#ExpertsLiveNO

Experts Live Norway

Threat Intelligence with Microsoft 365

Stefan Schörling - Innofactor

Weekend Offender - Daily Defender

🐦 @stefanschorling

Platinum Sponsor 2019

Microsoft

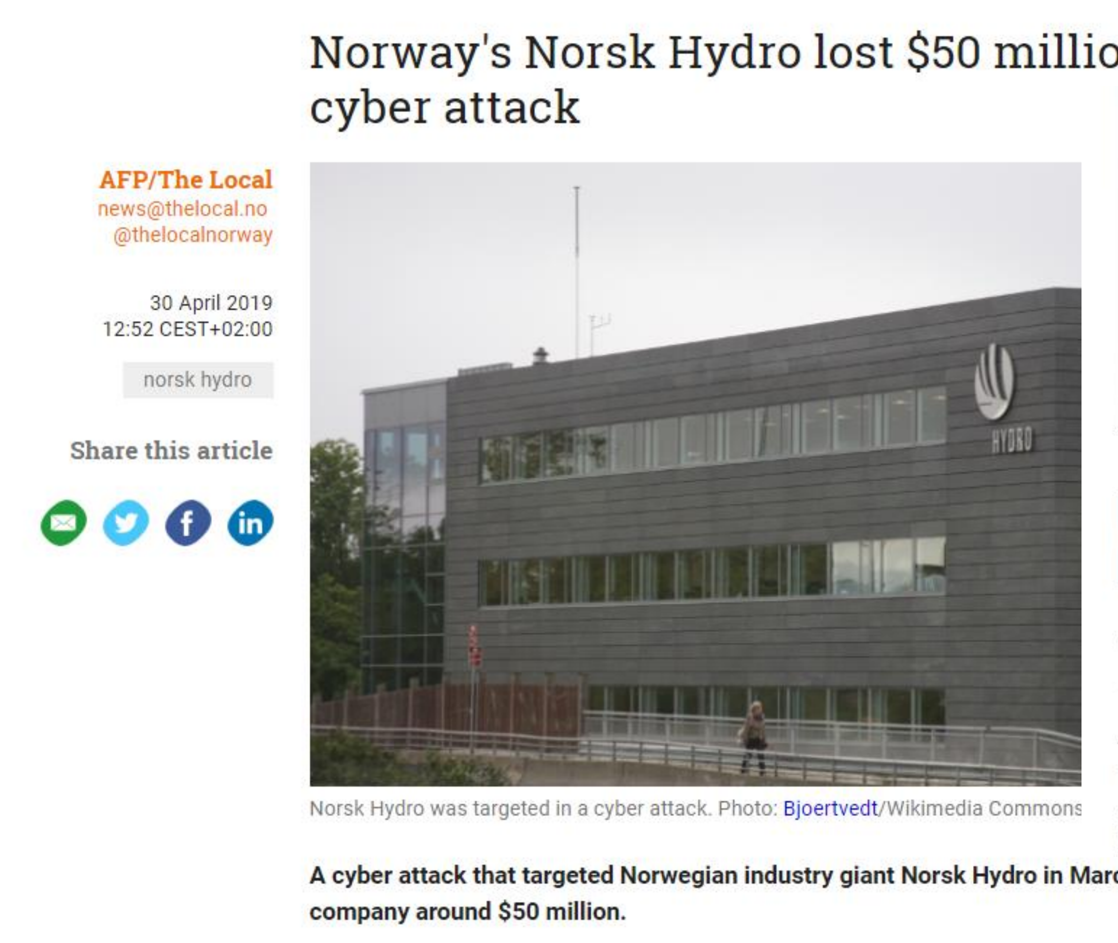
Microsoft 365

Windows 10

Enterprise
Mobility + Security

Office 365

Is there a need for Threat Protection?



Norway's Norsk Hydro lost $50 million in cyber attack

AFP/The Local
news@thelocal.no
@thelocalnorway

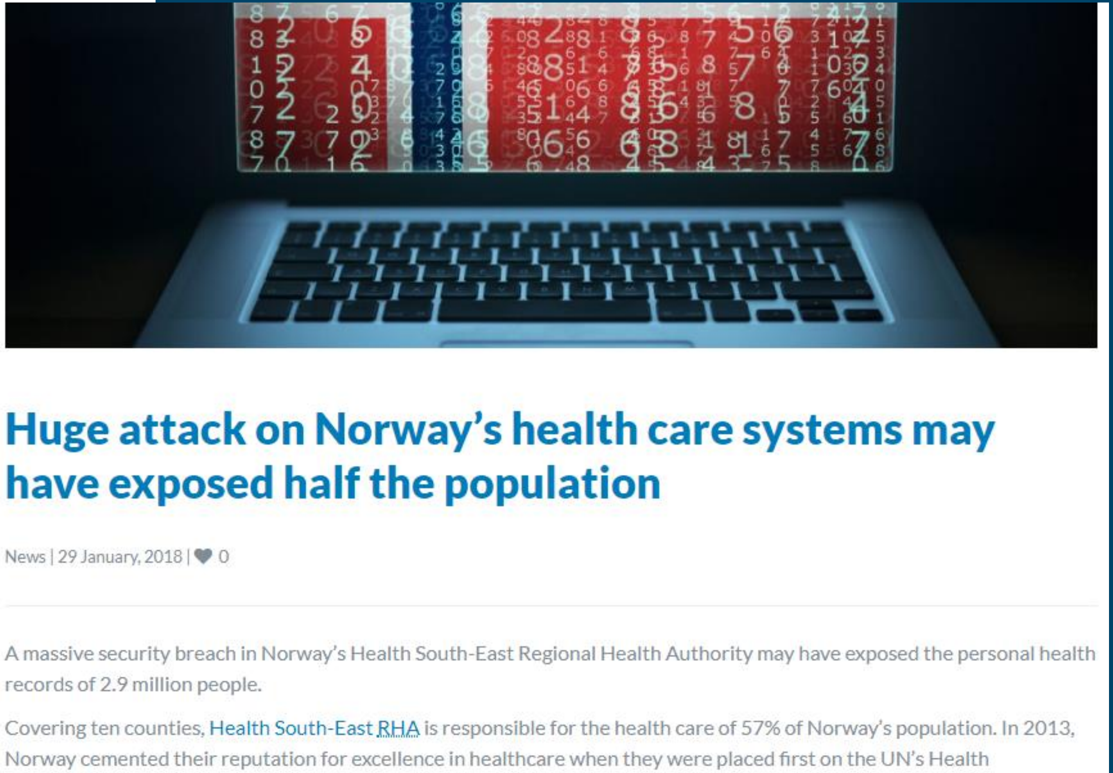
30 April 2019
12:52 CEST+02:00

norsk hydro

Share this article

Norsk Hydro was targeted in a cyber attack. Photo: Bjoertvedt/Wikimedia Commons

A cyber attack that targeted Norwegian industry giant Norsk Hydro in March cost the company around $50 million.



Huge attack on Norway's health care systems may have exposed half the population

News | 29 January, 2018 | ♥ 0

A massive security breach in Norway's Health South-East Regional Health Authority may have exposed the personal health records of 2.9 million people.

Covering ten counties, Health South-East RHA is responsible for the health care of 57% of Norway's population. In 2013, Norway cemented their reputation for excellence in healthcare when they were placed first on the UN's Health

Yes, attack services are inexpensive

Ransomware:
$66 upfront
Or
30% of the profit (affiliate model)

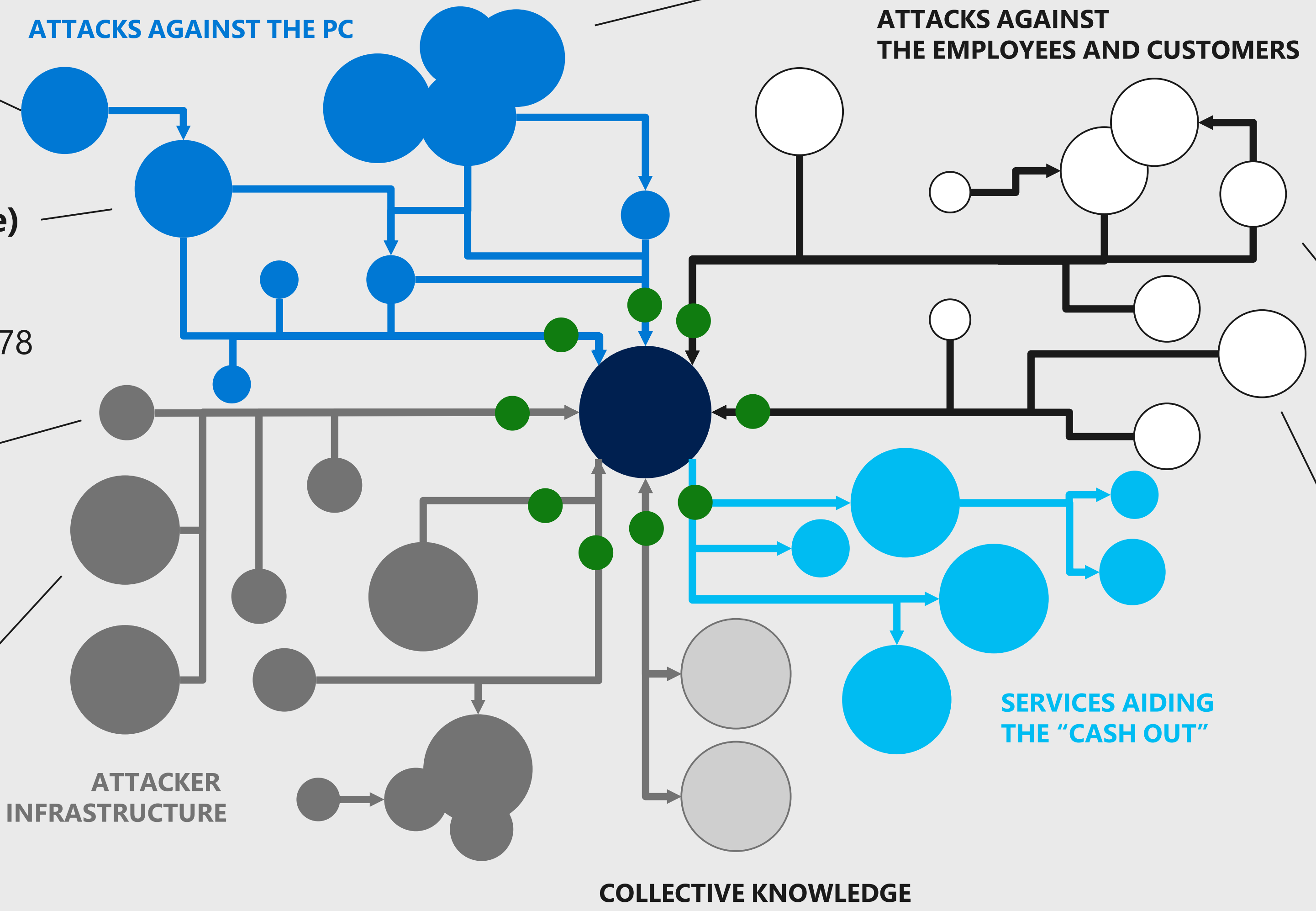
0days price range varies from $5,000 to $350,000

Loads (compromised device) average price ranges

- **PC** - $0.13 to $0.89
- **Mobile** - from $0.82 to $2.78

Denial of Service (DOS) average prices
day: $102.05
week: $327.00
month: $766.67

Proxy services to evade IP geolocation prices vary As low as $100 per week for 100,000 proxies.



ATTACKS AGAINST THE PC

ATTACKS AGAINST
THE EMPLOYEES AND CUSTOMERS

ATTACKER
INFRASTRUCTURE

COLLECTIVE KNOWLEDGE

SERVICES AIDING
THE "CASH OUT"

Spearphishing services range from $100 to $1,000 per successful account take over

Compromised accounts
As low as $150 for 400M.
Averages $0.97 per 1k.

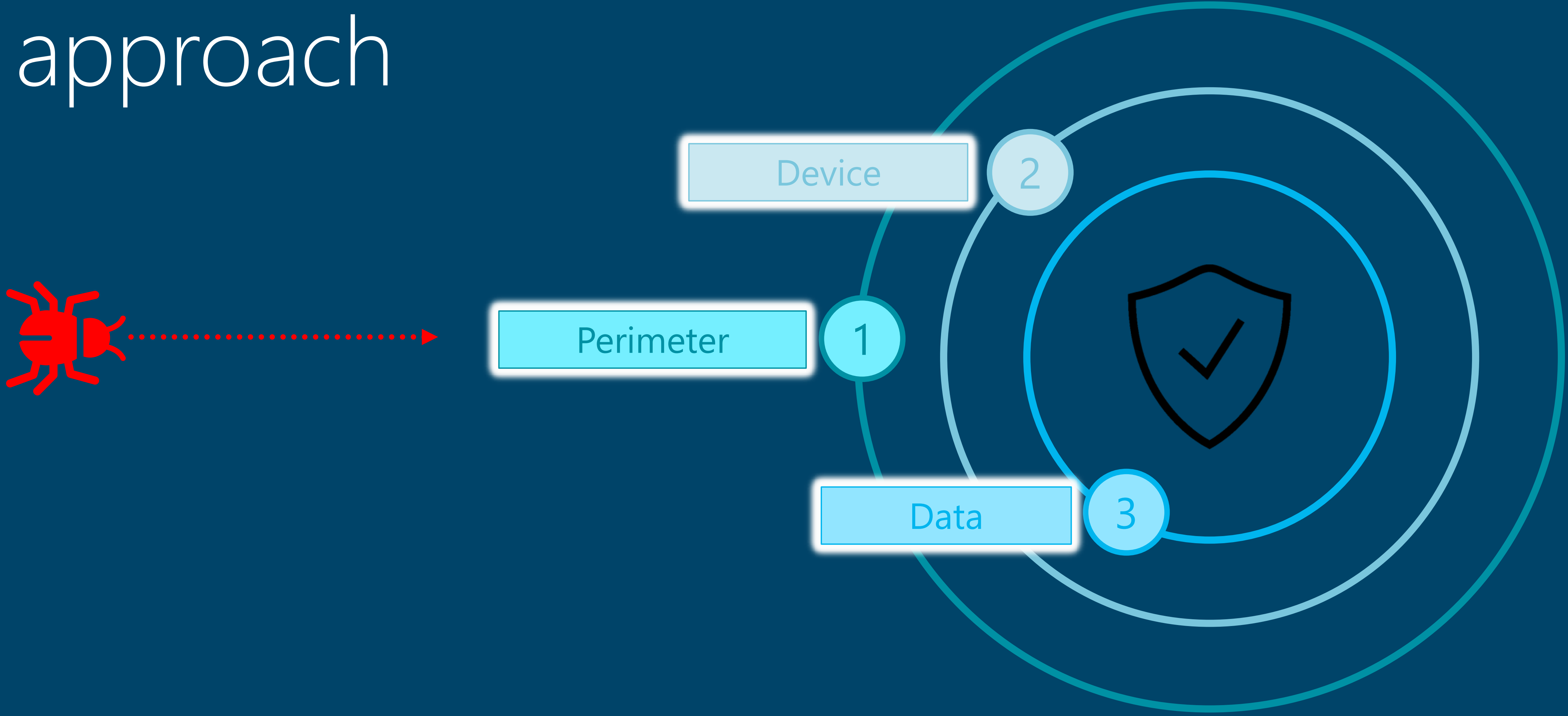
The challenge of securing your environment

More and more sophisticated attacks

Broad surface to secure

Time-consuming and expensive

Defense in depth with a layered approach



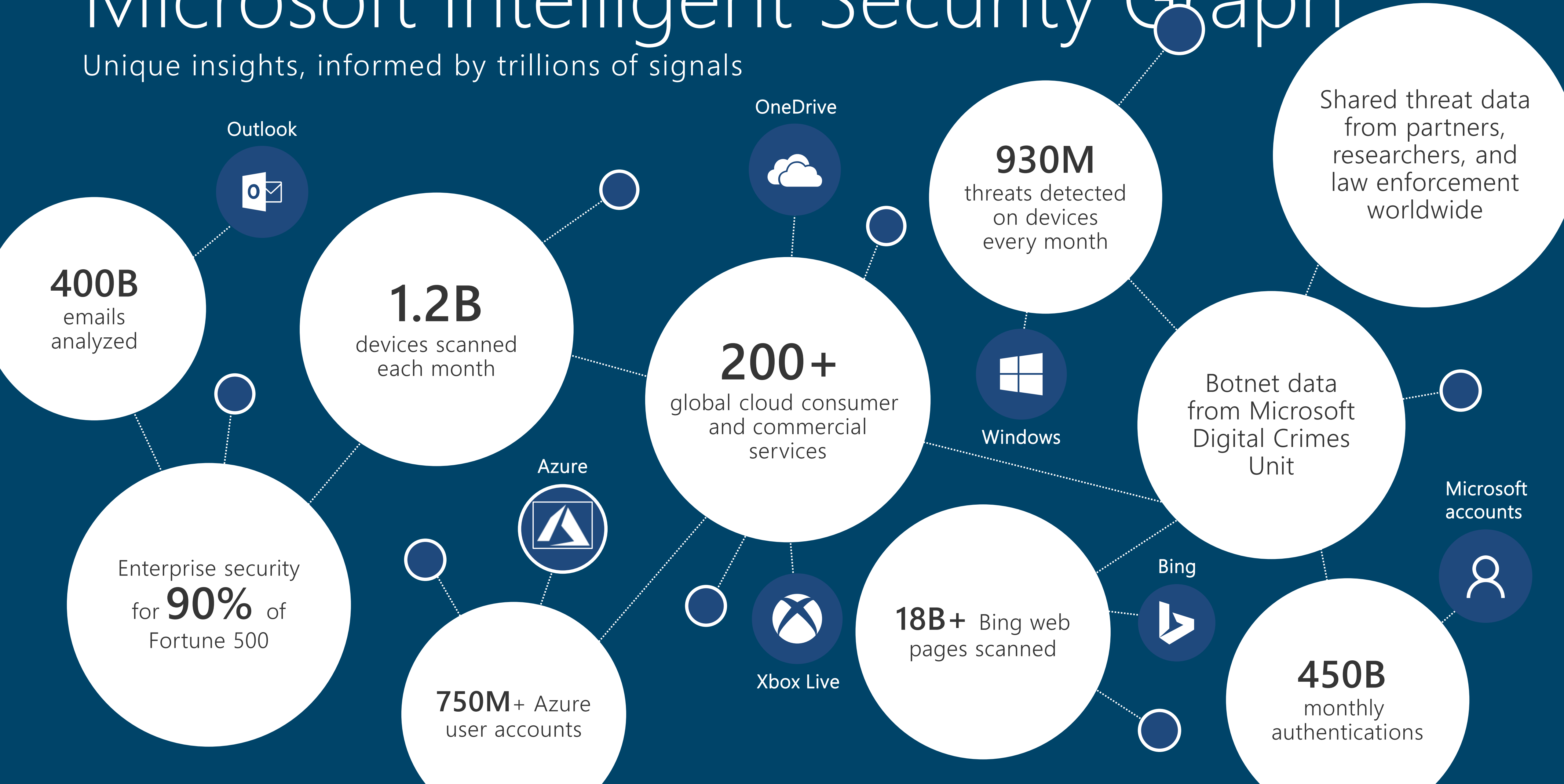
M365 – Security features

Complete Solution

	Office 365	Enterprise Mobility and Security	Windows 10
E3	Collaboration Tools	Identity Sync, Mobile Management, From RMS to AIP, ATA	BitLocker, Windows Firewall, Windows Defender
E5	E-discovery, advanced security [Office 365 ATP]	PIM, Identity Protection, CAS, Azure ATP	Windows Defender Advanced Threat Protection

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Outlook

OneDrive

400B emails analyzed

1.2B devices scanned each month

200+ global cloud consumer and commercial services

930M threats detected on devices every month

Shared threat data from partners, researchers, and law enforcement worldwide

Windows

Botnet data from Microsoft Digital Crimes Unit

Microsoft accounts

Azure

Enterprise security for **90%** of Fortune 500

750M+ Azure user accounts

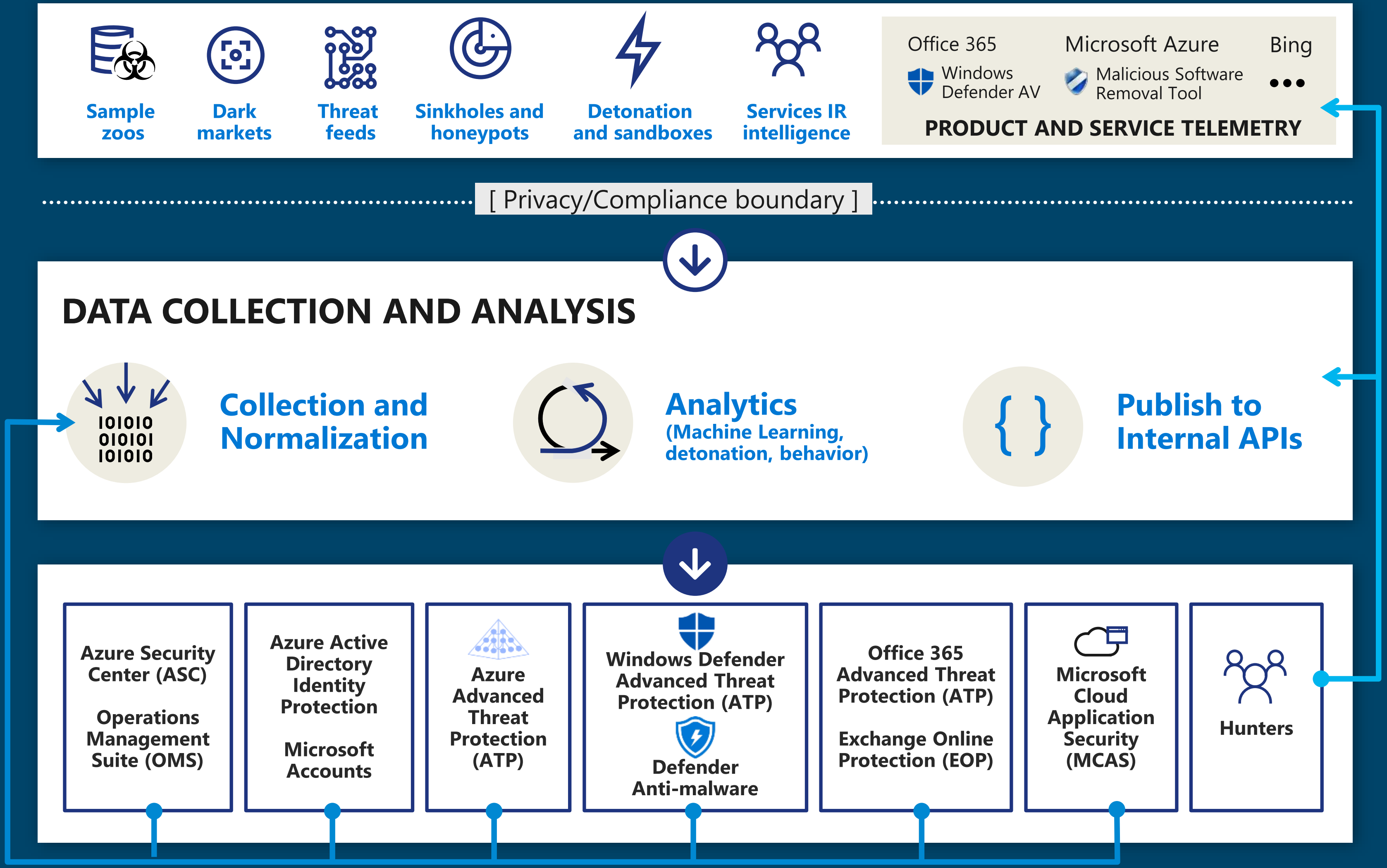
Xbox Live

18B+ Bing web pages scanned

Bing

450B monthly authentications

Inside The Intelligent Security Graph



Sample zoos

Dark markets

Threat feeds

Sinkholes and honeypots

Detonation and sandboxes

Services IR intelligence

Office 365

Windows Defender AV

Microsoft Azure

Malicious Software Removal Tool

Bing

•••

PRODUCT AND SERVICE TELEMETRY

[Privacy/Compliance boundary]

DATA COLLECTION AND ANALYSIS

Collection and Normalization

Analytics (Machine Learning, detonation, behavior)

Publish to Internal APIs

Azure Security Center (ASC)
Operations Management Suite (OMS)

Azure Active Directory Identity Protection
Microsoft Accounts

Azure Advanced Threat Protection (ATP)

Windows Defender Advanced Threat Protection (ATP)
Defender Anti-malware

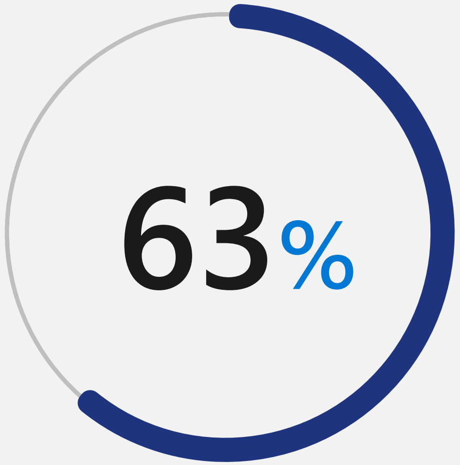
Office 365 Advanced Threat Protection (ATP)
Exchange Online Protection (EOP)

Microsoft Cloud Application Security (MCAS)

Hunters

- Products instrumented to strict privacy/compliance standards
  See Microsoft Trust Center
- Analytics help fuel new discoveries
- Products send data to graph
- Products use Interflow APIs to access results
- Products generate data which feeds back into the graph
- Hunters identify attacks, improve analytics, feed back into product design

Sobering statistics



63% of data breaches, attackers gain corporate network access through weak, default, or stolen user credentials

6k

Compromised admins/month in Azure AD/Office 365

99.9%

Decrease in compromise with MFA

THE DAILY NEWS

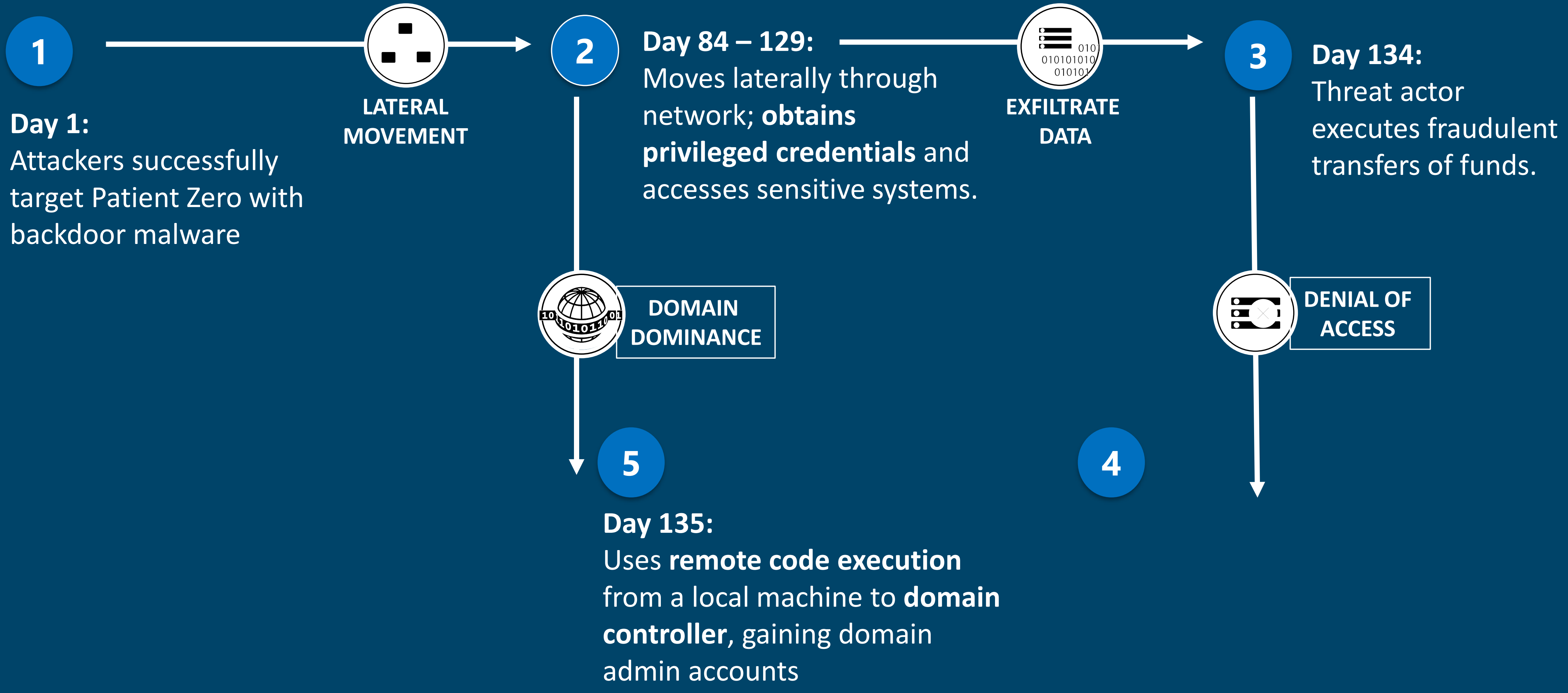
Attack shuts down [redacted] organization for 2 days

Investigation determined that threat actor was present on network for over 5 months.

Data sources indicate dozens of other institutions may be similarly impacted.

Wrecking ball malware was used to distract victim and response teams from main attack.

Attack timeline



1

Day 1:
Attackers successfully target Patient Zero with backdoor malware

LATERAL MOVEMENT

2

Day 84 – 129:
Moves laterally through network; **obtains privileged credentials** and accesses sensitive systems.

EXFILTRATE DATA

3

Day 134:
Threat actor executes fraudulent transfers of funds.

DENIAL OF ACCESS

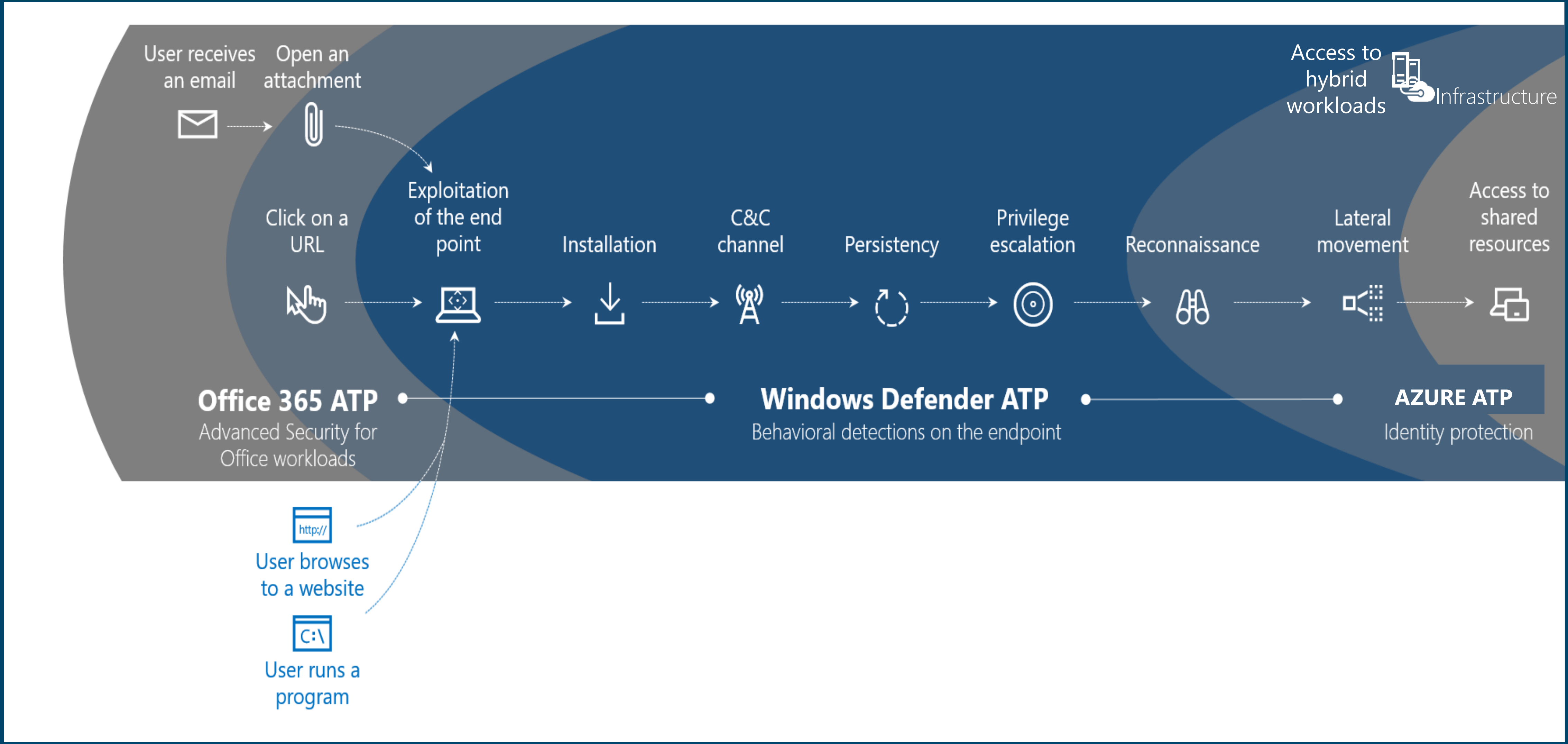
4

DOMAIN DOMINANCE

5

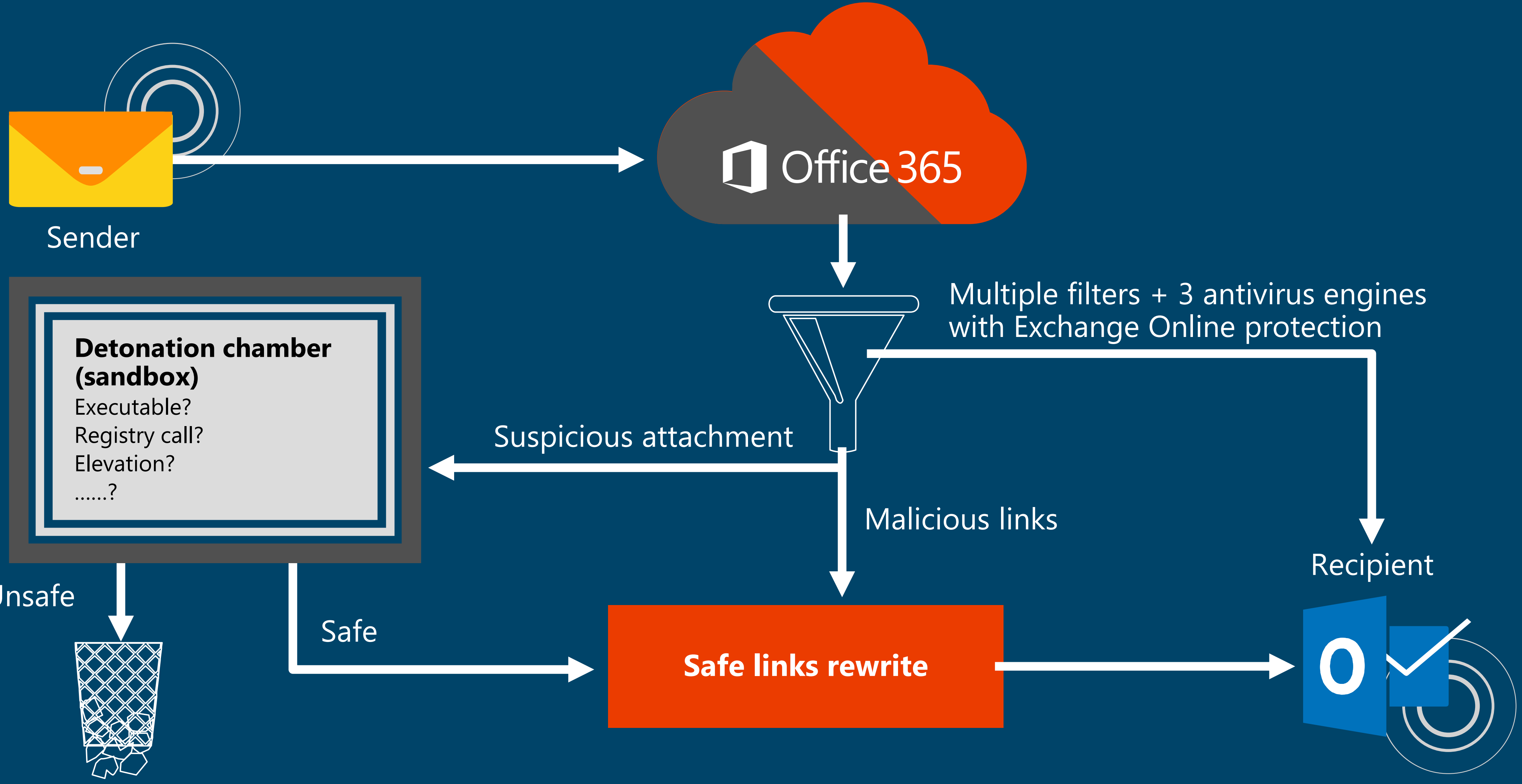
Day 135:
Uses **remote code execution** from a local machine to **domain controller**, gaining domain admin accounts

Pre and Post Breach



Protect at the front door

Threat Protection at the Perimeter



Sender

Multiple filters + 3 antivirus engines with Exchange Online protection

Detonation chamber (sandbox)
Executable?
Registry call?
Elevation?
……?

Suspicious attachment

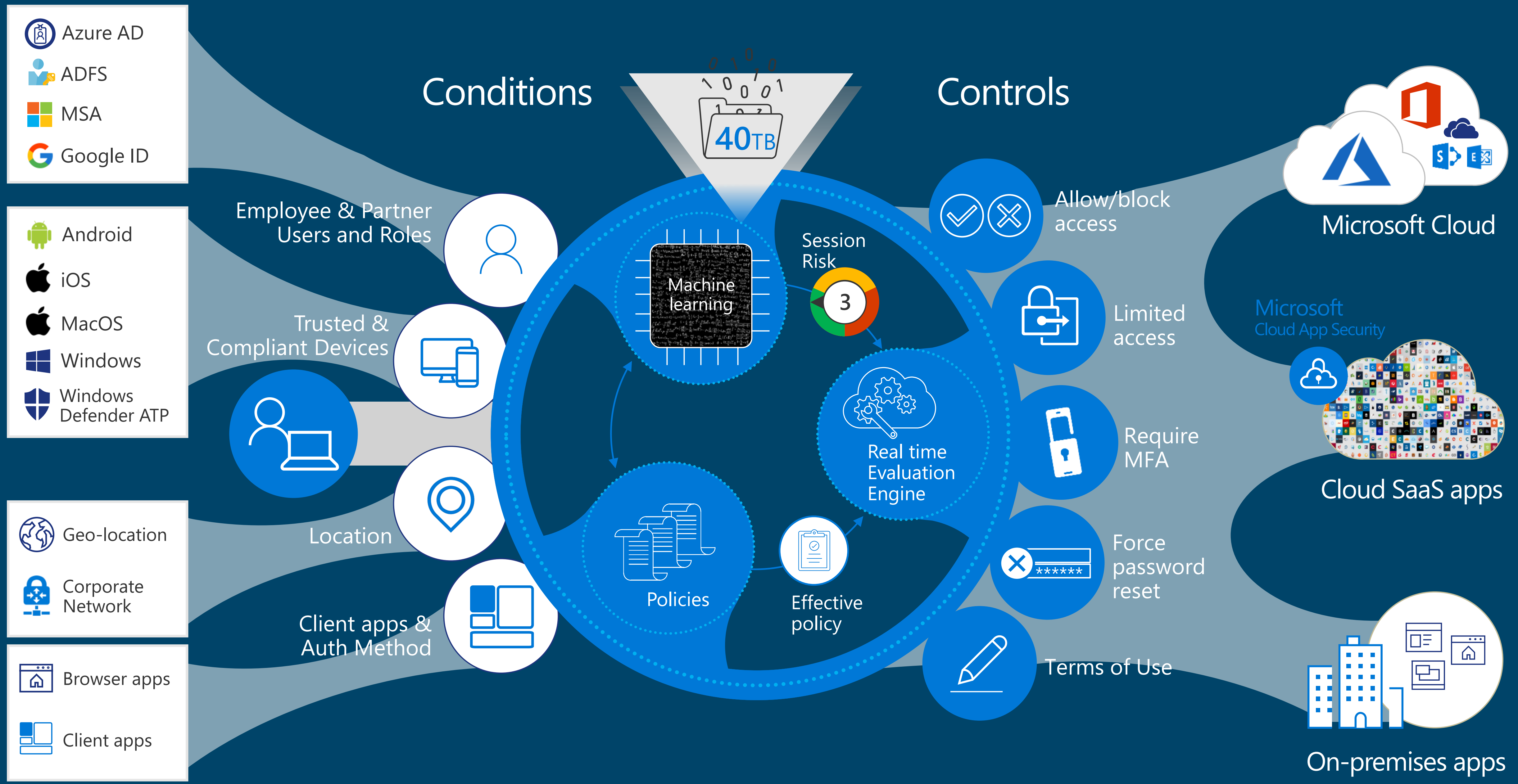
Malicious links

Recipient

Unsafe

Safe

Safe links rewrite



Azure AD

ADFS

MSA

Google ID

Android

iOS

MacOS

Windows

Windows Defender ATP

Geo-location

Corporate Network

Browser apps

Client apps

Conditions

Employee & Partner Users and Roles

Trusted & Compliant Devices

Location

Client apps & Auth Method

Machine learning

Session Risk

Real time Evaluation Engine

Policies

Effective policy

Controls

Allow/block access

Limited access

Require MFA

Force password reset

Terms of Use

Microsoft Cloud

Microsoft Cloud App Security

Cloud SaaS apps

On-premises apps

Demo

Office 365 ATP + CA

Threat Protection at the Device Level

PRE-BREACH → POST-BREACH →

OFF MACHINE

O365 (Email)

- Reducing email attack vector
- Advanced sandbox detonation

Proxy / Web filter

- URL Blocking
- AV Scanning

ON MACHINE

Locked Down Devices

- Windows 10S
- Applocker
- Credential Guard
- VSM

Application Control

- Whitelisting application

App Guard
(Virtualized Security)

- App isolation

Windows Defender Exploit Guard
(HIPS)

Attack Surface Reduction

- Set of rules to customize the attack surface

Controlled Folder Access

- Protecting data against access by untrusted process

Exploit Protection

- Mitigations against memory based exploits

Network Protection

- Blocking outbound traffic to low rep sources

Edge (Browser)

- Browser hardening
- Reduce script based attack surface
- App container hardening
- Reputation based blocking for downloads
- SmartScreen

Windows Defender Antivirus
(AV)

- Improved ML and heuristic protection
- Instantly protected with the cloud
- Enhanced Exploit Kit Detections

Windows Defender Antivirus Behavioral Engine
(Behavior Analysis)

- Enhanced behavioral and machine learning detection
- Memory scanning capabilities

Microsoft Defender ATP
(Advanced Threat Protection)

- Process tree visualizations
- Artifact searching capabilities
- Machine Isolation and quarantine

OFF MACHINE

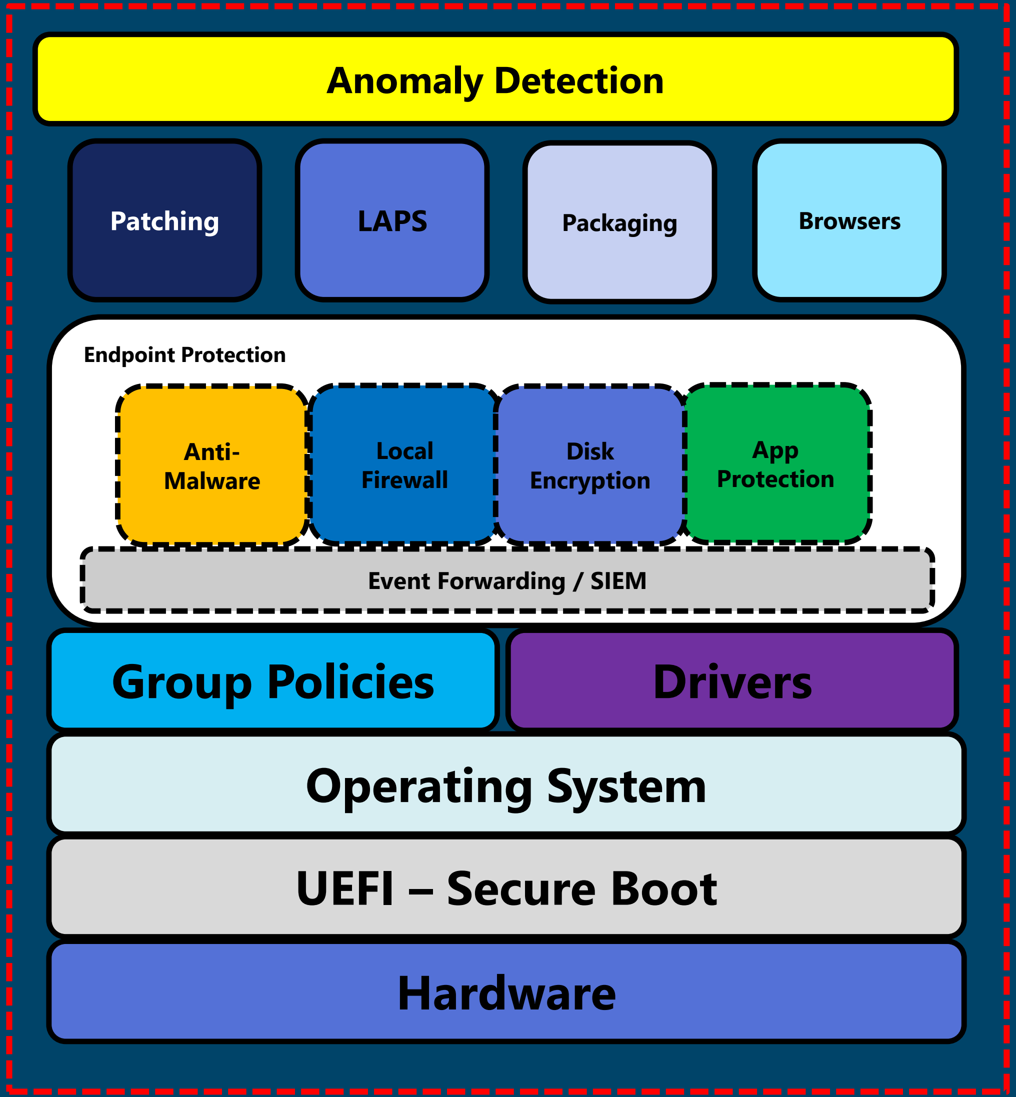
One Drive
(Cloud Storage)

- Reliable versioned file storage in the cloud
- Point in time file recovery

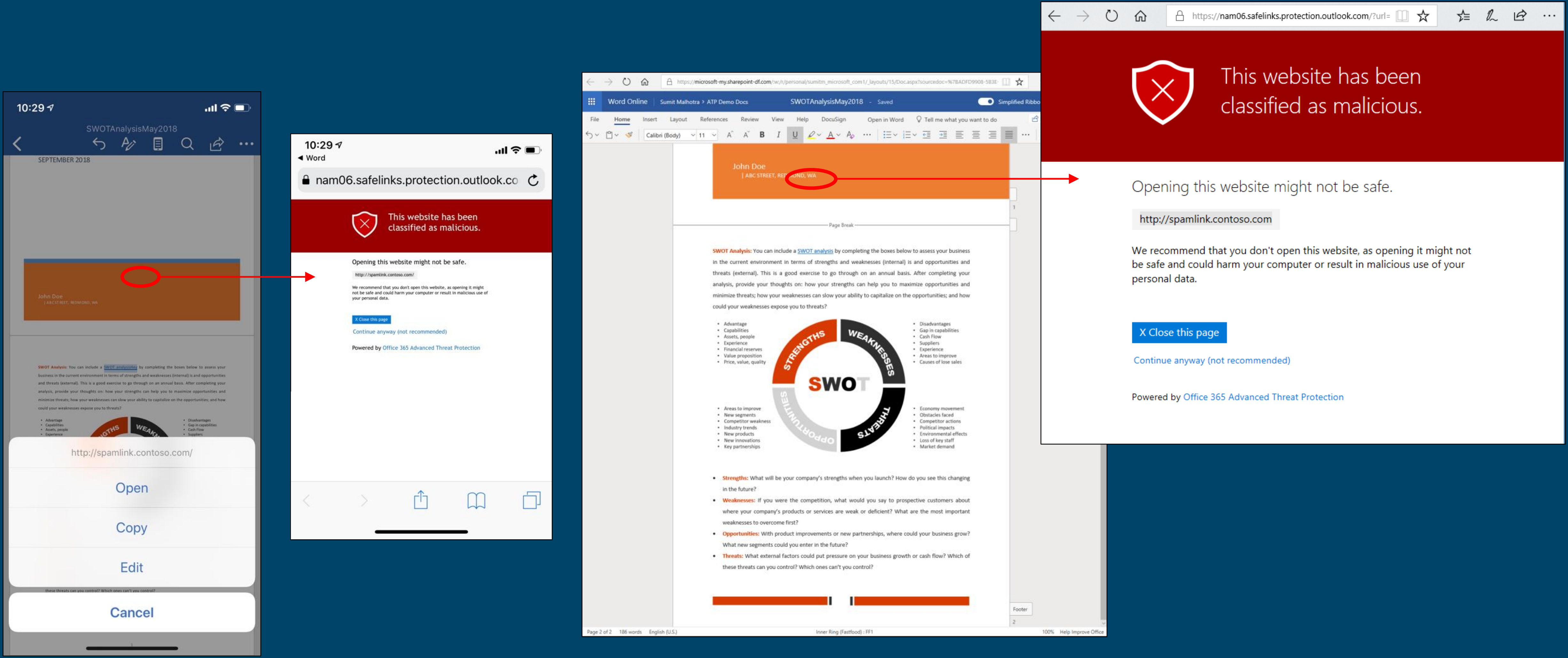
Demo

Windows 10 – Threat Protection

Client Security



Cloud Driven Threat Detection – Office clients/Online


10:29
SWOTAnalysisMay2018
SEPTEMBER 2018
John Doe
http://spamlink.contoso.com/
Open
Copy
Edit
Cancel
10:29
◀ Word
nam06.safelinks.protection.outlook.co

This website has been classified as malicious.

Opening this website might not be safe.

http://spamlink.contoso.com/

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

X Close this page
Continue anyway (not recommended)

Powered by Office 365 Advanced Threat Protection

https://microsoft-my.sharepoint-df.com/:w:/r/personal/sumitm_microsoft_com1/_layouts/15/Doc.aspx?sourcedoc=%7BADFD9908-5B3E-
Word Online
Sumit Malhotra > ATP Demo Docs
SWOTAnalysisMay2018 - Saved
Simplified Ribbo
File
Home
Insert
Layout
References
Review
View
Help
DocuSign
Open in Word
Tell me what you want to do
Calibri (Body)
11
John Doe
| ABC STREET, REDMOND, WA
Page Break

SWOT Analysis: You can include a SWOT analysis by completing the boxes below to assess your business in the current environment in terms of strengths and weaknesses (internal) is and opportunities and threats (external). This is a good exercise to go through on an annual basis. After completing your analysis, provide your thoughts on: how your strengths can help you to maximize opportunities and minimize threats; how your weaknesses can slow your ability to capitalize on the opportunities; and how could your weaknesses expose you to threats?

- Advantage
- Capabilities
- Assets, people
- Experience
- Financial reserves
- Value proposition
- Price, value, quality

- Disadvantages
- Gap in capabilities
- Cash Flow
- Suppliers
- Experience
- Areas to improve
- Causes of lose sales

- Areas to improve
- New segments
- Competitor weakness
- Industry trends
- New products
- New innovations
- Key partnerships

- Economy movement
- Obstacles faced
- Competitor actions
- Political impacts
- Environmental effects
- Loss of key staff
- Market demand

- **Strengths:** What will be your company's strengths when you launch? How do you see this changing in the future?
- **Weaknesses:** If you were the competition, what would you say to prospective customers about where your company's products or services are weak or deficient? What are the most important weaknesses to overcome first?
- **Opportunities:** With product improvements or new partnerships, where could your business grow? What new segments could you enter in the future?
- **Threats:** What external factors could put pressure on your business growth or cash flow? Which of these threats can you control? Which ones can't you control?

Footer
2
Page 2 of 2
186 words
English (U.S.)
Inner Ring (Fastfood) : FF1
100%
Help Improve Office
https://nam06.safelinks.protection.outlook.com/?url=

This website has been classified as malicious.

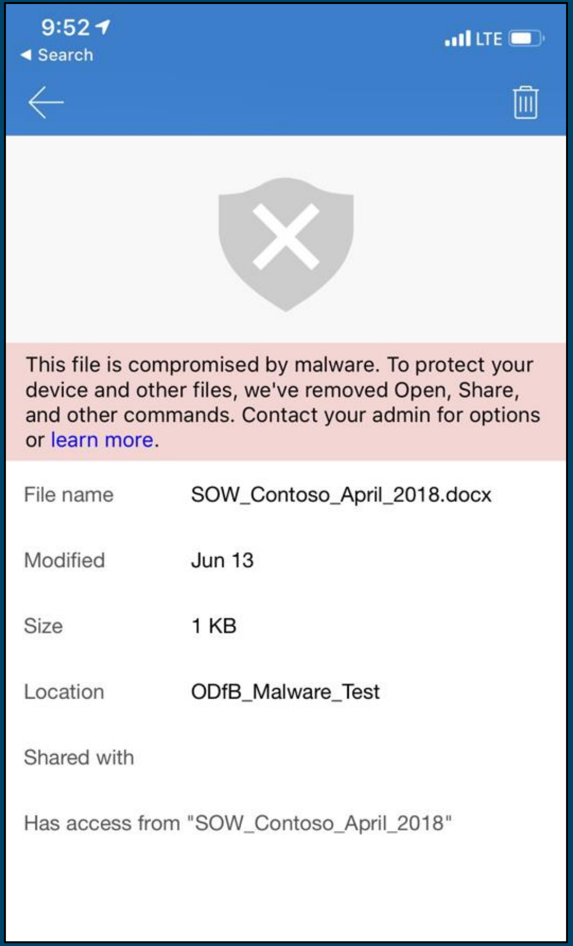
Opening this website might not be safe.

http://spamlink.contoso.com

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

Powered by Office 365 Advanced Threat Protection

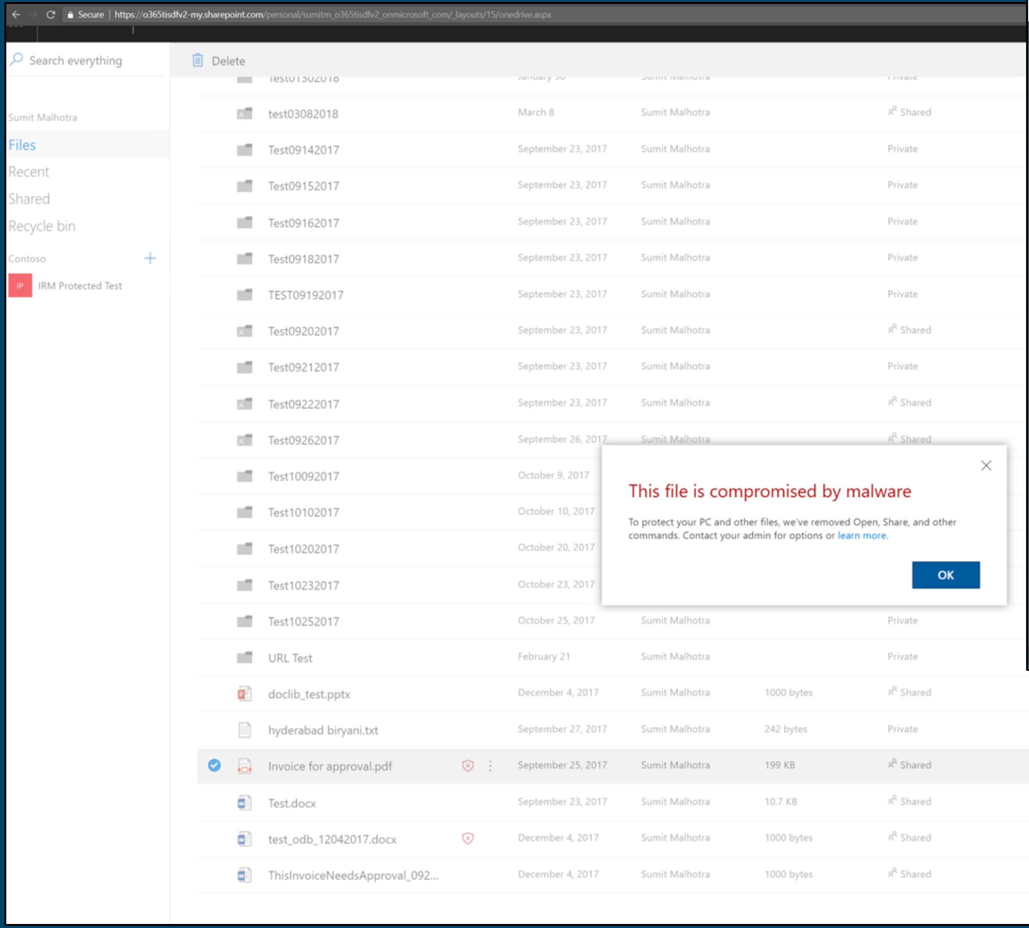
Cloud Driven Threat Detection – OneDrive, Teams, SPO



This file is compromised by malware. To protect your device and other files, we've removed Open, Share, and other commands. Contact your admin for options or learn more.

File name	SOW_Contoso_April_2018.docx
Modified	Jun 13
Size	1 KB
Location	ODfB_Malware_Test
Shared with	

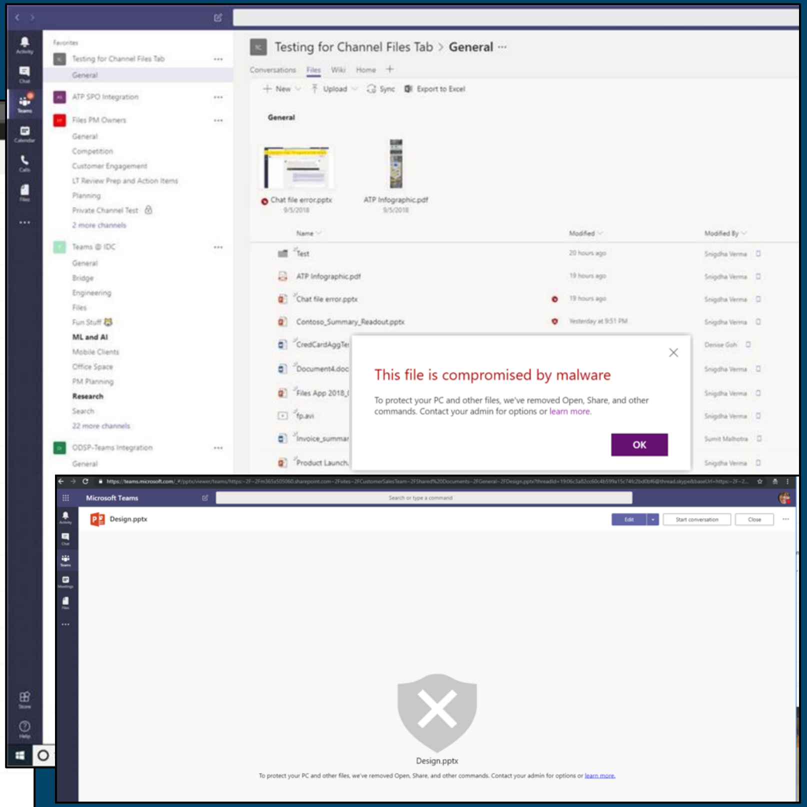
Has access from "SOW_Contoso_April_2018"


Secure | https://o365tisdfv2-my.sharepoint.com/personal/sumitm_o365tisdfv2_onmicrosoft_com/_layouts/15/onedrive.aspx
Search everything
Delete
Sumit Malhotra
Files
Recent
Shared
Recycle bin
Contoso
IRM Protected Test

Test01302018	January 30	Sumit Malhotra		Private
test03082018	March 8	Sumit Malhotra		Shared
Test09142017	September 23, 2017	Sumit Malhotra		Private
Test09152017	September 23, 2017	Sumit Malhotra		Private
Test09162017	September 23, 2017	Sumit Malhotra		Private
Test09182017	September 23, 2017	Sumit Malhotra		Private
TEST09192017	September 23, 2017	Sumit Malhotra		Private
Test09202017	September 23, 2017	Sumit Malhotra		Shared
Test09212017	September 23, 2017	Sumit Malhotra		Private
Test09222017	September 23, 2017	Sumit Malhotra		Shared
Test09262017	September 26, 2017	Sumit Malhotra		Shared
Test10092017	October 9, 2017			
Test10102017	October 10, 2017			
Test10202017	October 20, 2017			
Test10232017	October 23, 2017			
Test10252017	October 25, 2017	Sumit Malhotra		Private
URL Test	February 21	Sumit Malhotra		Private
doclib_test.pptx	December 4, 2017	Sumit Malhotra	1000 bytes	Shared
hyderabad biryani.txt	September 27, 2017	Sumit Malhotra	242 bytes	Private
Invoice for approval.pdf	September 25, 2017	Sumit Malhotra	199 KB	Shared
Test.docx	September 23, 2017	Sumit Malhotra	10.7 KB	Shared
test_odb_12042017.docx	December 4, 2017	Sumit Malhotra	1000 bytes	Shared
ThisInvoiceNeedsApproval_092...	December 4, 2017	Sumit Malhotra	1000 bytes	Shared

This file is compromised by malware

To protect your PC and other files, we've removed Open, Share, and other commands. Contact your admin for options or learn more.



Name	Modified	Modified By
Test	20 hours ago	Snigdha Verma
ATP Infographic.pdf	19 hours ago	Snigdha Verma
Chat file error.pptx	19 hours ago	Snigdha Verma
Contoso_Summary_Readout.pptx	Yesterday at 9:51 PM	Snigdha Verma
CredCardAggTe		Denise Goh
Document4.doc		Snigdha Verma
Files App 2018_		Snigdha Verma
fp.avi		Snigdha Verma
Invoice_summar		Sumit Malhotra
Product Launch.		Snigdha Verma

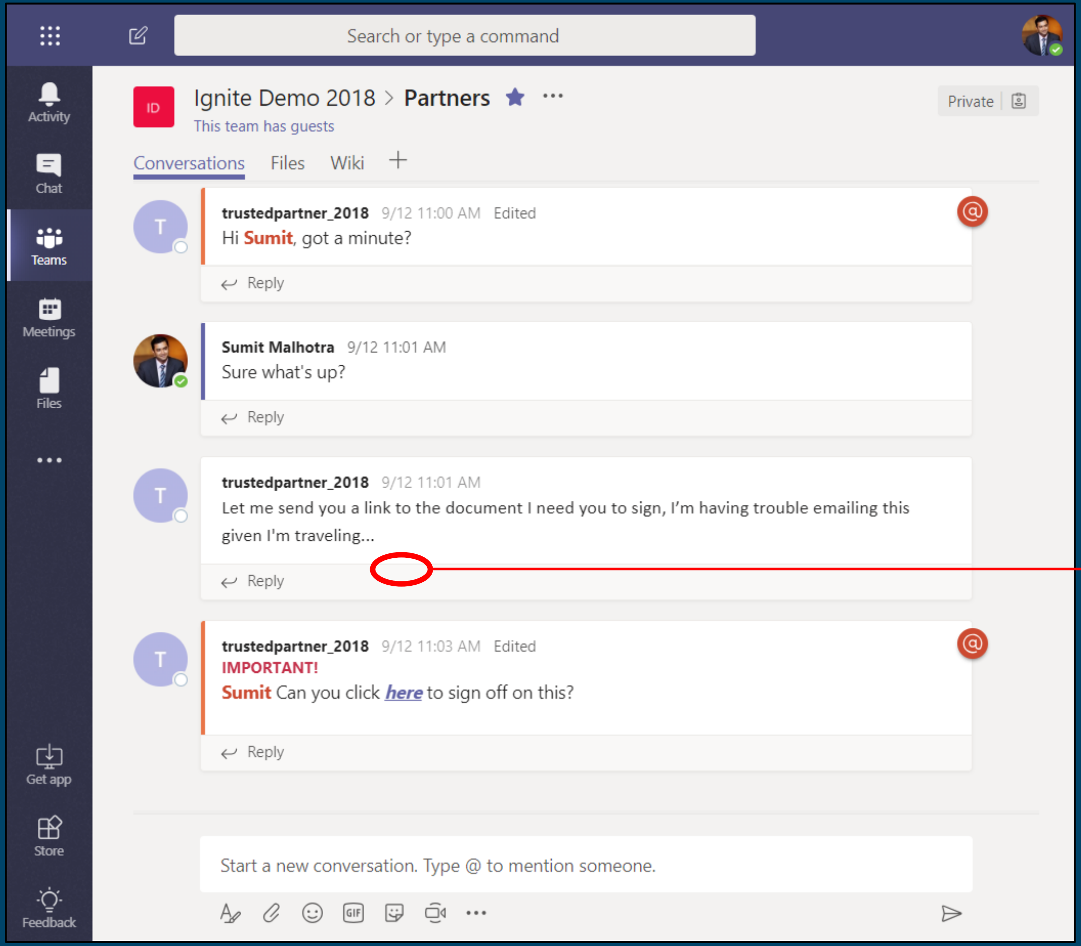
This file is compromised by malware

To protect your PC and other files, we've removed Open, Share, and other commands. Contact your admin for options or learn more.

Design.pptx

To protect your PC and other files, we've removed Open, Share, and other commands. Contact your admin for options or learn more.

Cloud Driven Threat Detection – Teams Safe Links



Ignite Demo 2018 > Partners

This team has guests

trustedpartner_2018 9/12 11:00 AM Edited
Hi **Sumit**, got a minute?

Reply

Sumit Malhotra 9/12 11:01 AM
Sure what's up?

Reply

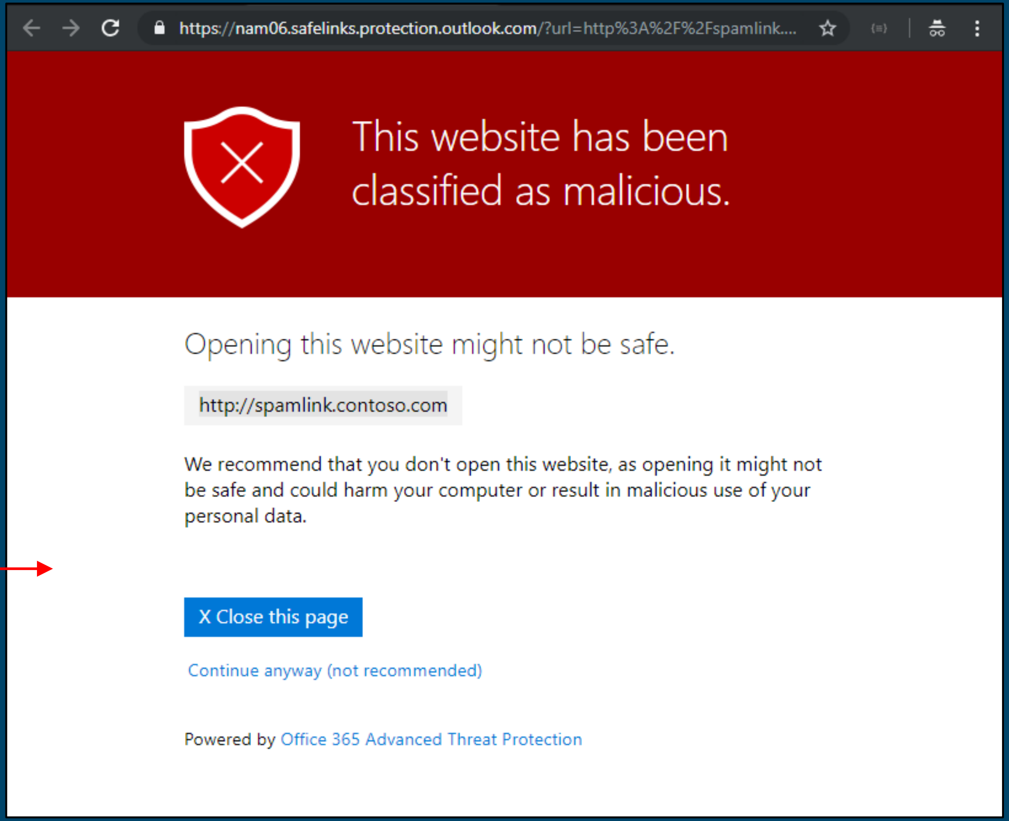
trustedpartner_2018 9/12 11:01 AM
Let me send you a link to the document I need you to sign, I'm having trouble emailing this given I'm traveling...

Reply

trustedpartner_2018 9/12 11:03 AM Edited
IMPORTANT!
Sumit Can you click *here* to sign off on this?

Reply

Start a new conversation. Type @ to mention someone.



https://nam06.safelinks.protection.outlook.com/?url=http%3A%2F%2Fspamlink....

This website has been classified as malicious.

Opening this website might not be safe.

http://spamlink.contoso.com

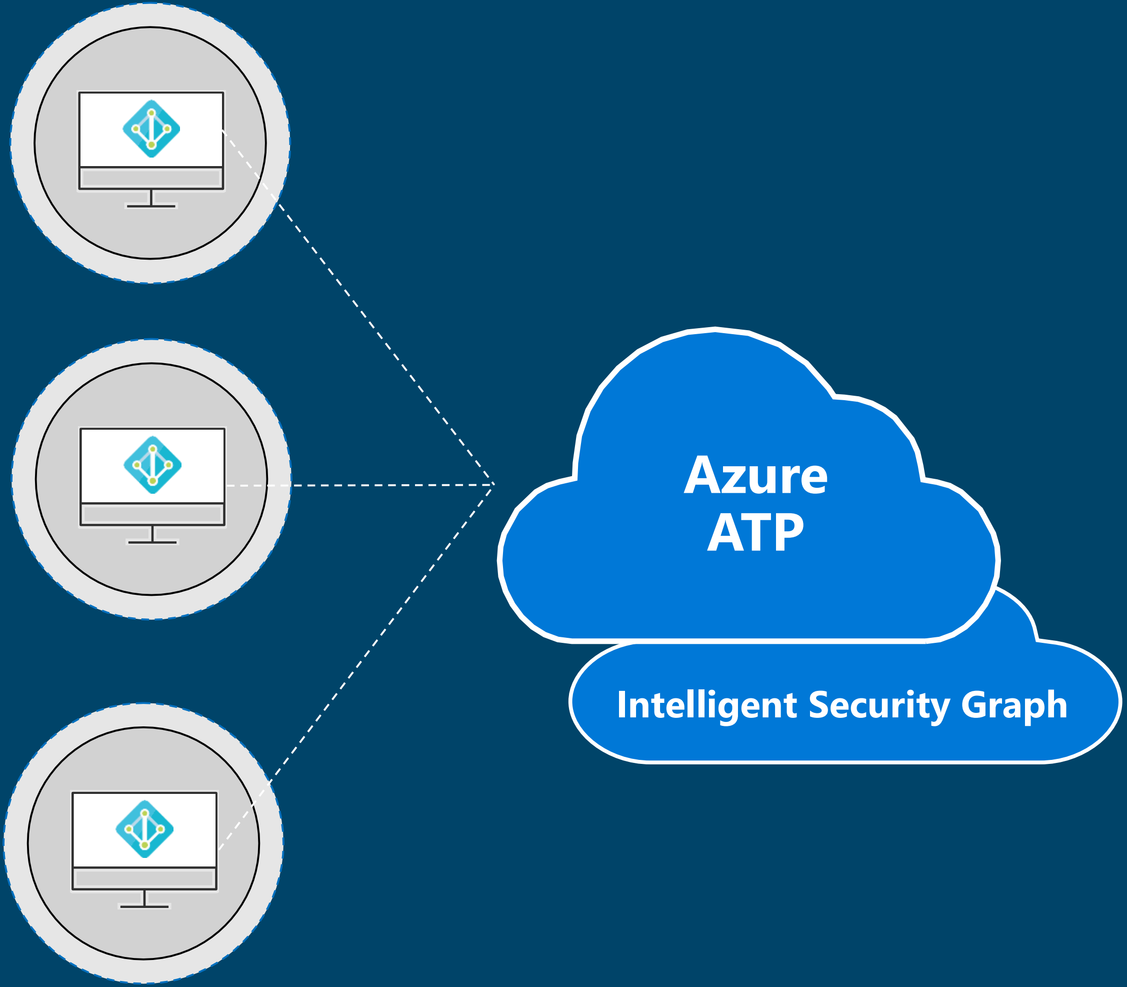
We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

X Close this page

Continue anyway (not recommended)

Powered by Office 365 Advanced Threat Protection

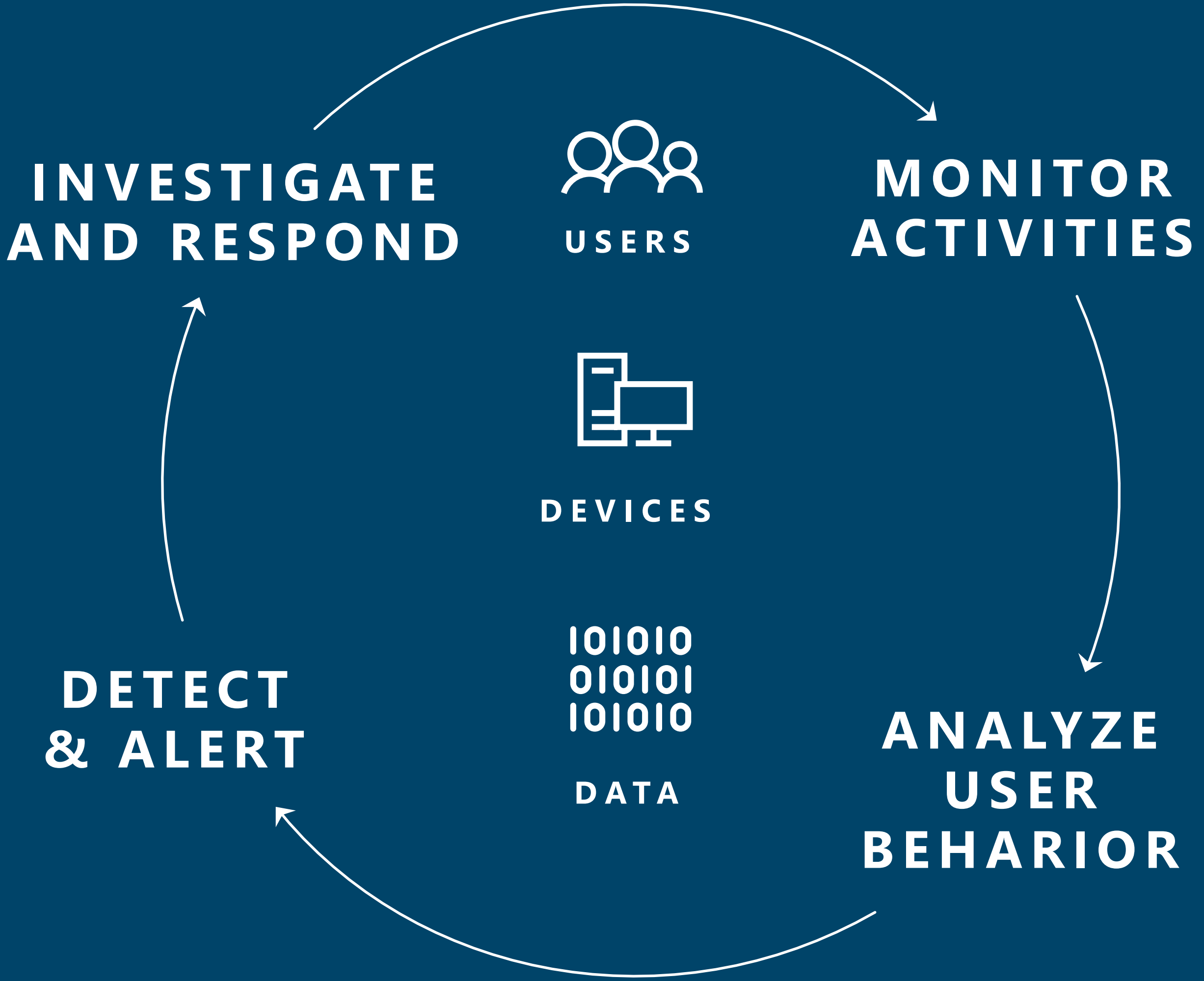
Azure ATP



Azure ATP

Intelligent Security Graph

Organizational domain controllers



INVESTIGATE AND RESPOND

MONITOR ACTIVITIES

ANALYZE USER BEHARIOR

DETECT & ALERT

USERS

DEVICES

DATA

Cloud App Security

Shadow IT

Identify cloud apps on your network and get risk assessment

Session Control

Control or limit access in real time based on conditions and session context

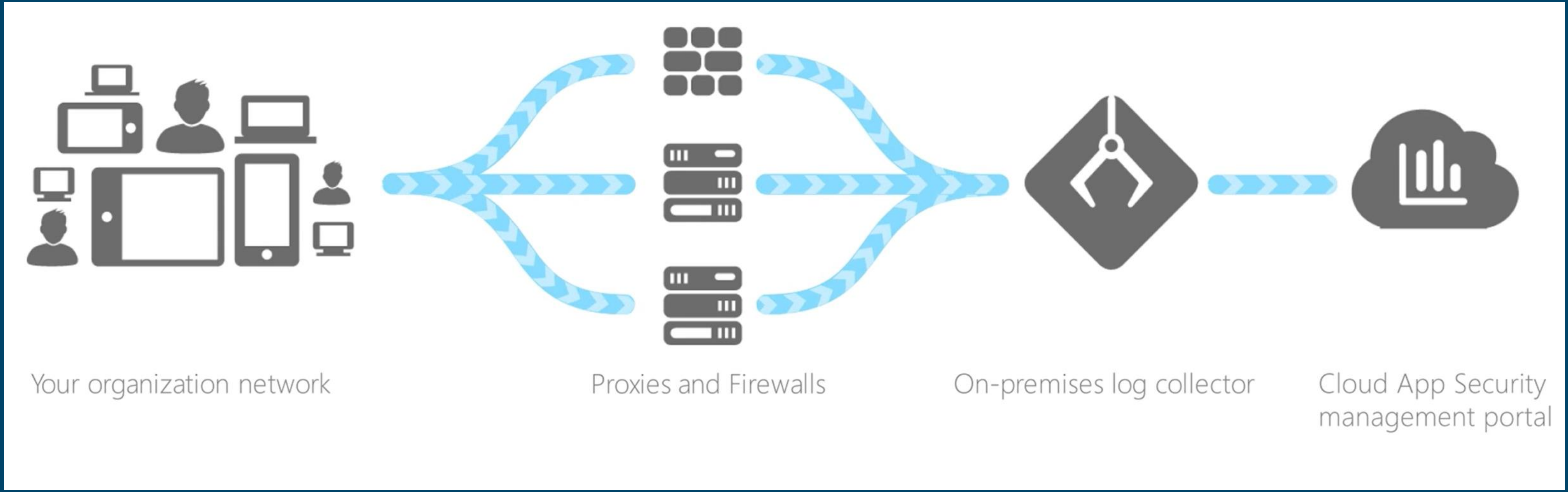
Information Protection

Built-in custom policies for data sharing and data loss prevention

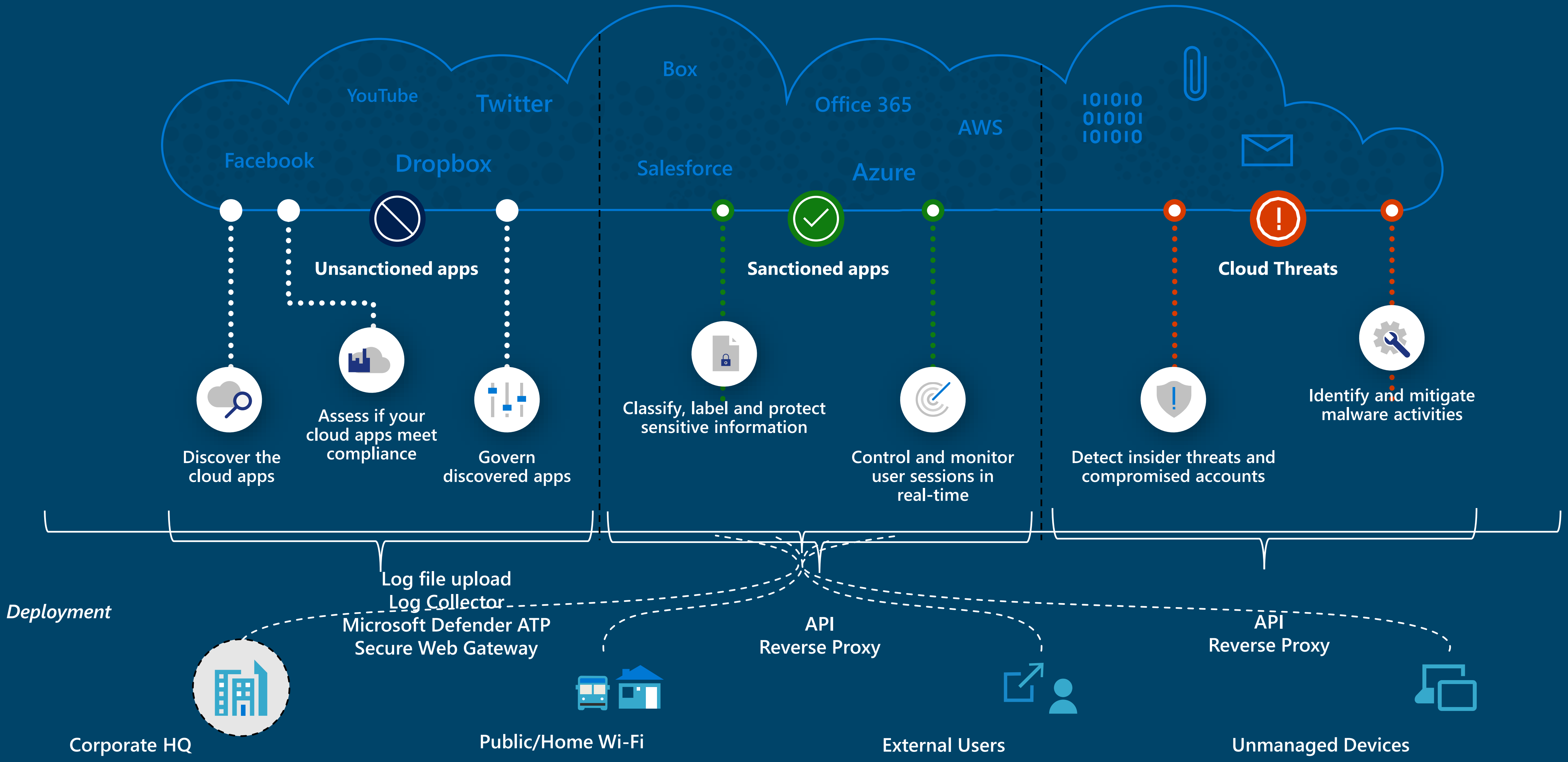
Threat Protection

Identify high risk usage and unusual user activities

CAS Architecture

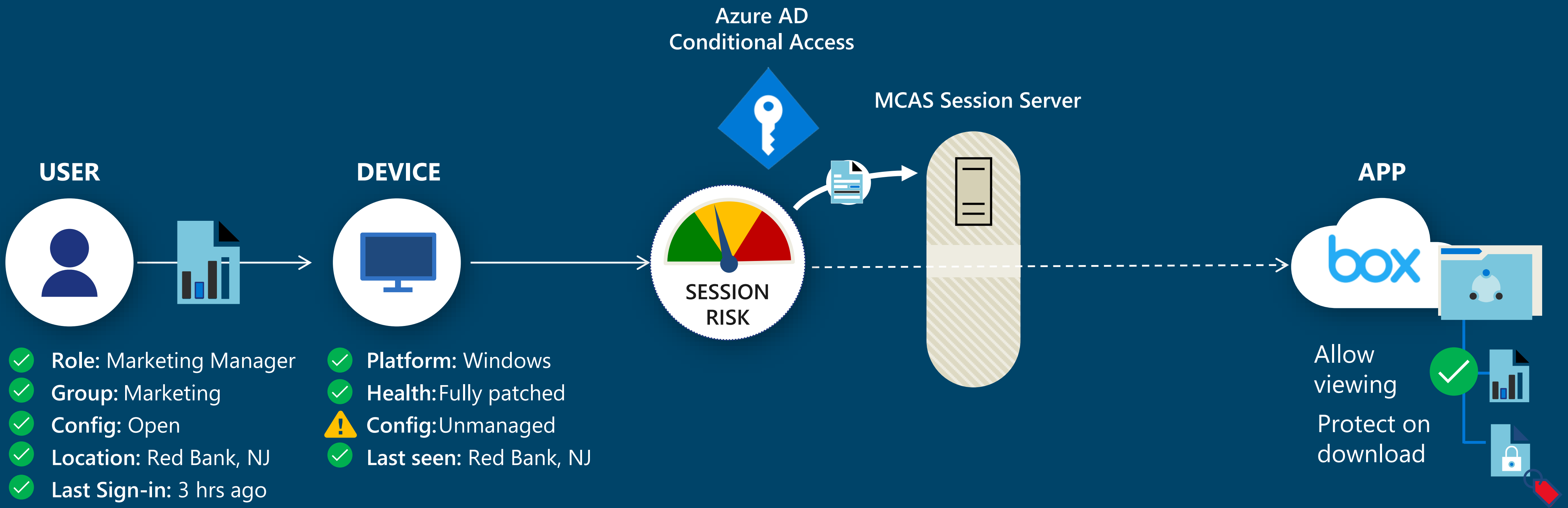

Your organization network
Proxies and Firewalls
On-premises log collector
Cloud App Security management portal

TOP CASB USE CASES



USE CASE: PREVENT DOWNLOAD OF FILES

Risk based in-session controls



Azure AD
Conditional Access

MCAS Session Server

USER

- ✓ **Role:** Marketing Manager
- ✓ **Group:** Marketing
- ✓ **Config:** Open
- ✓ **Location:** Red Bank, NJ
- ✓ **Last Sign-in:** 3 hrs ago

DEVICE

- ✓ **Platform:** Windows
- ✓ **Health:** Fully patched
- ⚠ **Config:** Unmanaged
- ✓ **Last seen:** Red Bank, NJ

SESSION
RISK

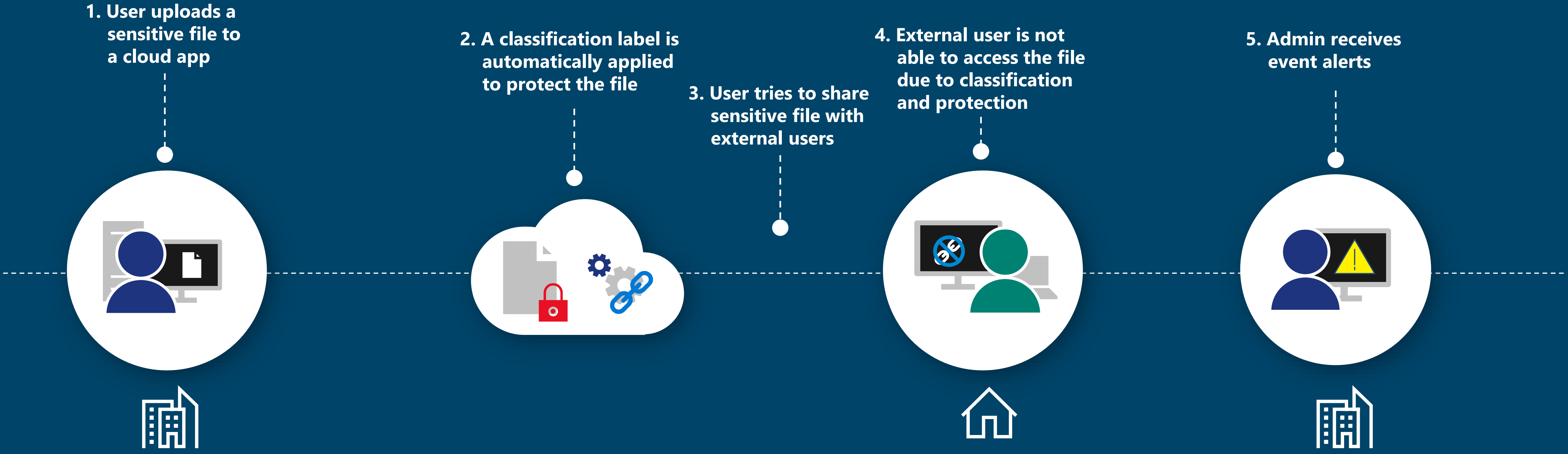
APP

Allow
viewing

Protect on
download

⚠ Device is unmanaged

Protect sensitive files in the cloud


1. User uploads a sensitive file to a cloud app

2. A classification label is automatically applied to protect the file

3. User tries to share sensitive file with external users

4. External user is not able to access the file due to classification and protection

5. Admin receives event alerts

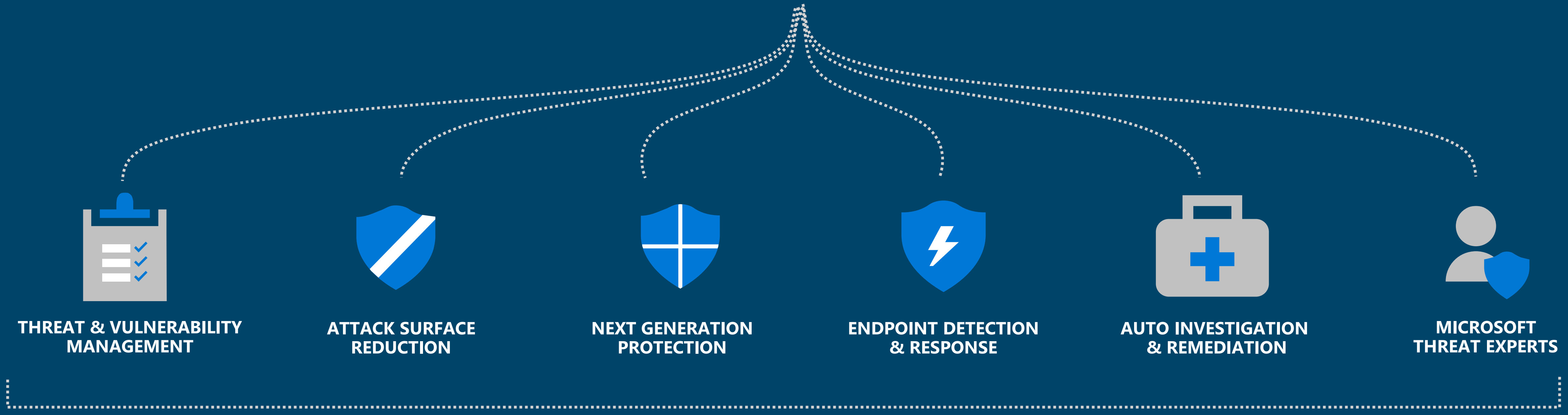
Demo

Cloud App Security

Microsoft Defender

Advanced Threat Protection

Built-in. Cloud-powered.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

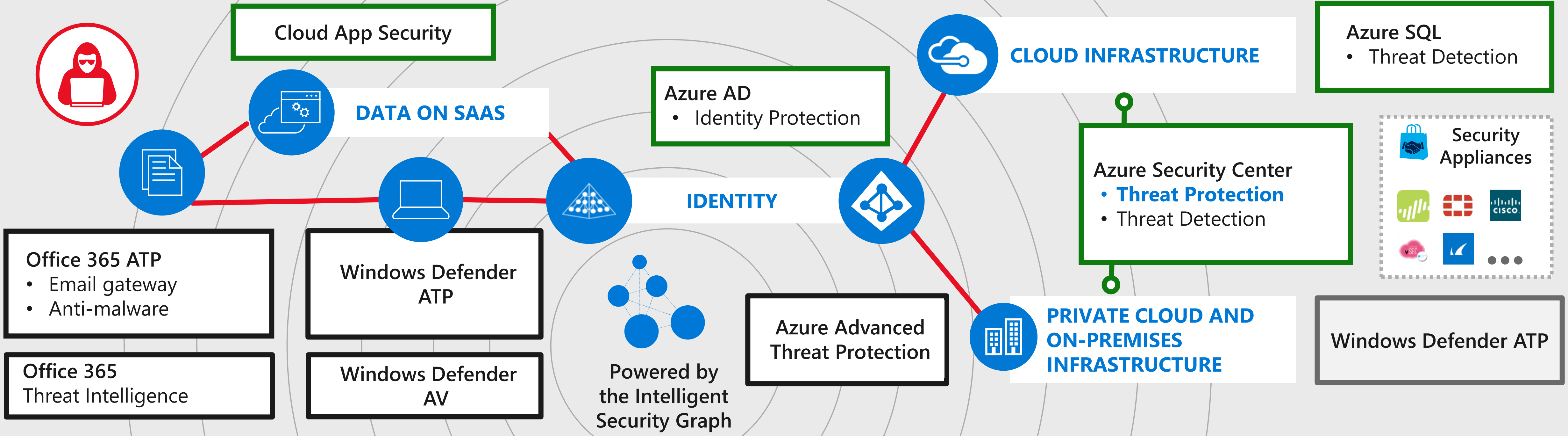
CENTRALIZED CONFIGURATION AND ADMINISTRATION, APIS

Demo

WDATP

Maximize internal visibility

Apply Threat Insights Across Your Hybrid Cloud Estate



Cloud App Security

DATA ON SAAS

Azure AD
- Identity Protection

CLOUD INFRASTRUCTURE

Azure SQL
- Threat Detection

IDENTITY

Azure Security Center
- **Threat Protection**
- Threat Detection

Security Appliances

Office 365 ATP
- Email gateway
- Anti-malware

Windows Defender ATP

Powered by the Intelligent Security Graph

Azure Advanced Threat Protection

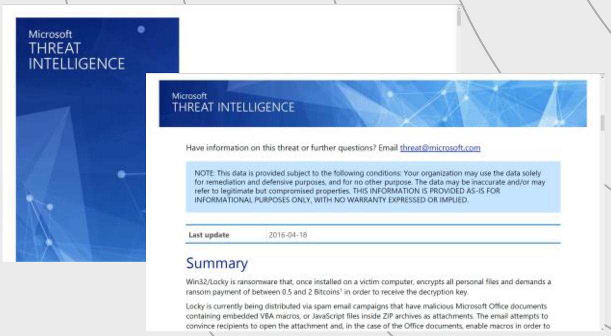
PRIVATE CLOUD AND ON-PREMISES INFRASTRUCTURE

Windows Defender ATP

Office 365 Threat Intelligence

Windows Defender AV

INTELLIGENCE AND ANALYSIS



Microsoft THREAT INTELLIGENCE

Microsoft THREAT INTELLIGENCE

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

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

Last update	2016-04-18

Summary

Win32/Locky is ransomware that, once installed on a victim computer, encrypts all personal files and demands a ransom payment of between 0.5 and 2 Bitcoins[1] in order to receive the decryption key.

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

Cybersecurity Operations Service (COS)

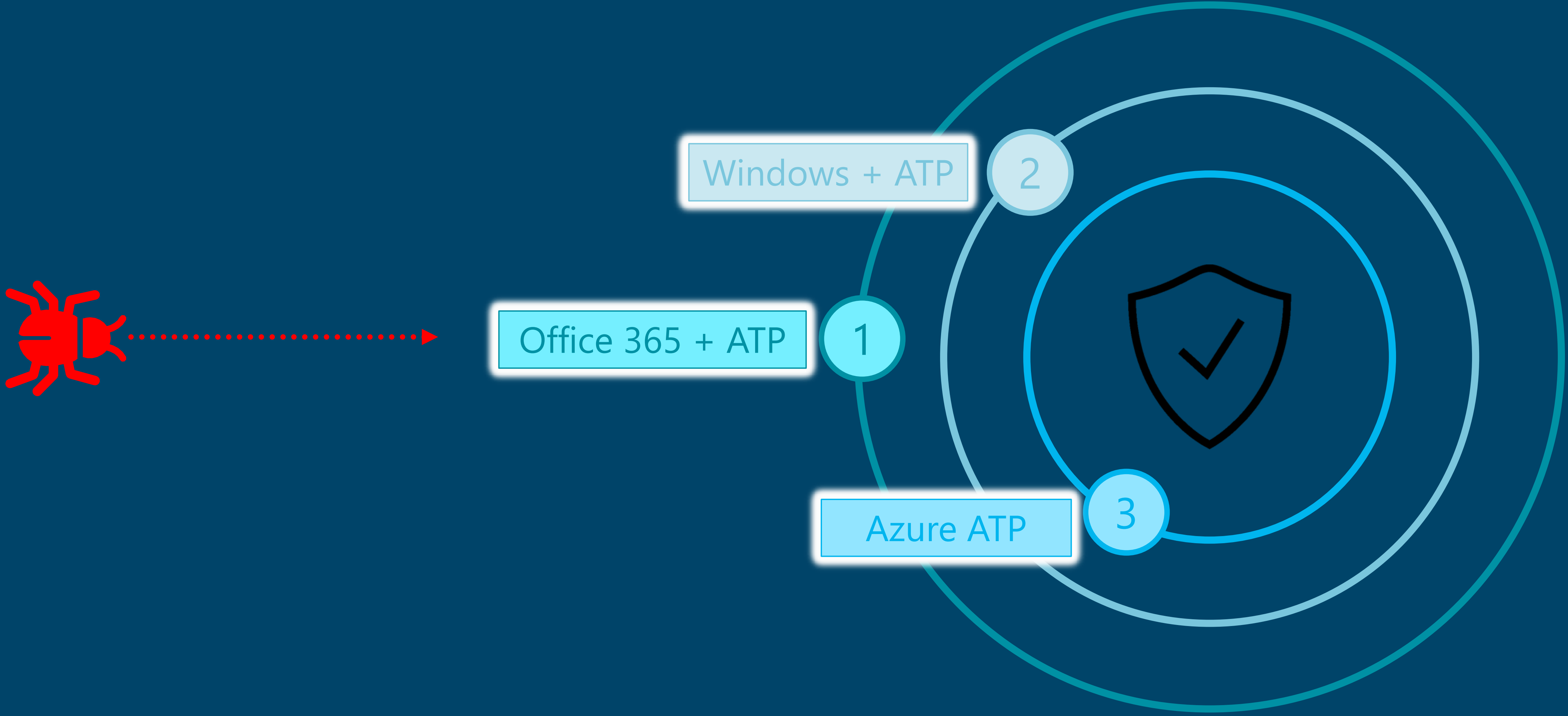
Incident Response and Recovery Services

Hunt for threats and persistent adversaries in your environment

Respond to Threats with seasoned professionals and deep expertise

Professional Services

Layered Approach is still they way to go



Thank You!

Platinum

Microsoft

Gold

audiocodes

Silver

au2mator

pexip

Jabra

logitech