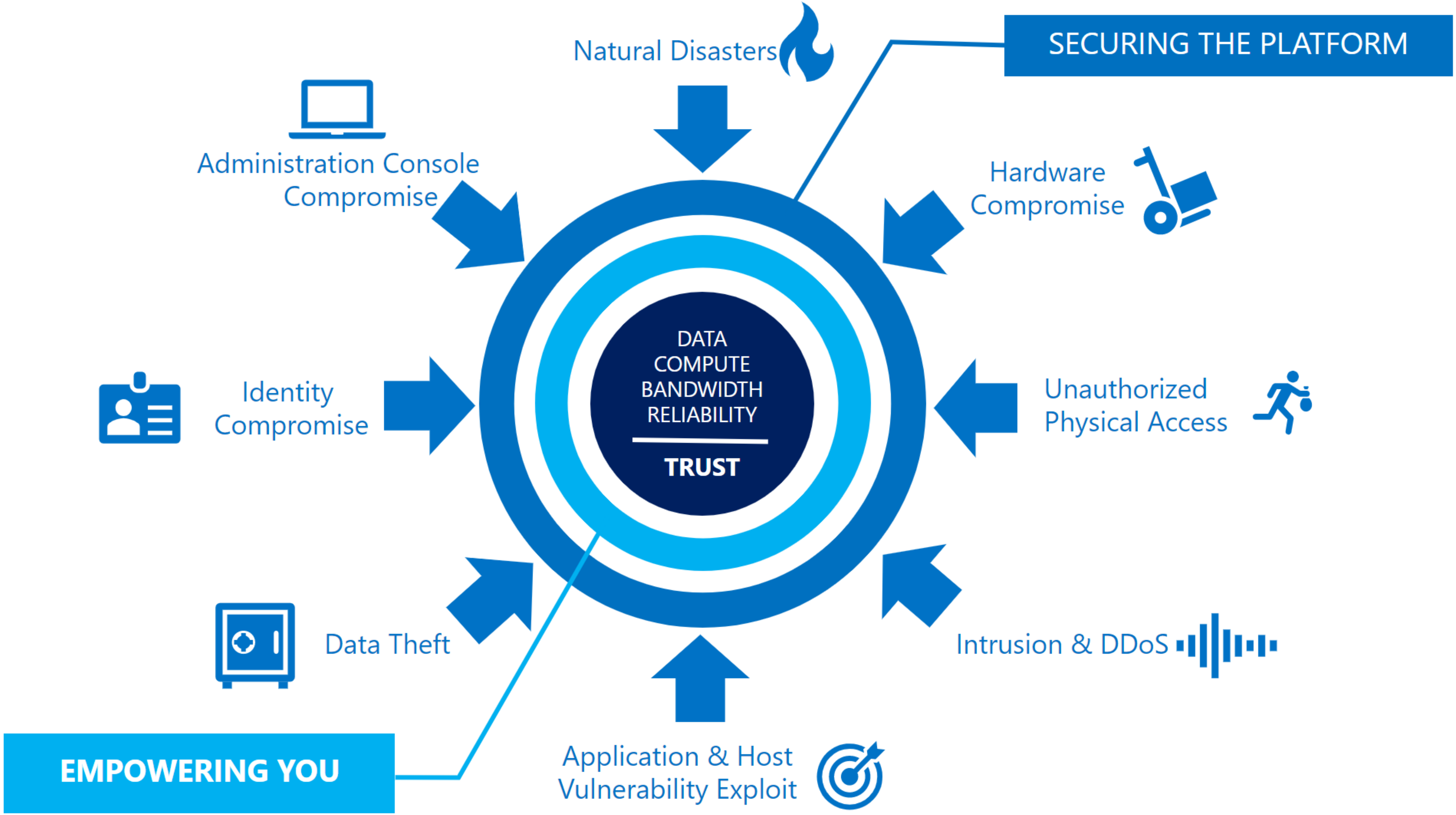
Microsoft Security Vision

Olivier van der Kruijf
Sr Partner Solution Architect
Microsoft

```
┌──(rajackar㉿Big-Loki)-[~]
└─$ whoami \
> Olivier van der Kruijf \
> Sr. Cloud Solutions Architect \
> Microsoft \
> olivier@microsoft.com \
> @ovdkruijf \
```


SECURING THE PLATFORM
Natural Disasters
Administration Console Compromise
Hardware Compromise
Identity Compromise
DATA
COMPUTE
BANDWIDTH
RELIABILITY
TRUST
Unauthorized Physical Access
Data Theft
Intrusion & DDoS
Application & Host Vulnerability Exploit
EMPOWERING YOU

Expanding digital estate

Vehicles

Smart cities

Sensors

Energy systems

Marketplaces

Equipment

Partners

Citizens

Customers

Supply chains

On-premises

Manufacturers

Mobile devices

Traditional SOC Challenges

- Sophistication of threats
- High volume of noisy alerts
- IT deployment & maintenance
- Rising infrastructure costs and upfront investment
- Too many disconnected products
- Lack of automation
- Security skills in short supply

Security Operations Team

Cloud + Artificial Intelligence

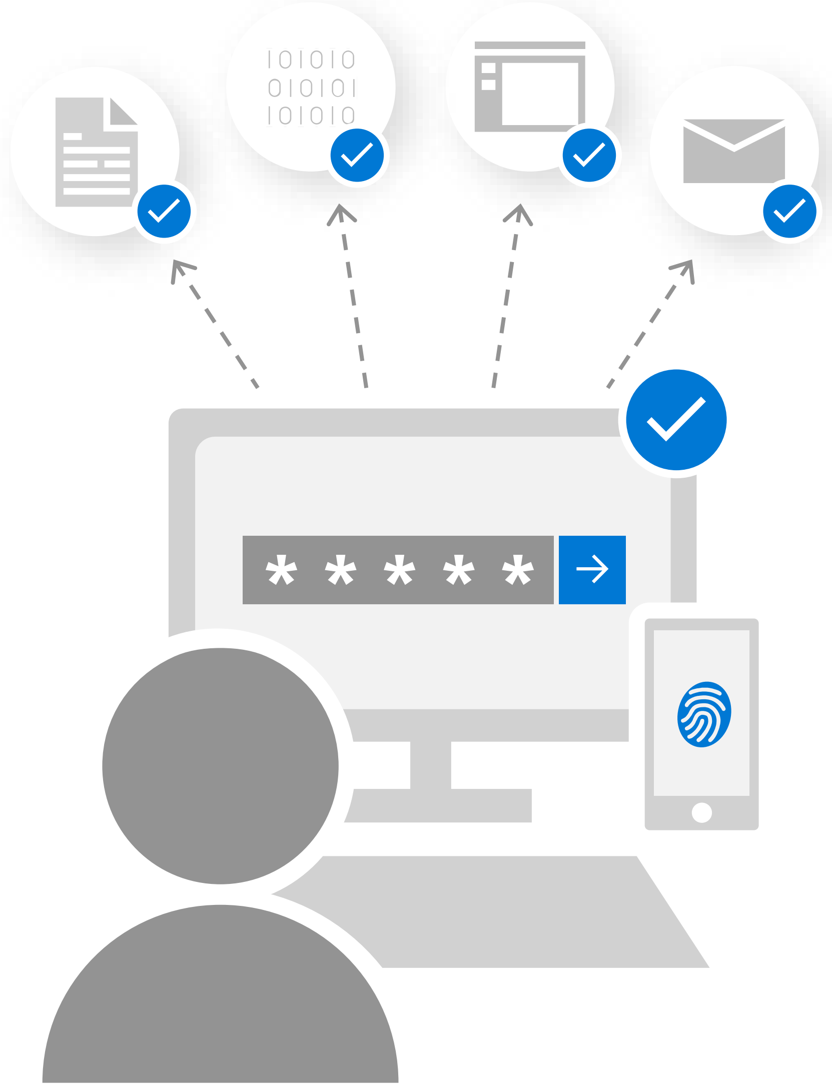
Our unique approach

Built-in experiences that work across platforms

AI and automation to secure your future

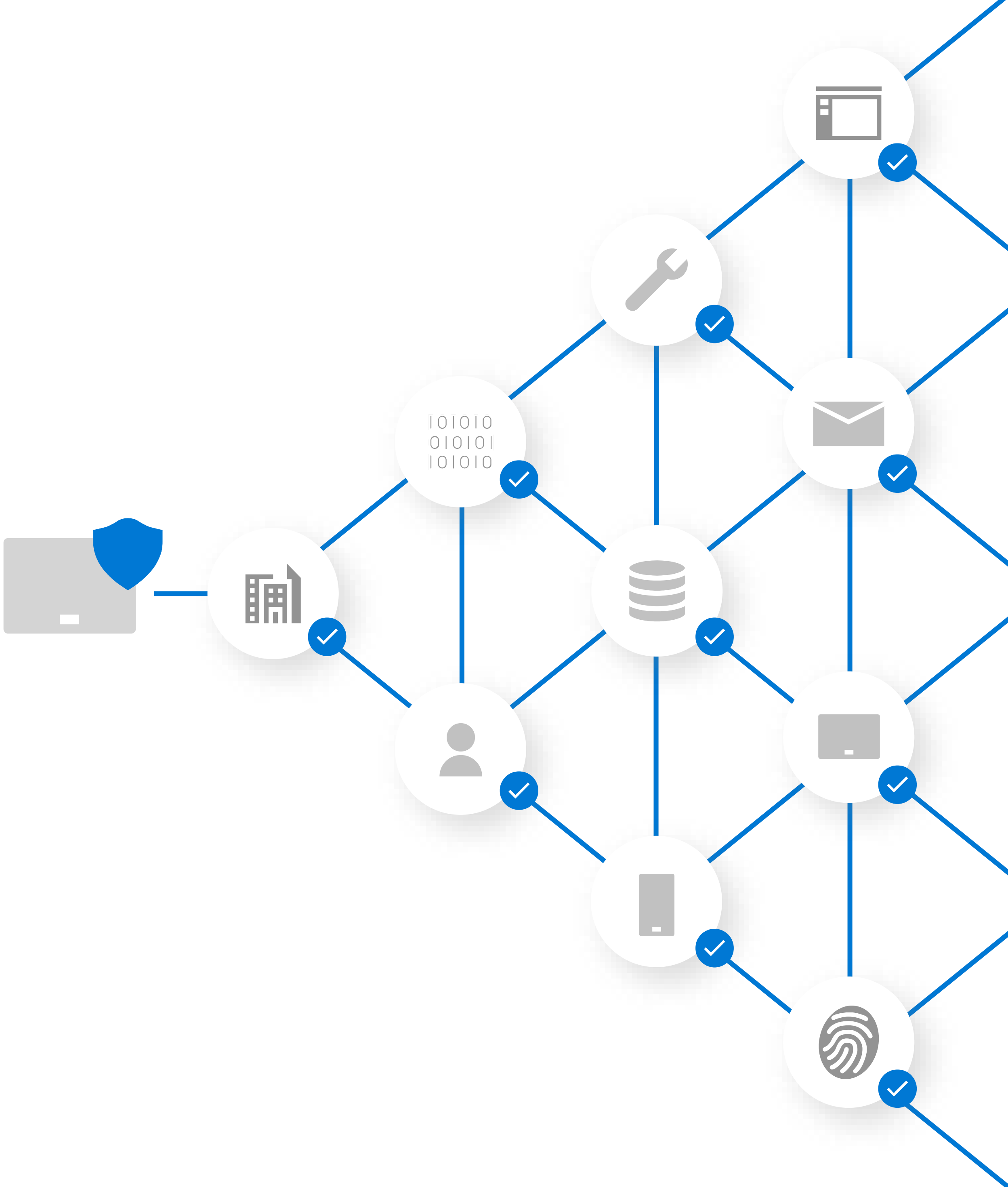
Integrated across people, devices, apps, and data

Built-in experiences that work across platforms



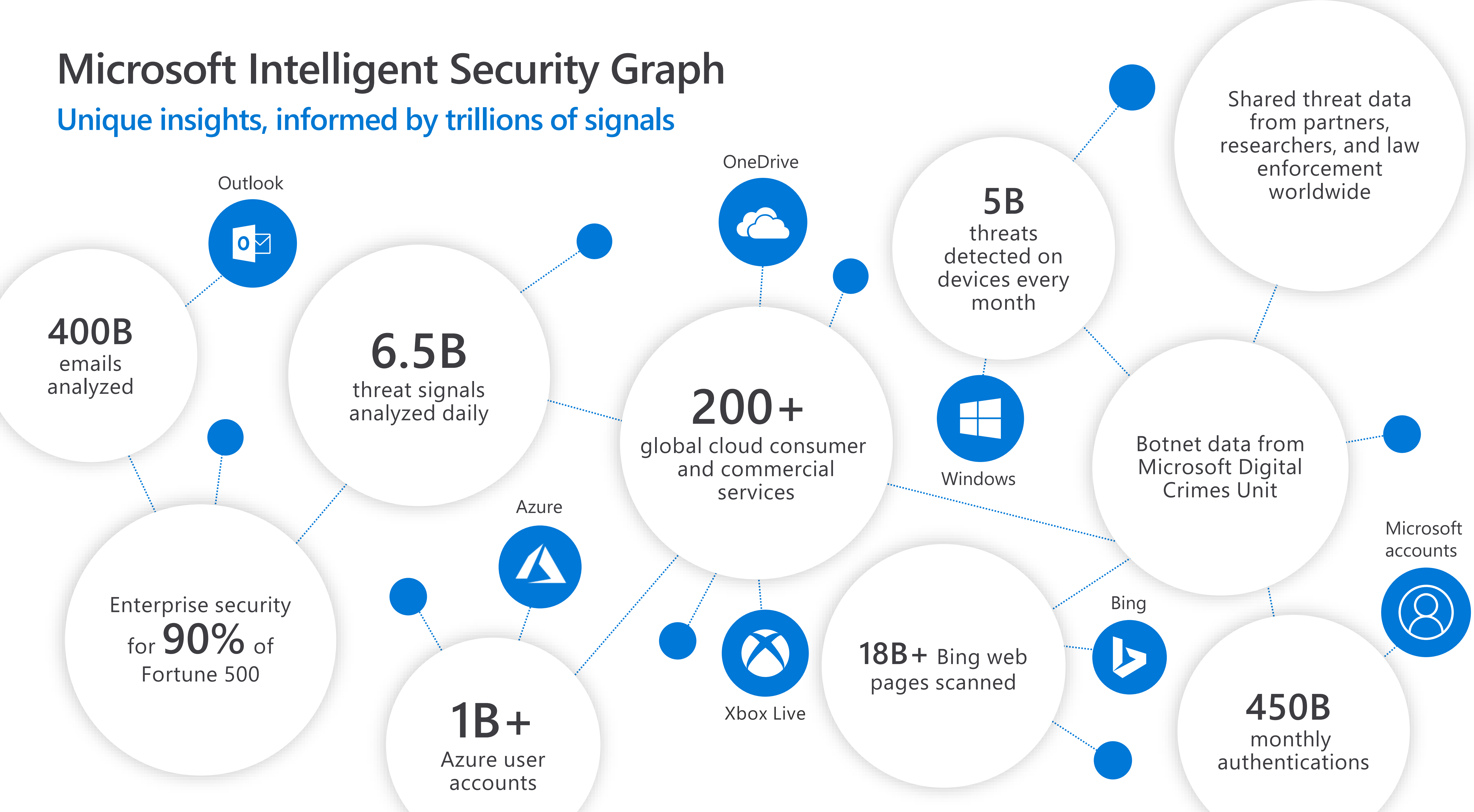
AI and automation
to secure your future

Integrated across people, devices, apps, and data



Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Outlook

400B emails analyzed

6.5B threat signals analyzed daily

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

Azure

1B+ Azure user accounts

OneDrive

200+ global cloud consumer and commercial services

Xbox Live

5B threats detected on devices every month

Windows

18B+ Bing web pages scanned

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

Botnet data from Microsoft Digital Crimes Unit

Bing

Microsoft accounts

450B monthly authentications

Building Cyber Resilience through Intelligent Security

Identity and access management

Your universal platform to manage and secure identities.

Threat protection

Stop attacks with integrated and automated security.

Information protection

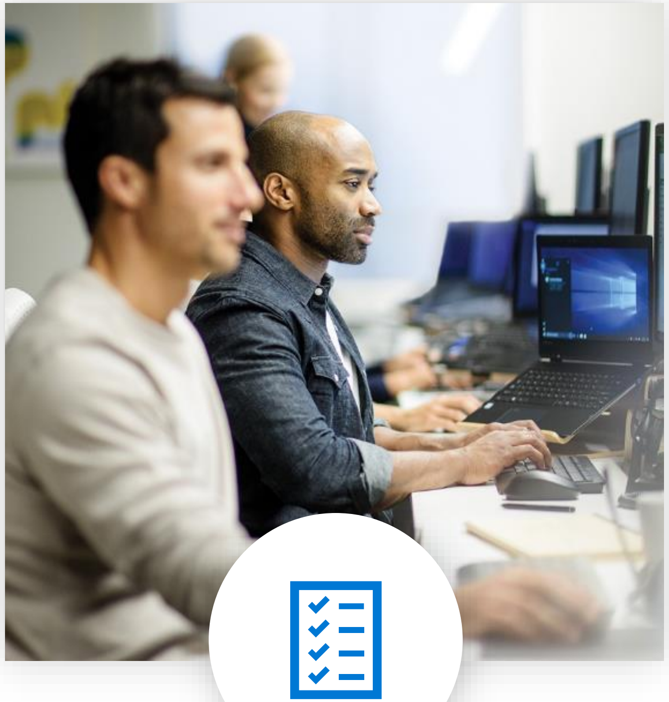
Protect your sensitive data—wherever it lives or travels.

Cloud security

Safeguard your cross-cloud resources.

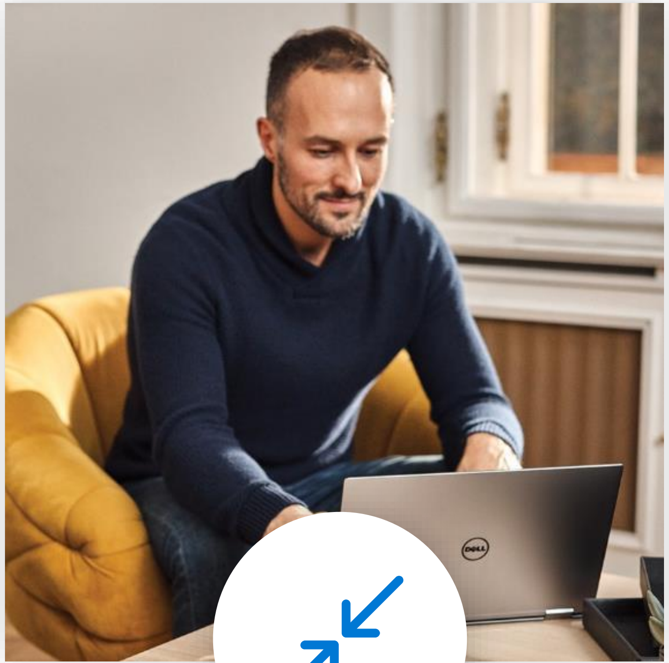
Phishing demo / Session token theft and abuse

Zero Trust Principles



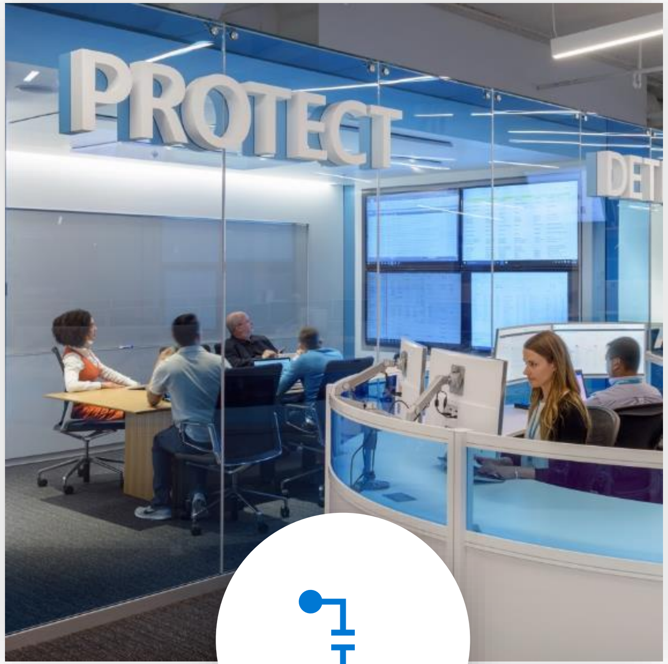
Verify explicitly

Validate trust of users, devices, applications, and more using data/telemetry



Use least privilege access

to limit the impact of any given compromise

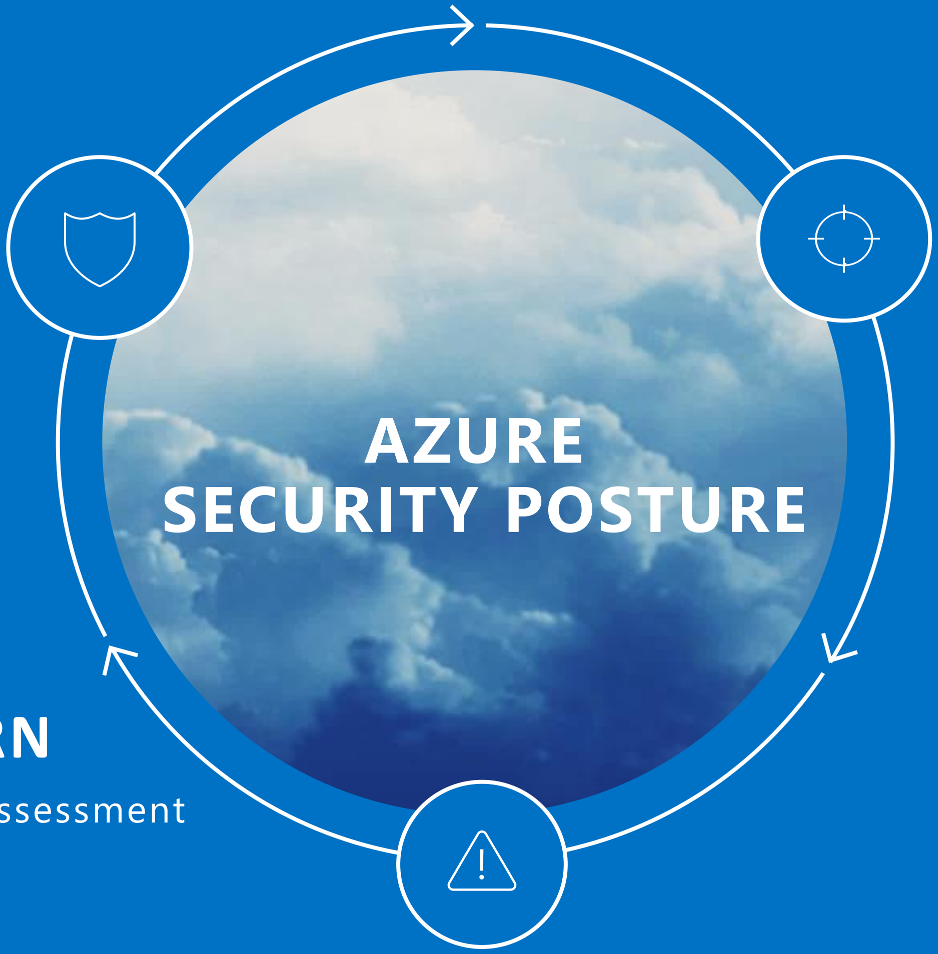


Assume breach

Assume that attackers will succeed (partially or fully) and design accordingly

Instead of assuming everything behind the corporate firewall is safe, Zero Trust assumes *an open environment where trust must be validated.*

ASSUME BREACH



AZURE SECURITY POSTURE

PROTECT

Security Development Lifecycle
Threat Modeling
Code Review
Security Testing
Network/User/Data/System security

DETECT

Auditing and Certification
Live Site Penetration Testing
Centralized Logging and Monitoring
Fraud and Abuse Detection

RESPOND

Breach Containment
Coordinated Security Response
Customer Notification

LEARN

Post-Breach Assessment

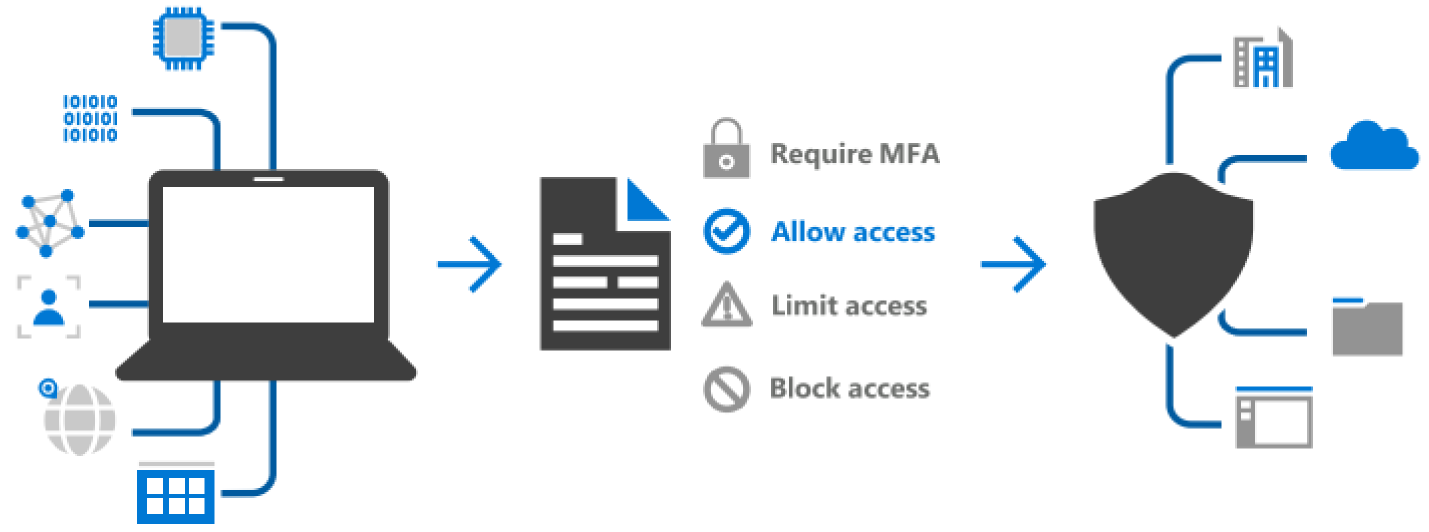
Zero Trust Model

Implementing a Zero Trust Model

Migrating to a Zero Trust Security Model allows you to simultaneously improve security over conventional network-based approaches and better enable users where and when they need access.

A Zero Trust model requires:

1. *Signal* to inform decisions,
2. *Policies* to make access decision and,
3. *Enforcement* capabilities to implement those decisions effectively.



Require MFA

Allow access

Limit access

Block access

Signal
to make an informed decision.

Zero Trust considers many signal sources—from identity systems to device management and device security tools—to create context-rich insights that help make informed decisions.

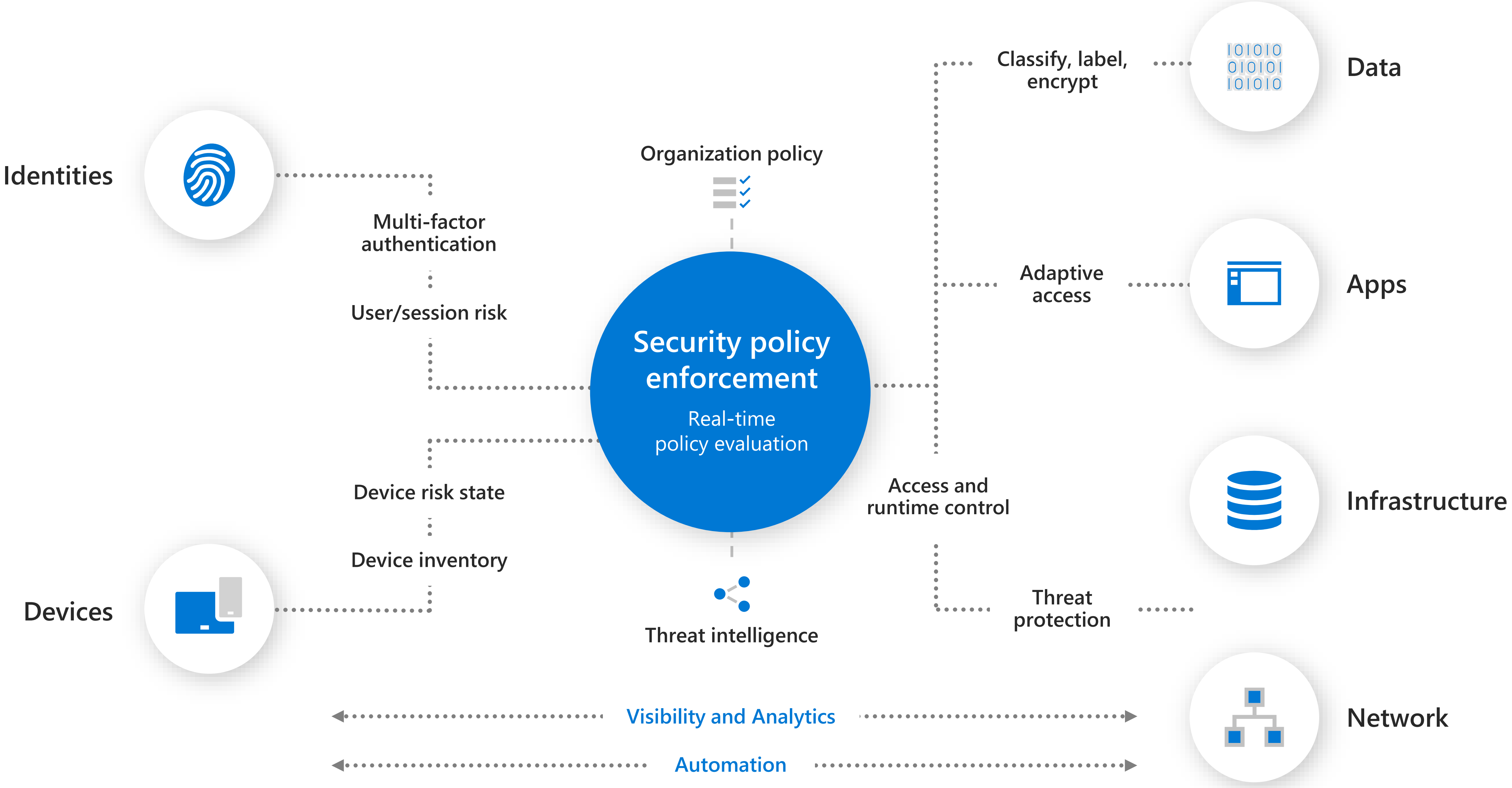
Decision
based on organizational policy.

The access request and signal are analyzed to deliver a decision based on finely-tuned access policies, delivering granular, organization-centric access control.

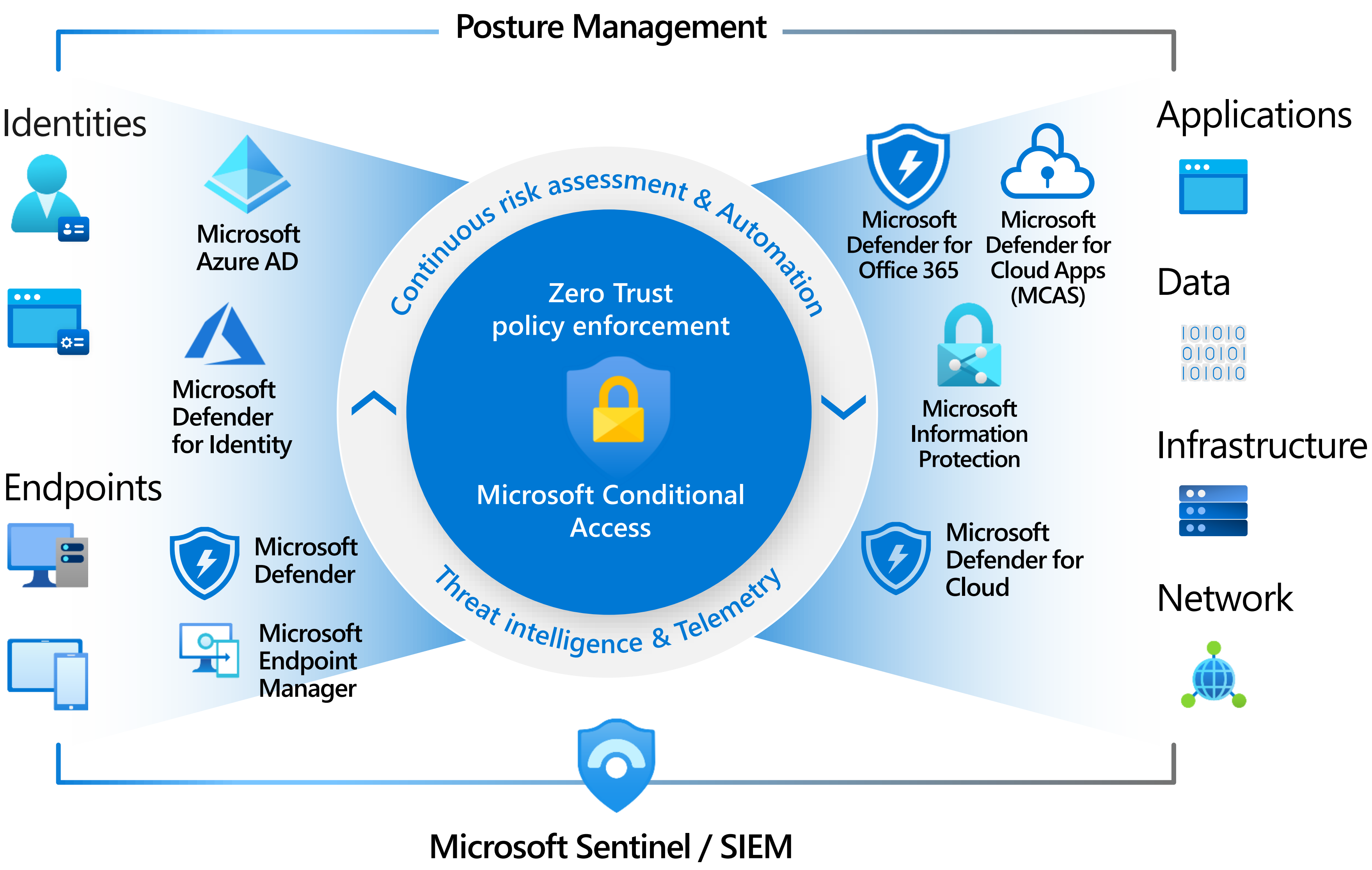
Enforcement
of the policy across resources.

Decisions are then enforced across the entire digital estate—such as read-only access to a SaaS app or remediating compromised passwords with a self-service password reset.

Zero Trust architecture

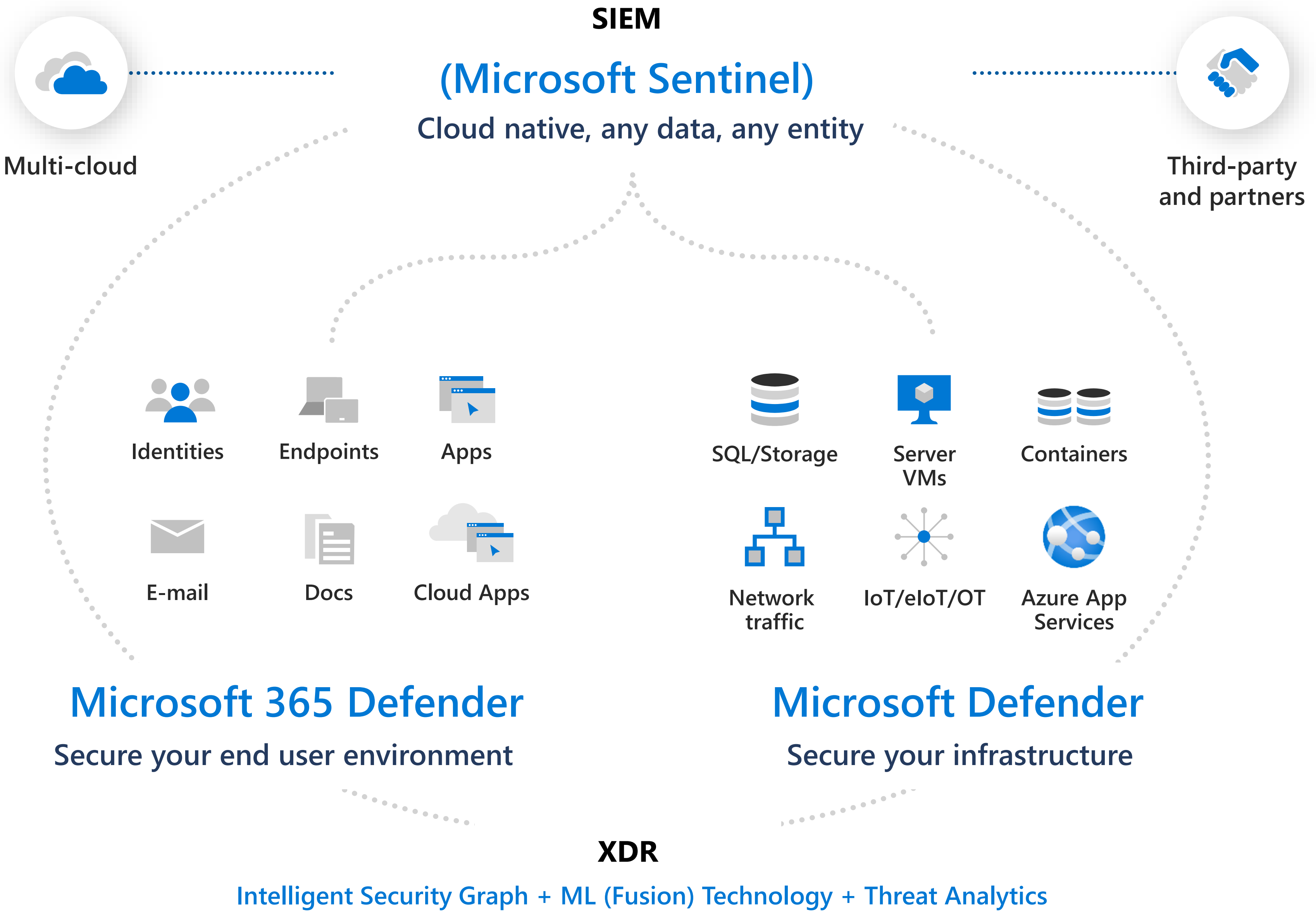


Microsoft Zero Trust Capabilities


Posture Management
Identities
Microsoft Azure AD
Microsoft Defender for Identity
Endpoints
Microsoft Defender
Microsoft Endpoint Manager
Continuous risk assessment & Automation
Zero Trust policy enforcement
Microsoft Conditional Access
Threat intelligence & Telemetry
Microsoft Defender for Office 365
Microsoft Defender for Cloud Apps (MCAS)
Microsoft Information Protection
Microsoft Defender for Cloud
Applications
Data
Infrastructure
Network
Microsoft Sentinel / SIEM

Microsoft Security Architecture

Defender for IoT Within Microsoft's Security Portfolio



SIEM

(Microsoft Sentinel)

Cloud native, any data, any entity

Multi-cloud

Third-party and partners

Identities

Endpoints

Apps

E-mail

Docs

Cloud Apps

SQL/Storage

Server VMs

Containers

Network traffic

IoT/eIoT/OT

Azure App Services

Microsoft 365 Defender

Secure your end user environment

Microsoft Defender

Secure your infrastructure

XDR

Intelligent Security Graph + ML (Fusion) Technology + Threat Analytics

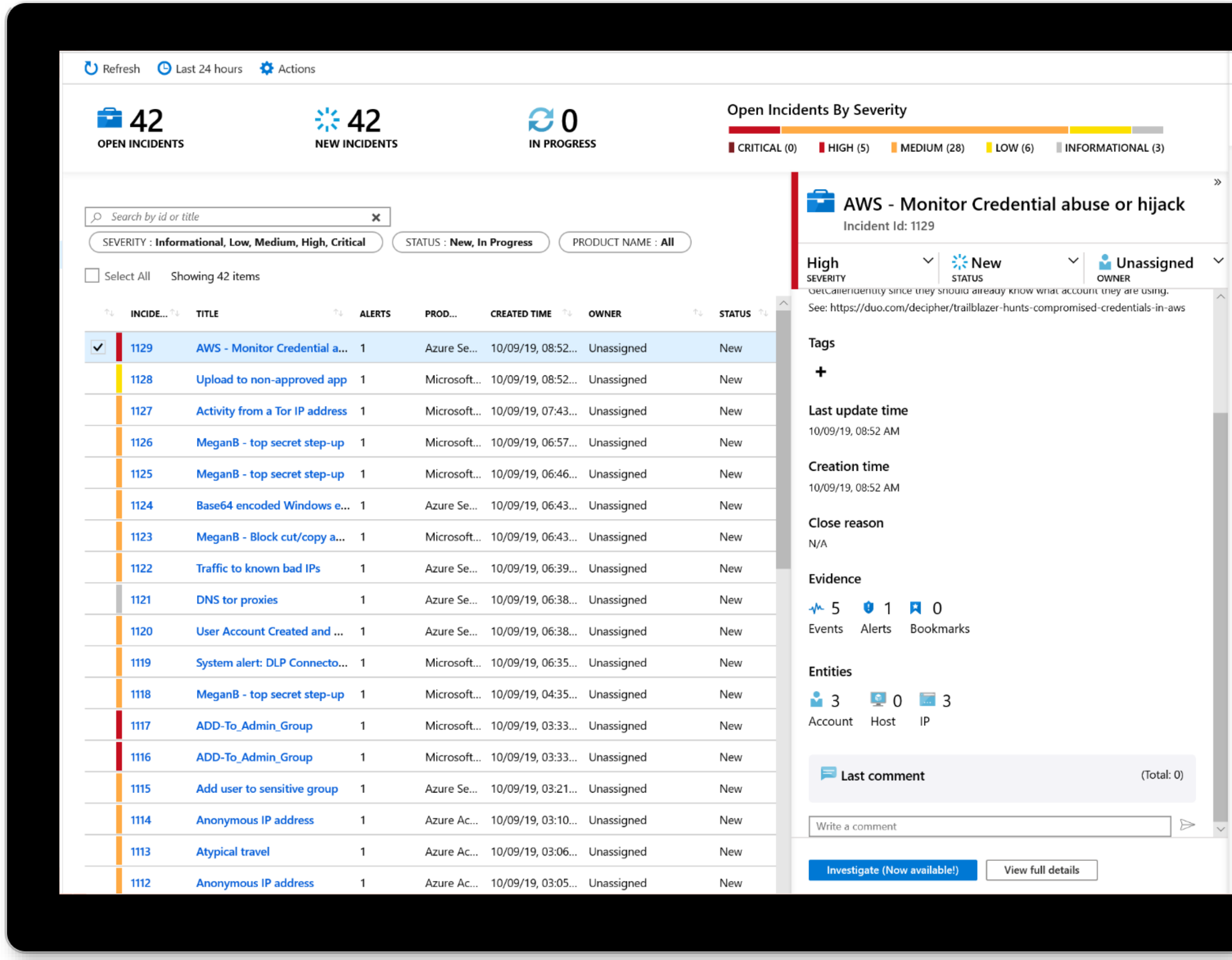
Start and track investigations from prioritized, actionable security incidents

Use incident to collect related alerts, events, and bookmarks

Manage assignments and track status

Add tags and comments

Integrate with your ticketing system



42 OPEN INCIDENTS

42 NEW INCIDENTS

0 IN PROGRESS

Open Incidents By Severity

CRITICAL (0) HIGH (5) MEDIUM (28) LOW (6) INFORMATIONAL (3)

SEVERITY : **Informational, Low, Medium, High, Critical**

STATUS : **New, In Progress**

PRODUCT NAME : **All**

□ Select All Showing 42 items

	INCIDE...	TITLE	ALERTS	PROD...	CREATED TIME	OWNER	STATUS
☑	1129	AWS - Monitor Credential a...	1	Azure Se...	10/09/19, 08:52...	Unassigned	New
	1128	Upload to non-approved app	1	Microsoft...	10/09/19, 08:52...	Unassigned	New
	1127	Activity from a Tor IP address	1	Microsoft...	10/09/19, 07:43...	Unassigned	New
	1126	MeganB - top secret step-up	1	Microsoft...	10/09/19, 06:57...	Unassigned	New
	1125	MeganB - top secret step-up	1	Microsoft...	10/09/19, 06:46...	Unassigned	New
	1124	Base64 encoded Windows e...	1	Azure Se...	10/09/19, 06:43...	Unassigned	New
	1123	MeganB - Block cut/copy a...	1	Microsoft...	10/09/19, 06:43...	Unassigned	New
	1122	Traffic to known bad IPs	1	Azure Se...	10/09/19, 06:39...	Unassigned	New
	1121	DNS tor proxies	1	Azure Se...	10/09/19, 06:38...	Unassigned	New
	1120	User Account Created and ...	1	Azure Se...	10/09/19, 06:38...	Unassigned	New
	1119	System alert: DLP Connecto...	1	Microsoft...	10/09/19, 06:35...	Unassigned	New
	1118	MeganB - top secret step-up	1	Microsoft...	10/09/19, 04:35...	Unassigned	New
	1117	ADD-To_Admin_Group	1	Microsoft...	10/09/19, 03:33...	Unassigned	New
	1116	ADD-To_Admin_Group	1	Microsoft...	10/09/19, 03:33...	Unassigned	New
	1115	Add user to sensitive group	1	Azure Se...	10/09/19, 03:21...	Unassigned	New
	1114	Anonymous IP address	1	Azure Ac...	10/09/19, 03:10...	Unassigned	New
	1113	Atypical travel	1	Azure Ac...	10/09/19, 03:06...	Unassigned	New
	1112	Anonymous IP address	1	Azure Ac...	10/09/19, 03:05...	Unassigned	New

AWS - Monitor Credential abuse or hijack

Incident Id: 1129

High SEVERITY | New STATUS | Unassigned OWNER

GetCallerIdentity since they should already know what account they are using.
See: https://duo.com/decipher/trailblazer-hunts-compromised-credentials-in-aws

Tags

+

Last update time
10/09/19, 08:52 AM

Creation time
10/09/19, 08:52 AM

Close reason
N/A

Evidence

5 Events 1 Alerts 0 Bookmarks

Entities

3 Account 0 Host 3 IP

Last comment (Total: 0)

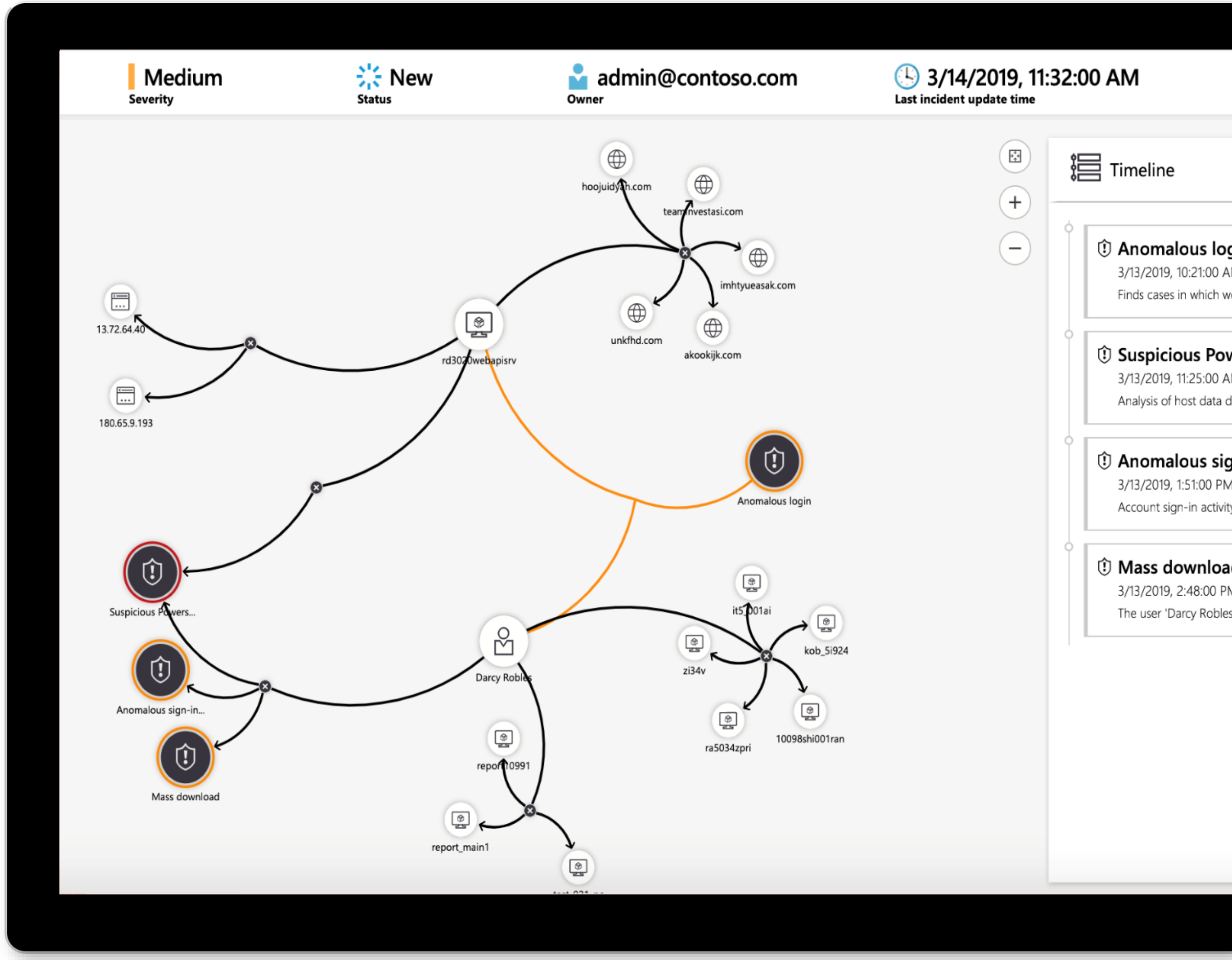
Visualize the entire attack to determine scope and impact

Navigate the relationships between related alerts, bookmarks, and entities

Expand the scope using exploration queries

View a timeline of related alerts, events, and bookmarks

Gain deep insights into related entities – users, domains, and more



Medium
Severity

New
Status

admin@contoso.com
Owner

3/14/2019, 11:32:00 AM
Last incident update time

Timeline

Anomalous log
3/13/2019, 10:21:00 A
Finds cases in which w

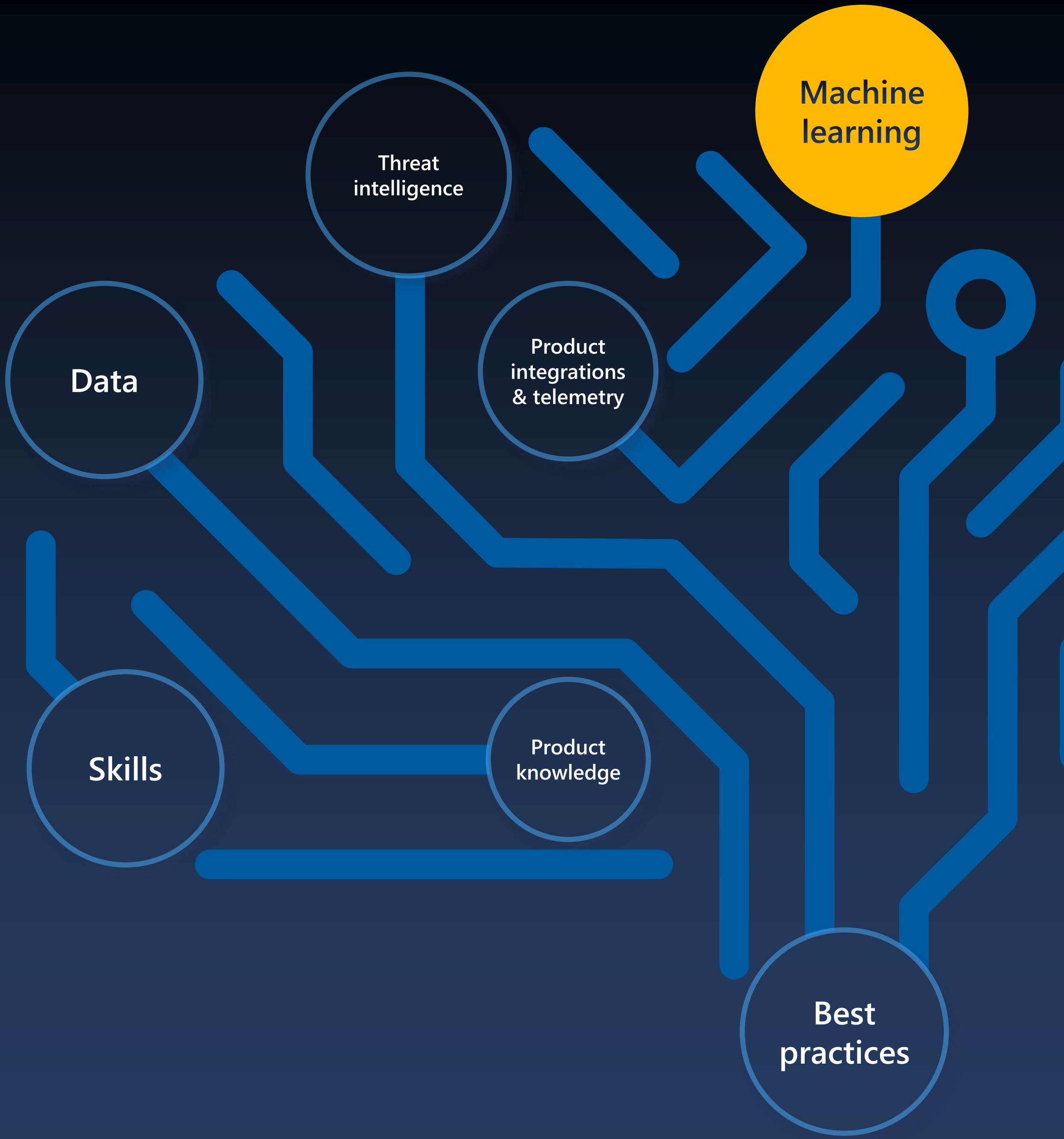
Suspicious Pov
3/13/2019, 11:25:00 A
Analysis of host data d

Anomalous sig
3/13/2019, 1:51:00 PM
Account sign-in activit

Mass downloa
3/13/2019, 2:48:00 PM
The user 'Darcy Robles

Microsoft Security Copilot

The first generative AI security product that empowers SOC analysts to defend their organizations at machine speed and scale



Classified as Microsoft Confidential

Microsoft Security Copilot

Defending at machine speed

> ***"It takes us three minutes to do a task that used to take at least a few hours"***

- Private preview customer

Enable response in minutes, not hours

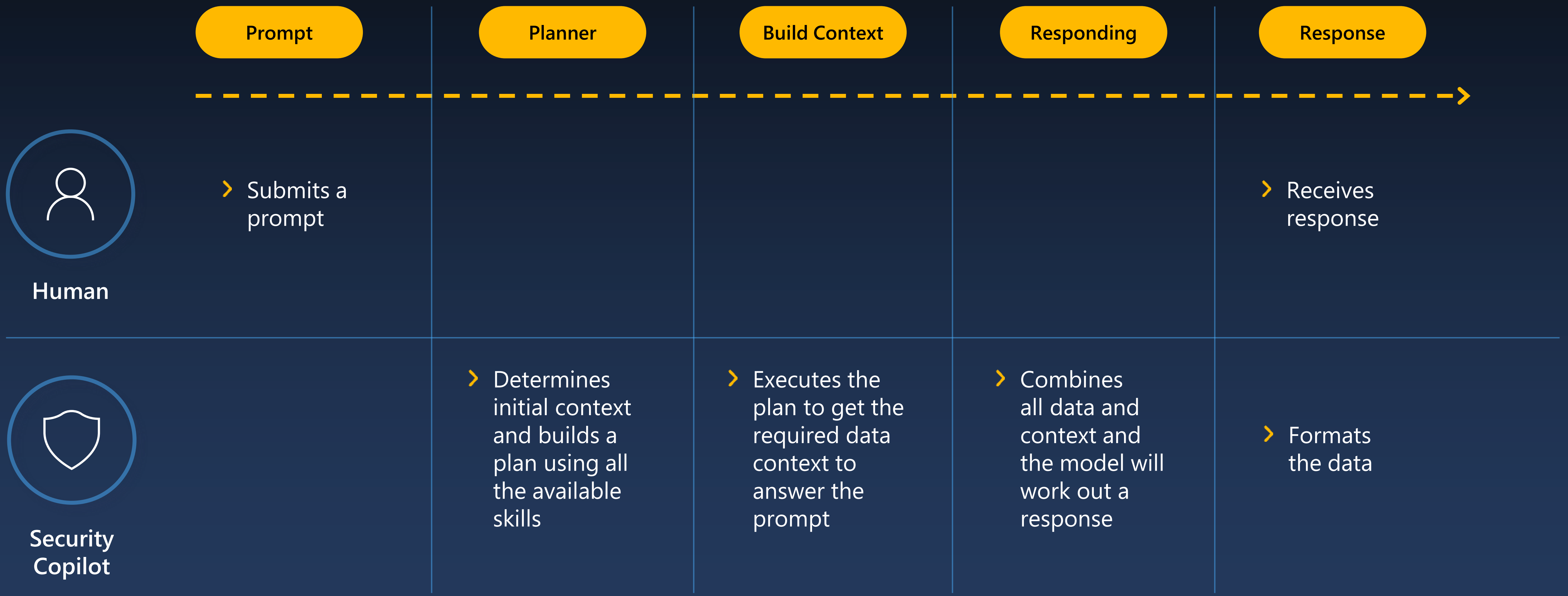
Simplify the complex with natural language prompts and easy reporting

Catch what others miss with deeper understanding of your enterprise

Upskill your security talent with cyber-trained generative AI

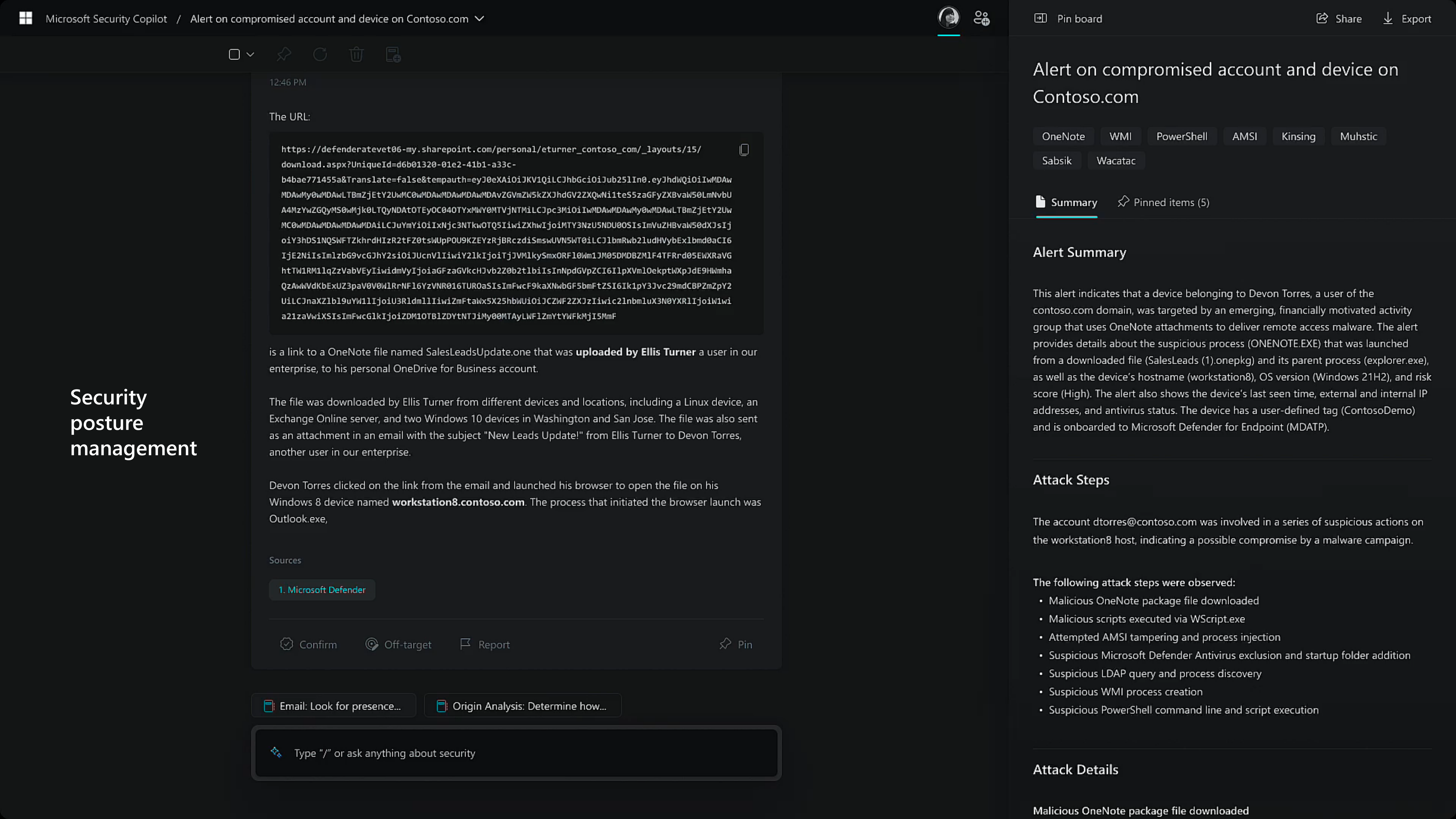
Classified as Microsoft Confidential

Operated with simple natural language queries



	Prompt	Planner	Build Context	Responding	Response
Human	Submits a prompt				Receives response
Security Copilot		Determines initial context and builds a plan using all the available skills	Executes the plan to get the required data context to answer the prompt	Combines all data and context and the model will work out a response	Formats the data

Security posture management


Microsoft Security Copilot / Alert on compromised account and device on Contoso.com
Pin board
Share
Export
12:46 PM
Confirm
Off-target
Report
Pin
Email: Look for presence...
Origin Analysis: Determine how...
Type "/" or ask anything about security
OneNote
WMI
PowerShell
AMSI
Kinsing
Muhstic
Sabsik
Wacatac
Summary
Pinned items (5)

The URL:

```
https://defenderatevet06-my.sharepoint.com/personal/eturner_contoso_com/_layouts/15/
download.aspx?UniqueId=d6b01320-01e2-41b1-a33c-
b4bae771455a&Translate=false&tempauth=eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJhdWQiOiIwMDAw
MDAwMy0wMDAwLTBmZjEtY2UwMC0wMDAwMDAwMDAwMDAvZGVmZW5kZXJhdGV2ZXQwNi1teS5zaGFyZXBvaW50LmNvbU
A4MzYwZGQyMS0wMjk0LTQyNDAtOTEyOC04OTYxMWY0MTVjNTMiLCJpc3MiOiIwMDAwMDAwMy0wMDAwLTBmZjEtY2Uw
MC0wMDAwMDAwMDAwMDAiLCJuYmYiOiIxNjc3NTkwOTQ5IiwiZXhwIjoiMTY3NzU5NDU0OSIsImVuZHBvaW50dXJsIj
oiY3hDS1NQSWFTZkhrdHIzR2tFZ0tsWUpPOU9KZEYzRjBRczdiSmswUVN5WT0iLCJlbmRwb2ludHVybExlbmd0aCI6
IjE2NiIsImlzbG9vcGJhY2siOiJUcnVlIiwiY2lkIjoiTjJVMlkySmxORFl0Wm1JM05DMDBZMlF4TFRrd05EWXRaVG
htTW1RM1lqZzVabVEyIiwidmVyIjoiaGFzaGVkcHJvb2Z0b2tlbiIsInNpdGVpZCI6IlpXVmlOekptWXpJdE9HWmha
QzAwWVdKbExUZ3paV0V0WlRrNFl6YzVNR016TUROaSIsImFwcF9kaXNwbGF5bmFtZSI6Ik1pY3Jvc29mdCBPZmZpY2
UiLCJnaXZlbl9uYW1lIjoiU3RldmlIIiwiZmFtaWx5X25hbWUiOiJCZWF2ZXJzIiwic2lnbmluX3N0YXRlIjoiW1wi
a21zaVwiXSIsImFwcGlkIjoiZDM1OTBlZDYtNTJiMy00MTAyLWFlZmYtYWFkMjI5MmF
```

is a link to a OneNote file named SalesLeadsUpdate.one that was **uploaded by Ellis Turner** a user in our enterprise, to his personal OneDrive for Business account.

The file was downloaded by Ellis Turner from different devices and locations, including a Linux device, an Exchange Online server, and two Windows 10 devices in Washington and San Jose. The file was also sent as an attachment in an email with the subject "New Leads Update!" from Ellis Turner to Devon Torres, another user in our enterprise.

Devon Torres clicked on the link from the email and launched his browser to open the file on his Windows 8 device named **workstation8.contoso.com**. The process that initiated the browser launch was Outlook.exe,

Sources

1. Microsoft Defender

Alert on compromised account and device on Contoso.com

Alert Summary

This alert indicates that a device belonging to Devon Torres, a user of the contoso.com domain, was targeted by an emerging, financially motivated activity group that uses OneNote attachments to deliver remote access malware. The alert provides details about the suspicious process (ONENOTE.EXE) that was launched from a downloaded file (SalesLeads (1).onepkg) and its parent process (explorer.exe), as well as the device's hostname (workstation8), OS version (Windows 21H2), and risk score (High). The alert also shows the device's last seen time, external and internal IP addresses, and antivirus status. The device has a user-defined tag (ContosoDemo) and is onboarded to Microsoft Defender for Endpoint (MDATP).

Attack Steps

The account dtorres@contoso.com was involved in a series of suspicious actions on the workstation8 host, indicating a possible compromise by a malware campaign.

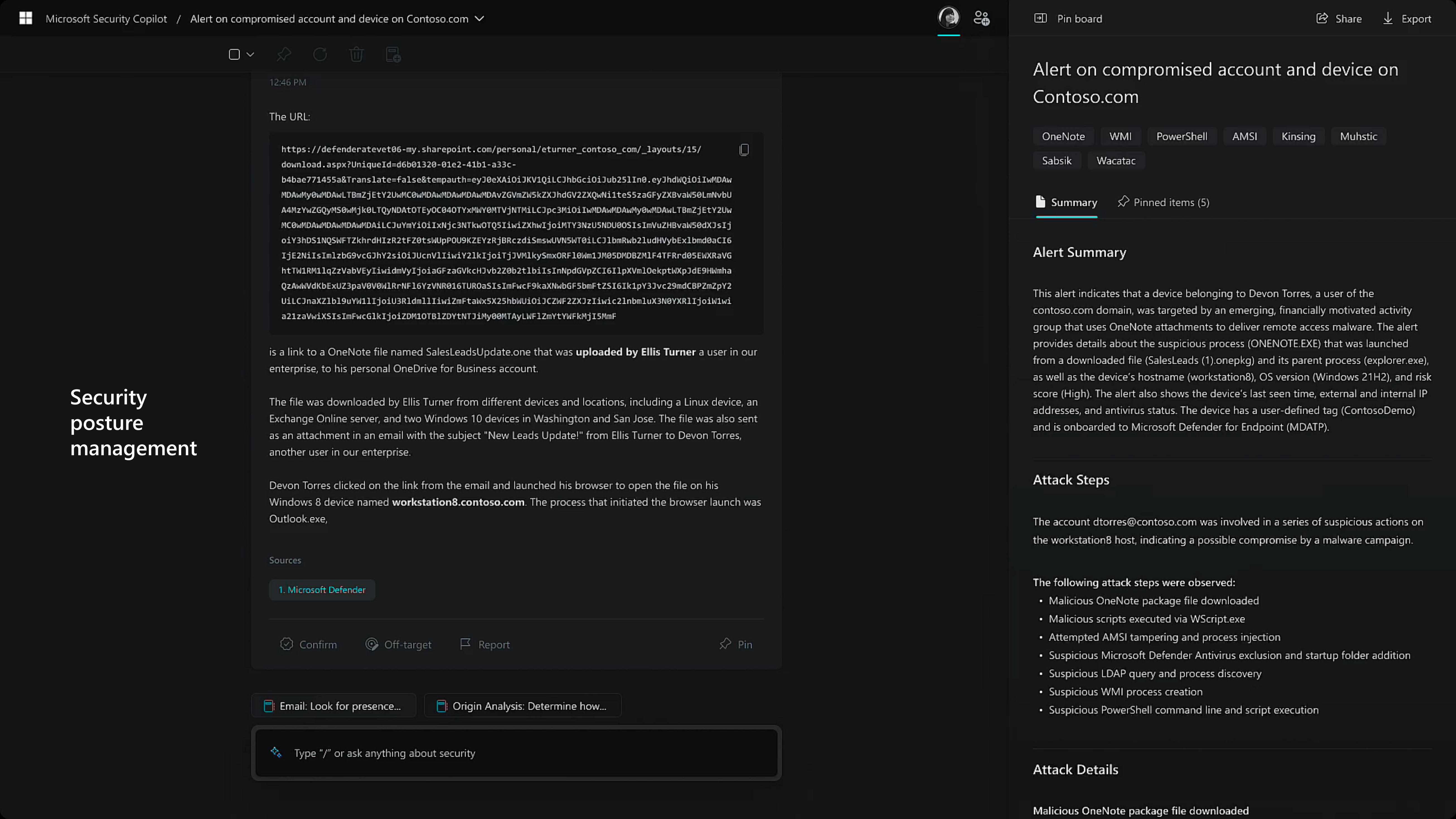
The following attack steps were observed:

- Malicious OneNote package file downloaded
- Malicious scripts executed via WScript.exe
- Attempted AMSI tampering and process injection
- Suspicious Microsoft Defender Antivirus exclusion and startup folder addition
- Suspicious LDAP query and process discovery
- Suspicious WMI process creation
- Suspicious PowerShell command line and script execution

Attack Details

Malicious OneNote package file downloaded

Security posture management


Microsoft Security Copilot / Alert on compromised account and device on Contoso.com
Pin board
Share
Export

12:46 PM

The URL:

```
https://defenderatevet06-my.sharepoint.com/personal/eturner_contoso_com/_layouts/15/
download.aspx?UniqueId=d6b01320-01e2-41b1-a33c-
b4bae771455a&Translate=false&tempauth=eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJhdWQiOiIwMDAw
MDAwMy0wMDAwLTBmZjEtY2UwMC0wMDAwMDAwMDAwMDAvZGVmZW5kZXJhdGV2ZXQwNi1teS5zaGFyZXBvaW50LmNvbU
A4MzYwZGQyMS0wMjk0LTQyNDAtOTEyOC04OTYxMWY0MTVjNTMiLCJpc3MiOiIwMDAwMDAwMy0wMDAwLTBmZjEtY2Uw
MC0wMDAwMDAwMDAwMDAiLCJuYmYiOiIxNjc3NTkwOTQ5IiwiZXhwIjoiMTY3NzU5NDU0OSIsImVuZHBvaW50dXJsIj
oiY3hDS1NQSWFTZkhrdHIzR2tFZ0tsWUpPOU9KZEYzRjBRczdiSmswUVN5WT0iLCJlbmRwb2ludHVybExlbmd0aCI6
IjE2NiIsImlzbG9vcGJhY2siOiJUcnVlIiwiY2lkIjoiTjJVMlkySmxORFl0Wm1JM05DMDBZMlF4TFRrd05EWXRaVG
htTW1RM1lqZzVabVEyIiwidmVyIjoiaGFzaGVkcHJvb2Z0b2tlbiIsInNpdGVpZCI6IlpXVmlOekptWXpJdE9HWmha
QzAwWVdKbExUZ3paV0V0WlRrNFl6YzVNR016TUROaSIsImFwcF9kaXNwbGF5bmFtZSI6Ik1pY3Jvc29mdCBPZmZpY2
UiLCJnaXZlbl9uYW1lIjoiU3RldmllIiwiZmFtaWx5X25hbWUiOiJCZWF2ZXJzIiwic2lnbmluX3N0YXRlIjoiW1wi
a21zaVwiXSIsImFwcGlkIjoiZDM1OTBlZDYtNTJiMy00MTAyLWFlZmYtYWFkMjI5MmF
```

is a link to a OneNote file named SalesLeadsUpdate.one that was **uploaded by Ellis Turner** a user in our enterprise, to his personal OneDrive for Business account.

The file was downloaded by Ellis Turner from different devices and locations, including a Linux device, an Exchange Online server, and two Windows 10 devices in Washington and San Jose. The file was also sent as an attachment in an email with the subject "New Leads Update!" from Ellis Turner to Devon Torres, another user in our enterprise.

Devon Torres clicked on the link from the email and launched his browser to open the file on his Windows 8 device named **workstation8.contoso.com**. The process that initiated the browser launch was Outlook.exe,

Sources

1. Microsoft Defender

Confirm
Off-target
Report
Pin
Email: Look for presence...
Origin Analysis: Determine how...
Type "/" or ask anything about security

Alert on compromised account and device on Contoso.com

Alert Summary

This alert indicates that a device belonging to Devon Torres, a user of the contoso.com domain, was targeted by an emerging, financially motivated activity group that uses OneNote attachments to deliver remote access malware. The alert provides details about the suspicious process (ONENOTE.EXE) that was launched from a downloaded file (SalesLeads (1).onepkg) and its parent process (explorer.exe), as well as the device's hostname (workstation8), OS version (Windows 21H2), and risk score (High). The alert also shows the device's last seen time, external and internal IP addresses, and antivirus status. The device has a user-defined tag (ContosoDemo) and is onboarded to Microsoft Defender for Endpoint (MDATP).

Attack Steps

The account dtorres@contoso.com was involved in a series of suspicious actions on the workstation8 host, indicating a possible compromise by a malware campaign.

The following attack steps were observed:

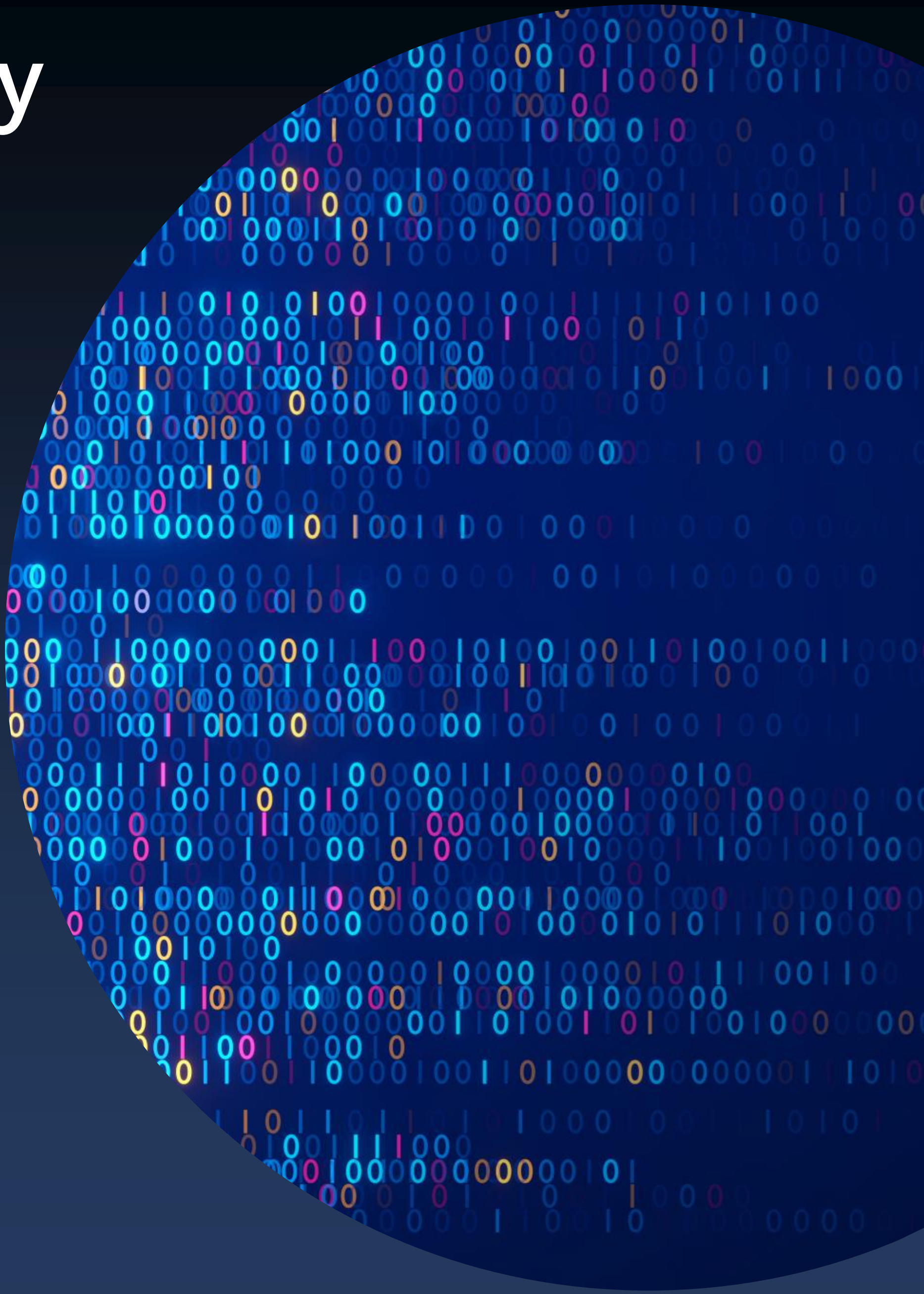
- Malicious OneNote package file downloaded
- Malicious scripts executed via WScript.exe
- Attempted AMSI tampering and process injection
- Suspicious Microsoft Defender Antivirus exclusion and startup folder addition
- Suspicious LDAP query and process discovery
- Suspicious WMI process creation
- Suspicious PowerShell command line and script execution

Attack Details

Malicious OneNote package file downloaded

Built on AI model trained for security

- Large language model (LLM) pretrained on trillions of points of security-specific telemetry and threat intelligence
- Works with natural language queries and requires no knowledge of KQL
- Processes any text-based security data and requires no parsers or data standardization
- Designed to improve with use; guided by user feedback



Built with security, privacy, and compliance.

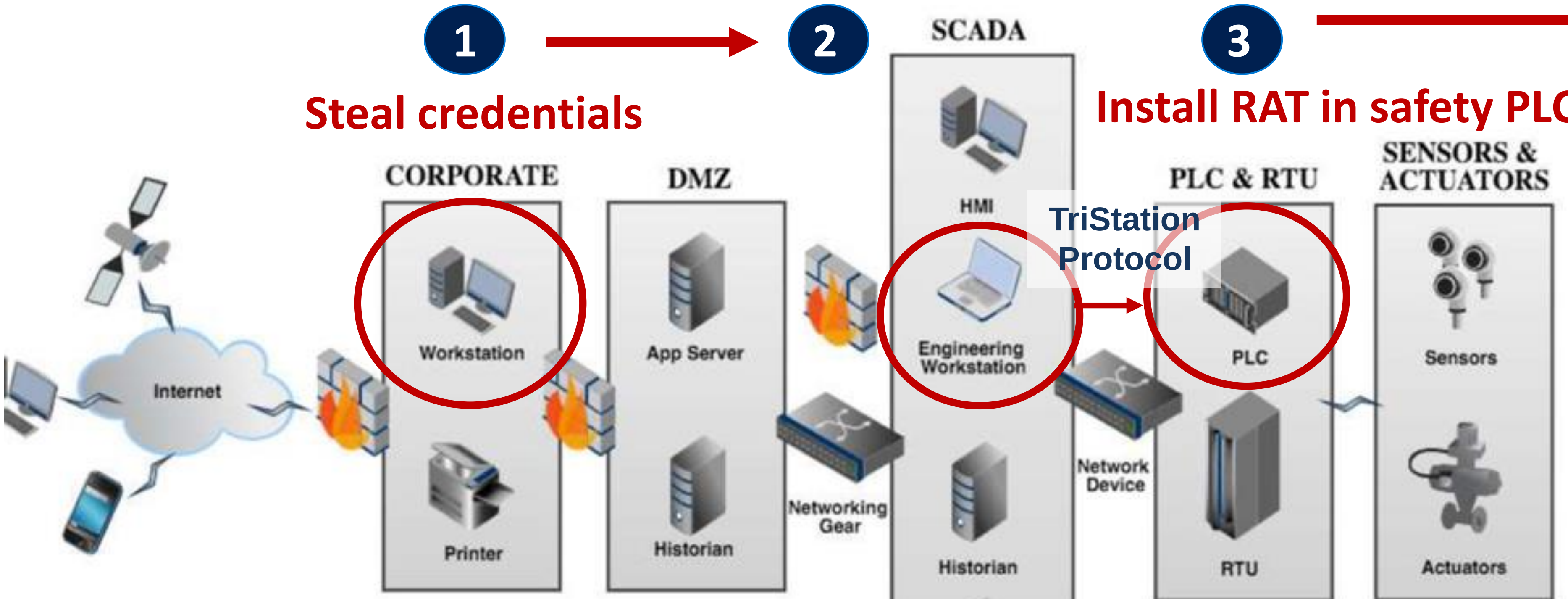
Your data is **your** data

Your data is **not** used to train the foundation AI models

Your data is protected by the **most comprehensive** enterprise compliance and security controls

TRITON Kill Chain Example

Microsoft Defender for Endpoint & Defender for IoT simultaneously detect suspicious RDP access from IT to OT network — alerts converged in Azure Sentinel incident



1 Steal credentials

2 Deploy PC malware

TriStation Protocol

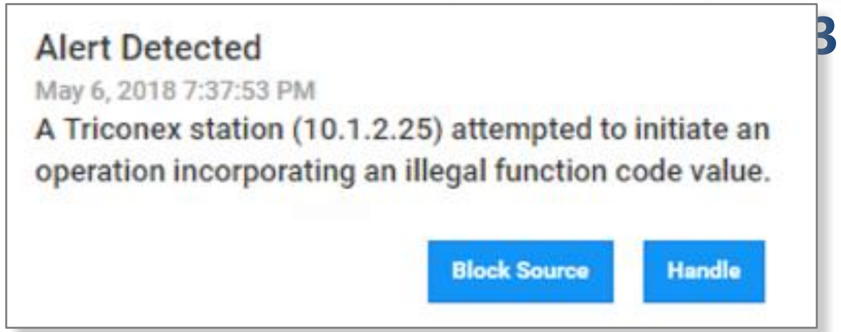
3 Install RAT in safety PLC

4 Disable safety PLC & launch 2nd cyberattack

3

L1

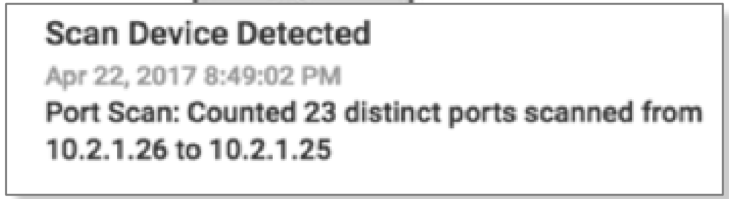
L0



Alert Detected

May 6, 2018 7:37:53 PM

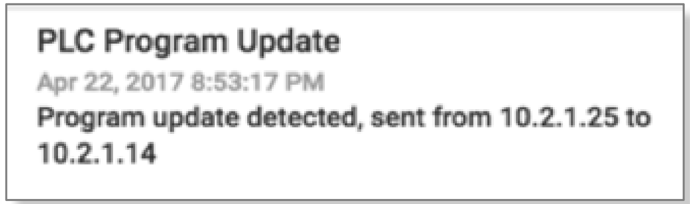
A Triconex station (10.1.2.25) attempted to initiate an operation incorporating an illegal function code value.



Scan Device Detected

Apr 22, 2017 8:49:02 PM

Port Scan: Counted 23 distinct ports scanned from 10.2.1.26 to 10.2.1.25



PLC Program Update

Apr 22, 2017 8:53:17 PM

Program update detected, sent from 10.2.1.25 to 10.2.1.14

Questions

Thank you!