

БИТВА ЗА ДОМЕН

PROTECT

DETECT

RESPOND

Windows Defender ATP

Unified platform for endpoint security

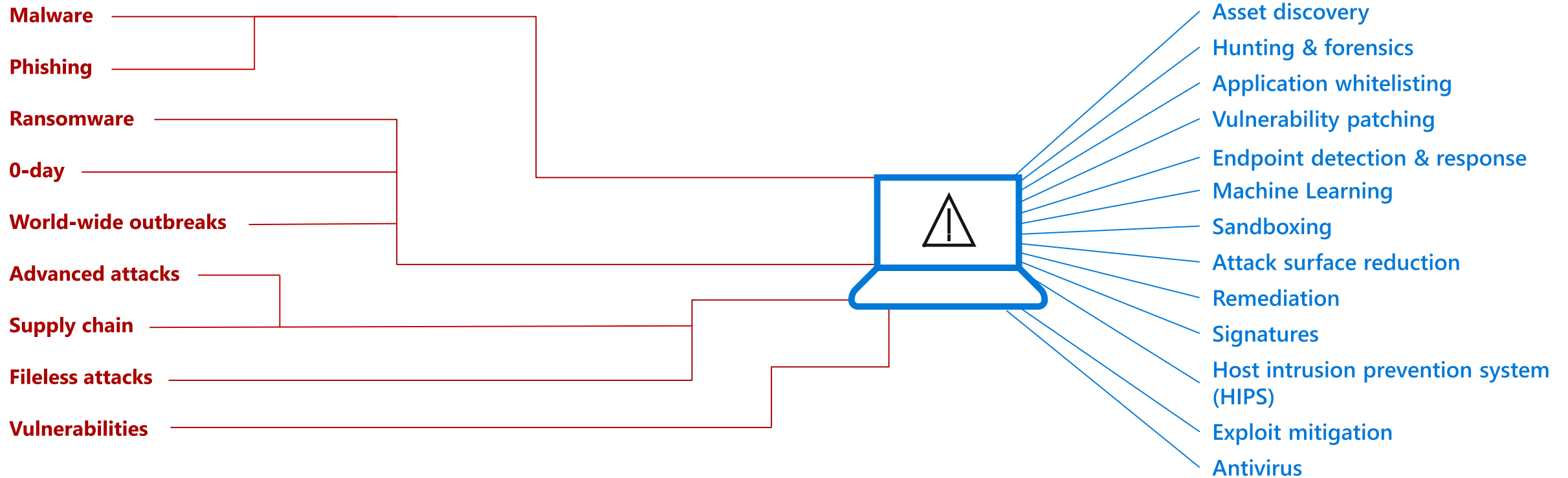
Дмитрий Узлов
Компания «ТЕХНОПОЛИС»

Protecting an endpoint is hard

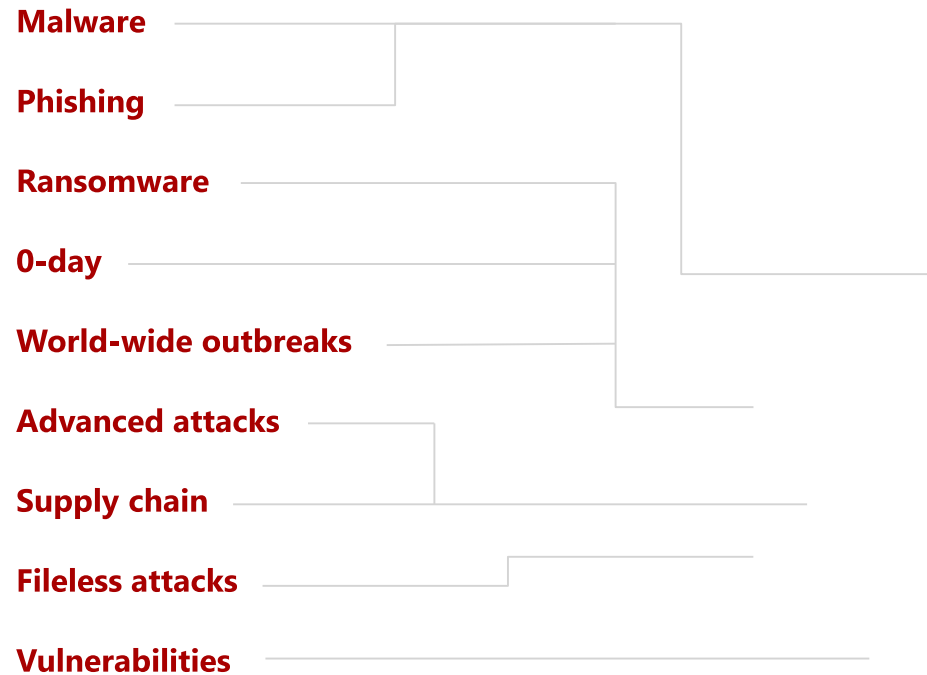
 **PERFORMANCE**
Hit on your endpoints

 **SECURITY TEAM**
Time and skills

 **COST**
Multiple solutions and on-prem infrastructure



Protecting an endpoint is was hard.



Windows Defender ATP

Built-in. Cloud-powered.





Windows Defender ATP

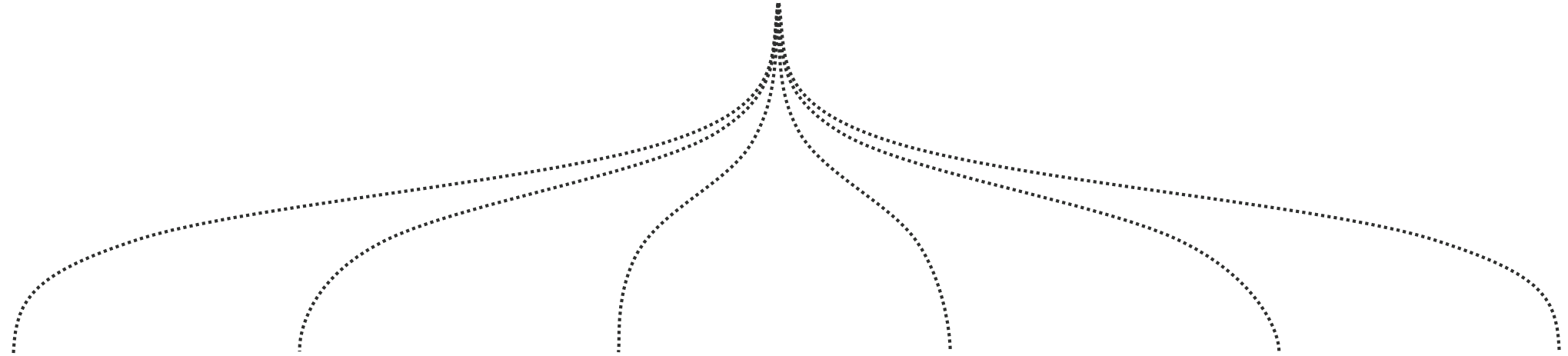
Built-in. Cloud-powered.

Trusted by IT. Loved by security teams.



Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations



NEXT GENERATION PROTECTION

Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks



AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



SECURITY POSTURE

Track and improve your organization security posture










ADVANCED HUNTING

Advanced threat hunting

Management and APIs

Platform coverage

Integrated configuration management in the cloud

CLIENT	SERVER	CROSS-PLATFORM
Windows 10	Server 2019	Mac (3rd party)   
Windows 8.1*	Server 2016	Linux (3rd party)   
Windows 7SP1*	Server 2012R2	Android, iOS (3rd party) 

Let's take a closer look



Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION
Resist attacks and exploitations



NEXT GENERATION PROTECTION
Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE
Detect, investigate, and respond to advanced attacks



AUTO INVESTIGATION & REMEDIATION
From alert to remediation in minutes at scale



SECURITY POSTURE
Track and improve your organization security posture



ADVANCED HUNTING
Advanced threat hunting

Management and APIs

Attack Surface Reduction

Resist attacks and exploitations



HW BASED ISOLATION

APPLICATION CONTROL

EXPLOIT PROTECTION

NETWORK PROTECTION

CONTROLLED FOLDER ACCESS

Isolate access to untrusted sites

Isolate access to untrusted Office files

Host intrusion prevention

Exploit mitigation

Ransomware protection for your files

Block traffic to low reputation destinations

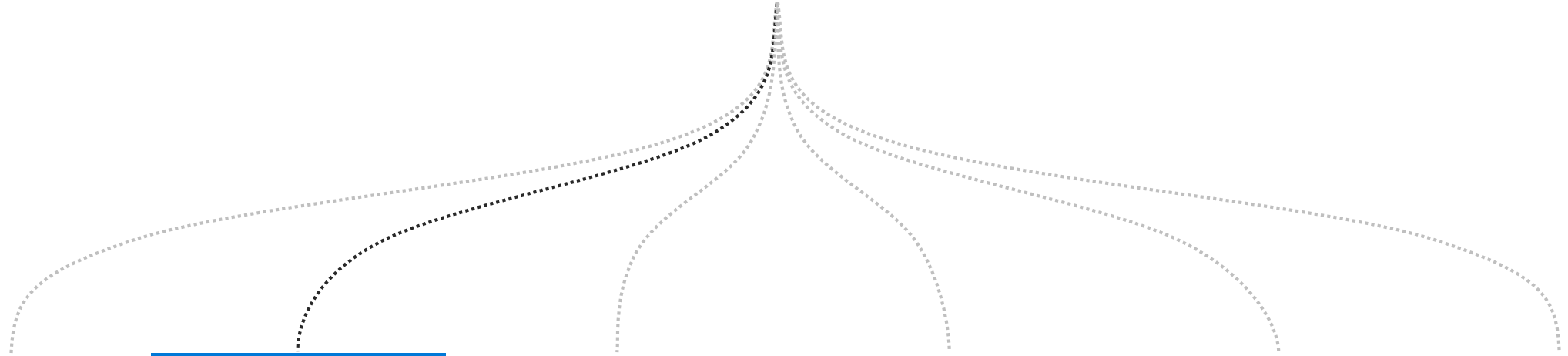
Protect your legacy applications

Only allow trusted applications to run



Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations



NEXT GENERATION PROTECTION

Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks



AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



SECURITY POSTURE

Track and improve your organization security posture





ADVANCED HUNTING

Advanced threat hunting

Management and APIs

Next generation protection

Protect against all types of emerging threats

Client  → Cloud 

Protection in milliseconds

Most common malware are blocked by high-precision detection in Windows Defender AV

Protection in milliseconds

ML-powered cloud rules evaluate suspicious files based on metadata sent by the Windows Defender AV client during query and make a determination

Protection in seconds

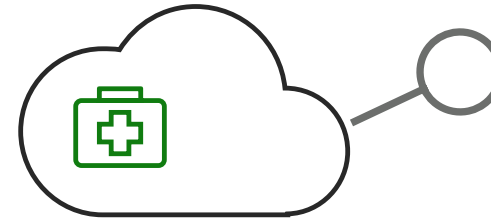
If needed a copy of the suspicious file is uploaded for inspection by multi-class ML classifiers

Protection in minutes

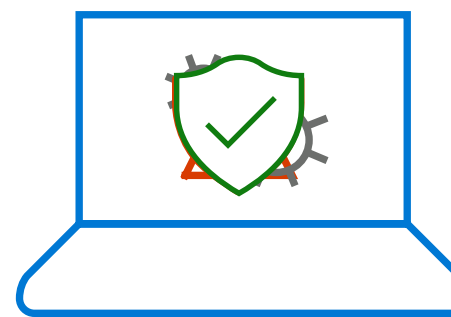
If additional checking is required the suspicious file is executed in a sandbox for dynamic analysis by multi-class ML classifiers

Protection in hours

The most advanced and innovative samples can be further checked against ML models and expert rules using correlated signals from a vast network of sensors to automatically classify threats



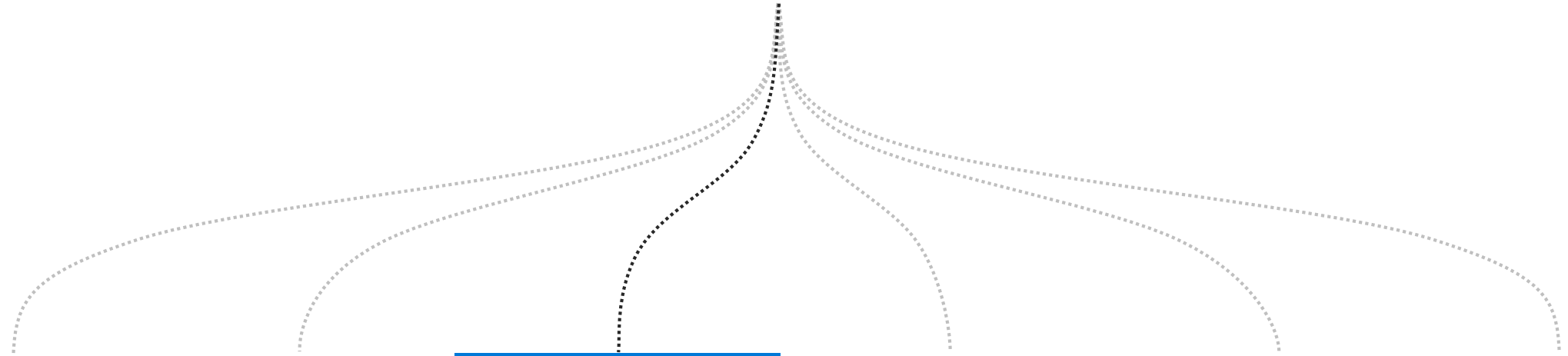
- Component 1
- Component 2





Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations



NEXT GENERATION PROTECTION

Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks



AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



SECURITY POSTURE

Track and improve your organization security posture



ADVANCED HUNTING

Advanced threat hunting

Management and APIs

Endpoint detection & response

Detect. Investigate.
Respond to advanced attacks.

Client 

Deep OS recording sensor

Cloud 

Machine learning, behavioral
& anomaly detection

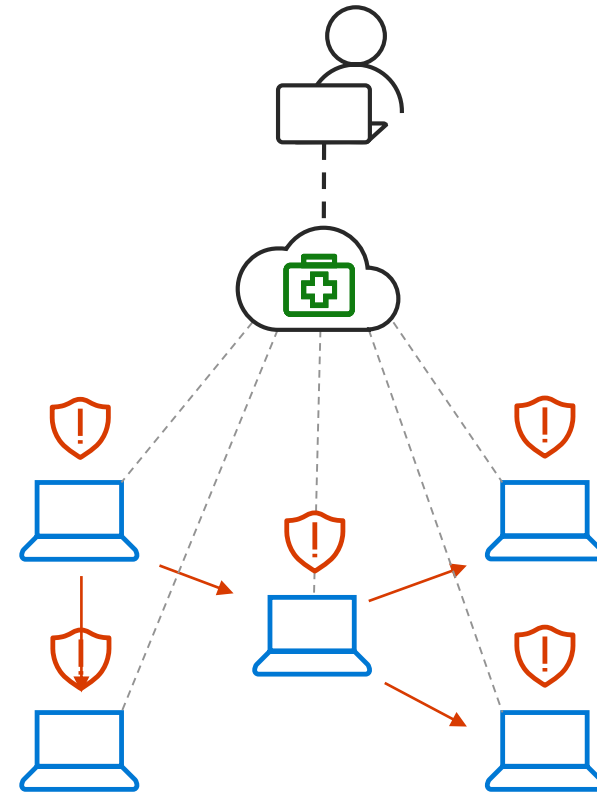
Response and containment

Sandbox analysis

Rich investigation across machines,
files, users, IPs, URLs

Realtime and historical
threat hunting

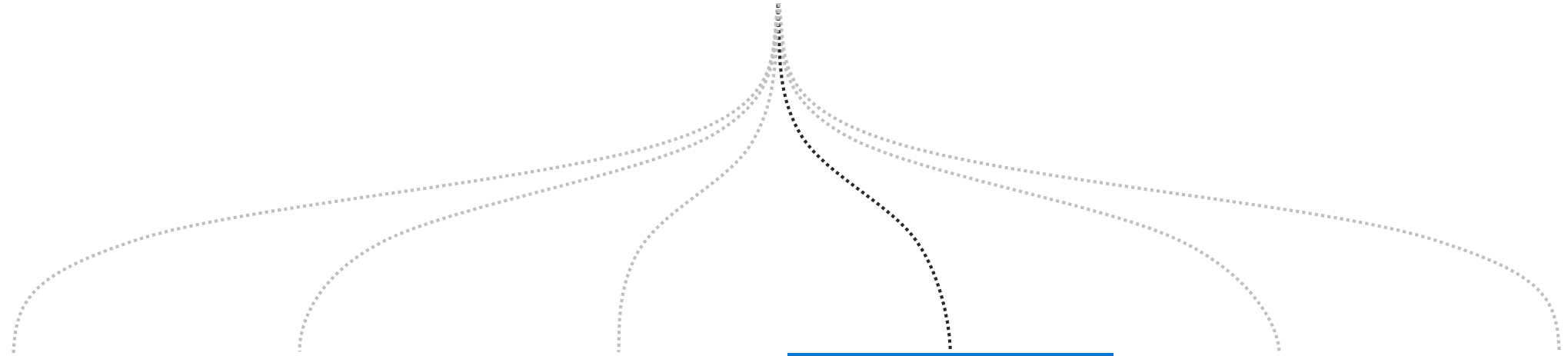
Threat intelligence and
custom detections





Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations



NEXT GENERATION PROTECTION

Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks



AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



SECURITY POSTURE

Track and improve your organization security posture



ADVANCED HUNTING

Advanced threat hunting

Management and APIs

Automated investigation & remediation

From alert to remediation in minutes at scale

Client 

Forensic collector

Response orchestrator

Cloud 

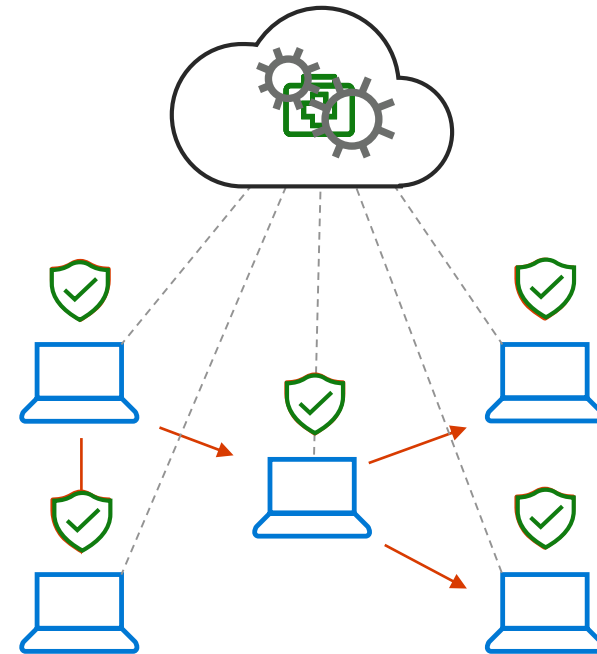
Historical endpoint data

Response orchestration

AI-based response playbooks

File/IP reputation

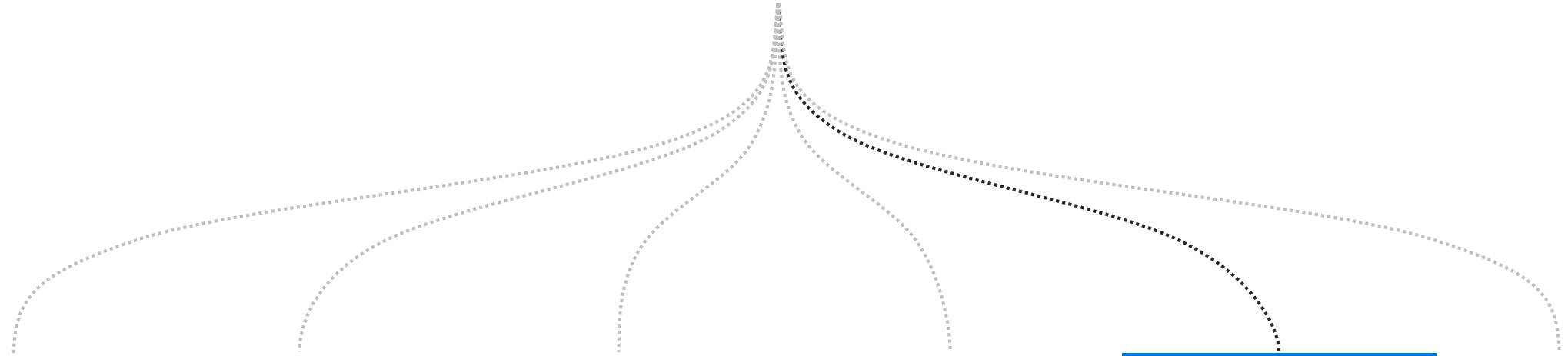
Sandbox





Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations



NEXT GENERATION PROTECTION

Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks



AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



SECURITY POSTURE

Track and improve your organization security posture



ADVANCED HUNTING

Advanced threat hunting

Management and APIs

Security posture

Understand and improve your organization security posture

Asset inventory

Identify unprotected systems

Recommended improvement actions

Prioritize your next steps

Threat to posture view

The screenshot displays the Windows Defender Security Center interface. The main content area is titled "Threat analytics" and features a detailed view for the "Ursnif (Gozi) trojan".

Overview: The threat is identified as "Ursnif (Gozi) trojan". An executive summary states: "Ursnif, also known as Gozi, is a banking trojan that has been active for over a decade. Apart from stealing banking credentials, it also attempts to collect credentials for cloud storage, webmail, and cryptocurrency exchanges. To do this, it takes screenshots, logs keystrokes, and exfiltrates certificates. Ursnif often deploys anti-VM technologies to evade antivirus scanners and stifle attempts to use virtualized detonation environments. To distribute Ursnif, its operators use creative and frequently changing phishing lures. Campaign emails look like reply emails and are sent to highly targeted subjects. While Ursnif operators incorporate many innovative social engineering and anti-analysis techniques, their campaigns rely heavily on macro malware embedded in Office documents—a vector that is shared by many malware campaigns and can be mitigated by commonly available tools."

Analysis: A flow diagram illustrates the attack path: "Social engineering" leads to an "Email with document", which contains a "Malicious document". This document is "User-enabled macro code" that executes "PowerShell" commands, leading to the "Ursnif" trojan. A "Download" icon is also shown.

Machines with alerts: A donut chart shows 0 machines with alerts. Legend: Active [0], Resolved [0].

Mitigation status: A donut chart shows 20 machines. Legend: Mitigated [0], Unmitigated [18], Unavailable [2].

Mitigation recommendations: The recommendation is to "Update to threat definition version 1.269.807.0 or later" and to "Turn on cloud-delivered protection and automatic sample submission".

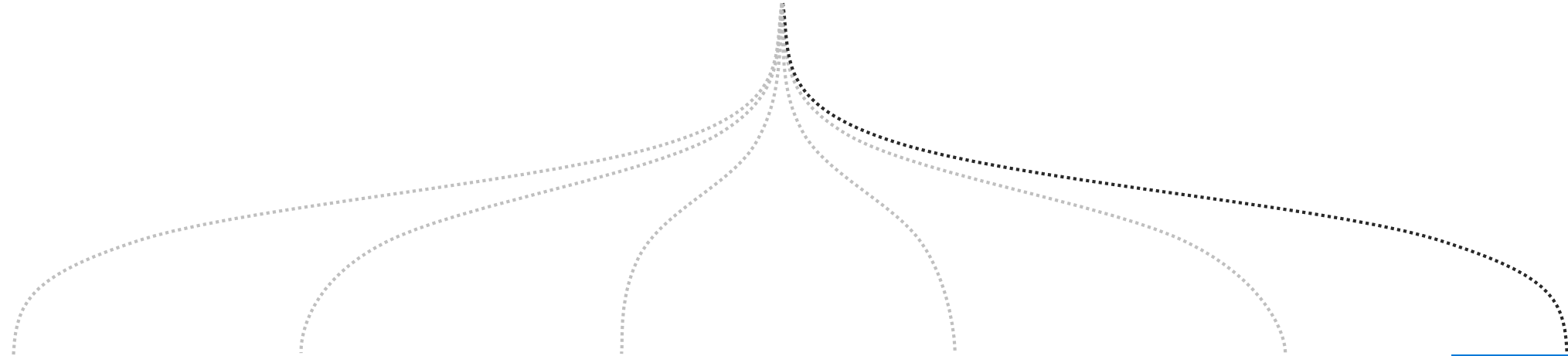
Threat List (Left Panel):

- Ursnif (Gozi) trojan**
Last updated: Sep 15, 2018, 5:50:00 AM
Published: Sep 15, 2018, 4:24:51 AM
0/0
- Emotet distributes Trickbot**
Last updated: Sep 14, 2018, 11:37:00 PM
Published: Jul 23, 2018, 4:13:41 AM
1/2
- ALPC local privilege elevation**
Last updated: Sep 13, 2018, 12:45:26 AM
Published: Aug 31, 2018, 1:47:41 AM
0/0
- Remote Manipulator System**
Last updated: Sep 6, 2018, 10:55:57 AM
Published: Sep 5, 2018, 1:52:06 PM
0/0
- Gadolinium targets Cambodian votes**
Last updated: Aug 30, 2018, 4:04:00 PM
Published: Jul 23, 2018, 3:17:50 AM
0/0
- Samas ransomware**
Last updated: Aug 27, 2018, 7:00:00 AM
Published: Aug 27, 2018, 11:46:41 AM
0/0
- AngelWind SQL mining**
Last updated: Aug 11, 2018, 7:04:24 AM
Published: Aug 10, 2018, 2:31:58 AM
0/0
- Leafminer**
Last updated: Aug 4, 2018, 3:15:04 AM
Published: Aug 1, 2018, 1:48:04 AM
0/0
- Orangeworm targets healthcare**
Last updated: Aug 1, 2018, 12:26:00 PM
Published: Jul 31, 2018, 12:26:05 PM
0/0



Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations



NEXT GENERATION PROTECTION

Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks



AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



SECURITY POSTURE

Track and improve your organization security posture



ADVANCED HUNTING

Advanced threat hunting

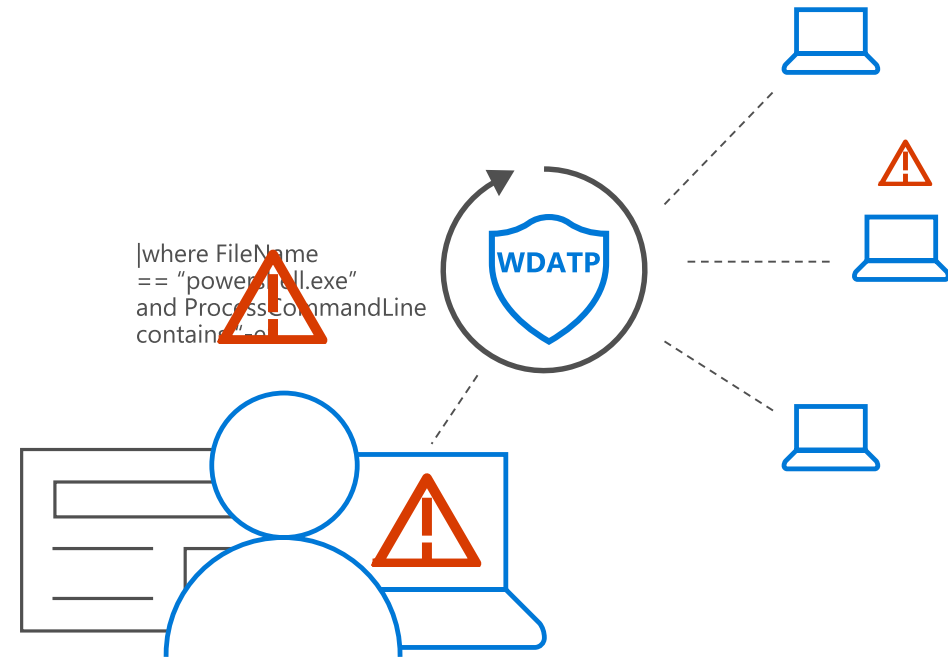
Management and APIs

Custom TI detection and advanced hunting

Sec ops reads about a new threat they heard from insider in same vertical

They use advanced hunting to create a query for detection

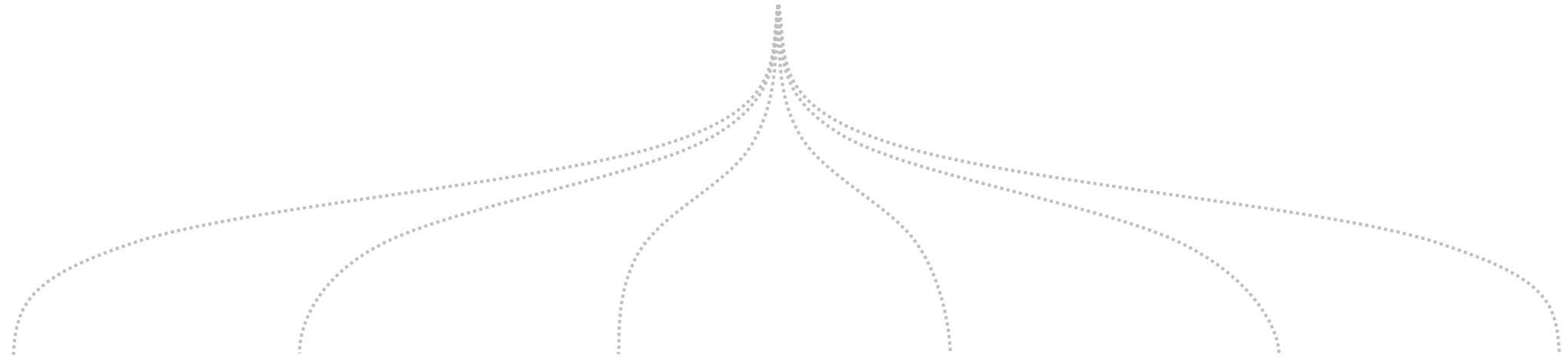
Windows Defender ATP will continue to run custom detection logic automatically and will alert Sec Ops if a detection is found





Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations



NEXT GENERATION PROTECTION

Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks



AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



SECURITY POSTURE

Track and improve your organization security posture



ADVANCED HUNTING

Advanced threat hunting

Management and APIs

Security management

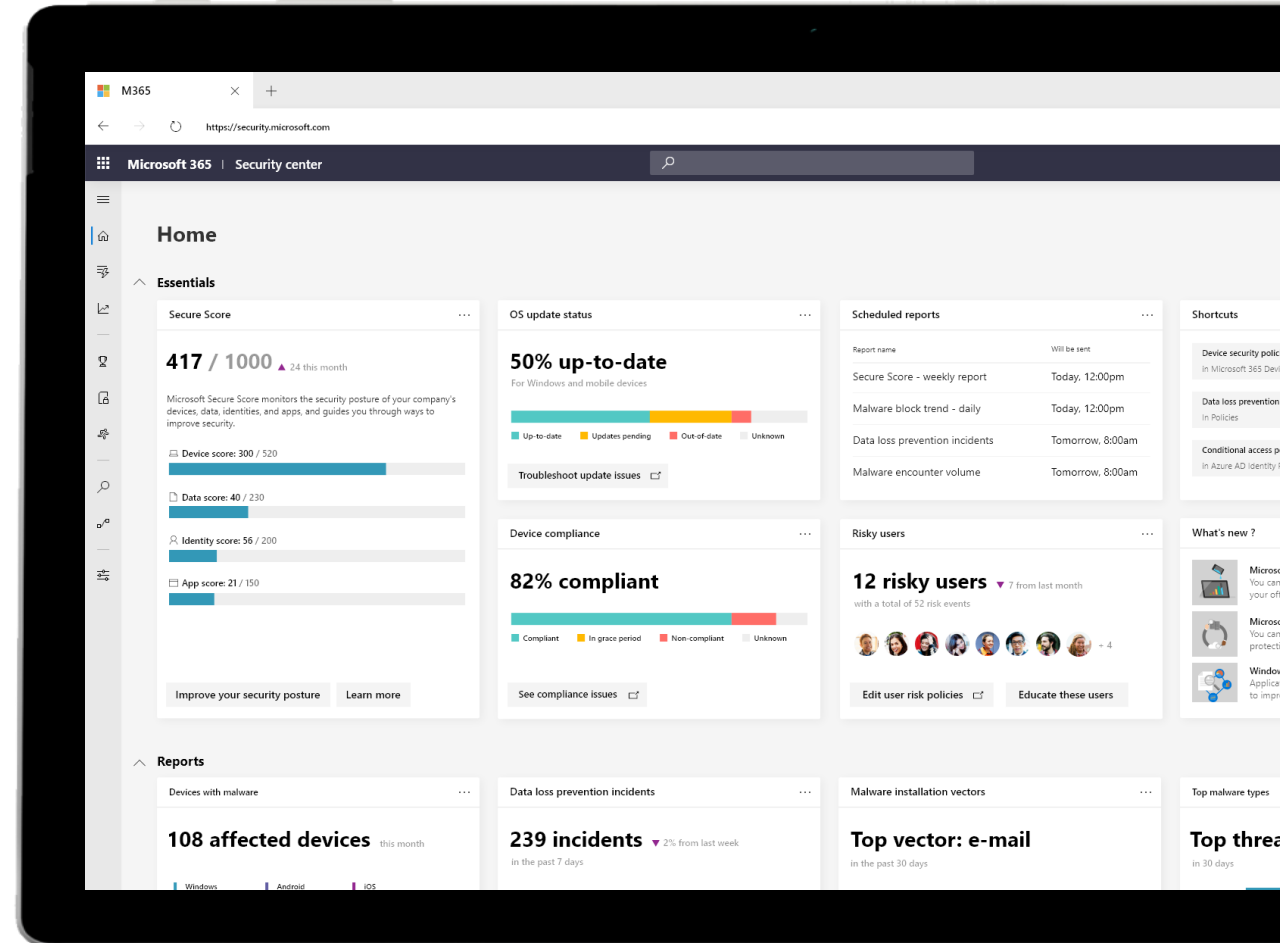
Understand what is happening, has happened and prepare for the future

Dashboards and trends

Threat monitoring

Threat reporting

Configuration management



APIs

Customize and enhance your data

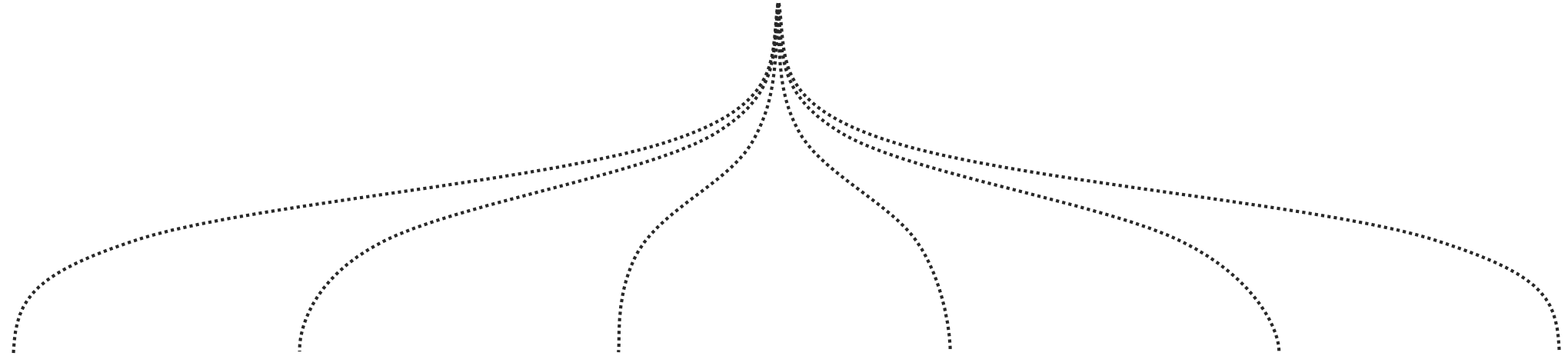


- AUTOMATE YOUR OWN WORKFLOWS
- INTEGRATE YOUR EXISTING SOLUTIONS
- QUERY DATA
- DRIVE REMEDIATION ACTIONS
- CREATE CUSTOM DETECTIONS



Windows Defender ATP

Built-in. Cloud-powered.



ATTACK SURFACE REDUCTION

Resist attacks and exploitations



NEXT GENERATION PROTECTION

Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks



AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



SECURITY POSTURE

Track and improve your organization security posture

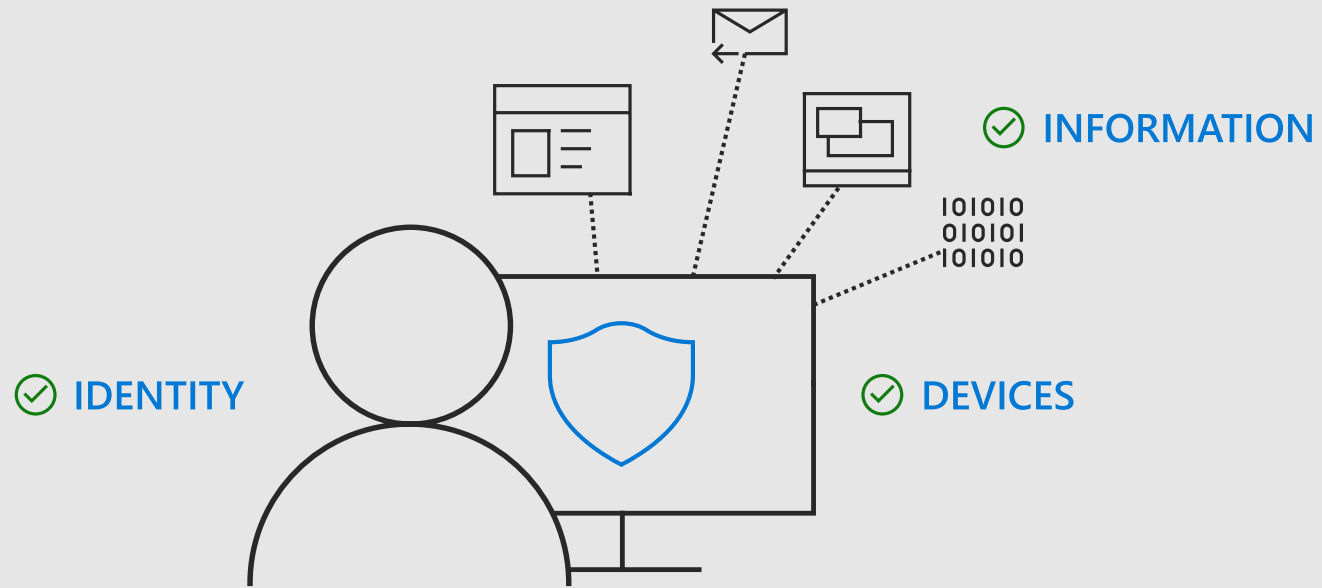


ADVANCED HUNTING

Advanced threat hunting

Management and APIs

There is more...



Microsoft Threat Protection

Detection

Active Incidents

27 active incidents Updated 6:20 pm today

High (4) | Medium (16) | Low (7)

Incident name	Severity	Last activity
Golden ticket compromise	High	June 18, 2018 11:12 AM
Phishing email campaign detected	High	June 18, 2018 11:10 AM
Suspicious PowerShell Activity	High	June 18, 2018 11:07 AM
Phishing email campaign detected	High	June 18, 2018 10:56 AM
Insider threat identified – sensitive data	Medium	June 18, 2018 10:52 AM
Potential Dofoil activity – malicious C2	Medium	June 18, 2018 10:50 AM
Windows Defender AV detected an active 'Azden' malware	Medium	June 18, 2018 11:12 AM
Windows Defender AV detected 'Reimage' unwanted software	Medium	June 18, 2018 11:11 AM

[Show more](#)

Identity protection

Users with threat detections

Updated 6:20 pm today

User	Alerts
Jesse Wallin	56
Robin Goolsby	45
Eva Macias	32
Jonathan Wolcott	27
Rex Fredrickson	16
Donovan Eagle	15
Jess Passmore	8
Antoine Hindman	4
Wayne Wallin	2

[Show more](#)

Device protection

34 devices at risk / 1,254

Updated 6:20 pm today

Device	Risk score
RDP_SRV_10	High
RDP_SRV_5	High
FIN_SRV_HQ	High
DC_SRV_US	High
cont-evamacias	High
cont-jonathanwolcott	High
cont-jesswallin	Medium
RDP_SRV_25	Medium
RDP_SRV_25	Medium

[See more](#)

Email protection

12 email accounts at risk / 1,022

Updated 6:20 pm today

Email account	User
---------------	------

Device threat analytics

Assess your defenses against high-profile threats

Updated 6:20 pm today

Get interactive reports on Windows Defender ATP about emerging threats

- Spectre and Meltdown: 23 active / 132
- Advanced Trojan Outbreak: 16 active / 182
- NotPetya: 13 active / 254
- Black Energy: 13 active / 142

Threat News

- "BadKitten" - New threat in town**
Check organization vulnerability
- Start hunting!**
GitHub shared new query

Prevention

Microsoft Secure Score

Secure score: 417 / 1000

Microsoft Secure Score monitors the security state of your company's devices, data, identities, apps, and Azure resources.

Category	Protected	Total
Devices	300	520
Data	40	230
Identity	36	100
Apps	21	150
Infrastructure	20	100

[Improve your security state](#) | [View history](#)

Device compliance

68% devices compliant

Of your 190k enrolled devices, 68% are compliant with the device compliance policies you created.

[View details in Device Management Admin Console](#)

Device malware state

85 unresolved threats

Of detections by Windows Defender Antivirus in the last 24 hours:

[View details](#)

Email protection overview

Malicious email content blocked by Office Advanced Threat Protection in the past 30 days.

8067 Phishing blocked
1272 Malware blocked

[View details in Office 365 Security & Compliance Center](#)

Identity protection overview

For accounts protected by Azure AD Identity Protection:

55 Users flagged for risk
88 Risky sign-in events in 30 days
8 Global admins

[View details in Azure AD Identity Protection](#)

Top discovered app categories

Cloud storage	200GB
Collaboration	191GB
CRM	185GB
Webmail	170GB

[View all in Cloud App Security](#)

DLP policy matches

Policy 1 (Green) | **Policy 2** (Cyan) | **Policy 3** (Blue)

Infrastructure protection overview

185 protected resources

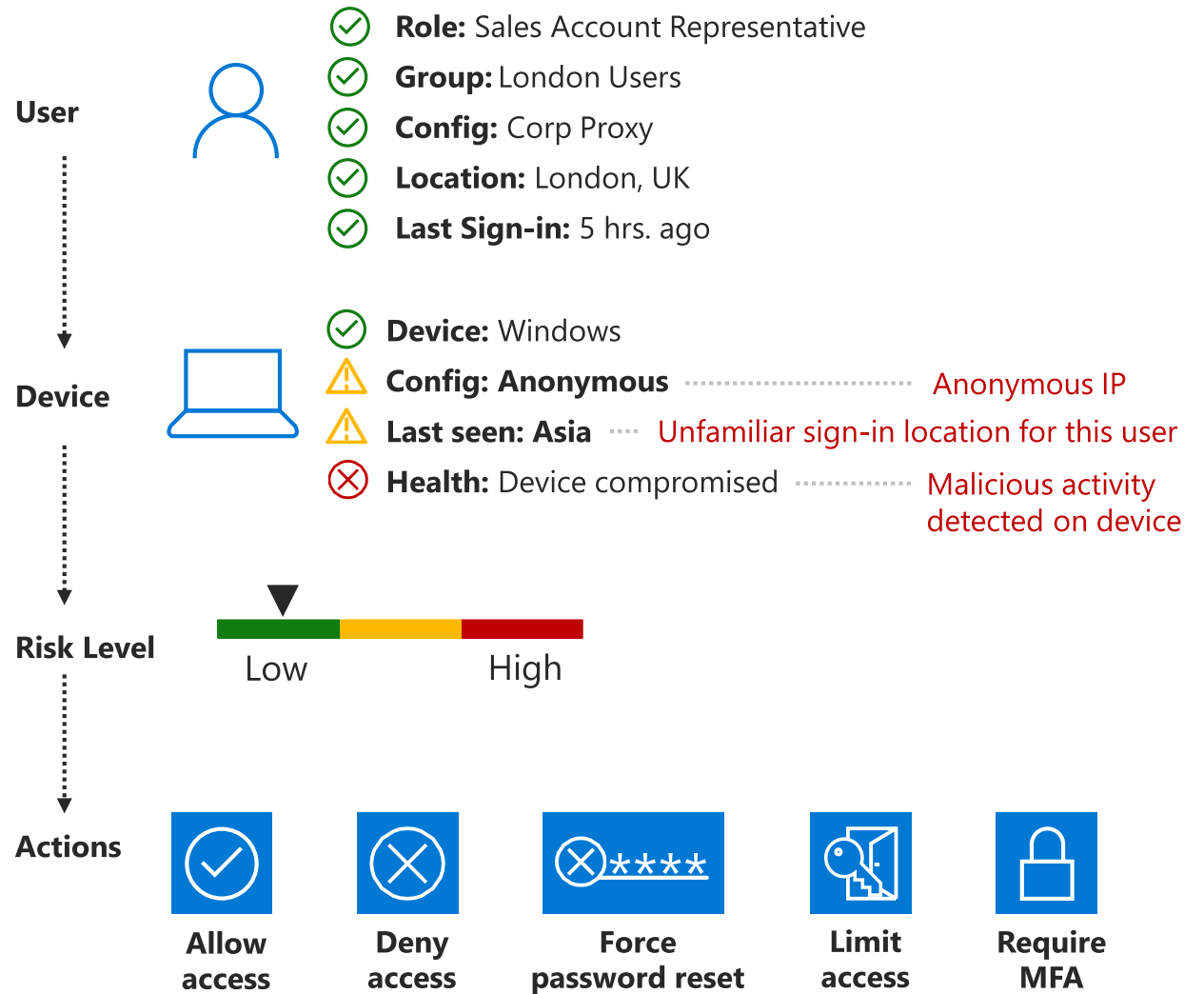
Covered by your Azure Security Center subscription.

- 2 alerts
- 44 recommendations

Protect at the Front door with Conditional Access

Conditional Access policies can be applied based on device state, application sensitivity, location and user rules

By configuring these policies, you can select certain conditions, and allow access or require further identification

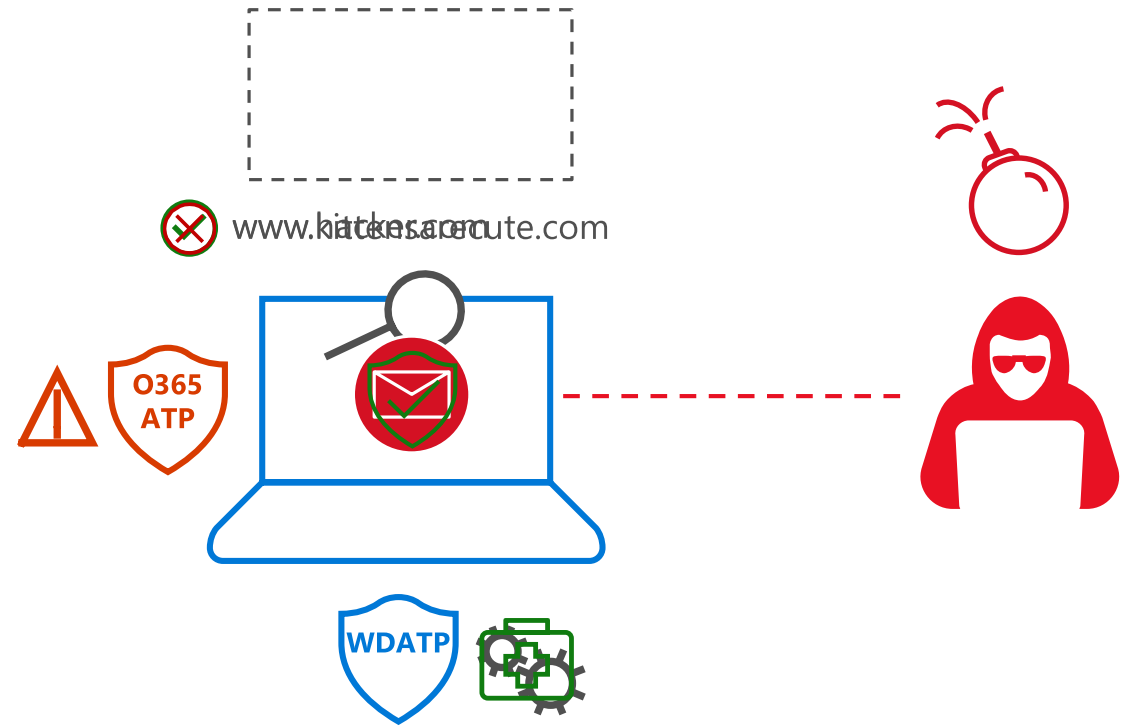


Synched ACTIONS across Office 365 ATP and Windows Defender ATP

An attacker sends a phishing email campaign to a company. It is analyzed by Office ATP and the embedded URL is linked to a legitimate and safe website

After 24 hours, the attacker "arms" the URL by redirecting to a malicious download which Office ATP detects and quarantines emails

Office ATP sends an alert to Windows Defender ATP to locate user with malicious attachment and clean the infection



Search (Ctrl+/)

General

Quick start

Dashboards

Usage report (Preview)

Activity logs (Preview)

Data discovery (Preview)

Classifications

Labels

Policies

Manage

Configure analytics (Preview)

Languages

Protection activation

Log Analytics

Location type

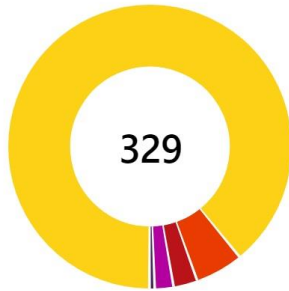
Any

Location

Search

Apply

Labels



LOCATION TYPE	LOCATION
File repository	\\sislands\public\
Endpoint	W10-IW-CLIENT1
Endpoint	W10-IW-CLIENT2

jonathanw-pc



cont-jonathanw

Laptop North America

Machine details

Risk level High

Domain Contoso

OS Windows 10 64-bit

Network activity

First seen 09/15/2017 12:00

Last seen 03/15/2018 13:30

See all IPs >

Information protection

Data sensitivity Confidential

See files in Azure Information Protection

Collect investigation package Run AV scan Restrict app execution Isolate machine Manage tags Action center

Active alerts (6)



See all alerts

Logged on users (12)

Most frequent: Jonathan Wolcott

Least frequent: Eva Macias

See all users

Secure score



2 security controls require attention

Manage score

Timeline

Search in machine timeline

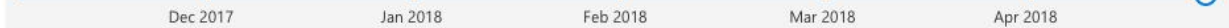
All event types

All user accounts

Display

Export

03/15/2018 13:29



Date/time	Event	Details	User
13:29:32	chrome.exe created document.pdf	explorer.exe > chrome.exe > document.pdf	Jonathan Wolcott



chrome.exe
 036c56034539719cecc1353bd641b6c2584411a0
 C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
 "chrome.exe"



Document.pdf
 b7dd479039a6885d77eef8020e59513f32983b5e
 C:\Users\Jonathan\Downloads\Document.pdf
 Confidential

Information Protection
 Integration with Microsoft Information Protection for
 sensitive data discovery and enforcement on endpoints

Cloud Discovery

Continuous report Win10 Endpoint Users Timeframe Last 90 days

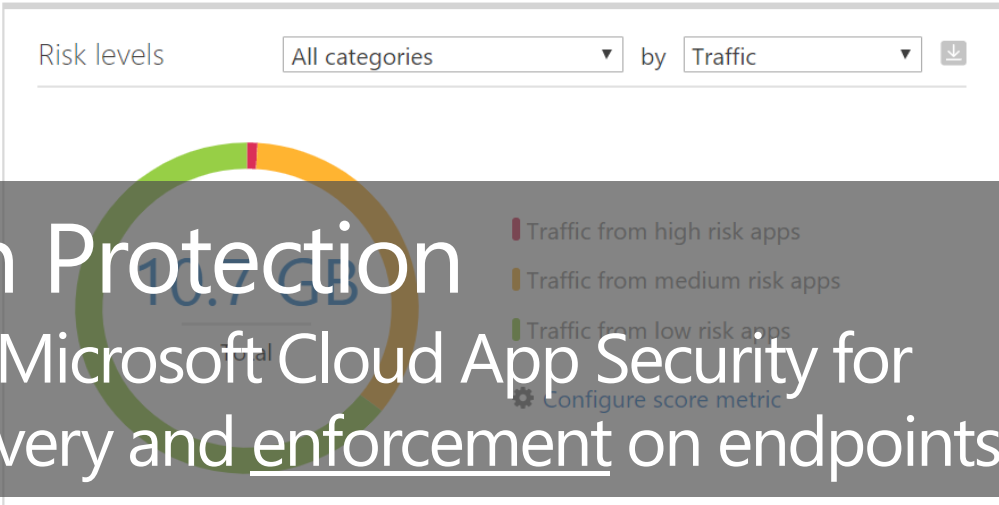
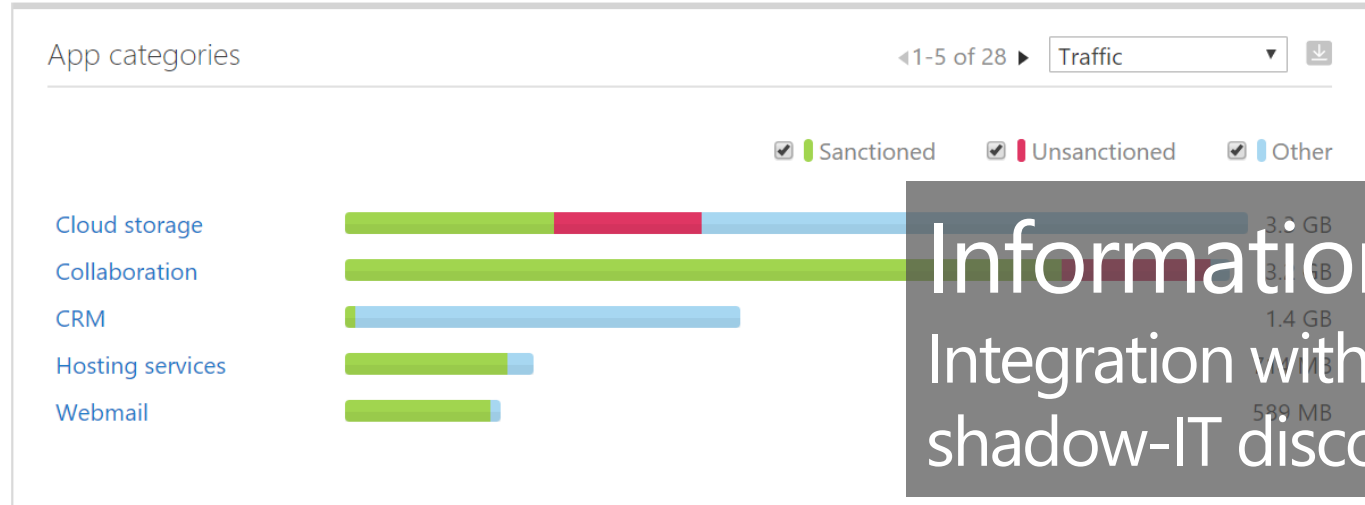
- Dashboard
- Discovered apps
- IP addresses
- Users
- Machines

Updated on Jul 18, 2018

Apps: 128 IP addresses: 2458 Users: 1113 Machines: 1113 Traffic: 10.7 GB ↑ 7.2 GB ↓ 3.5 GB

Cloud Discovery open alerts + Create policy

48 Cloud Discovery alerts 0 Suspicious use alerts



Information Protection
Integration with Microsoft Cloud App Security for shadow-IT discovery and enforcement on endpoints

Discovered apps ◀ 1-15 of 128 ▶ View all apps All categories Traffic

Sanctioned Unsanctioned Other

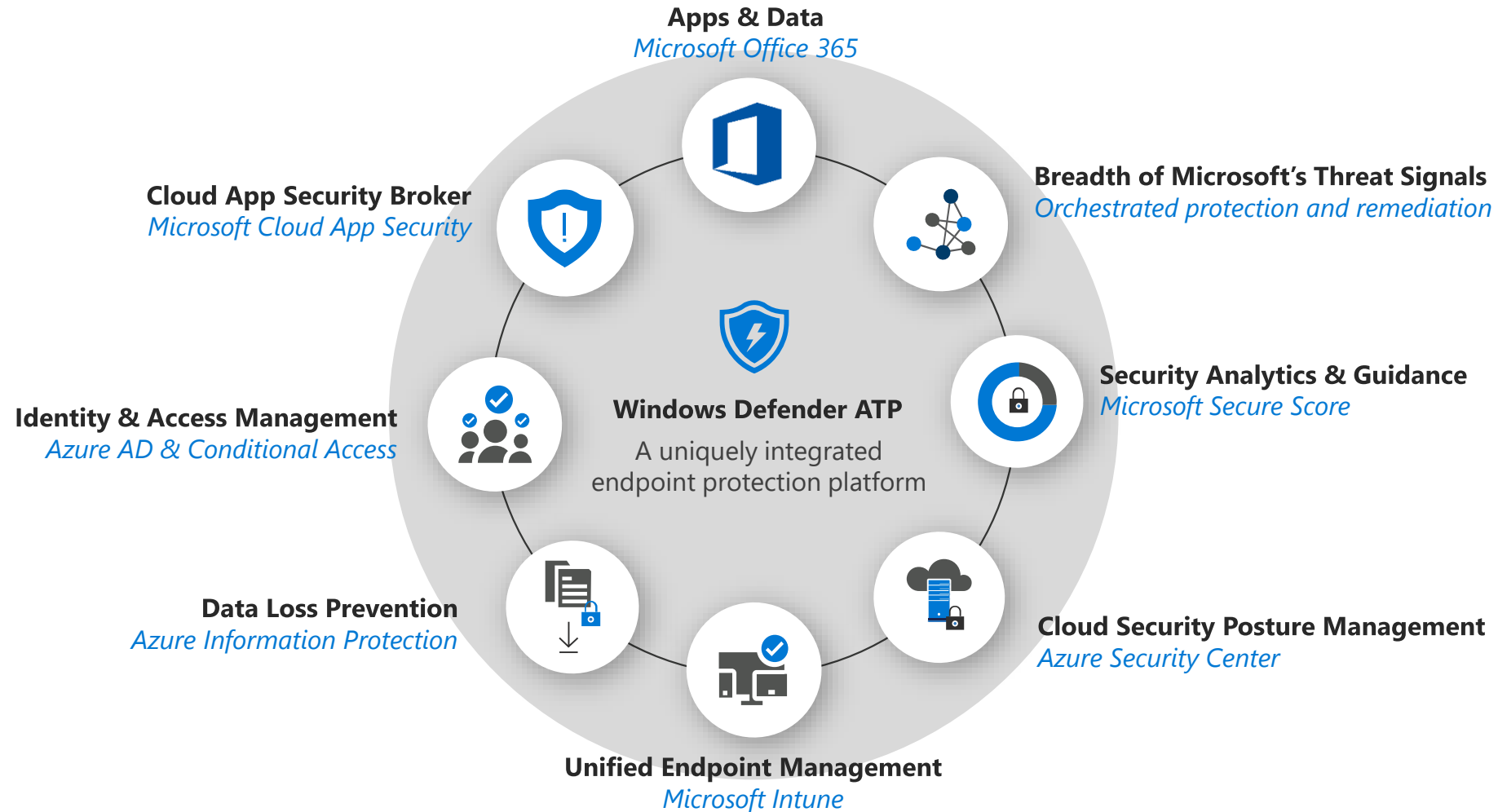
App	Traffic
Microsoft Dynamics	1.4 GB
Microsoft SharePo...	1.3 GB
Microsoft Teams	909 MB
Amazon Web Serv...	648 MB

Top entites View all users User by Traffic

User	Total
CONTOSO/Bob	306 MB
CONTOSO/Chaya	44 MB
CONTOSO/Sloane	40 MB
CONTOSO/M/...	10 MB

Windows Defender ATP

Elevate the security for all your workloads





Windows Defender ATP

Built-in. Cloud-powered.

Trusted by IT. Loved by security teams.