



# Azure OpenAI & Microsoft Security

# Our partnership with OpenAI



*Ensure that artificial general intelligence (AGI) benefits humanity.*



*Empower every person and organization on the planet to achieve more*

---

## Azure OpenAI Service

**GPT-3**

Generate and Understand Text

**Codex**

Generate and Understand Code




**DALL·E** *preview*

Generate images from text prompts

**ChatGPT** *preview*

Generate conversational responses

# What is the difference for OpenAI & Azure OpenAI?

Feature	OpenAI 	Azure OpenAI  
<b>Security &amp; Data Privacy</b>	Basic Security	Enterprise Security, RBAC, Customer-Managed Keys
<b>Compliance</b>	None	SOC2, ISO, HIPAA, CSA STAR
<b>Reliability</b>	No SLA (yet)	Azure SLA, Dedicated Capacity Option (soon)
<b>Responsible AI</b>	Separate Safety Classifier (adds latency)	Built-in, enterprise-grade, low latency moderation and harm prevention
<b>Holistic Solution</b>	Advanced LLM & Image Generation, Basic Speech	OpenAI Models, Complete AI Solution, and a Complete PaaS
<b>Pricing</b>	Per-token (today), Dedicated Capacity (soon)	Per-token (today), Dedicated Capacity (soon)
<b>APIs</b>	REST APIs + Python SDK	REST APIs + Python, C#, etc. SDKs
<b>Generative Models</b>	Language & Image	Language & Image





## Generative AI

### GPT-3

Prompt:

Write a tagline for an ice cream shop.

Response:

We serve up smiles with every scoop!

### Codex

Prompt:

Table customers,  
columns =  
[CustomerId,  
FirstName, LastName,  
Company, Address,  
City, State,  
Country, PostalCode]

Create a SQL query for all customers in Texas named Jane  
query =

Response:

```
SELECT *  
FROM customers  
WHERE State = 'TX'  
AND FirstName =  
'Jane'
```

### DALL·E *preview*

Prompt: A white Siamese cat

Response:



### ChatGPT *preview*

What is the fastest animal on land?

the cheetah (*Acinonyx jubatus*), which can reach speeds of up to 60 miles (97 kilometers) per hour.

What makes them so fast?

Cheetahs are built for speed and have several adaptations that make them the fastest land animal: lean body, long legs, flexible spine, large nostrils and claws that don't retract.





# | Azure OpenAI | GPT-3 Prompt Design

Extract the mailing address from this email:

Hi John Doe,

It was great to meet up at Build earlier this week. I thought the AI platform talk was great and I really enjoyed it.

I appreciate the offer for the book. If you are OK, you can mail it to me at home, or 123 Microsoft Way, Bellevue WA 92004.

Regards,

Chris Hoder

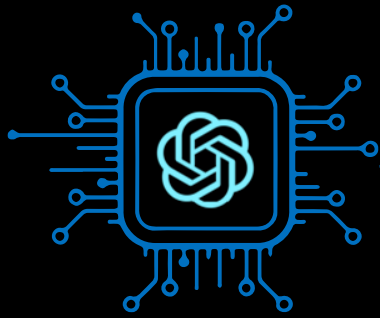
123 Microsoft Way, Bellevue WA 92004

**Prompt** – Text input that provides some context to the engine on what is expecting.

**Completion** – Output that GPT-3 generates based on the prompt.



OpenAI Codex  
Model



Public code and text  
on the internet

GitHub



GitHub  
Copilot Service



Don't fly solo.

Provide editor context

Provide suggestions

Improve suggestions

Private code

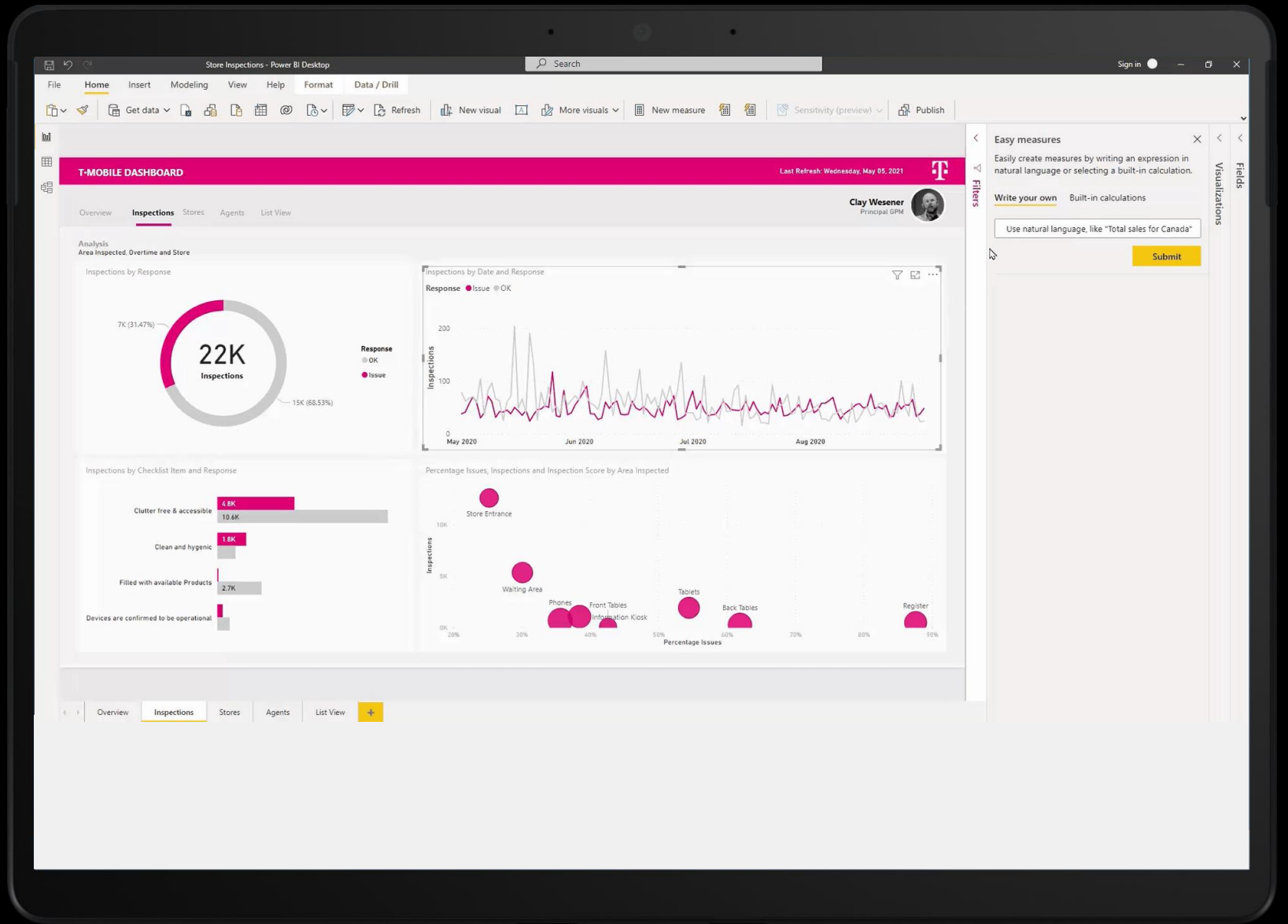
```
JS fetch_pic.js push_to
1  const fetchNASAPictureOfTh
2  return fetch('https://ap
3      method: 'GET',
4      headers: {
5          'Content-Type': 'app
6      },
7  })
8  .then(response => resp
9  .then(json => {
10     return json;
11  });
12 }
```

Copilot



# Power BI

Generating DAX expressions with natural language





# Power Platform

## Power Fx formulas

The screenshot displays the Power Apps Canvas environment. The top navigation bar includes 'Power Apps | Canvas', 'Environment', and user profile. The ribbon contains 'File', 'Home', 'Insert', 'View', 'Action', and 'Settings'. The 'Items' property of the selected 'BrowseGallery1' control is set to 'Contacts'. The 'Tree view' on the left shows the app structure with 'BrowseGallery1' selected. The main canvas shows a gallery with a search bar containing 'scott' and a list of contact records. The right-hand 'Properties' pane is open to the 'Ideas' tab, displaying machine-generated suggestions for filtering and sorting the gallery data.

Name	Email
Yvonne McKay (sample)	someone_a@example.com
Susanna Stubberod (sample)	someone_b@example.com
Nancy Anderson (sample)	someone_c@example.com
Maria Campbell (sample)	someone_d@example.com
Sidney Higa (sample)	someone_e@example.com
Scott Konersmann (sample)	someone_f@example.com
Robert Lyon (sample)	someone_g@example.com
Paul Cannon (sample)	someone_h@example.com
Rene Valdes (sample)	someone_i@example.com

**Properties** | **Advanced** | **Ideas**

Use the input to describe what you want done. Place double quotes around strings you want to reference. Learn more

Get ideas

- Show records of **Contacts Modified On in the last 7 days**  
Filter(Contacts, 'Modified On' > DateAdd(Today(), - 7, Days))
- Sort **Contacts by Modified On**  
Sort(Contacts, 'Modified On', Ascending)
- Top 10 **Contacts**  
FirstN(Contacts, 10)

Ideas generated by machine learning are unpredictable. If an idea is inappropriate, use Report it now to help Microsoft improve the AI model.

# DALL·E 2

An astronaut riding a horse in a photorealistic style



Teddy bear working on new AI research on the moon in 1980



A bowl of soup that looks like a monster knitted out of wool

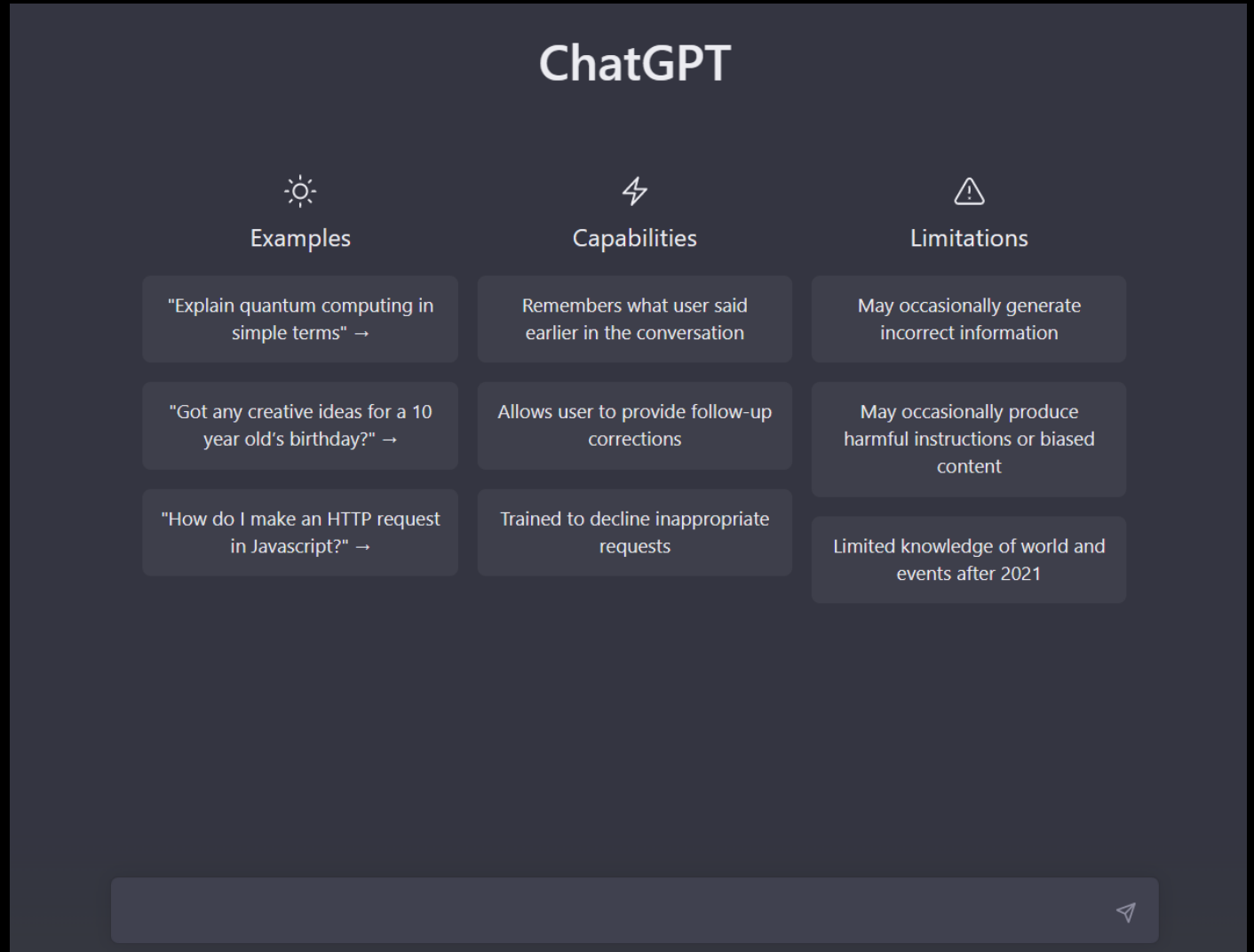


# The ChatGPT model

Unlike previous GPT-3 models, the ChatGPT model is specifically designed to be a conversational interface.

The conversational nature of the model makes it easier to interact with and to take advantage of the full power of its capabilities. This is part of the reason the model became so successful.

The prompts used with the ChatGPT model are also different than previous models.





# Working with the ChatGPT model

## Previous GPT-3 models

Previous models were text-in and text-out

(i.e., they accepted a prompt string and returned a completion to append to the prompt).

Answer questions from the context below.

Context:

A neutron star is the collapsed core of a massive supergiant star, which had a total mass of between 10 and 25 solar masses, possibly more if the star was especially metal-rich.

Q: What is a neutron star?

A:

## The ChatGPT model

The ChatGPT model is conversation-in and message-out.

(i.e., it expects a prompt string that is formatted in a specific chat-like transcript format and returns a completion that represents a model-written message in the chat)

```
<|im_start|>system  
Assistant is an AI Chatbot designed to answer questions from the  
context provided below.
```

Context:

A neutron star is the collapsed core of a massive supergiant star, which had a total mass of between 10 and 25 solar masses, possibly more if the star was especially metal-rich.

```
<|im_end|>
```

```
<|im_start|>user
```

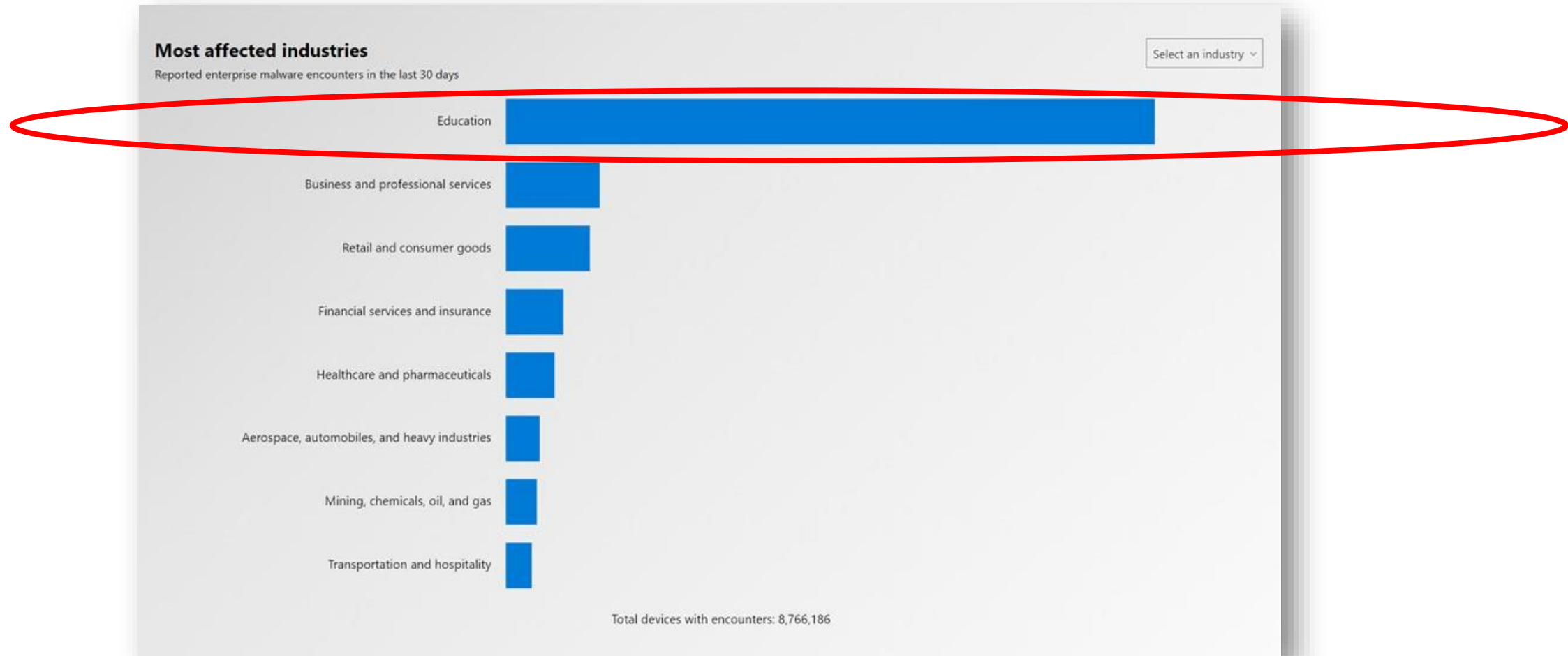
What is a neutron star?

```
<|im_end|>
```

```
<|im_start|>assistant
```

# Navigating a shifting world - Education Sector is on red alert

Microsoft Security Intelligence: Real-time tracking of cybersecurity attacks worldwide, by industry  
[Cyberthreats, viruses, and malware - Microsoft Security Intelligence](#)





# Microsoft Security: Leader in 8 Forrester Wave and New Wave reports

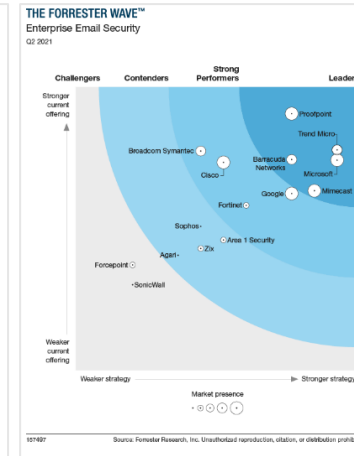
1. The Forrester Wave™: Security Analytics Platforms, Q4 2020, Joseph Blankenship, Claire O'Malley, December 2020
2. The Forrester Wave™: Enterprise Email Security Q2 2021 Joseph Blankenship, Claire O'Malley, April 2021
3. The Forrester Wave™: Endpoint Security Software as a Service, Q2 2021, Chris Sherman, May 2021
4. The Forrester Wave™: Unified Endpoint Management, Q4 2019, Andrew Hewitt, November 2021
5. The Forrester Wave™: Unstructured Data Security Platforms, Q2 2021, Heidi Shey, May 2021
6. The Forrester Wave™: Cloud Security Gateways, Q2 2021, Andras Cser, May 2021
7. The Forrester Wave: Identity As A Service (IDaaS) For Enterprise, Q3 2021" Sean Ryan, August 2021
8. The Forrester New Wave™: Extended Detection And Response (XDR), Q4 2021, Allie Mellen, October 2021

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

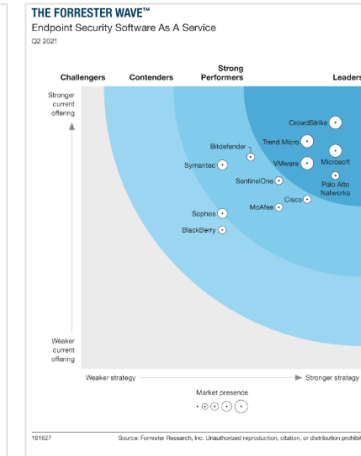
The Forrester New Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of Forrester's call on a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester New Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.



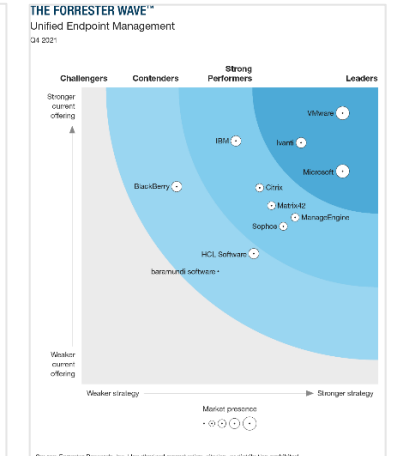
Security Analytics Platform



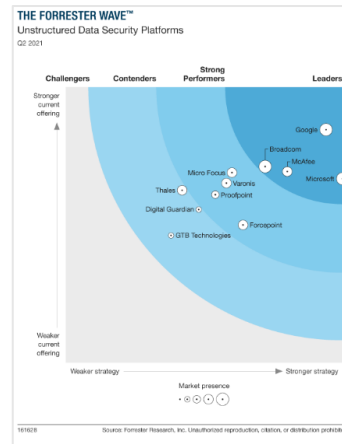
Enterprise Email Security



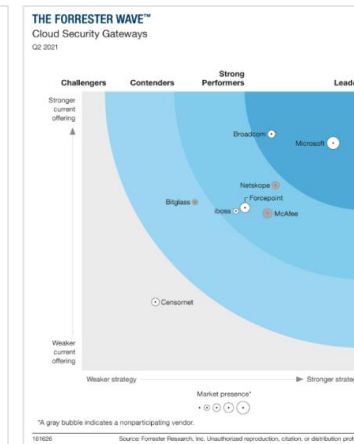
Endpoint Security Software as a Service



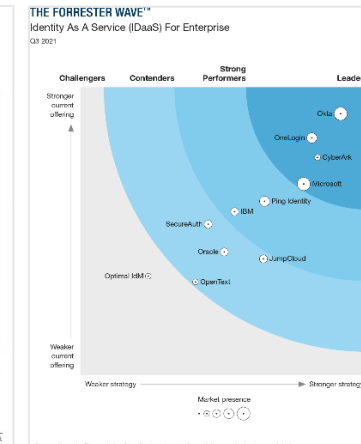
Unified Endpoint Management



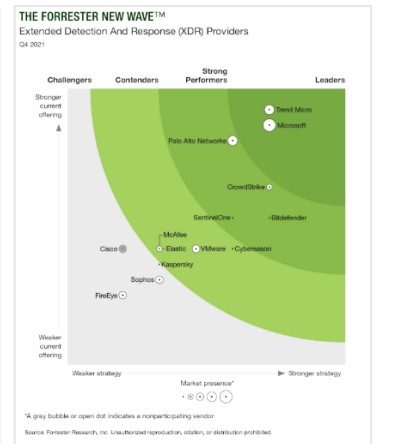
Unstructured Data Security Platforms



Cloud Security Gateways



Identity As a Service



Extended Detection And Response (XDR)



# An industry leader in endpoint security

**Gartner**

Gartner names Microsoft a **Leader in 2021 Endpoint Protection Platforms Magic Quadrant.**

**MITRE** | ATT&CK™

Microsoft **leads in real-world detection** in MITRE ATT&CK evaluation.

**FORRESTER**

Forrester names Microsoft a **Leader in 2021 Endpoint Security Software as a Service Wave.**



Microsoft Defender for Endpoint awarded a **perfect 5-star rating by SC Media** in 2020 Endpoint Security Review

**FORRESTER**

Forrester names Microsoft a **Leader in 2020 Enterprise Detection and Response Wave.**



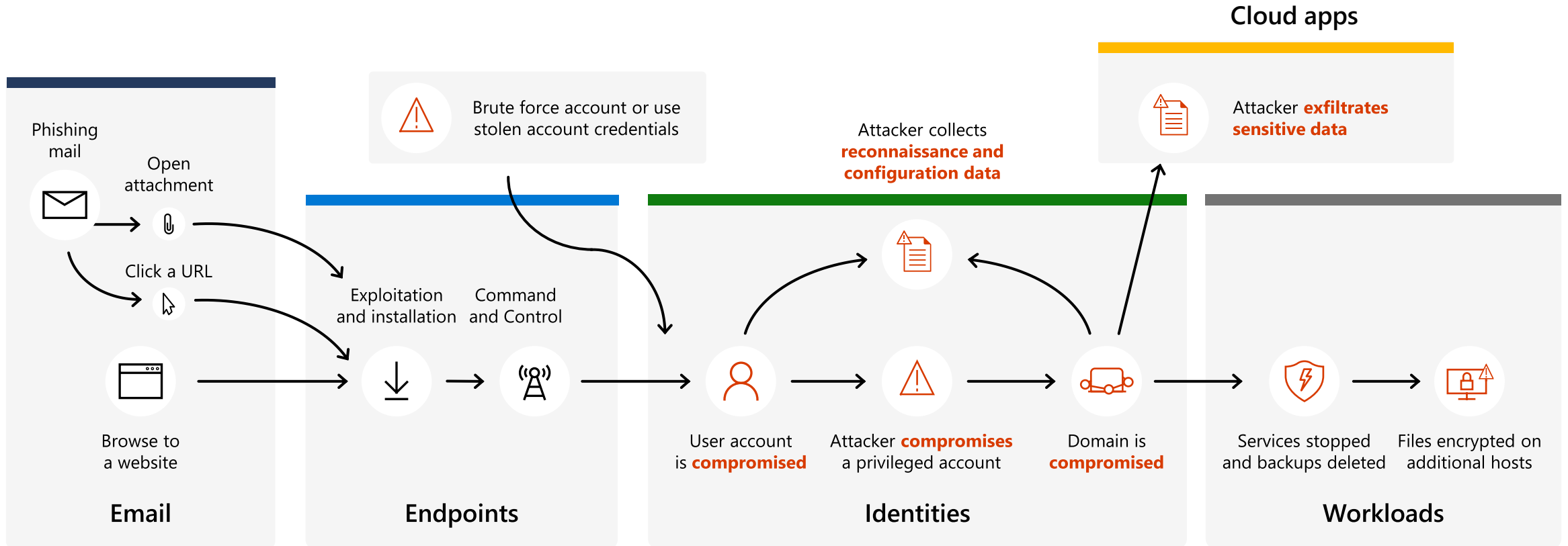
Microsoft won six security awards with **Cyber Defense Magazine** at RSAC 2021:

- ✓ Best Product Hardware Security
- ✓ Market Leader Endpoint Security
- ✓ Editor's Choice Extended Detection and Response (XDR)
- ✓ Most Innovative Malware Detection
- ✓ Cutting Edge Email Security

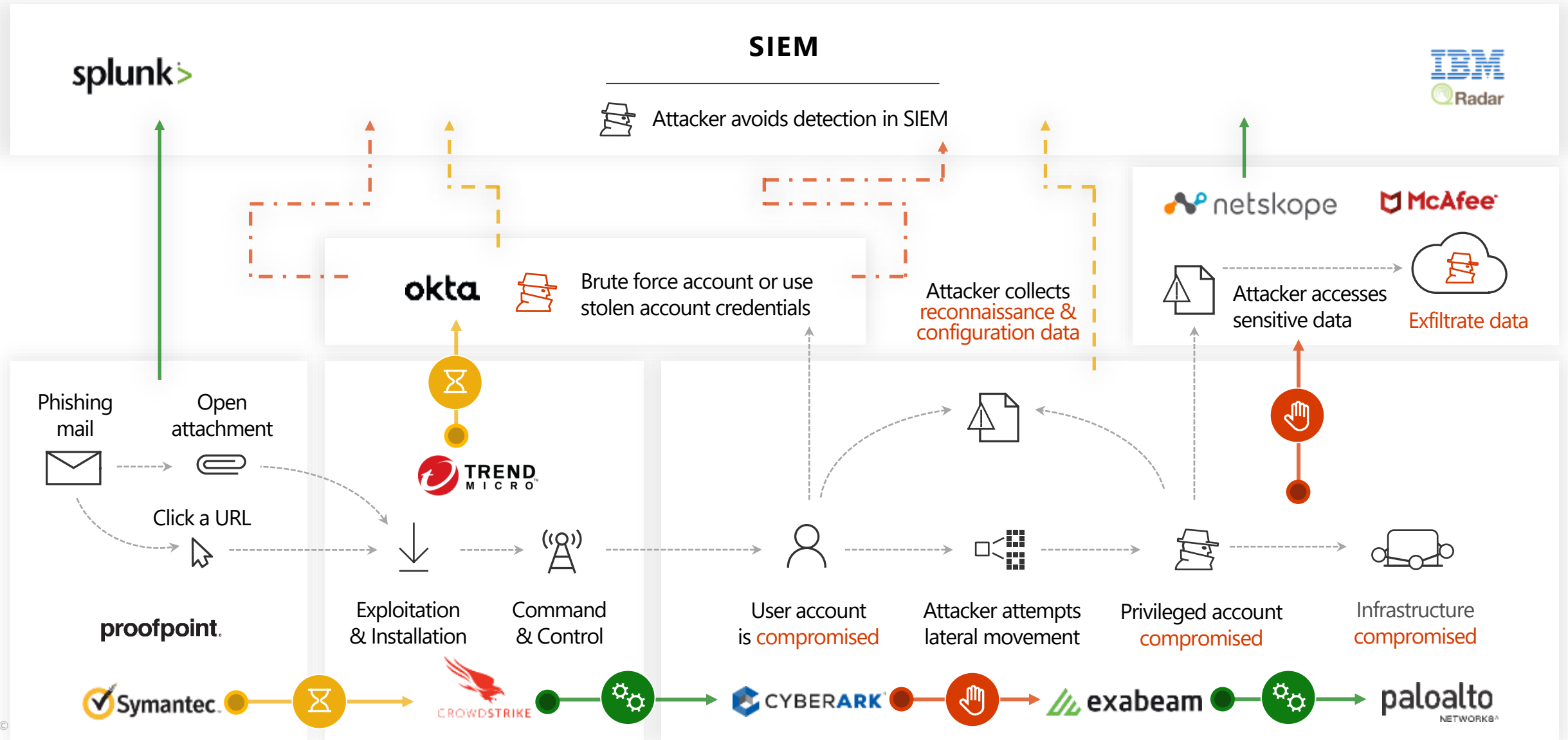


Our antimalware capabilities consistently achieve **high scores in independent tests.**

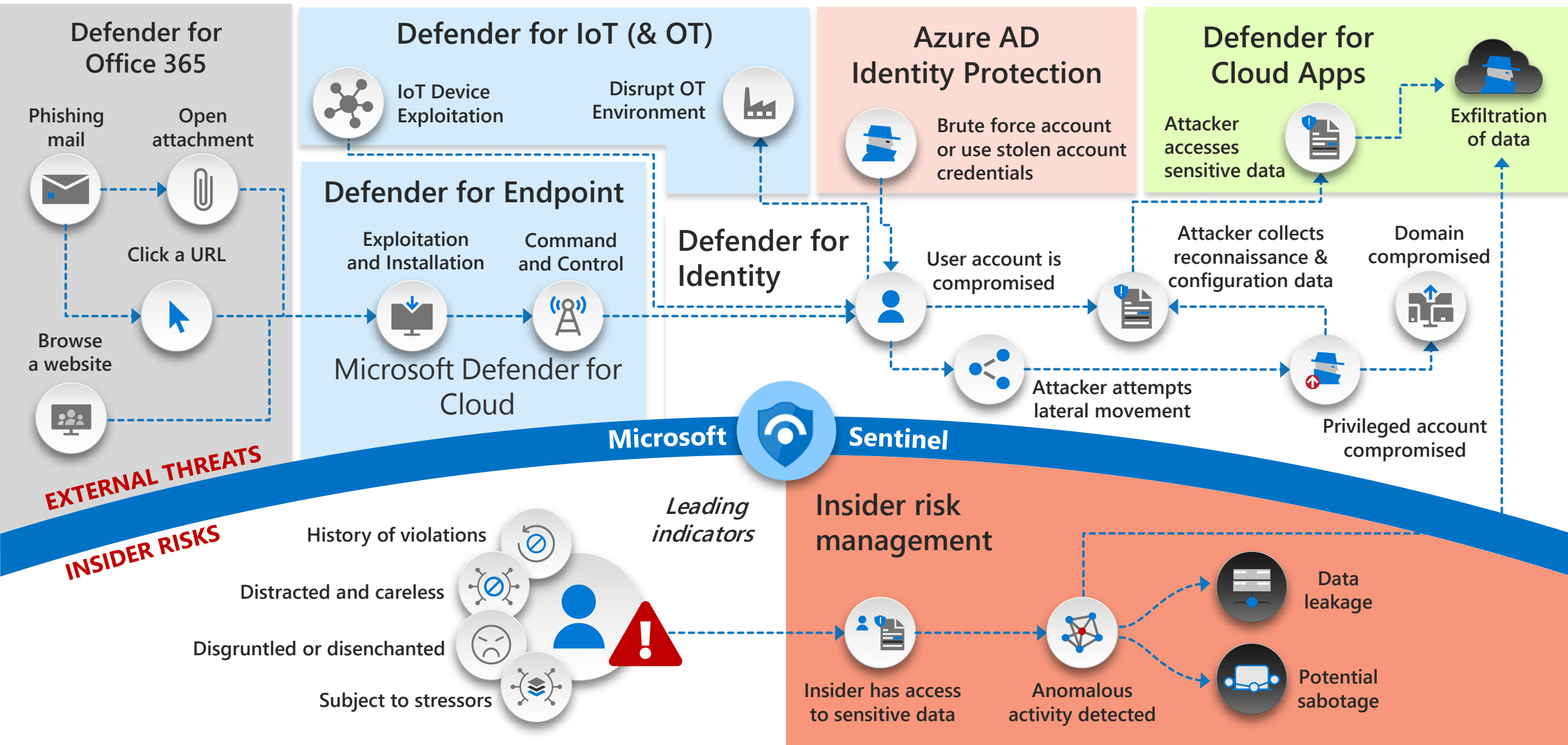
# Typical human-operated ransomware campaign



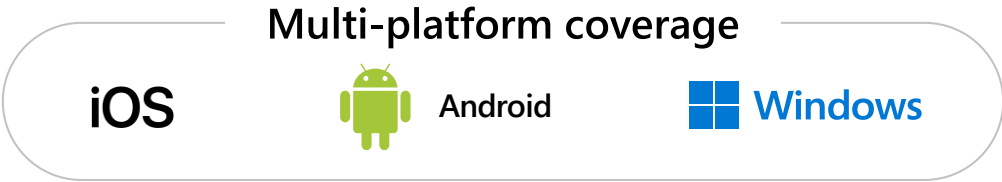
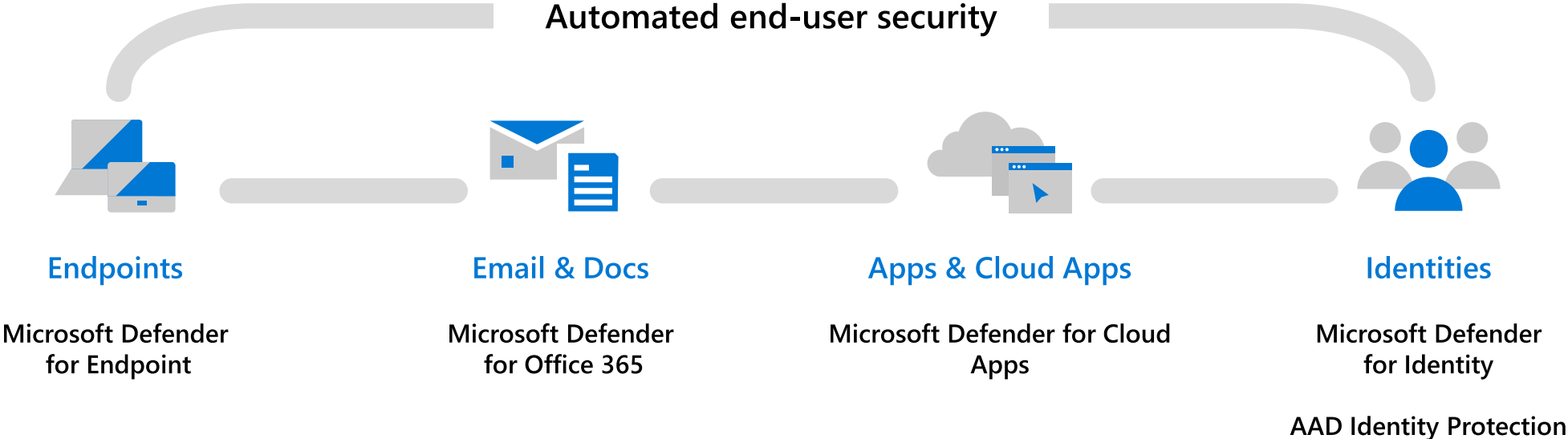
# Siloed security leads to gaps and increased operational overhead



# Defend across attack chain with extended detection and response (XDR)



# Microsoft 365 Defender







# Defender for Endpoint

---

# Microsoft Defender for Endpoint



Windows



macOS



iOS

Windows 365  
Azure Virtual Desktop



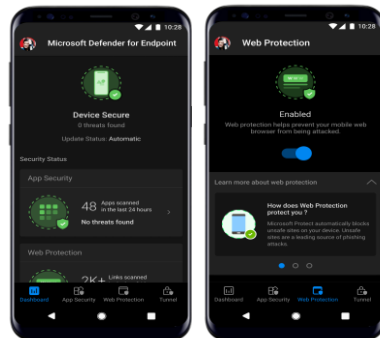
Cisco  
Juniper Networks

HP Enterprise  
Palo Alto Networks

Endpoints and servers



Mobile device OS



Virtual desktops

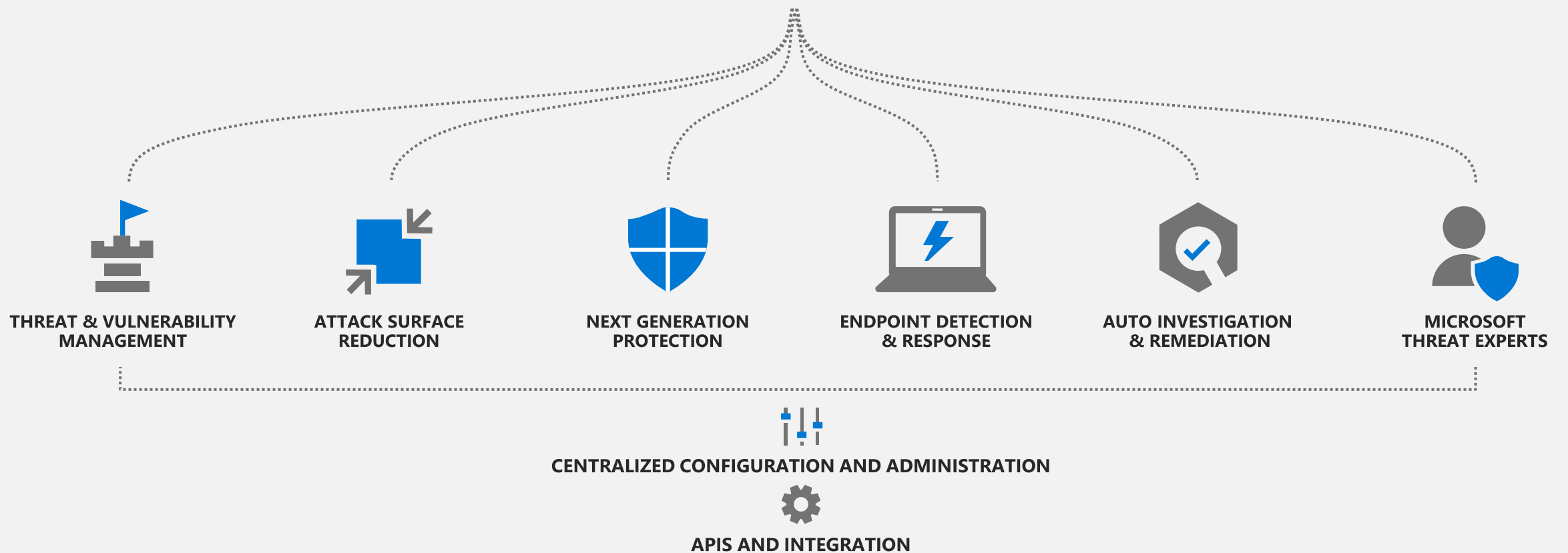
Network devices

Mobile Threat Defense



# Microsoft Defender for Endpoint

Threats are no match.



# Threat & Vulnerability Management

A risk-based approach to mature your vulnerability management program

1



Continuous real-time discovery

2

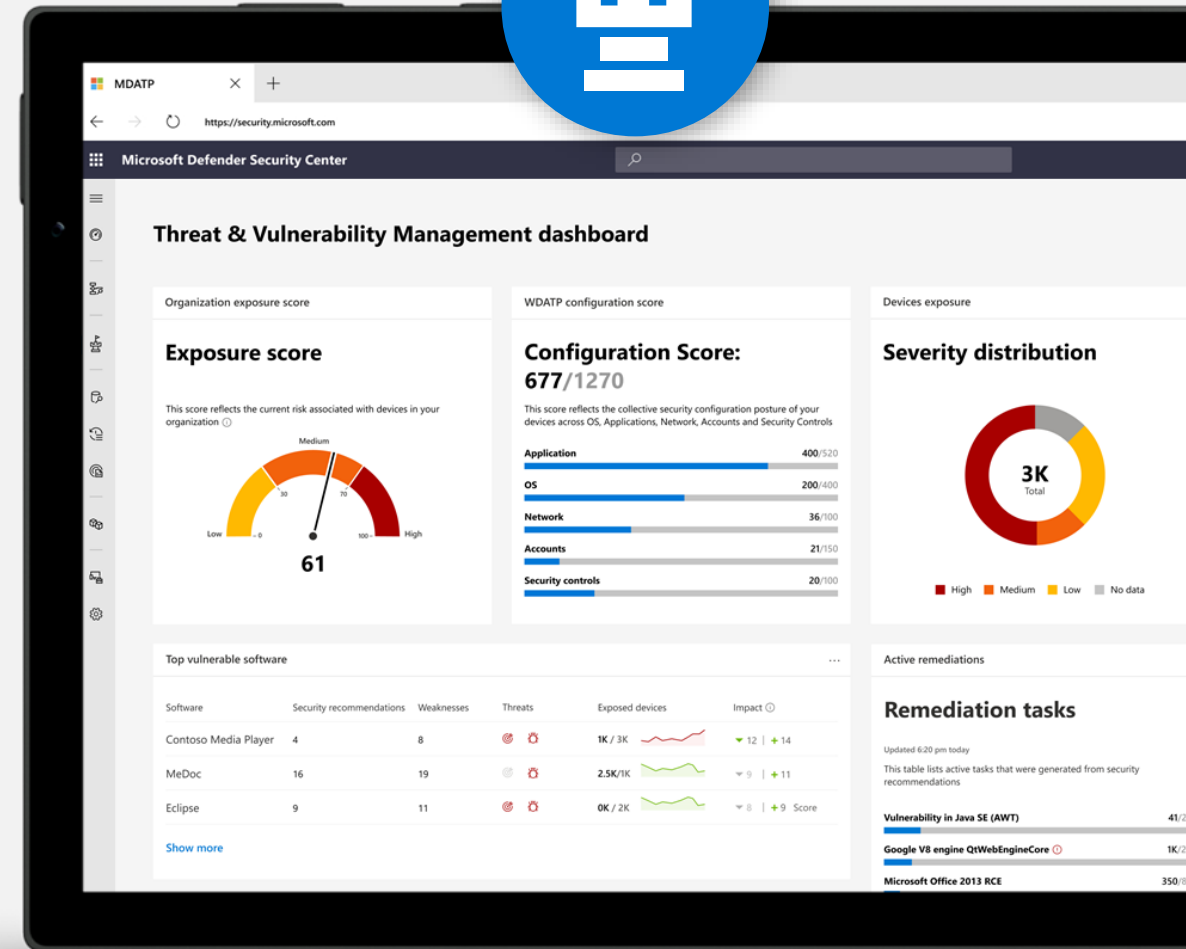
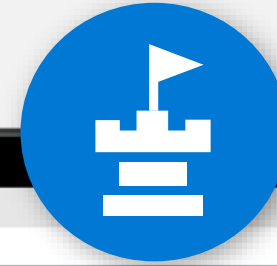


Context-aware prioritization

3



Built-in end-to-end remediation process



# Attack Surface Reduction

Eliminate risks by reducing the surface area of attack



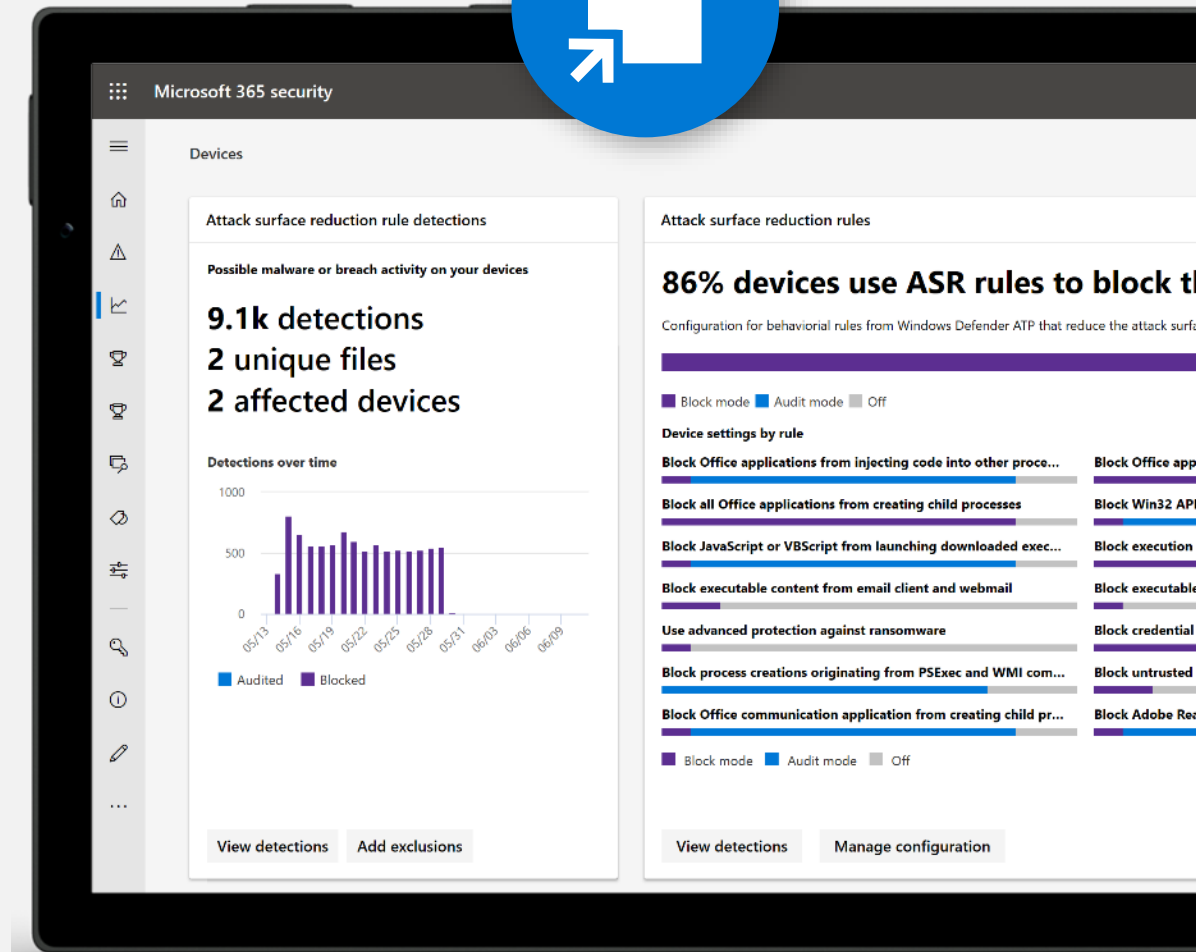
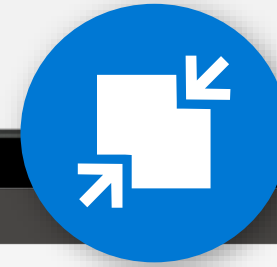
System hardening without disruption



Customization that fits your organization



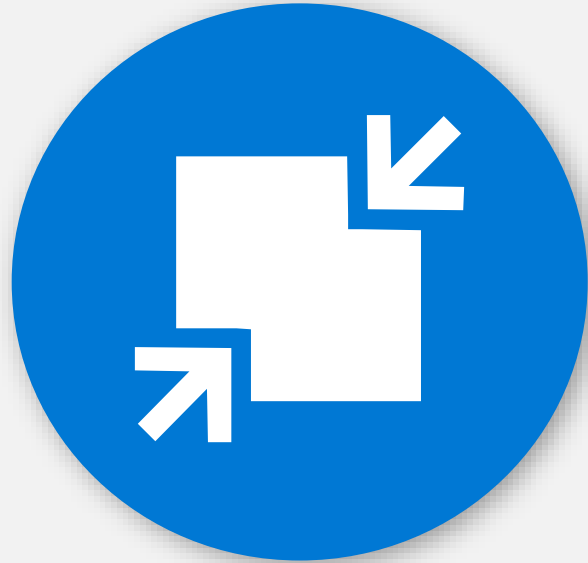
Visualize the impact and simply turn it on





# Attack Surface Reduction

Resist attacks and exploitations



HW based isolation

Application control

Exploit protection

Network protection

Controlled folder access

Device control

Web protection

Ransomware protection

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

# Next Generation Protection

Blocks and tackles sophisticated threats and malware



Behavioral based real-time protection



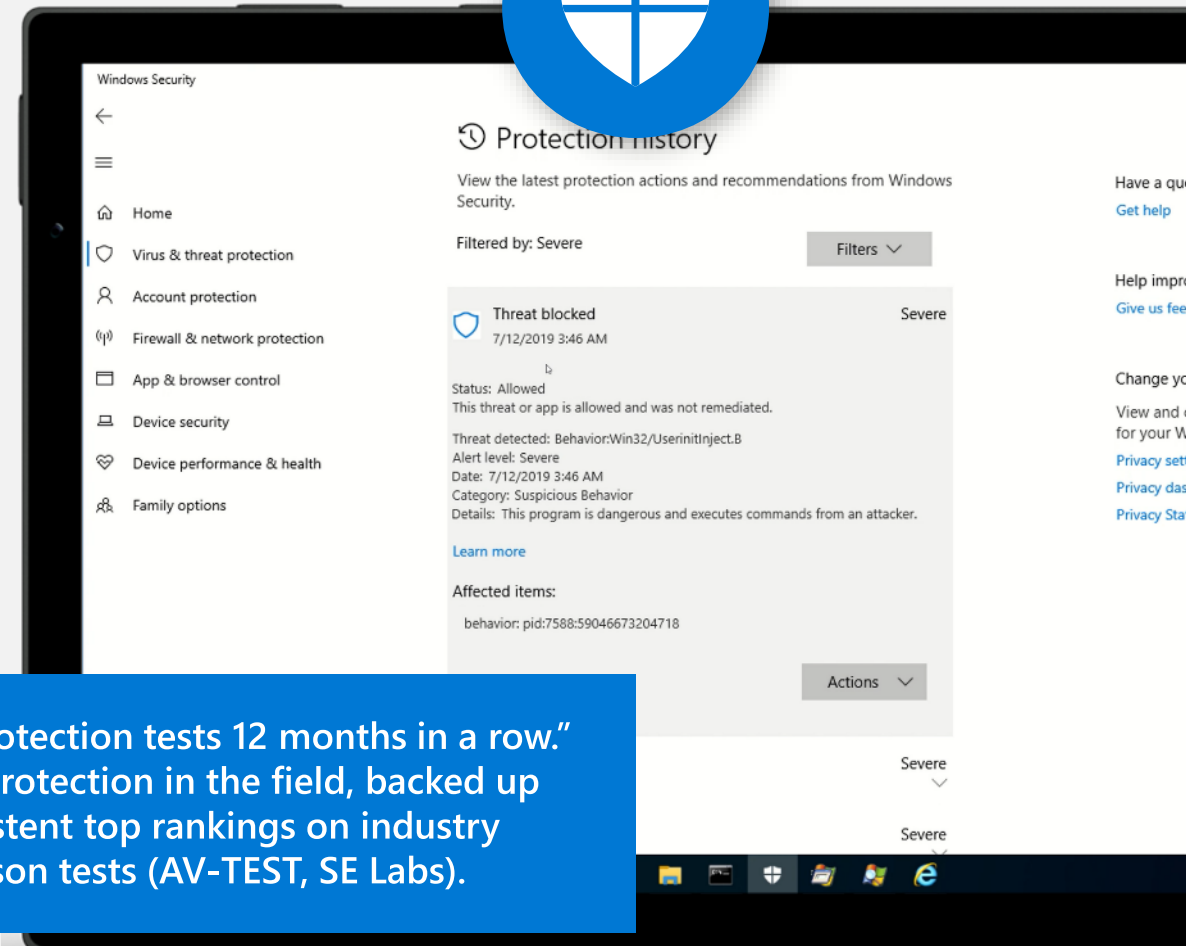
Blocks file-based and fileless malware



Stops malicious activity from trusted and untrusted applications



"Aced protection tests 12 months in a row."  
Proven protection in the field, backed up  
by consistent top rankings on industry  
comparison tests (AV-TEST, SE Labs).



# Microsoft Defender for Endpoint next generation protection engines



## Metadata-based ML

Stops new threats quickly by analyzing metadata



## Behavior-based ML

Identifies new threats with process trees and suspicious behavior sequences



## AMSI-paired ML

Detects fileless and in-memory attacks using paired client and cloud ML models



## File classification ML

Detects new malware by running multi-class, deep neural network classifiers



## Detonation-based ML

Catches new malware by detonating unknown files



## Reputation ML

Catches threats with bad reputation, whether direct or by association



## Smart rules

Blocks threats using expert-written rules



## ML

Spots new and unknown threats using client-based ML models



## Behavior monitoring

Identifies malicious behavior, including suspicious runtime sequence



## Memory scanning

Detects malicious code running in memory



## AMSI integration

Detects fileless and in-memory attacks



## Heuristics

Catches malware variants or new strains with similar characteristics



## Emulation

Evaluates files based on how they would behave when run



## Network monitoring

Catches malicious network activities

# Endpoint Detection & Response

Detect and investigate advanced persistent attacks



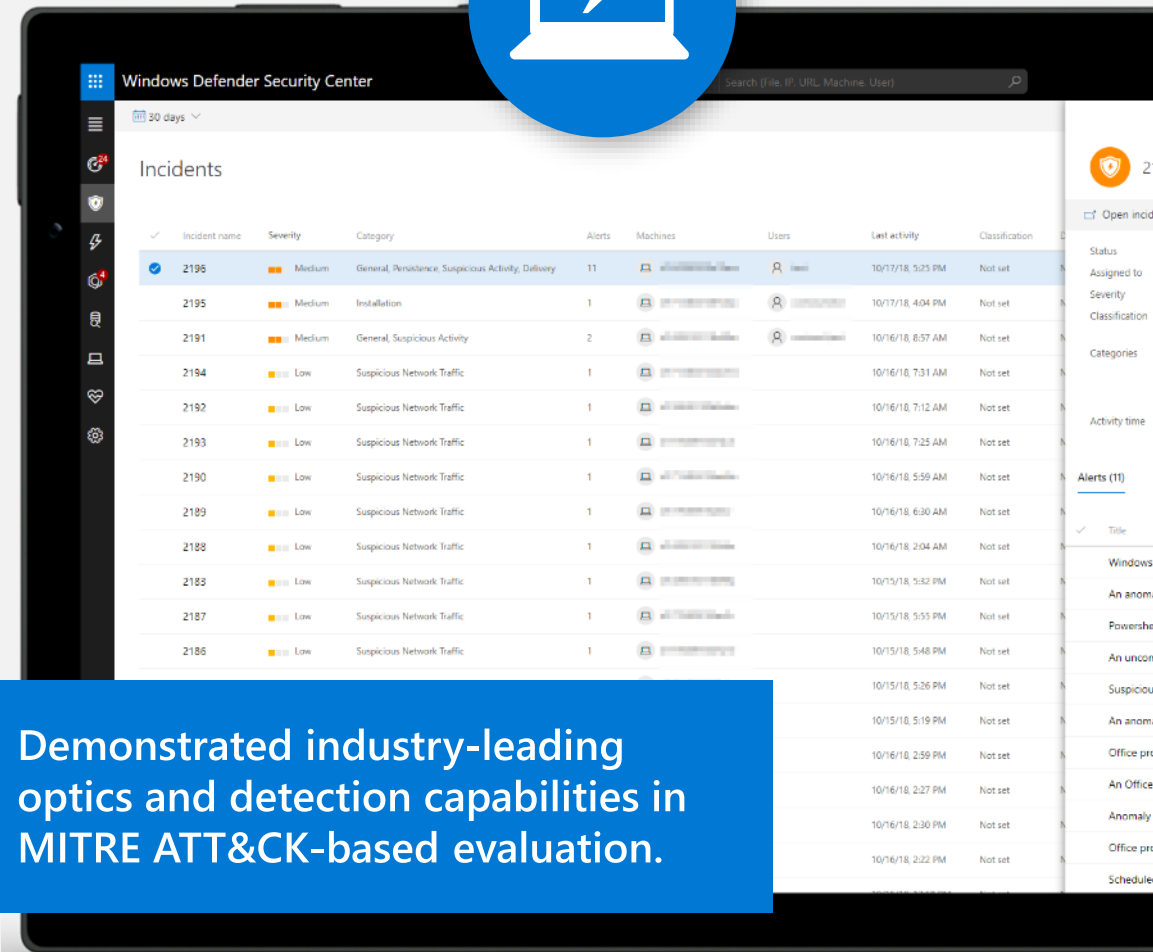
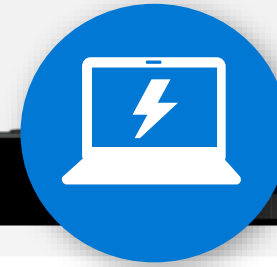
Correlated behavioral alerts



Investigation & hunting over 6 months of data



Rich set of response actions



Demonstrated industry-leading optics and detection capabilities in MITRE ATT&CK-based evaluation.

# Endpoint Detection & Response



Correlated post-breach detection

Investigation experience

Incident

Advanced hunting

Response actions (+EDR blocks)

Deep file analysis

Live response

Threat analytics



# Auto Investigation & Remediation

Automatically investigates alerts and remediates complex threats in minutes



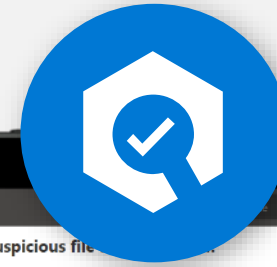
Mimics the ideal steps analysts would take



Tackles file or memory-based attacks



Works 24x7, with unlimited capacity



The screenshot displays the Microsoft Defender Security Center interface. The main heading is "Office ATP Alert - Suspicious file found based on an Office ATP alert". Below this, it states "Investigation #88 is complete - Remediated". The interface is divided into two main sections: "Investigation details" on the left and an "Investigation graph" on the right. The "Investigation details" section shows the status as "Remediated" with a green checkmark icon, and notes that "Malicious entities found were successfully remediated." It also lists the alert severity as "Medium", the category as "Malware", and the detection source as "Office ATP". The "Investigation graph" section shows a flowchart starting from "Alert received Office ATP" leading to "Machine (1) BARBARAM-PC", then to "Entities analyzed (5224)", which includes 3998 files (1 remediated), 193 processes, 291 services, 414 drivers, 15 IP addresses, and 315 persistence methods. The graph concludes with "Evidence 1 entity found" and a "Result Remediated" status.

# Auto investigation queue

The screenshot displays the Microsoft Defender Security Center interface on a tablet. The main content area is titled "Automated Investigations" and shows a list of investigation events. The interface includes a top navigation bar with "Machine" and "Search Microsoft Defender ATP" options, and a right-hand sidebar with filter controls for Status, Triggering alert, and Detection Source.

Triggering alert	ID	Status	Detection Source	Entities	Start Date	Duration
'Powersploit' malware was detected	99	Remediated	Antivirus	barbaram-pc.mtpdemos.net	10/28/19, 10:51 PM	14:47m
Office ATP Alert - Suspicious file found based on an Office ATP alert	98	Remediated	OfficeATP	barbaram-pc.mtpdemos.net	10/26/19, 2:05 AM	15:40m
Automated investigation started manually	94	No threats found	AutomatedInvestigation	robertot-pc.mtpdemos.net	10/23/19, 6:10 PM	13:33m
Automated investigation started manually	93	Partially investigated	AutomatedInvestigation	barbaram-pc.mtpdemos.net	10/23/19, 5:41 PM	1:14h
Automated investigation started manually	92	No threats found	AutomatedInvestigation	andrewf-pc.mtpdemos.net	10/21/19, 4:07 PM	21:55m
Hacktool Mimikatz detected	91	Remediated	EDR	barbaram-pc.mtpdemos.net	10/19/19, 8:31 AM	1:29h
Hacktool Mimikatz detected	90	Remediated	EDR	barbaram-pc.mtpdemos.net	10/18/19, 10:32 PM	1:32h
'AutoKMS' unwanted software was detected	89	Partially remediated	Antivirus	andrewf-pc.mtpdemos.net	10/18/19, 9:48 PM	1:07h
Office ATP Alert - Suspicious file found based on an Office ATP alert	88	Remediated	OfficeATP	barbaram-pc.mtpdemos.net	10/18/19, 9:06 PM	16:25m
Automated investigation started manually	85	No threats found	AutomatedInvestigation	gaile-pc.mtpdemos.net	10/17/19, 4:01 AM	42h
Automated investigation started manually	84	No threats found	AutomatedInvestigation	barbaram-pc.mtpdemos.net	10/16/19, 5:50 PM	2d
Automated investigation started manually	83	Terminated by system	AutomatedInvestigation	aarifs-pc	10/16/19, 10:02 AM	3d
Automated investigation started manually	80	No threats found	AutomatedInvestigation	barbaram-pc.mtpdemos.net	10/11/19, 3:33 PM	4:55h
Automated investigation started manually	77	Terminated by system	AutomatedInvestigation	gaile-pc.mtpdemos.net	10/10/19, 3:29 PM	3d
Automated investigation started manually	75	No threats found	AutomatedInvestigation	robertot-pc.mtpdemos.net	10/10/19, 2:50 PM	13:12m
'WmiRegBasedCommand' malware was detected	73	No threats found	Antivirus	barbaram-pc.mtpdemos.net	10/5/19, 7:16 AM	7:32m

**Filters**

**Status**

- Any
- No threats found (7)
- Remediated (6)
- Terminated by system (2)
- Partially investigated (1)
- Partially remediated (1)

**Triggering alert**

- Any
- Automated investigation started ma... (9)
- 'WmiRegBasedCommand' malware ... (2)
- Hacktool Mimikatz detected (2)
- Office ATP Alert - Suspicious file fou... (2)
- 'AutoKMS' unwanted software was d... (1)

**Detection Source**

- Any
- AutomatedInvestigation (9)
- Antivirus (4)
- EDR (2)
- OfficeATP (2)

# Investigation graph

The screenshot displays the Microsoft Defender Security Center interface for an investigation titled "'Powersploit' malware was detected". The investigation is marked as "Remediated" and "Investigation #99 is complete".

**Investigation details:**

- Status: Remediated (Malicious entities found were successfully re-mediated.)
- Alert severity: Informational
- Category: Malware
- Detection source: Antivirus

**Investigation graph:**

- Machine (1):** BARBARAM-PC
- Entities analyzed (4182):** 2941 Files (1 Remediated), 197 Processes, 291 Services, 414 Drivers, 27 IP Addresses
- Alert received:** "'Powersploit' malware was detected" with 4 correlated alerts.
- Evidence:** 1 entity found
- Process flow:** Waited for machine(s) → Waited for 5 Seconds → Result: Remediated

# Microsoft Threat Experts

Bring deep knowledge and proactive threat hunting to your SOC



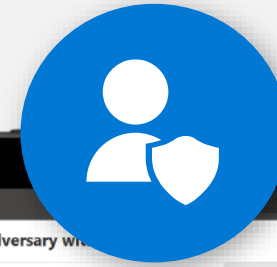
Expert level threat monitoring and analysis



Environment-specific context via alerts



Direct access to world-class hunters



The screenshot displays the Microsoft Defender Security Center interface. The main alert is titled "Detection of file linked to adversary with supply chain attacks" and is categorized as "High" severity and "Execution" category. The alert source is "Microsoft Threat Experts". The interface includes sections for "Alert context", "Description", "Executive summary", "Timeline of observed events", "Impacted machines", "Recommended actions", "Recommendation summary", and "Indicators of Compromise".

**Alert context**

Severity: High  
Category: Execution  
Detection source: Microsoft Threat Experts

**Alert context**

desktop-c7ud4hh  
janedoe

First activity: 9.10.2019 | 23:43:38  
Last activity: 9.10.2019 | 23:43:38

**Description**

**Executive summary**

This alert provides additional context for an alert you have received. [Windows Defender AV detected 'Winnti' high-severity malware](#). We observed suspicious activity within your organization from a file, confirmed to be a true-positive antivirus signature associated with a documented Supply Chain attack. The command-and-control servers associated with the original attack have already been taken down and are no longer active, you can read more about the associated action [here](#). While it is unlikely that the second stage of this payload for the original attack was received, this attack highlights the importance of limiting users from having local administrator privileges, which can be a target for attackers targeting domain credentials with malicious binaries.

**Timeline of observed events**

Date/Time	Notes
2019-09-10T20:46:58.702Z	Install (2).exe executes, causing approximately 200 files to be installed, including InstallConfig.exe
2019-09-10T21:19:51.768Z	InstallLauncher.exe performs a connection out to a command-and-control server
2019-09-10T21:19:52.563Z	Network connection to IP address 131.107.147.82

**Impacted machines**

Machine Id	Notes
fb7e23d4a69a18071013f69cc016f1508b76e9a22	Impacted machine 1

**Recommended actions**

**Recommendation summary**

1. Fully investigate the machine in question.
2. Practice the principle of least-privilege and maintain cred...
3. Restricting local administrative privileges can help limit in...
4. Enforce strong, randomized local administrator passwords...
5. If you have any questions about this alert, you can ask the select "Consult a threat expert".
6. If you need immediate help from Microsoft Incident Resp...
6. Examine the Indicators of Compromise (IOCs) in the table investigation.

**Indicators of Compromise**

IOC

Install (2).exe [\[explore\]](#)

InstallConfig.exe [\[explore\]](#)

InstallLauncher.exe [\[explore\]](#)

881ba9b12040d4576b5e09de73e5eb33de2e44b4 [\[explore\]](#)

ab16cd1b09e5157791a568456a12659aae926801 [\[explore\]](#)

131.107.147.82 [\[explore\]](#)

# Alerts > Detection of file linked to adversary with supp...

**Microsoft Threat Experts** **BARIUM** Detection of file linked to adversary with supply chain attacks  
 This alert is part of incident (54693)

Automated investigation is not applicable to alert type

Severity: High  
 Category: Execution  
 Detection source: Microsoft Threat Experts

### Alert context

desktop-c7ud4hh  
 janedoe

First activity: 9.10.2019 | 23:43:38  
 Last activity: 9.10.2019 | 23:43:38

### Description

#### Executive summary

This alert provides additional context for an alert you have received, [Windows Defender AV detected 'Winnti' high-severity malware](#). We observed suspicious activity within your organization from a file, confirmed to be a true-positive antivirus signature associated with a documented Supply Chain attack. The command-and-control servers associated with the original attack have already been taken down and are no longer active, you can read more about the associated action [here](#). While it is unlikely that the second stage of this payload for the original attack was received, this attack highlights the importance of limiting users from having local administrator privileges, which can be a target for attackers targeting domain credentials with malicious binaries.

### Timeline of observed events

Date/Time	Notes
2019-09-10T20:46:58.702Z	Install (2).exe executes, causing approximately 200 files to be installed, including InstallConfig.exe
2019-09-10T21:19:51.768Z	InstallLauncher.exe performs a connection out to a command-and-control server
2019-09-10T21:19:52.563Z	Network connection to IP address 131.107.147.82

### Impacted machines

Machine Id	Notes
fb7e23d4a69a1807013f69cc416f1508b76e9a22	Impacted machine 1

- ### Recommended actions
- #### Recommendation summary
- Fully investigate the machine in question
  - Practice the principle of least-privilege by Restricting local administrative privileges
  - Enforce strong, randomized local admini
  - If you have any questions about this alert select 'Consult a threat expert'.
  - If you need immediate help from Micros
  - Examine the Indicators of Compromise (I


### Indicators of Compromise

IOC
Install (2).exe <a href="#">[explore]</a>
InstallConfig.exe <a href="#">[explore]</a>
InstallLauncher.exe <a href="#">[explore]</a>
881ba9b12040d4576b5e09de73e5eb33de2e <a href="#">[explore]</a>
ab16cd1b09e5157791a568456a12659aae92 <a href="#">[explore]</a>
131.107.147.82 <a href="#">[explore]</a>

### Microsoft Threat Experts - Trial

Your Experts on Demand trial version expires in 41 days from your Microsoft Threat Experts enrolment. Contact your Microsoft representative to get a full subscription.

Learn more about [Microsoft Threat Experts – Experts on Demand](#)



## Consult a threat expert

Get Microsoft Threat Experts advice and insights about suspicious activities in your organization.

Ensure that the portal page for the alert or machine in question is in view while providing information for this inquiry.

Note: This and other relevant information will be shared with Microsoft Threat Experts to enable the best response to your inquiry.

**Inquiry topic \***

**Email \***

Enter the email address you'd like Microsoft Threat Experts to send their reply

[Privacy statement.](#)



# Security Management

Assess, configure and respond to changes in your environment



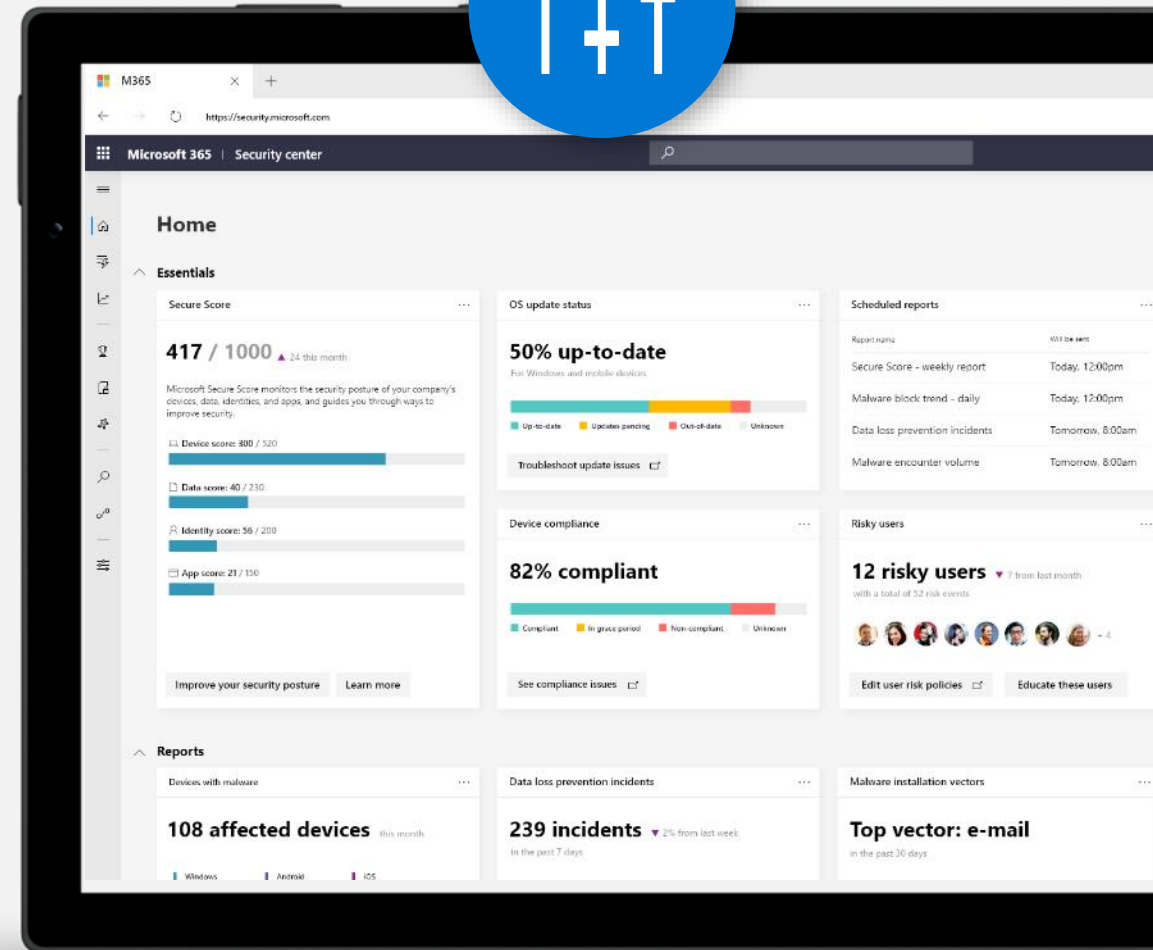
Centrally assess & configure your security



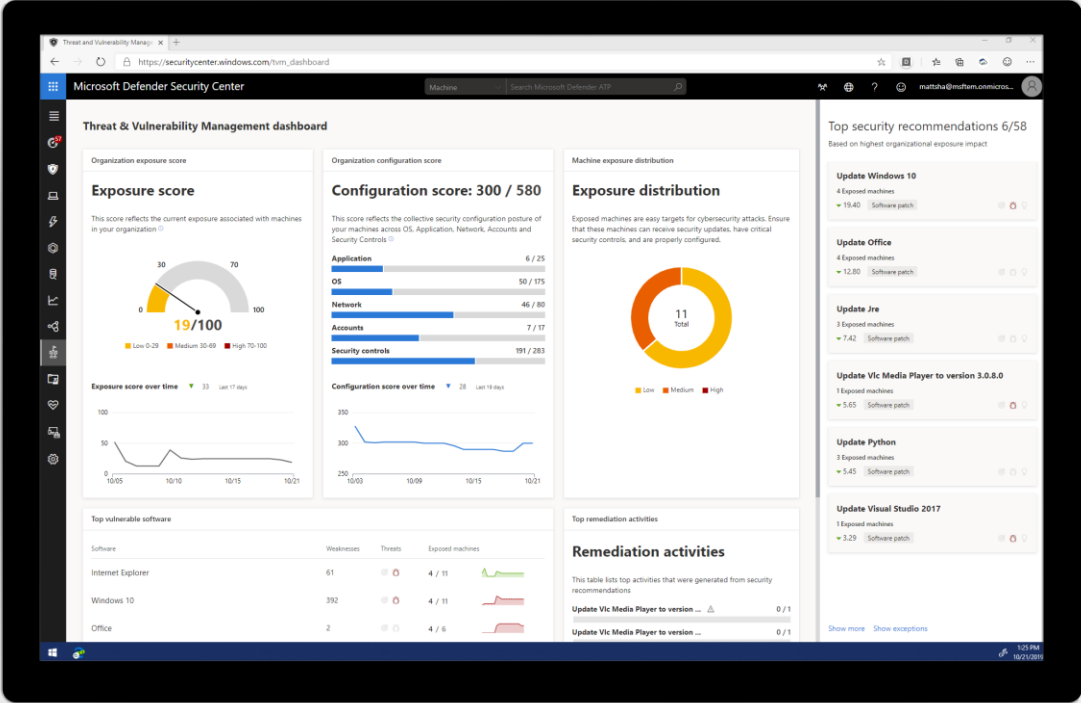
Variety of reports and dashboards for detailed monitoring and visibility



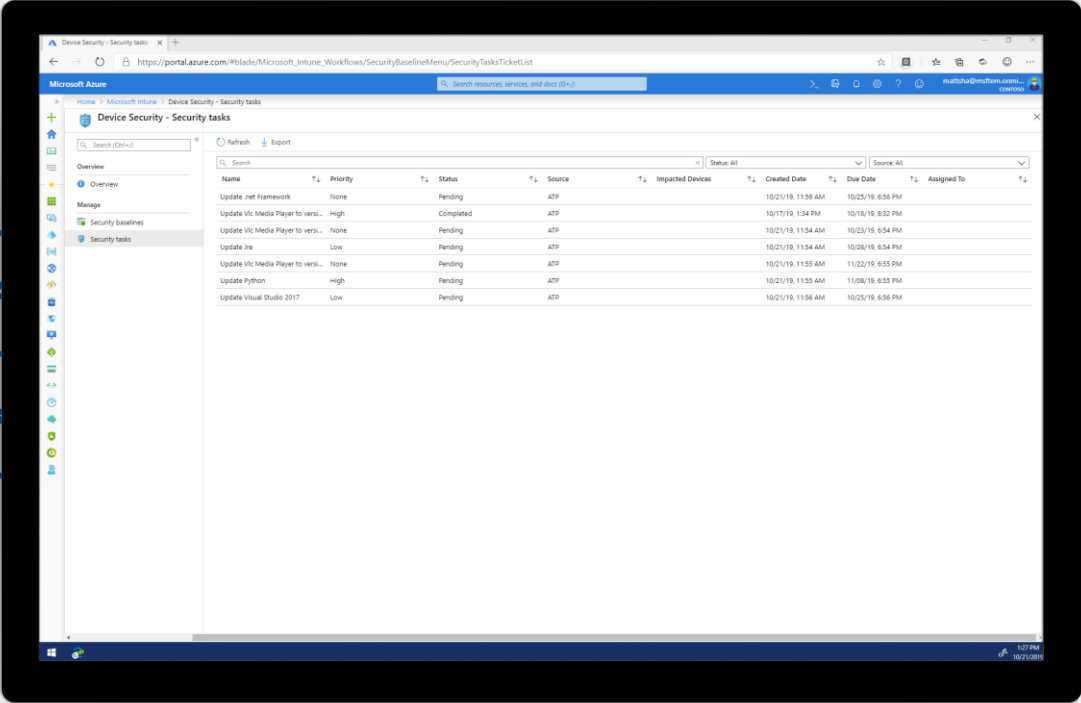
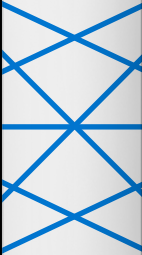
Seamless integration between policy assessment and policy enforcement



# Seamless integration



Microsoft Defender for Endpoint  
Policy Assessment

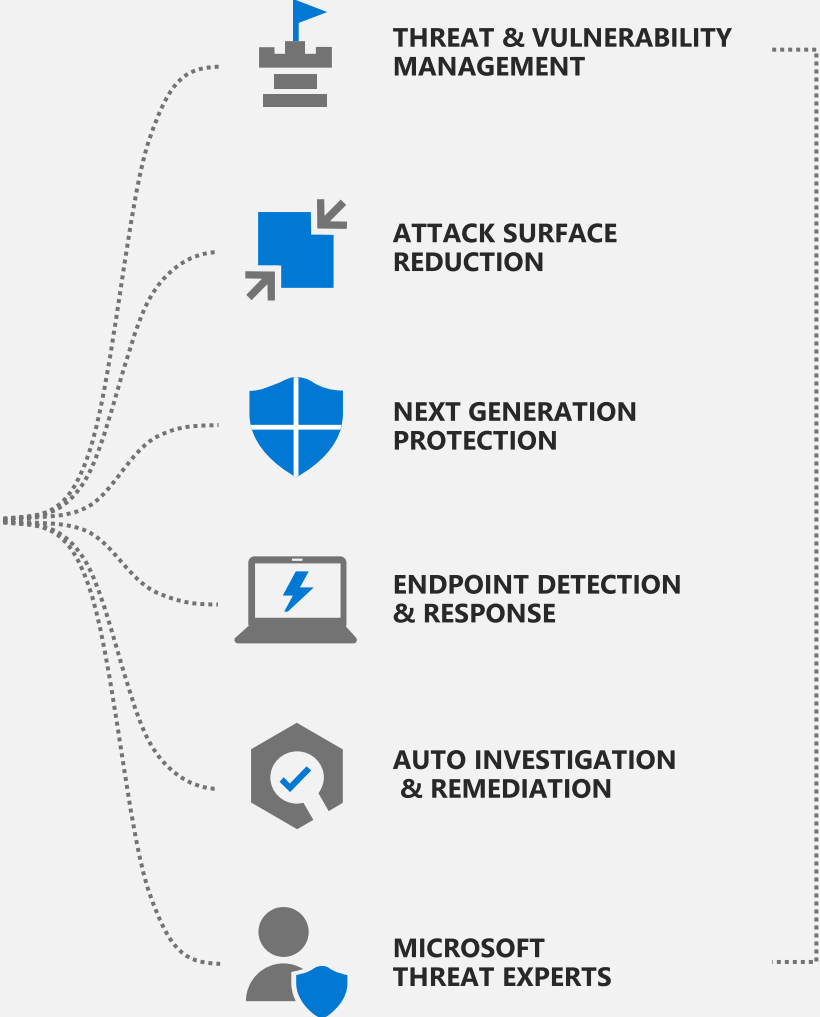


Microsoft Endpoint Manager  
Policy Enforcement

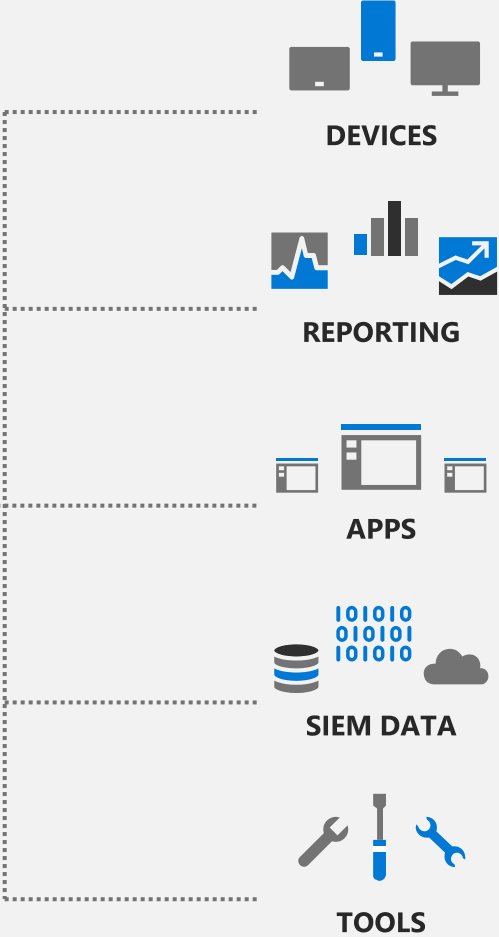
# Connecting with the platform



Threats are no match.



**APIS AND INTEGRATION**



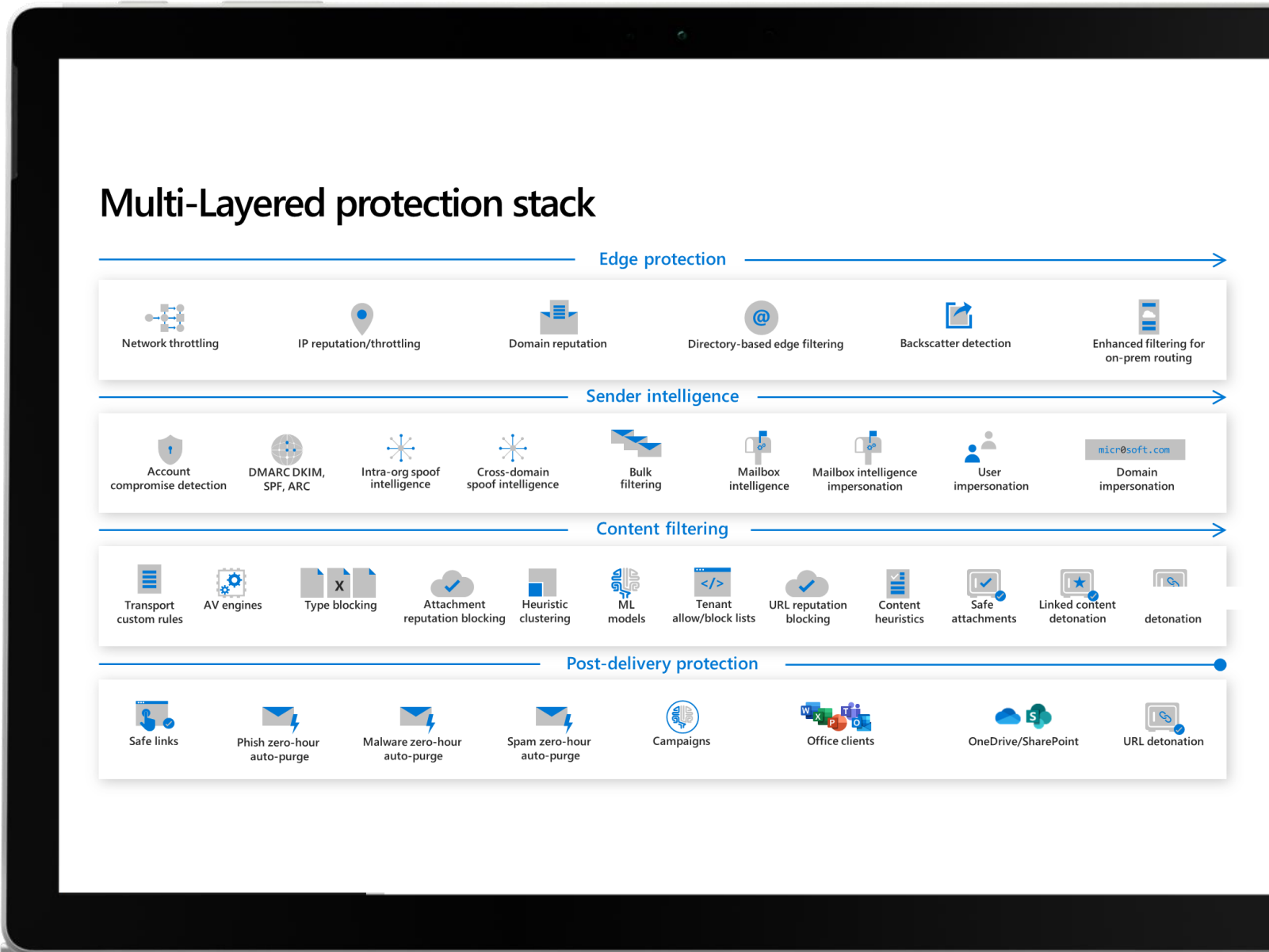


# Defender for O365

---

# Prevention

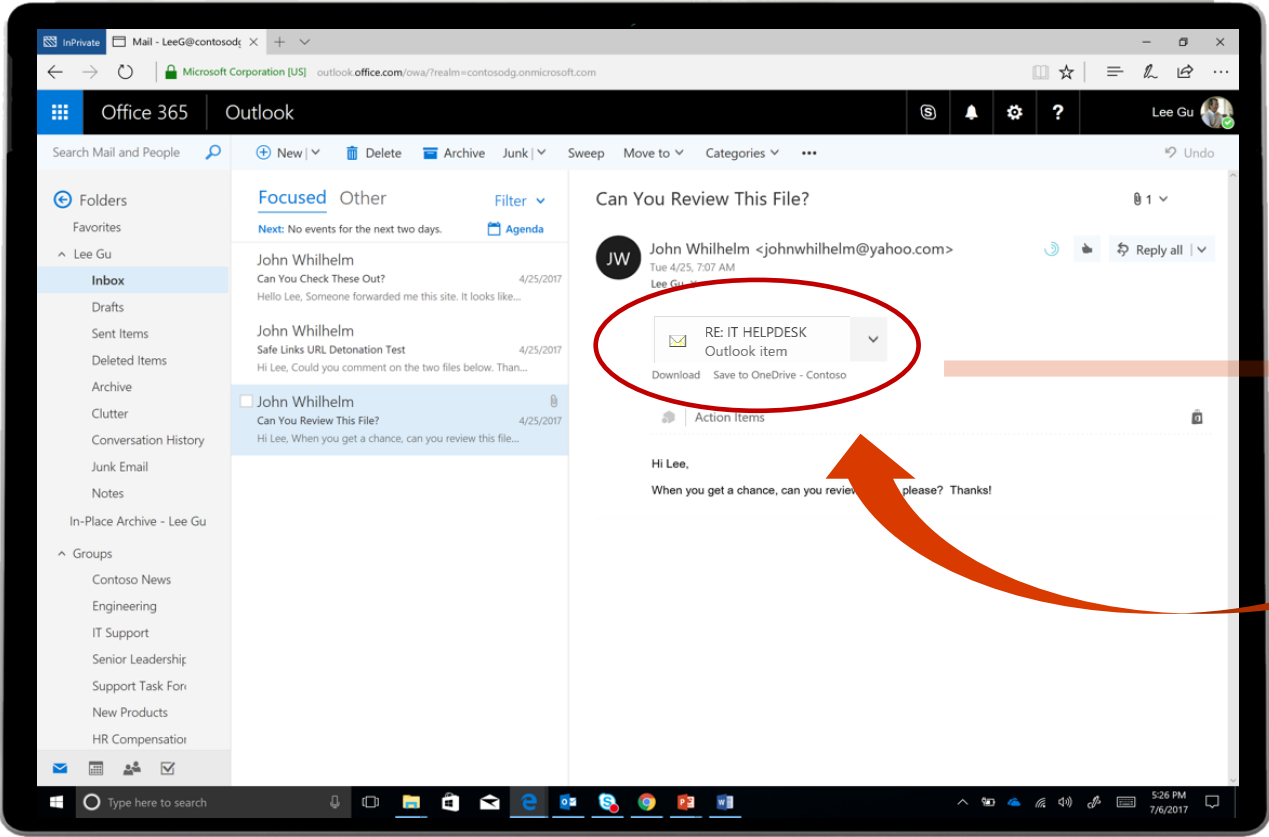
- Multi-layered filtering stack to protect against wide variety of attacks
- Advanced protection against credential phishing, BEC, and account takeover
- Protection beyond email



# Prevention

## Safe Attachments

Sandboxing technology for protecting against malicious attachments



Sandboxing

Observed Behavior

Network Traffic

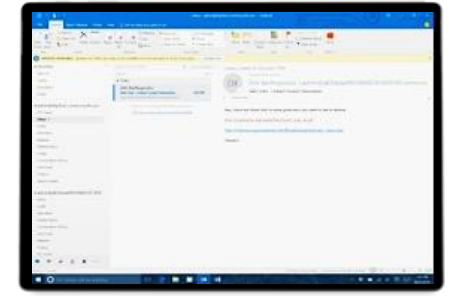
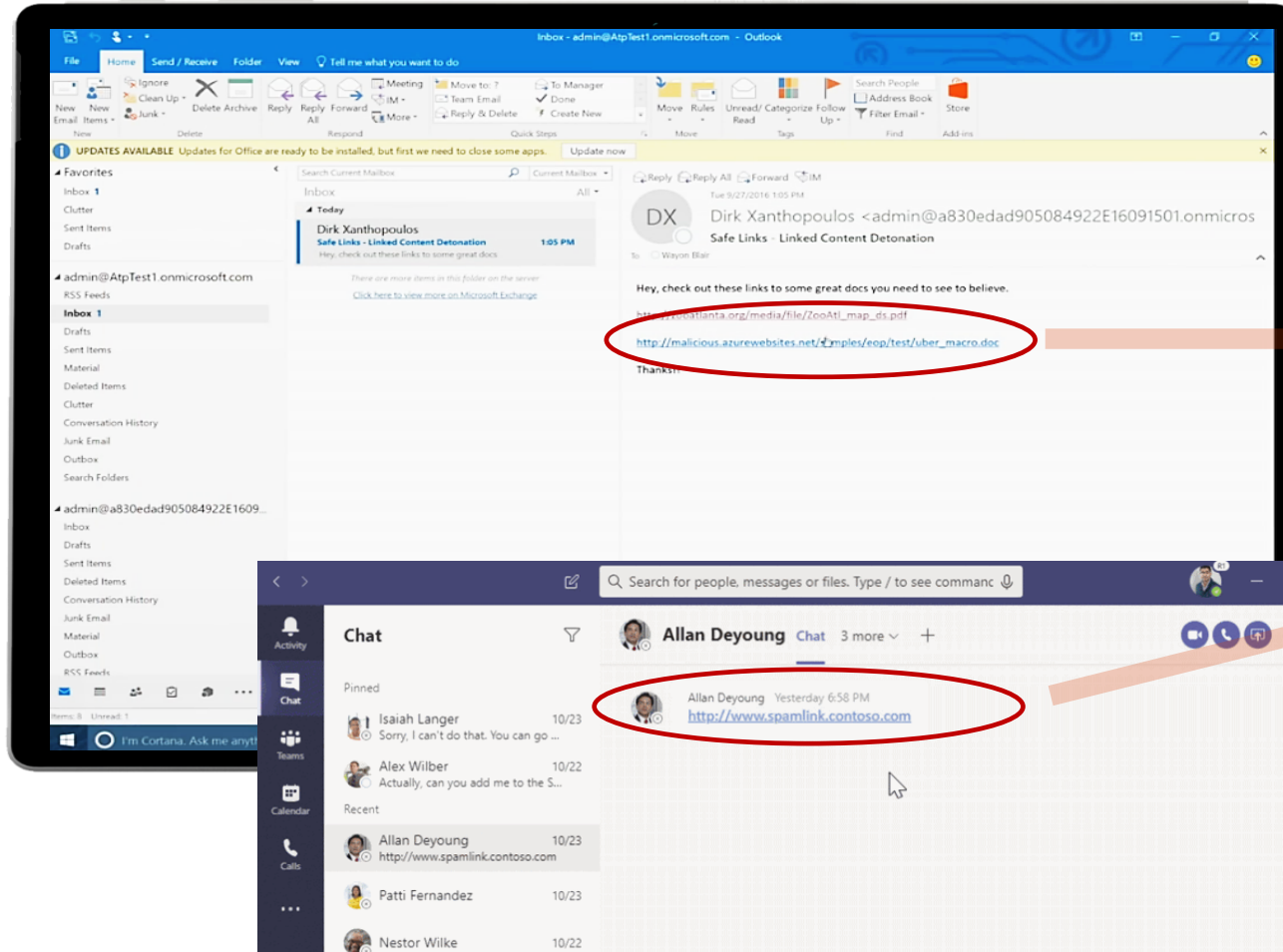
Downloaded Files



# Prevention

## Safe Links for Email & Microsoft Teams

URL detonation within emails & Teams chat



Email with re-written url



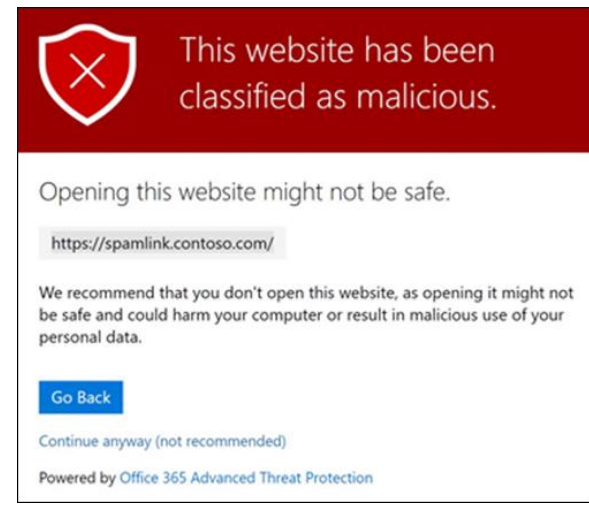
User clicking URL is taken to EOP web servers for the latest check at the "time-of-click"



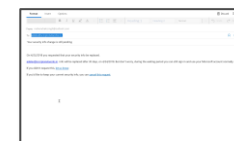
URL Analysis Sandboxing



Link added to reputation serv



VIDEO DEMO



# Prevention

## Protection within your Office Applications

ATP Time-Of-Click URL Protection for your Office Desktop & Mobile clients

Protection provided Irrespective of the document source – Corporate / Personal email, USB, Google drive etc.



VIDEO DEMO



Word



Excel



PowerPoint

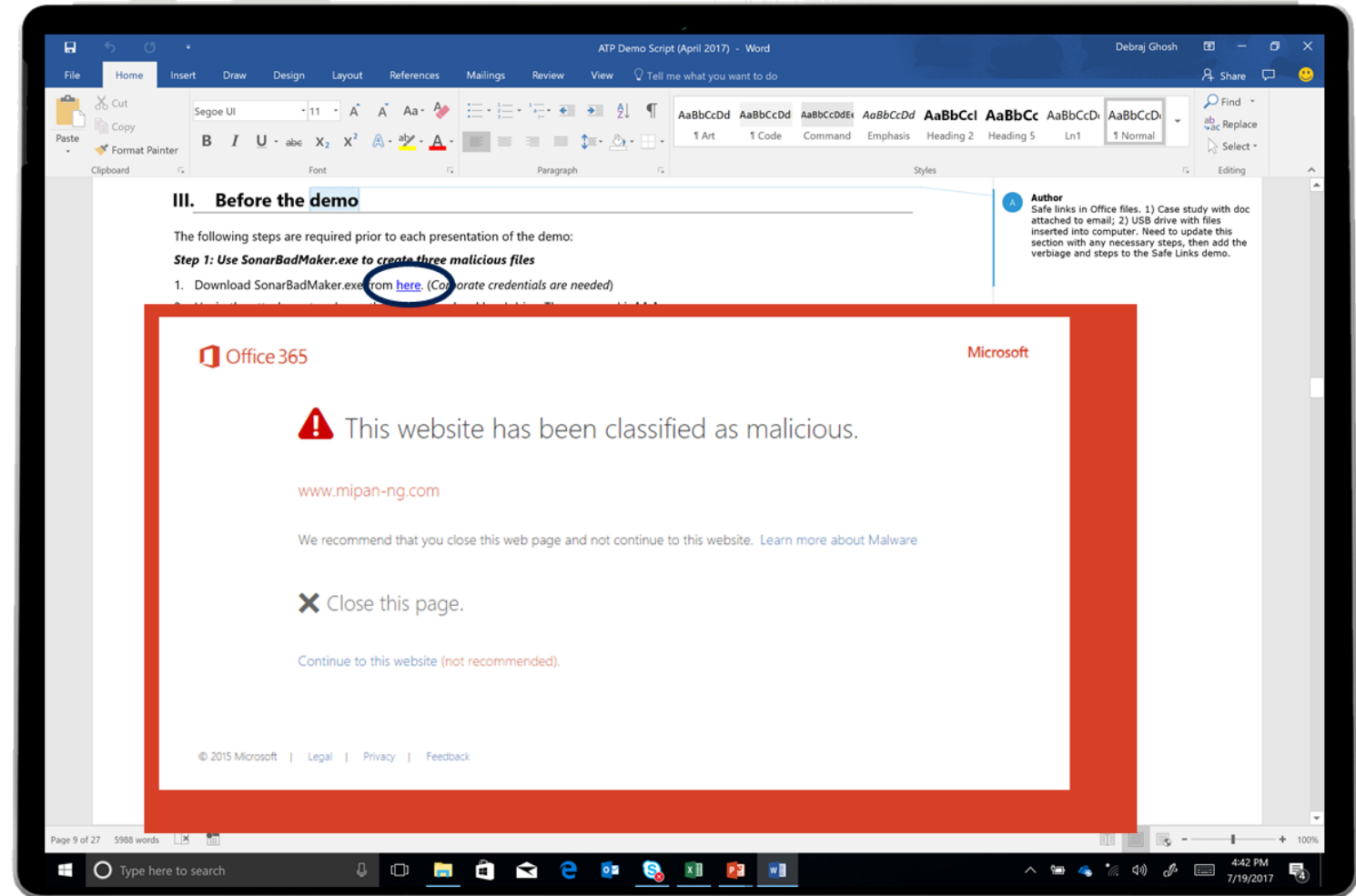


Visio

Improve your security against advanced threats, unknown malware, and zero-day attacks

Protect users from malicious links with time-of-click protection

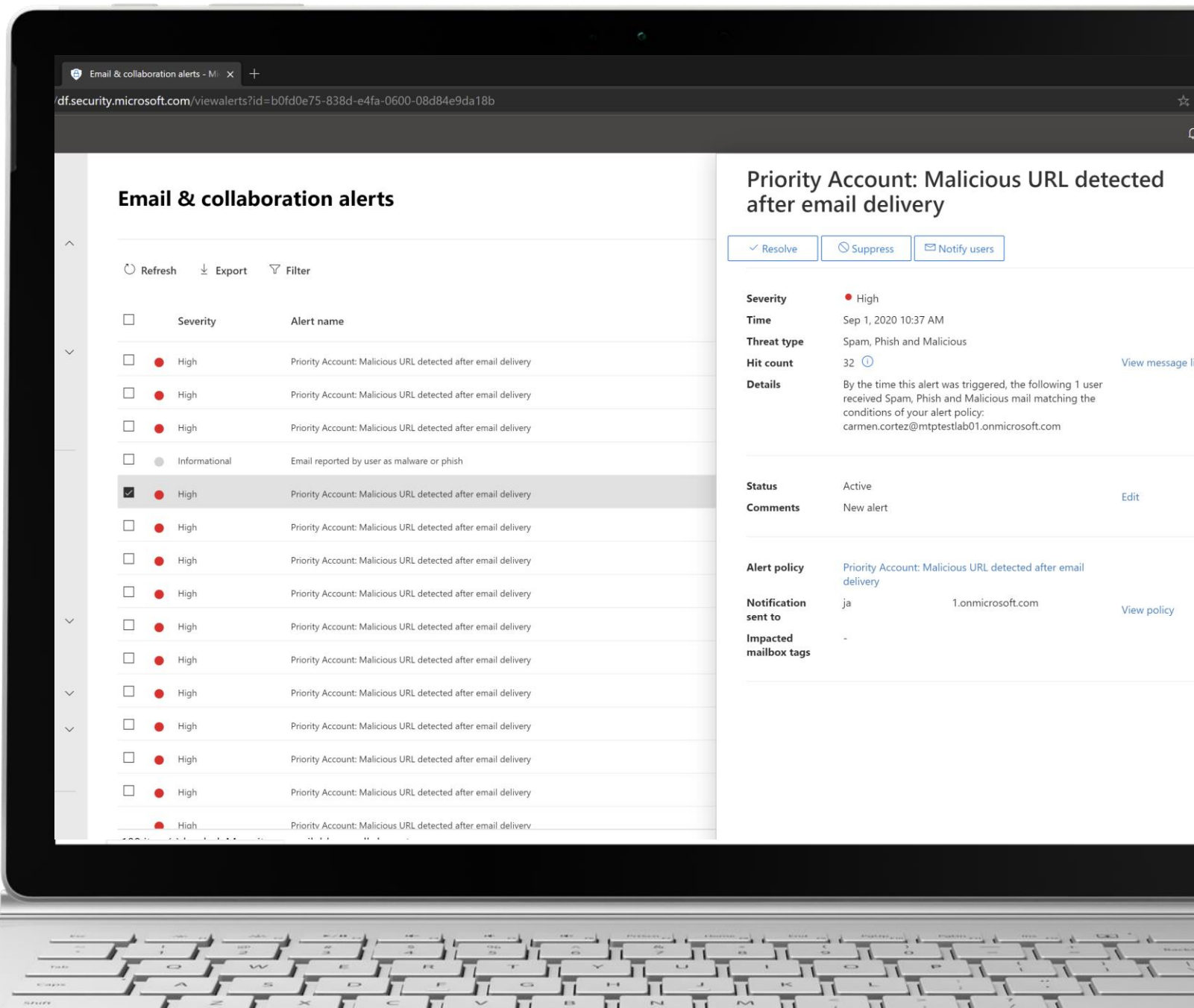
Safeguard your environment from malicious documents using virtual environments





# Detection

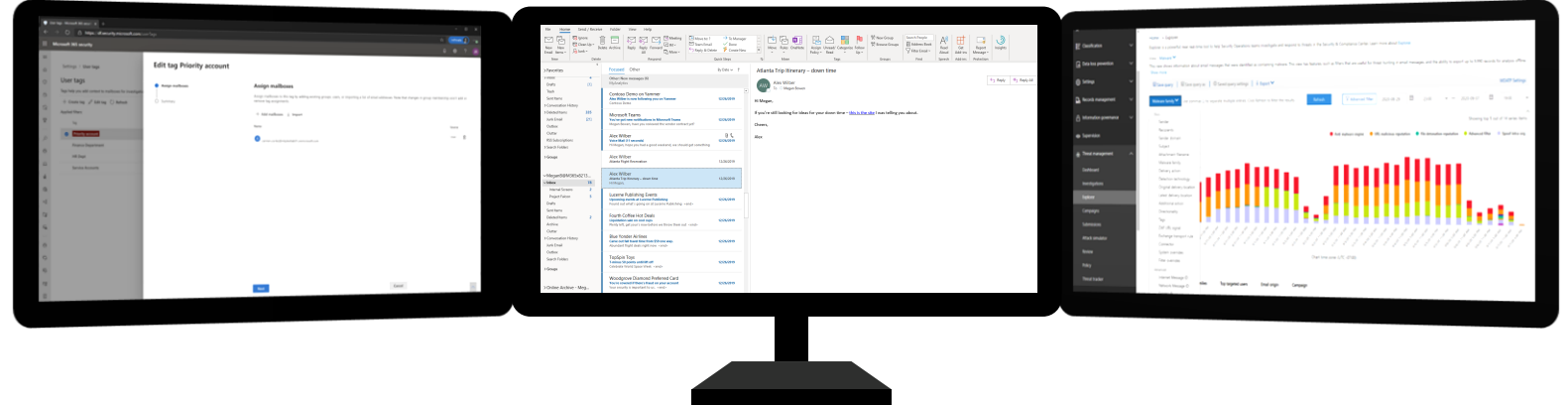
- Campaign Views leverage AI to surface coordinated attacks designed to evade detection
- Detailed alerts
- Detection of content weaponized after delivery



# Investigation & Hunting

## Investigation & Hunting

- Prioritized focus through Priority accounts
- User & Admin Submissions
- Threat Explorer



# Investigation & Hunting

- Prioritized focus through Priority accounts
- User & Admin Submissions
- Threat Explorer

The screenshot displays the Microsoft Threat Explorer interface for an email titled "re: I need specific ranks t...". The interface is divided into several sections:

- Threat Management > Explorer > re: I need specific ranks t...** (Breadcrumbs)
- Tags** (Dropdown menu)
- Detection details** (Dropdown menu)
- Threat**: Malware, Phish, Spam
- Latest delivery location**: Quarantine
- Original delivery location**: Quarantine
- Detection tech**: Advanced filter, Antimalware protection, Spoof intra-org
- Delivery action**: Blocked
- No overrides** (Dropdown menu)
- Email details** (Dropdown menu)
- Directionality**: Inbound
- Recipient (To)**: johndoe@... microsoft.com
- Sender (From)**: ...@gmail.com
- Time received**: Sep 18, 2020 9:21 AM
- Timeline** (Selected): Analysis, Attachments, URL, Similar emails
- Email detection details** (Dropdown menu)
- System override(s)**: None
- Exchange Transport Rule(s)**: -
- Junk mailbox rule**: -
- Bulk complaint level (BCL)**: -
- Spam confidence level (SCL)**: 9
- Policy**: -
- Policy action**: -
- Campaign ID**: N/A
- Sender-Recipient details** (Dropdown menu)
- Sender name**: Louise Lint
- Sender IP**: 74.208.194.182
- Domain name**: ...org
- Domain owner**: Unspam Technologies, Inc.
- Location**: US
- Domain creation date**: Jun 30, 2004
- Return-path**: ...org
- Plain-text email header** (Dropdown menu)
- Received headers**:
  - Received: from BL2NAM06FT009.Eop-nam06.prod.protection.outlook.com (10.152.106.51) by BL2NAM06HT009.Eop-nam06.prod.protection.outlook.com (10.152.106.153) with Microsoft SMTP Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.3433.0: Fri, 18 Sep 2020 16:21:51 +0000
  - Received: from NAM06-BL2-obe.outbound.protection.outlook.com (104.47.53.75) by BL2NAM06FT009.mail.protection.outlook.com (10.152.106.105) with Microsoft SMTP Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.3433.0 via Frontend Transport: Fri, 18 Sep 2020 16:21:50 +0000
  - Received: from MN2PR01CA0019.prod.exchangelabs.com (2603:10b6:208:10c::32) by BYAPR00MB0613.namprd00.prod.outlook.com (2603:10b6:a03:105::11) with Microsoft SMTP Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.3434.0: Fri, 18 Sep 2020 16:21:48 +0000
  - Received: from BL2NAM06FT011.Eop-nam06.prod.protection.outlook.com (2603:10b6:208:10c:cafe:a2) by MN2PR01CA0019.outlook.office365.com (2603:10b6:208:10c::32) with Microsoft SMTP Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.3391.11 via Frontend Transport: Fri, 18 Sep 2020 16:21:48 +0000
  - Authentication-Results: spf=pass (sender IP is 74.208.194.182) smtp.mailfrom=... dkim=none (message not signed) header.d=none:... dmarc=fail action=none header.from=gmail.com:compauth=pass reason=117
  - Received-SPF: Pass (protection.outlook.com: domain of ... org designates 74.208.194.182 as permitted sender) receiver=protection.outlook.com; client-ip=74.208.194.182; helo=u15366316.onlinehome-server.com;
  - Received: from u15366316.onlinehome-server.com (74.208.194.182) by



## Response & Remediation

- Guided hunting with inline actions
- Automated response playbooks
- Zero-Hour Auto-Purge (ZAP)

Home > Threat Investigation

Automated investigation and response (AIR) capabilities enable you to run automated investigation processes in response to well known threats. [Learn more](#)

↓ Export ↻ Refresh

Applied filters: Time range: 8/30/2020-9/10/2020

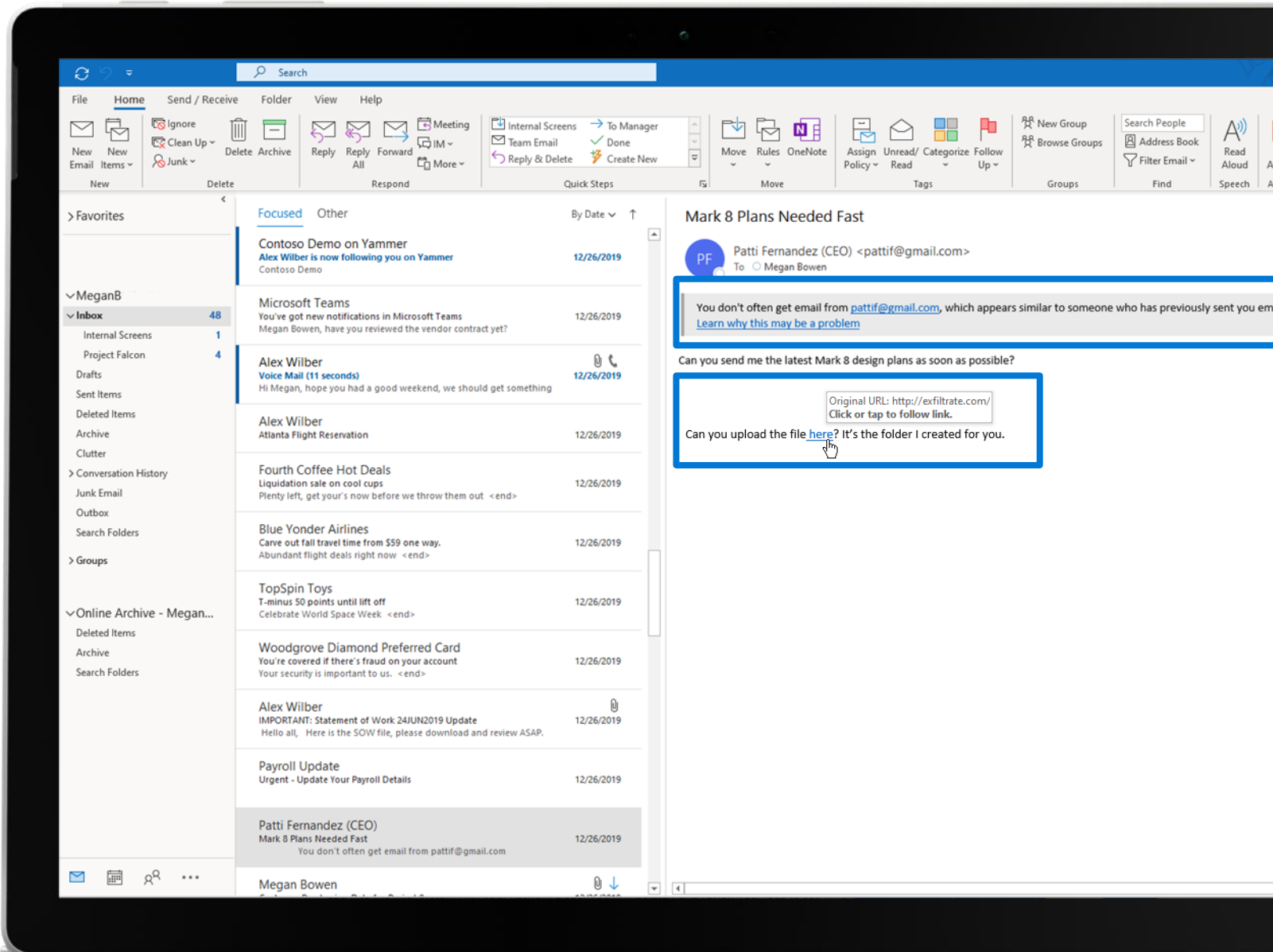
ID	Status	Detection Source	Investigation	Users
98824f	Pending Action	Office365	Email investigation for '回复: paid invoice'	johndoe@o onmicrosoft.co
d56b18	Remediated		Email was moved by hunting bulk action	sjain@o3 .onmicrosoft.com
10a2bd	Remediated		Email was moved by hunting bulk action	secreader@o3 onmicrosoft
97e196	Remediated		Email URL was blocked by hunting bulk action	secreader@o3 onmicrosoft
9f0442	Remediated		Email was moved by hunting bulk action	secreader@o3 onmicrosoft
f8589a	Remediated		Email was moved by hunting bulk action	secreader@o36 onmicrosoft
4a385d	Remediated		Email URL was blocked by hunting bulk action	tific@o36 inmicrosoft.com
14a6f9	Remediated		Email was moved by hunting bulk action	tific@o36 onmicrosoft.com
cb7228	Pending Action	Office365	User suspected of being compromised - testinguser28@o	testinguser28@o 2.onmicro
ee0ca5	Pending Action	Office365	User suspected of being compromised - secreader	secreader@o3 onmicrosoft
e7f455	Pending Action	Office365	User suspected of being compromised - johndoe	johndoe@o 2.onmicrosoft.o
e9c5ca	Remediated		Email was moved by hunting bulk action	tific@o36 onmicrosoft.com
c7249b	Failed		Email sender was blocked by hunting bulk action	sjain@o3 !.onmicrosoft.com

Data Investigations 50 item(s) out of 13491 loaded. More items available, scroll down to see more.



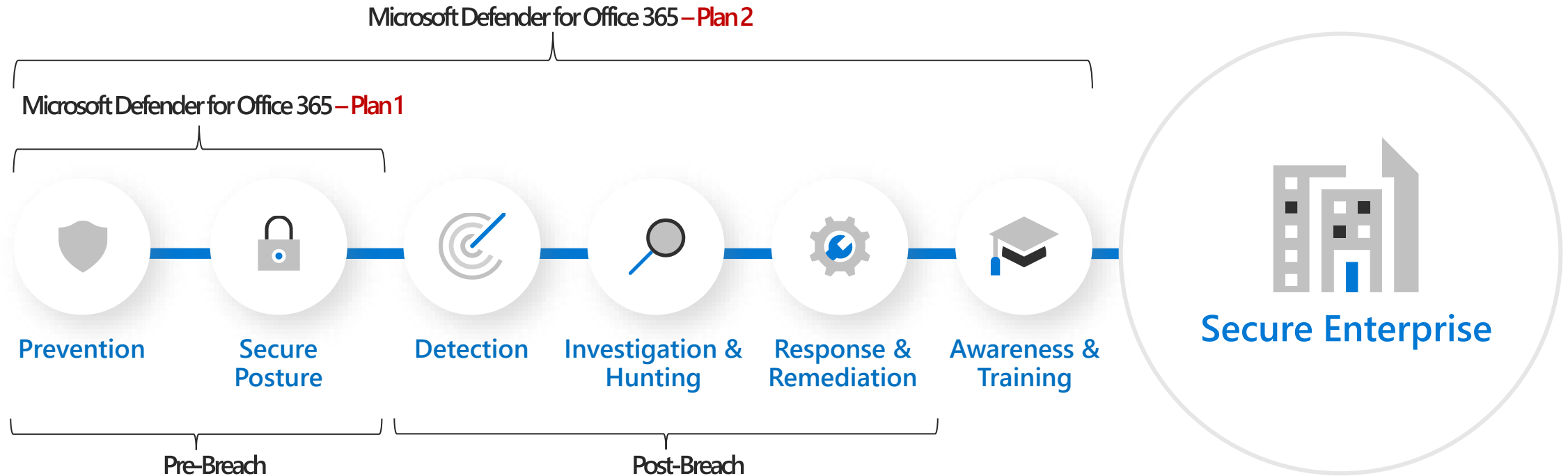
# Awareness & Training

- Enhanced simulation management
- Dynamic end user training
- Detailed reporting and insights
- Native experiences foster user awareness



# Microsoft Defender for Office 365

Securing your enterprise requires more than just prevention

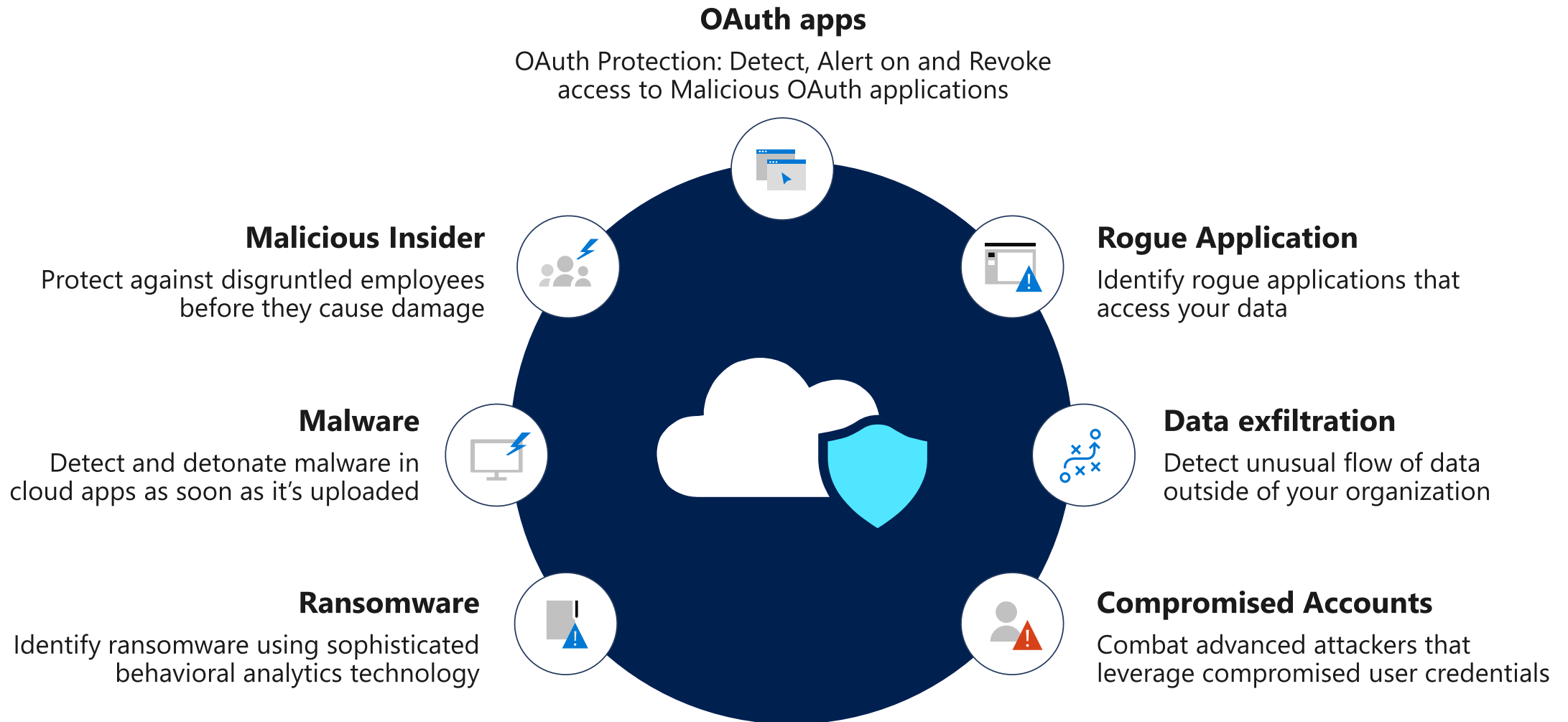




# Defender for Cloud App

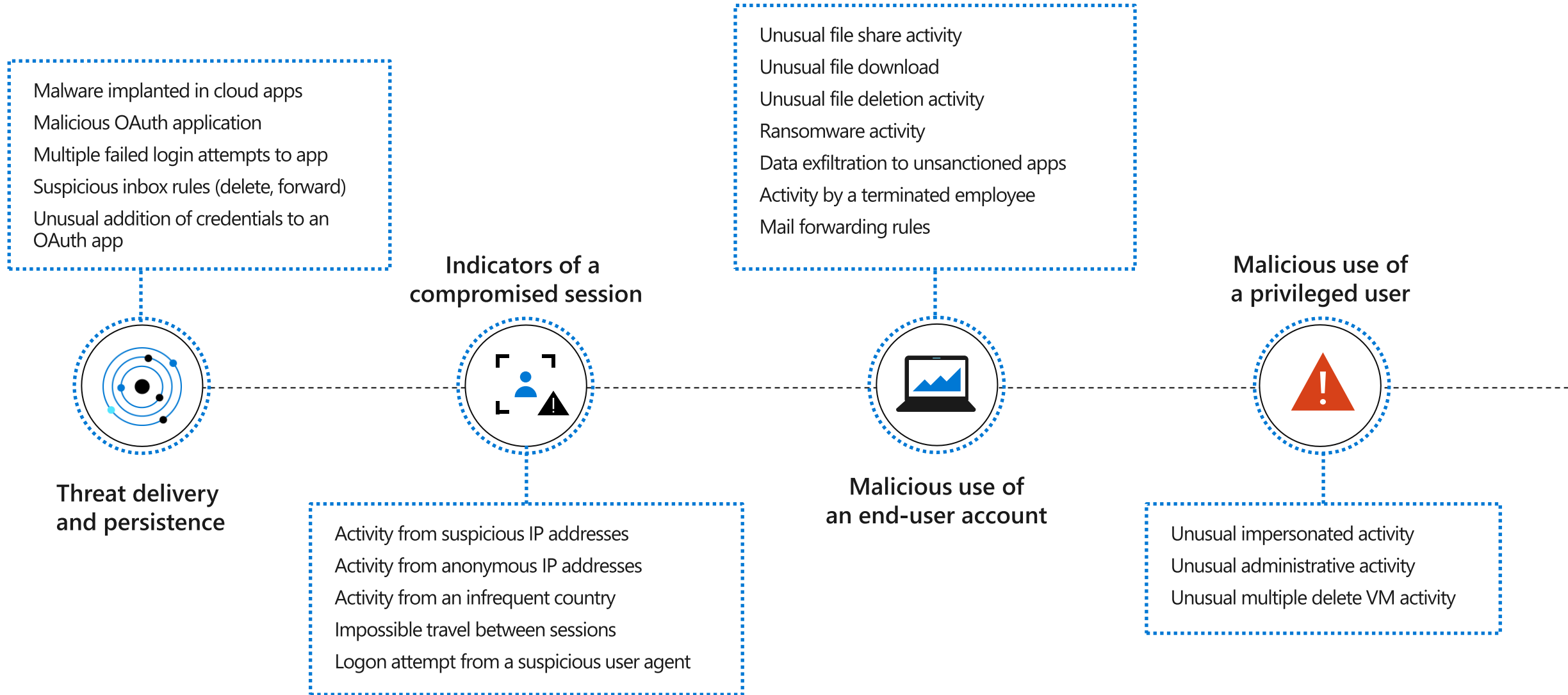
---

# Protection against cloud threats





# Detections across cloud apps



# Cloud Discovery with Microsoft Defender for Endpoint

## Native, endpoint-based discovery of Shadow IT

Connect your Defender for Endpoint system and gain visibility to your shadow IT from endpoints across your environment

## Discovery of cloud apps beyond the corporate network from any managed Windows 10 device

Discover cloud app usage from any managed Windows 10 device anytime, anywhere, by anyone

## Single-click enablement

With one click, stream traffic data from your managed Windows 10 devices into your Defender for Cloud Apps instance

## Device-based Discovery

Go beyond user-based discovery and attribute cloud app usage to managed devices in the organization

## Deep dive investigation in Microsoft Defender for Endpoint

In Microsoft Defender for Endpoint, drill down into each discovered device's behavior across your organization

The screenshot displays the Microsoft Defender for Cloud Apps interface. At the top, there's a navigation bar with 'Cloud App Security' and a search bar. Below it, the 'Cloud Discovery' section is active, showing tabs for 'Dashboard', 'Discovered apps', 'IP addresses', 'Users', and 'Machines'. A 'Continuous report' for 'Win10 Endpoint Users' is highlighted in the top right, with a timeframe of 'Last 90 days'. The main area shows a list of discovered apps with columns for App, Score, Traffic, Upload, Transactions, Users, IP addresses, Machines, Last seen (UTC), and Actions. The 'Machines' column is highlighted with a blue box. A sidebar on the left lists categories like 'Cloud storage', 'Hosting services', 'Marketing', etc., with 'Cloud storage' selected. The table lists various cloud storage services like Microsoft OneDrive, Dropbox, Mozy, iCloud, iDrive, Livedrive, SugarSync, and BitTitan.

App	Score	Traffic	Upload	Transactions	Users	IP addresses	Machines	Last seen (UTC)	Actions
Microsoft OneDrive for Cloud storage	10	98.5 GB	65.8 GB	125K	1109	2540	1110	Sep 20, 2018	✓ ⌂ ⋮
Dropbox Cloud storage	8	3.5 GB	2.5 GB	11.8K	918	1328	919	Sep 24, 2018	✓ ⌂ ⋮
Mozy Cloud storage	7	1.1 GB	732 MB	1.3K	187	127	188	Sep 24, 2018	✓ ⌂ ⋮
iCloud Cloud storage	7	1.1 GB	689 MB	1.3K	182	132	182	Sep 24, 2018	✓ ⌂ ⋮
iDrive Cloud storage	6	443 MB	272 MB	1.7K	235	174	235	Sep 24, 2018	✓ ⌂ ⋮
Livedrive Cloud storage	6	258 MB	180 MB	1.5K	213	157	213	Sep 24, 2018	✓ ⌂ ⋮
SugarSync Cloud storage	6	1.5 GB	1.1 GB	1.6K	224	169	225	Sep 24, 2018	✓ ⌂ ⋮
BitTitan	6	24 MB	21 MB	1.2K	178	132	178	Sep 24, 2018	✓ ⌂ ⋮

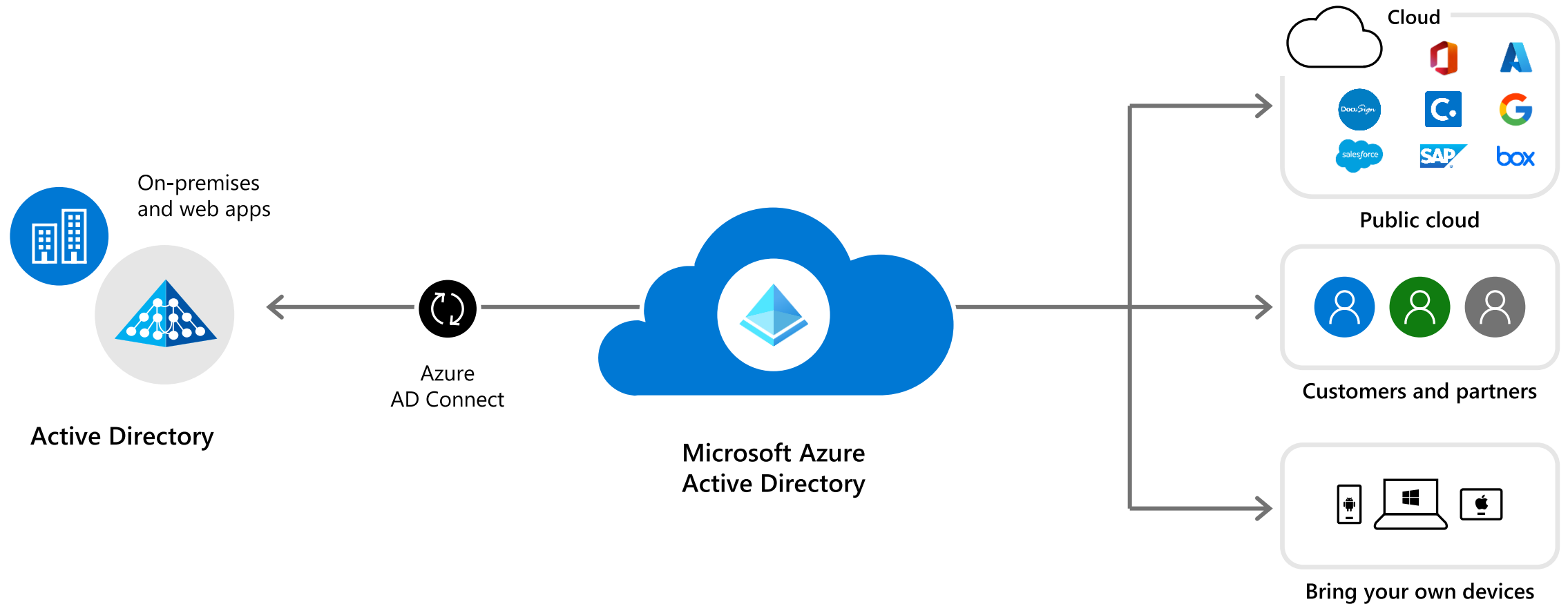


# Defender for Identity

---

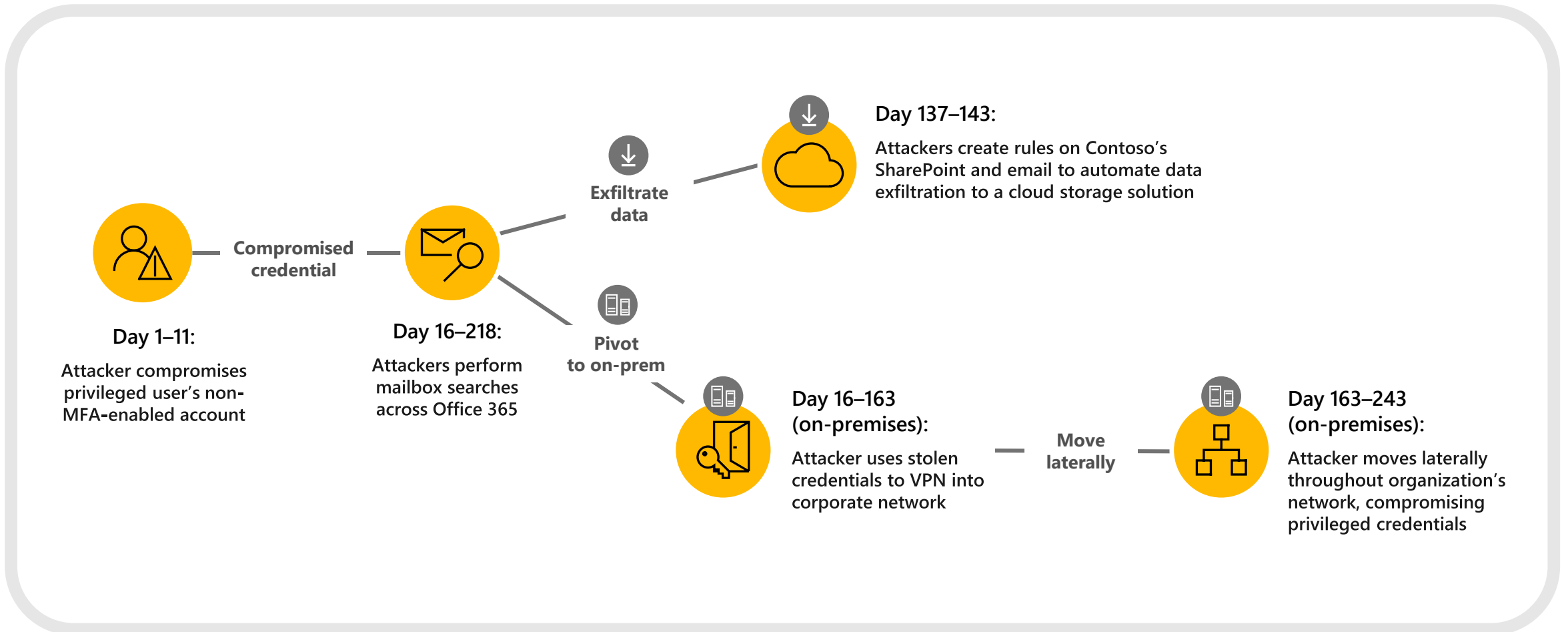
# The complexity of the enterprise identity security landscape

Enterprise security environments are complex—and include both on-premises and cloud assets



# Anatomy of an on-premises and cloud environment attack

One example of how an attack happens and compromises an entire organization



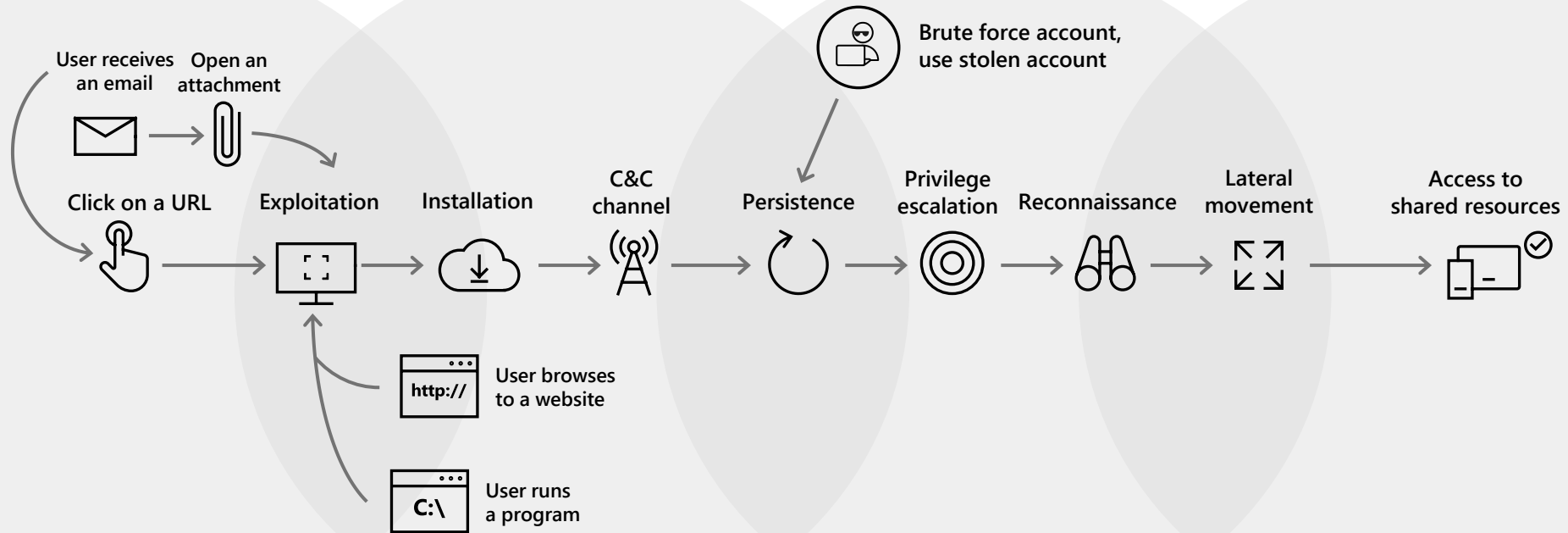
# Attacks go across perimeter defense stack boundaries

**Applications**  
Application protection

**Endpoints**  
Endpoint protection

**Identity**  
Identity protection

**Data**  
Email and data protection



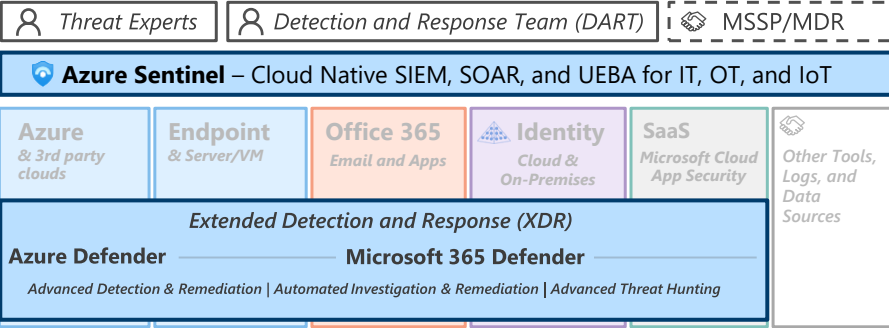
Microsoft Defender for Office 365  
Microsoft Defender for Cloud Apps  
SmartScreen

Microsoft Defender for Endpoint

Microsoft Defender for Identity  
Azure Active Directory  
Microsoft Defender for Cloud Apps

Microsoft Defender for Office 365  
Microsoft Defender for Cloud Apps

# Security Operations / SOC



# Cybersecurity Reference Architecture

## Security modernization with Zero Trust Principles

May 2021 – <https://aka.ms/MCRA>

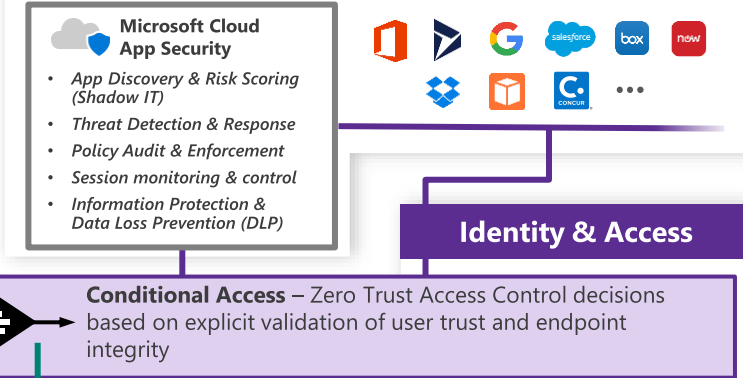
This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

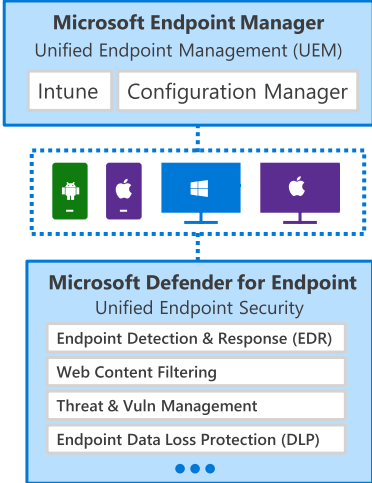
### Security Guidance

1. [Security Documentation](#)
2. [Microsoft Best Practices](#)
3. Azure Security [Top 10 | Benchmarks](#) | [CAF](#) | [WAF](#)

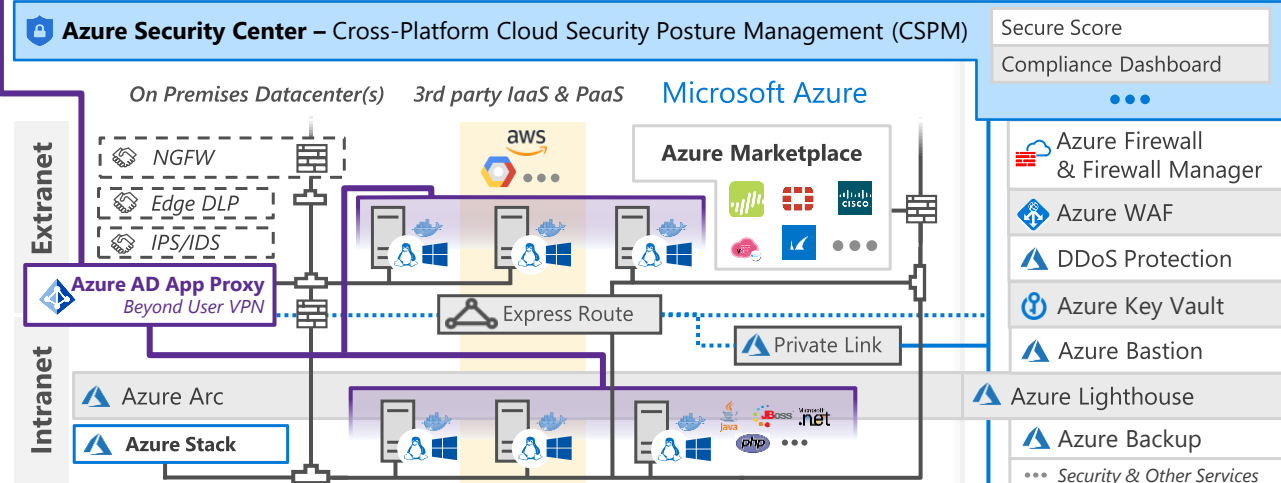
# Software as a Service (SaaS)



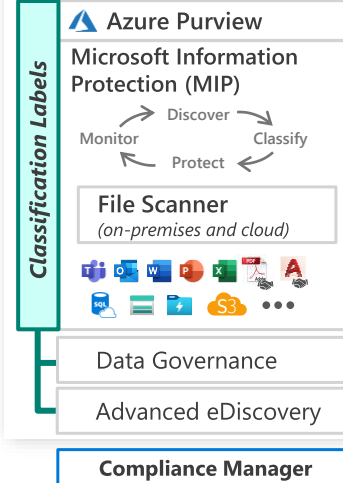
# Endpoints & Devices



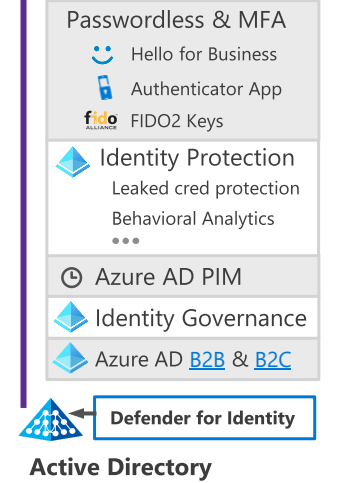
# Hybrid Infrastructure – IaaS, PaaS, On-Premises



# Information Protection



# Azure Active Directory

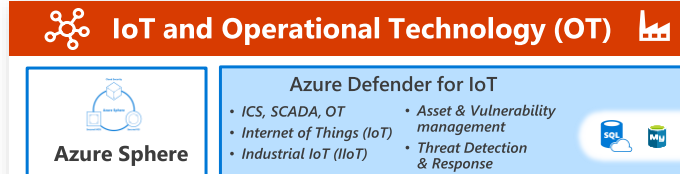
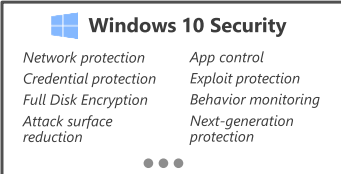


**Securing Privileged Access** – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

**Privileged Access Workstations (PAWs)** - Secure workstations for administrators, developers, and other sensitive users

**Microsoft Secure Score** – Measure your security posture, and plan/prioritize rapid improvement with included guidance

**Microsoft Compliance Score** – Prioritize, measure, and plan improvement actions against controls



**Threat Intelligence** – 8+ Trillion signals per day of security context

**Service Trust Portal** – How Microsoft secures cloud services

**Security Development Lifecycle (SDL)**