길수록
보호받지 못하는 영역 확대



# 항상 최신 업데이트

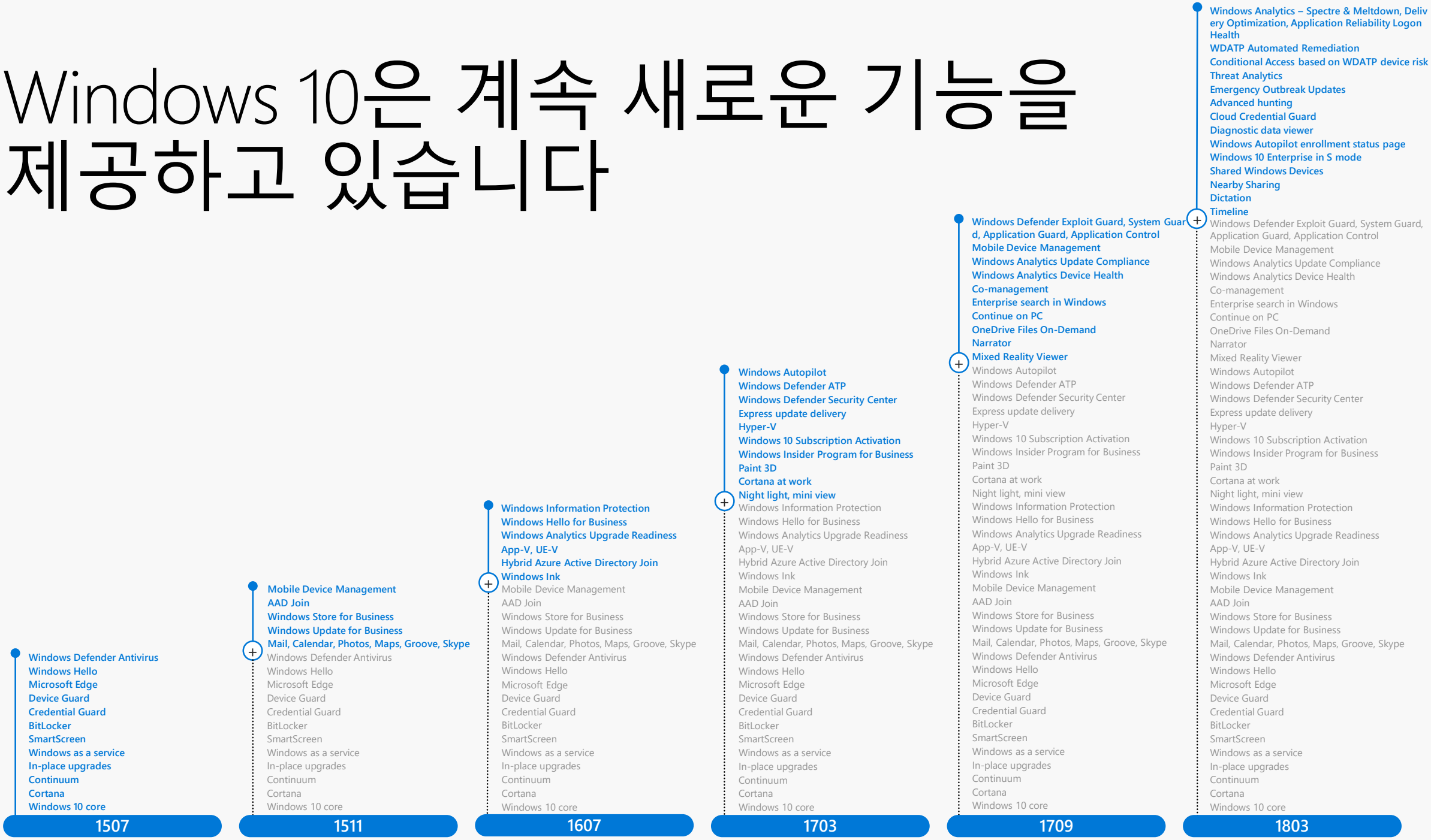
- 향상된 보안
- 향상된 생산성
- 단순화된 배포




매년 2회* (3월, 9월)

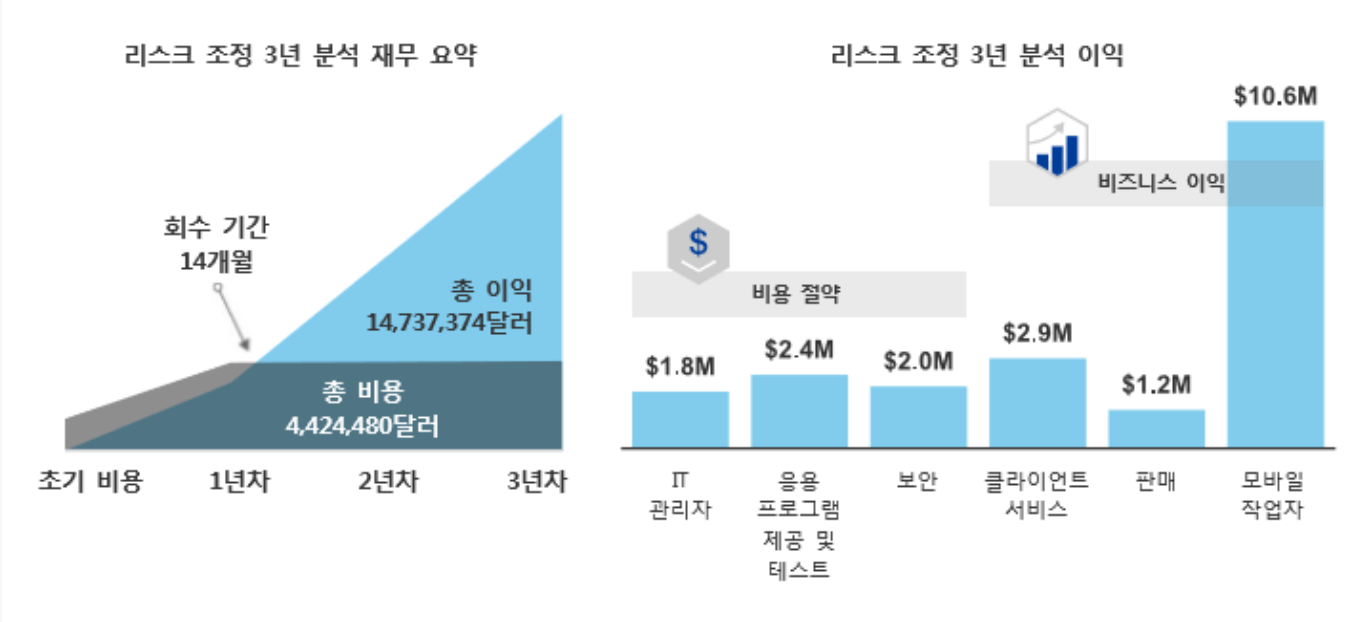
*For the supported lifetime of the device.

# Windows 10은 계속 새로운 기능을 제공하고 있습니다



# 안전한 Windows 10 도입에 따른 경제적 효과

> Forrester는 Windows 10를 사용하는 고객사와의 인터뷰를 통해 하나의 가상의 복합조직을 만들어, Windows 10을 사용함에 따른 도입효과를 산정하였습니다.




**14개월**
투자회수기간

**33%**
Windows 10 사용시 보안문제 감소 효과

**233%**
ROI

Source: "The Total Economic Impact™ Of Windows 10

# 보안과 생산성, 선택의 문제가 아닙니다.

생산성

보안

# 보안과 생산성은 모두 필수입니다.

# 질의 응답