

May 13th, 2023

#GlobalAzureAthens



Let's Attack Azure

George Kavvalakis

Risk Management & Security Architect @ BNP Paribas Fortis
CEO @ Blacktrack Consulting Ltd.

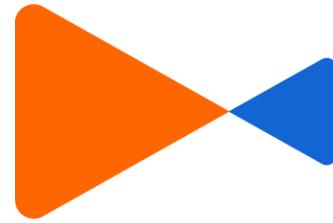
Top 100 Leaders in Global Healthcare (IFAH 2019)
Outstanding Leadership Award (Health 2.0 2022)
Visionaries Award (Health 2.0 2022)
Microsoft Azure Solutions Architect

BSc, MSc, MCSA, Interoperability Influencer

Dear Global Azure Athens
2023 sponsors,
your support made all the
difference — **thank you!**



#GlobalAzureAthens



kaizen
GAMING



About me



Risk Management & Security Architect @ BNP Paribas Fortis
Top 100 Leaders in Global Healthcare (IFAH 2019)
Outstanding Leadership Award (Health 2.0 2022)
Visionaries Award (Health 2.0 2022)
Microsoft Azure Solutions Architect
BSc, MSc, MCSA, Interoperability Influencer

20+ years of experience in IT

CIO for 14 Years at Vamvas Medicals (Vamvas Group)

Founder & CEO of BlackTrack Consulting

Founder & CEO of Hood Groove Management



www.blacktrack.gr



fb.com/blacktrackbnt



[georgeblackman](https://in.linkedin.com/in/georgeblackman)

About me



Risk Management & Security Architect @ BNP Paribas Fortis
Top 100 Leaders in Global Healthcare (IFAH 2019)
Outstanding Leadership Award (Health 2.0 2022)
Visionaries Award (Health 2.0 2022)
Microsoft Azure Solutions Architect
BSc, MSc, MCSA, Interoperability Influencer



...and more

Autoexec.gr Admin & Azureheads.gr Member

Entrepreneur | Speaker | Gamer | Pen-Test hobbyist | Hip Hop Enthusiast



www.blacktrack.gr



fb.com/blacktrackbnt



georgeblackman

Agenda

-
- Information protection vs security
 - Know Your Data
 - Know Your Environment
 - Attacking Azure
 - Security first

#GlobalAzureAthens

Introduction



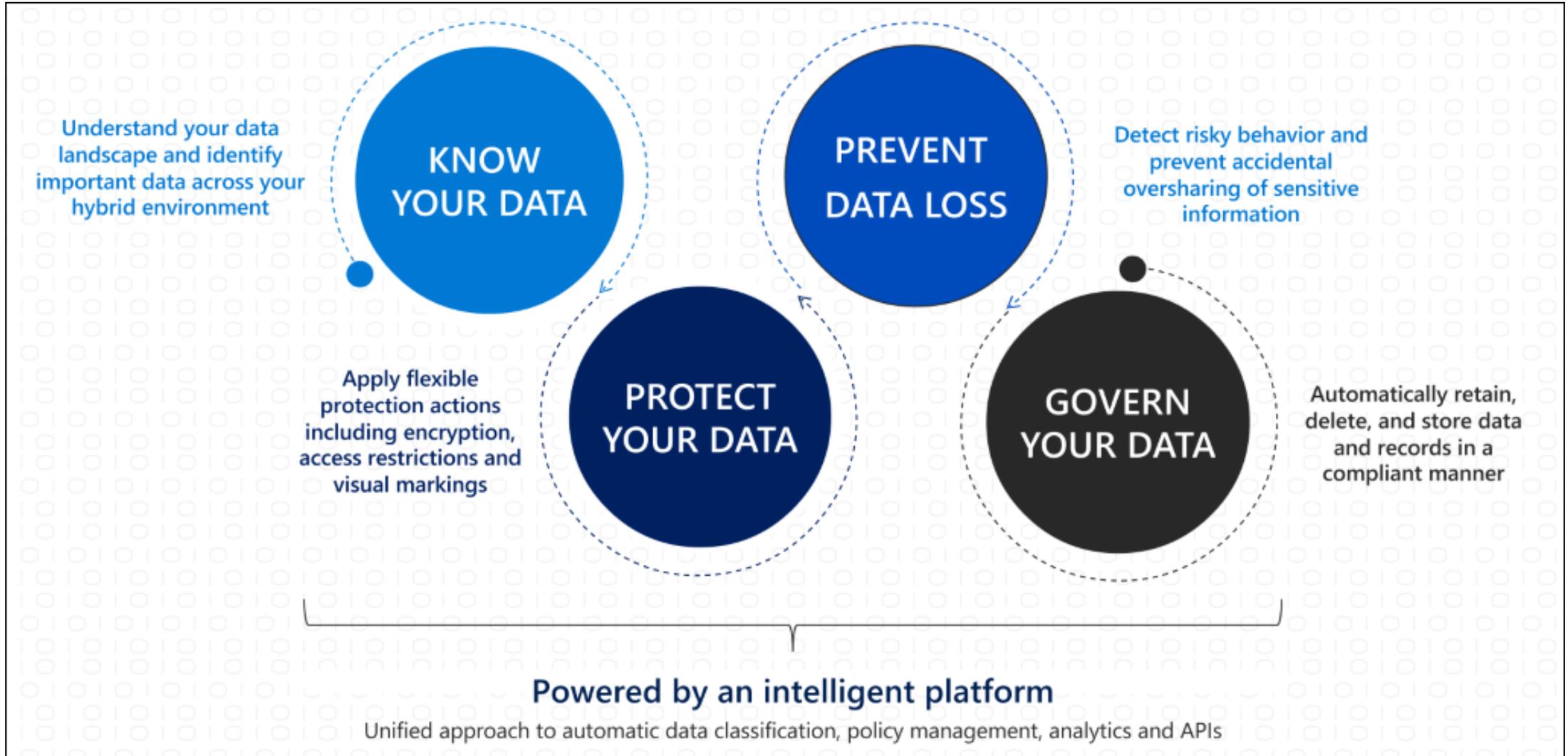
#GlobalAzure

Shared responsibility model

Responsibility	SaaS	PaaS	IaaS	On-Prem	
Information and data	Customer	Customer	Customer	Customer	RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER
Devices (Mobile and PCs)	Customer	Customer	Customer	Customer	
Accounts and identities	Customer	Customer	Customer	Customer	
Identity and directory infrastructure	Microsoft	Microsoft	Customer	Customer	RESPONSIBILITY VARIES BY SERVICE TYPE
Applications	Microsoft	Microsoft	Customer	Customer	
Network controls	Microsoft	Microsoft	Customer	Customer	
Operating system	Microsoft	Microsoft	Customer	Customer	RESPONSIBILITY TRANSFERS TO CLOUD PROVIDERS
Physical hosts	Microsoft	Microsoft	Microsoft	Customer	
Physical network	Microsoft	Microsoft	Microsoft	Customer	
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer	

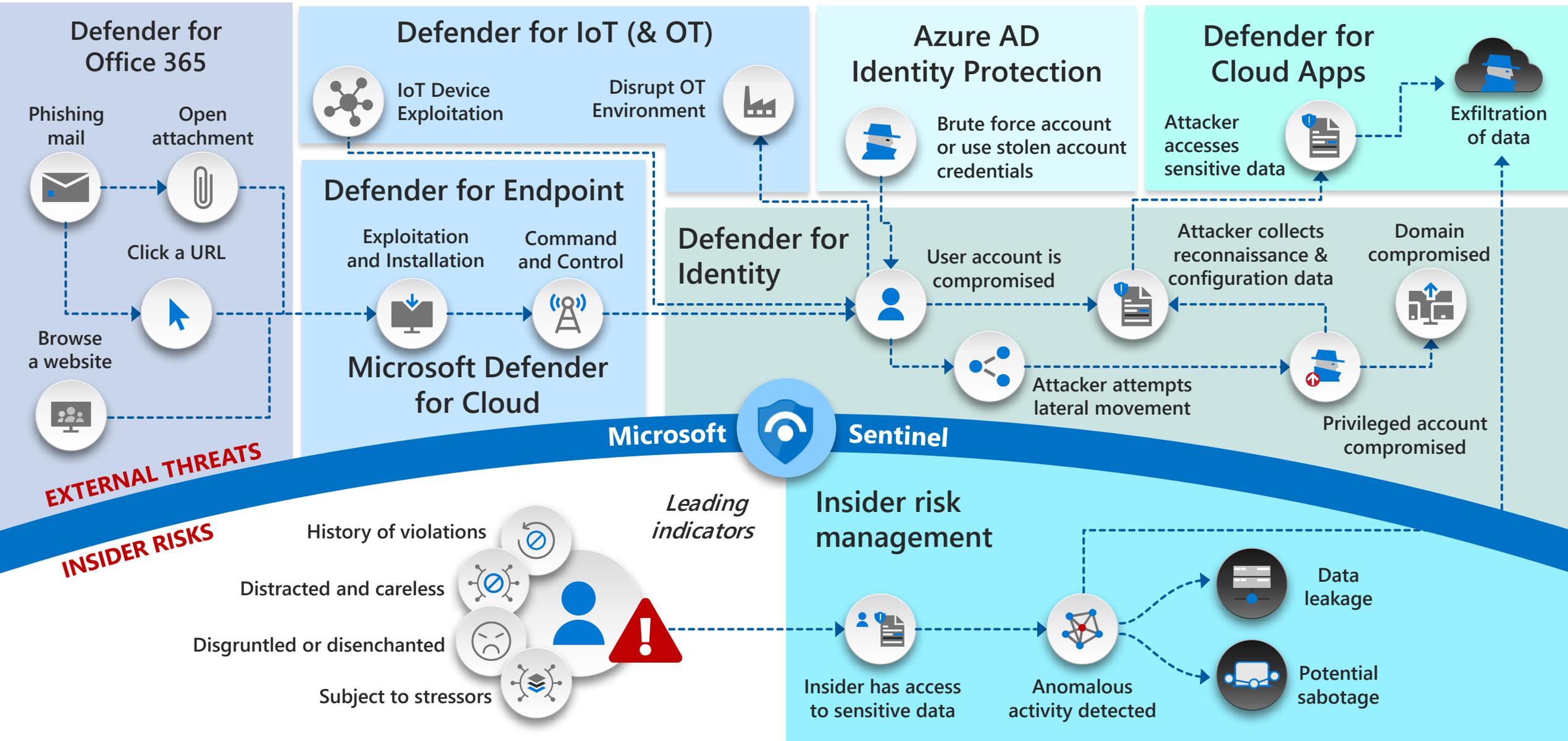
Microsoft
 Customer

Data Protection and Compliance



Defend across attack chains

Insider and external threats



Security Operations

Microsoft Reference Architecture

Legend

- Event Log Based Monitoring
- Investigation & Proactive Hunting

- Outsourcing
- Consulting and Escalation
- Native Resource Monitoring

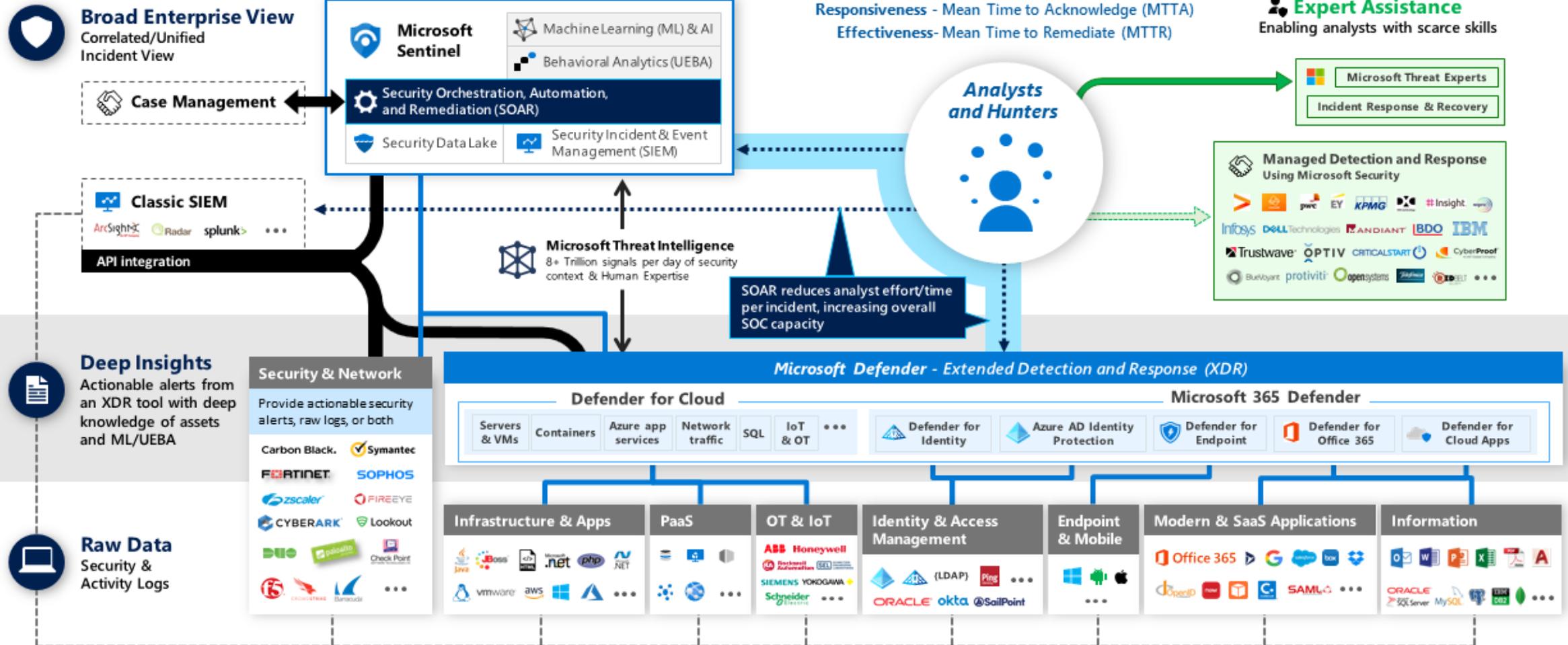


December 2021 – <https://aka.ms/MCRA>

Align to Mission + Continuously Improve

Responsiveness - Mean Time to Acknowledge (MTTA)
Effectiveness - Mean Time to Remediate (MTTR)

Expert Assistance
Enabling analysts with scarce skills

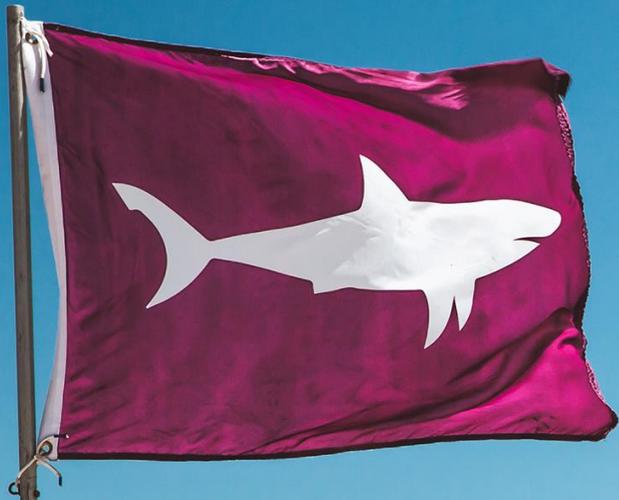


#GlobalAzureAthens

The idea



#GlobalAzure



Migrating? Step by step? Ok let's attack each step



Why?

Verify Explicitly

Use least Privileged access

Assume breach

An illustration of a hand holding a smartphone. The phone's screen is dark blue and displays the words "ZERO TRUST" in white, bold, uppercase letters. The hand is rendered in a light brown color. The background features a dark blue hexagonal grid pattern with several padlock icons scattered throughout, symbolizing security and trust.

**ZERO
TRUST**

Migration – Digital Transformation

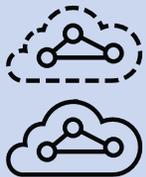
- Office 365
- Azure AD registered
- Network flows towards Azure
- Check Azure Access
- RBAC not configured properly
 - Followed the on-premise access rights
- Portal access
- Azure PowerShell



PowerZure



PowerZure is a PowerShell project created to assess and exploit resources within Microsoft Azure. PowerZure was created out of the need for a framework that can both perform reconnaissance and exploitation of Azure, AzureAD, and the associated resources.



We imported PowerZure in Azure PowerShell.

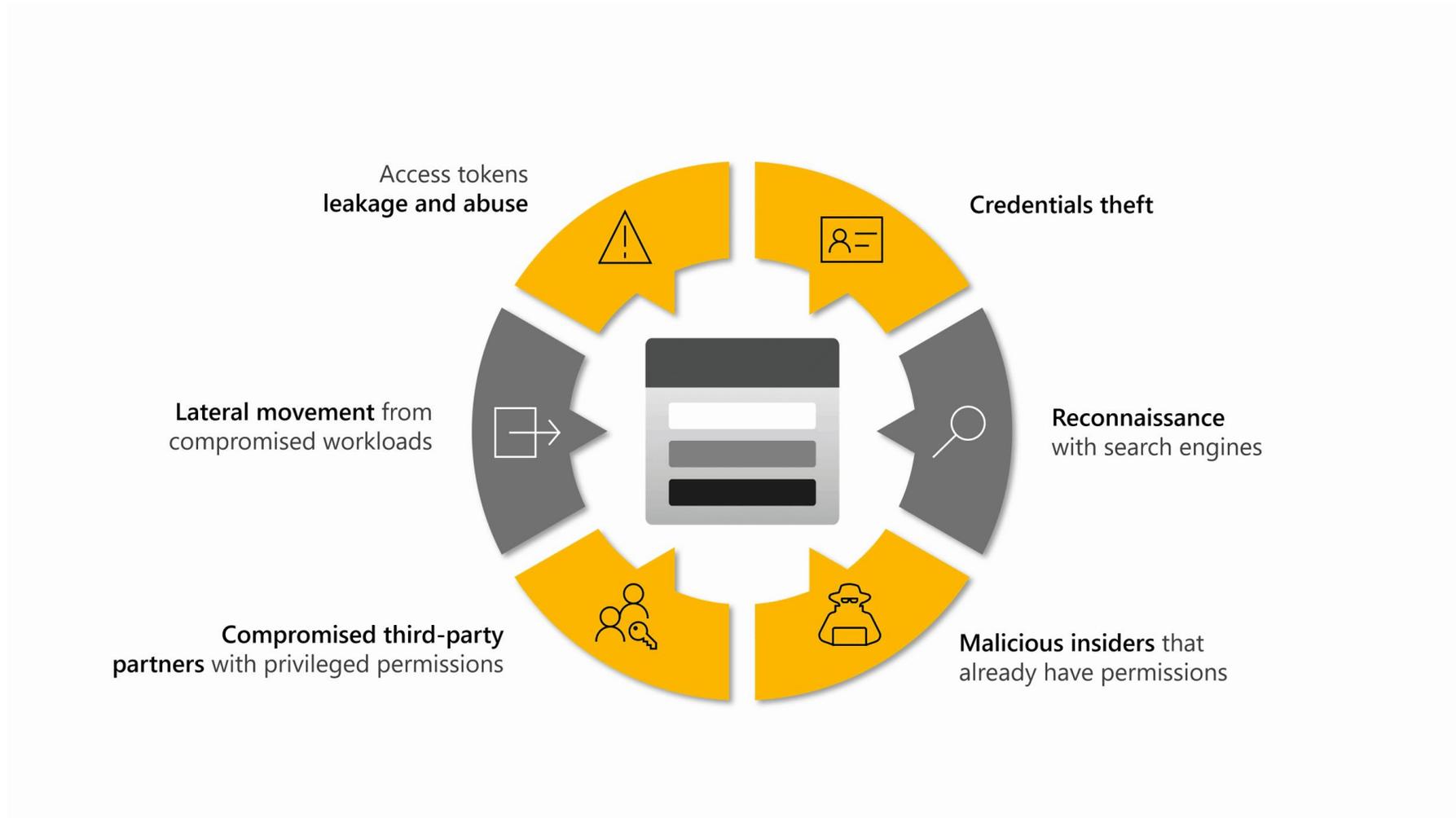


Attack on Hybrid

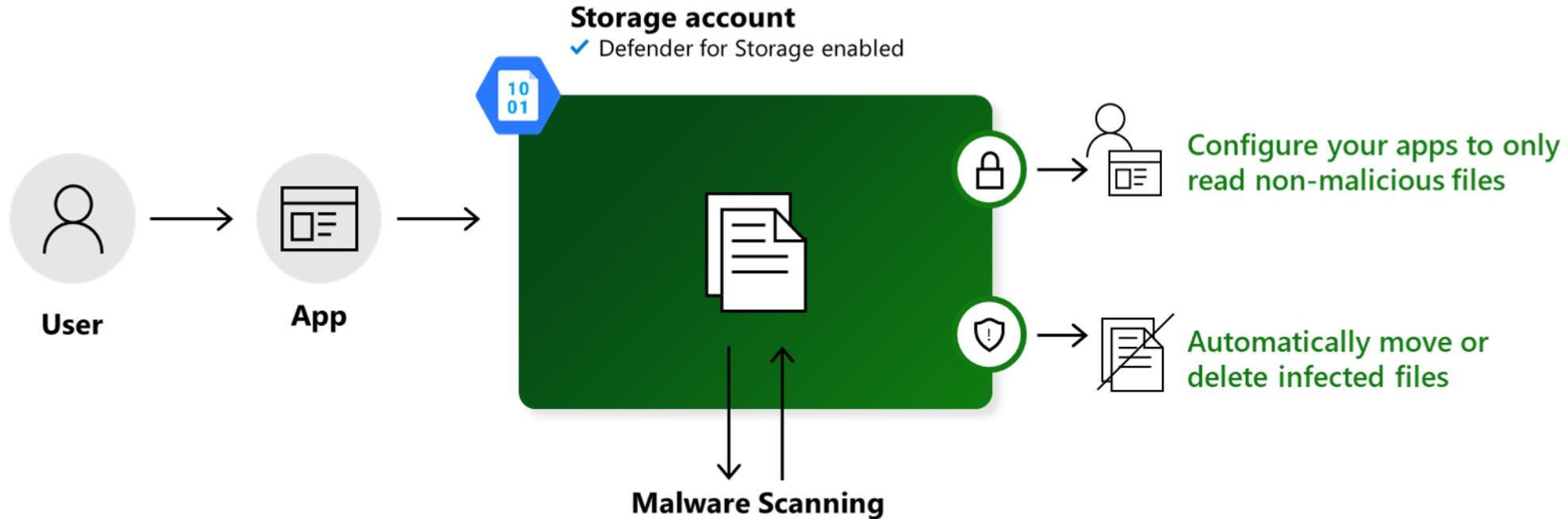
- Azure AD Connect
- Manipulate Admin Groups
- Azure AD Sync
- Access to Azure Resources
- Manipulate Azure RBAC
 - Give access to uncommon Admin accounts



Azure Storage – Defender for Storage



Malware scanning for Defender for Storage



Simple **agentless setup**, at scale enablement

Near real-time malware scanning across all file types

Metamorphic and polymorphic malware detection

Faster response with automatic workflows and SIEM integration



Persistence

Security First



Consult a Security Architect in each step of the migration



Audit each step



Identify new risks



Always assume breach



Don't follow the "On Premise" way of doing things



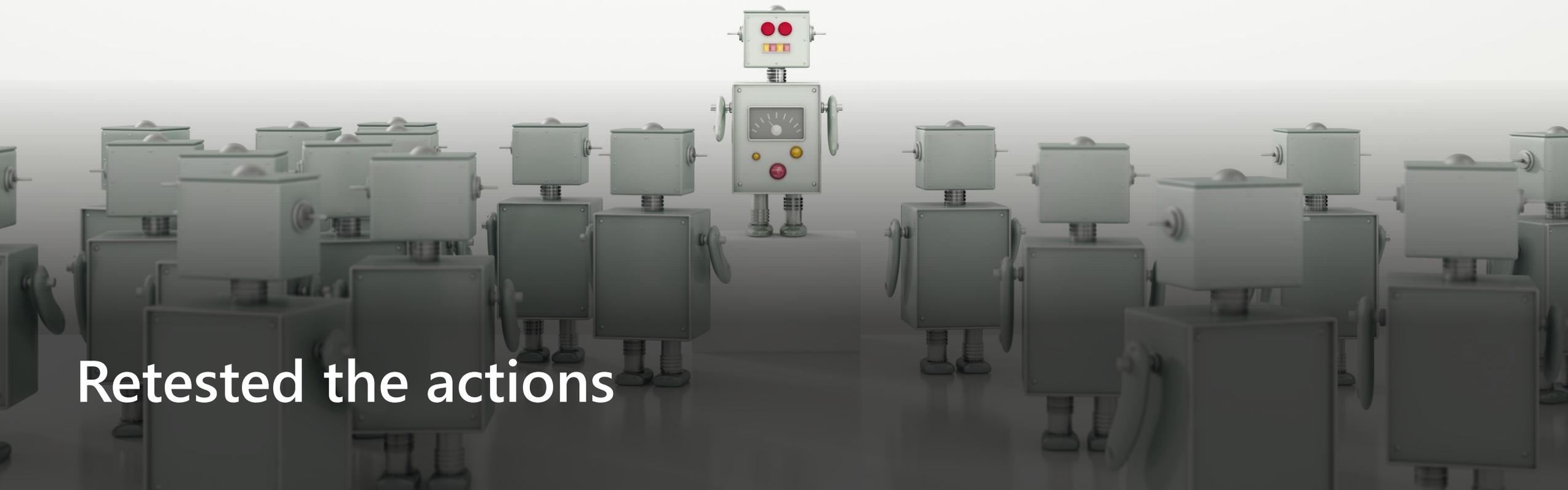
Digital Transformation goes along Security First

Actions

- Enabled Defender for Cloud
- Defender for Storage
- Privilege Identity Management
- Access Rights
- Reviewed RBAC
- Setup SENTINEL

Note: AI, Machine Learning, Behavioral Analysis

Retested the actions



Common Attacks & Common Azure Defense features

Identity attacks

- Brute Force
- MFA
 - <https://github.com/fin3ss3g0d/evilgophish>
- Location
- ENTR





https://localhost:3333

- Import bookmarks...
- Getting Started
- Getting Started
- Homepage
- Forum
- Wiki
- UptimeRobot
- Kali Linux
- Kali Training
- K



Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User Management **Admin**

Webhooks **Admin**

User Guide

Dashboard

No campaigns created yet. Let's create one!



☰ README.md



evilginx.

Evilginx 3.0

Evilginx is a man-in-the-middle attack framework used for phishing login credentials along with session cookies, which in turn allows to bypass 2-factor authentication protection.

This tool is a successor to [Evilginx](#), released in 2017, which used a custom version of nginx HTTP server to provide man-in-the-middle functionality to act as a proxy between a browser and phished website. Present version is fully written in GO as a standalone application, which implements its own HTTP and DNS server, making it extremely easy to set up and use.



☰ README.md

evilgophish

Combination of [evilginx2](#) and [GoPhish](#).

Credits

Before I begin, I would like to say that I am in no way bashing [Kuba Gretzky](#) and his work. I thank him personally for releasing [evilginx2](#) to the public. In fact, without his work this work would not exist. I must also thank [Jordan Wright](#) for developing/maintaining the incredible [GoPhish](#) toolkit.

Prerequisites

You should have a fundamental understanding of how to use `GoPhish`, `evilginx2`, and `Apache2`.

Disclaimer

I shall not be responsible or liable for any misuse or illegitimate use of this software. This software is only to be used in authorized penetration testing or red team engagements where the operator(s) has(ve) been given explicit written permission to carry out social engineering.



← ↻ 🏠 https://portal.azure.com/#view/Microsoft_Azure_PIMCommon/CommonMenuBlade/~~/quickStart 📄 🗂️ ⌕ ⚙️ ⚠️ 3 ⚙️ ? 🗨️

Web Slice Gallery 📄 Suggested Sites 🌐 Ξεκινώντας 📄 Getting Started 📄 Kali Linux 🗺️ Kali Training 🗡️ Kali Tools 📄 Kali Docs 🗺️ Kali Forums 📄 Ne

Microsoft Azure 🔍 Search resources, services, and docs (G+)

Home > **Privileged Identity Management | Quick start** ⚙️ ...

Privileged Identity Management

📄 Quick start

Tasks

- 👤 My roles
- 📄 My requests
- 📄 Approve requests
- 👤 Review access

Manage

- 🔹 Azure AD roles
- 👤 Groups (Preview)
- 🌿 Azure resources

Activity

- 📄 My audit history

Troubleshooting + Support

- ✂️ Troubleshoot

What's new Get started

Manage your privileged accounts

Use Privileged Identity Management to manage the lifecycle of role assignments, time access policy, and discover who has what roles. [Learn](#)

Manage access
Users with excessive access are vulnerable in the

Activate just in time
Reduce the potential for



- Home
- Favorites
- Azure Active Directory
- Permissions Management
- Verified ID



Microsoft Entra admin center

Secure your entire identity infrastructure with identity management and beyond. Protect your decentralized identity, identity protection, governance and more in a multi-cloud environment.

[Learn more](#)



Azure Active Directory

Secure and manage identities to connect them with apps, devices and data.

[Go to Azure Active Directory](#)



Permissions Management

Discover, remediate, and monitor permission risks for any i or resource.

[Go to Permissions Management](#)



Showing 73 subscriptions

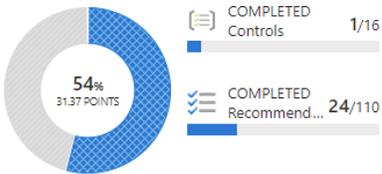
[Subscriptions](#) [What's new](#)

73 Azure subscriptions	4 AWS accounts	4 GCP projects	5984 Assessed resources	209 Active recommendations	7336 Security alerts
----------------------------------	--------------------------	--------------------------	-----------------------------------	--------------------------------------	--------------------------------

Secure score

Unhealthy resources
4101 To harden these resources and improve your score, follow the security recommendations

Current secure score

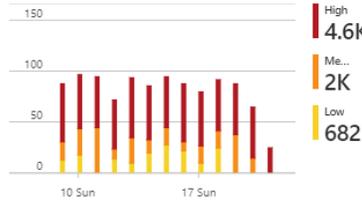


[Improve your secure score >](#)

Workload protections

Resource coverage
98% For full protection, enable 11 resource plans

Alerts by severity



[Enhance your threat protection capabilities >](#)

Regulatory compliance

Azure Security Benchmark New
1 of 40 passed controls

Lowest compliance regulatory standards by passed controls

CMMC Level 3	0/55
NIST SP 800 53 R5	2/55
ISO 27001	1/20

[Improve your compliance >](#)

Insights

Most prevalent recommendations (by resources)

Audit diagnostic setting	1025
Append a tag and its value to resou...	549
Storage account should use a privat...	447
Storage accounts should restrict net...	446

New security alerts

145 new alerts were detected by Defender for Cloud in the last 48 hours.

View full alerts list >	5
Microsoft Defender for SQL on machine...	7

Controls with the highest potential increase

Remediate vulnerabilities	+10% (6pt)
Remediate security configurations	+6% (4pt)
Enable MFA	+6% (10pt)

[View controls >](#)

Firewall Manager

5 Firewalls	3 Firewall policies	4 Regions with firewalls
-----------------------	-------------------------------	------------------------------------

Network protection status by resource

Virtual hubs	0/0
Virtual networks	8/249

[Improve your network security >](#)

Inventory

Unmonitored VMs
134 To better protect your organization, we recommend installing agents

Total Resources
5984

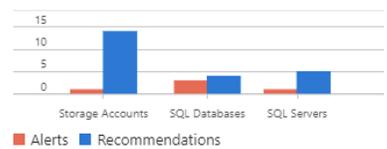


[Explore your resources >](#)

Information protection Preview

Resource scan coverage
1% For full coverage [scan](#) additional resources

Recommendations & Alerts by classified resources



[View classified resources in inventory >](#)



Data (M365)

← ↻ 🏠 <https://compliance.microsoft.com/dataclassificationclassifiers?viewid=classifiers> 🔍 ⭐

🔗 Web Slice Gallery 📄 Suggested Sites 🌐 Ξεκινώντας 📄 Getting Started 📄 Kali Linux 🗑️ Kali Training 🗑️ Kali Tools 📄 Kali Docs 🗑️ Kali Forums 📄

☰ Microsoft Purview

- ☰
- 🏠 Home
- 🕒 Compliance Manager
- 🔗 Data classification ^
 - Overview
 - Classifiers**
 - Content explorer
 - Activity explorer
- 🔗 Data connectors
- ⚠️ Alerts
- 📊 Reports
- 🔧 Policies
- 🔍 Roles & scopes v
- 🎁 Trials

Solutions

Classifiers

Trainable classifiers Sensitive info types EDM classifiers

Use built-in or custom classifiers to identify specific categories of content based on existing items in your organization. These classifiers can be used in several compliance solutions to detect related content and classify it, protect it, or remove it. [Learn more](#)

i To set you up for creating trainable classifiers, we're currently scanning your content locations to generate analytics that show the amount of content in your organization. This process will take 7 to 14 days to complete. [Learn about trainable classifiers](#)

+ Create trainable classifier 🔄 Refresh

Filters: Language: Any ▾ Type: Any ▾ Name: Any ▾ Status: Any ▾ 🔍 Filters

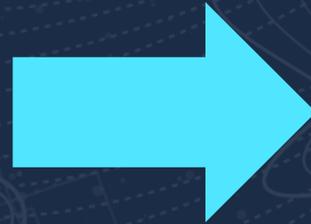
	Name	Accuracy	Status	Type
▾	Published (93)			
<input type="checkbox"/>	Agreements	🔗 -	Ready to use	Built-In
<input type="checkbox"/>	Bank statement	🔗 -	Ready to use	Built-In
<input type="checkbox"/>	Budget	🔗	Ready to use	Built-In



VMs

· Attacks

Brute Force
Port Scanning



· Services

JIT
NSG
Defender

Showing 73 subscriptions

Subscriptions What's new

73 Azure subscriptions

4 AWS accounts

4 GCP projects

5984 Assessed resources

209 Active recommendations

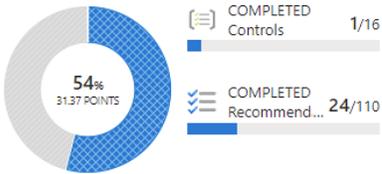
7336 Security alerts

Secure score

Unhealthy resources

4101 To harden these resources and improve your score, follow the security recommendations

Current secure score



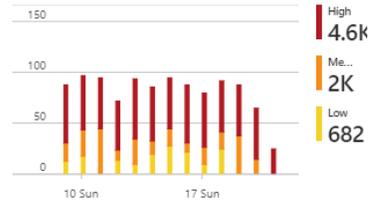
Improve your secure score >

Workload protections

Resource coverage

98% For full protection, enable 11 resource plans

Alerts by severity



Enhance your threat protection capabilities >

Regulatory compliance

Azure Security Benchmark

1 of 40 passed controls

Lowest compliance regulatory standards by passed controls



Improve your compliance >

Insights

Most prevalent recommendations (by resources)

Audit diagnostic setting	1025
Append a tag and its value to resou...	549
Storage account should use a privat...	447
Storage accounts should restrict net...	446

New security alerts

145 new alerts were detected by Defender for Cloud in the last 48 hours.

- View full alerts list > 5
- Microsoft Defender for SQL on machine... 7

Controls with the highest potential increase

- Remediate vulnerabilities +10% (6pt)
- Remediate security configurations +6% (4pt)
- Enable MFA +6% (10pt)

View controls >

Firewall Manager

5 Firewalls, 3 Firewall policies, 4 Regions with firewalls

Network protection status by resource



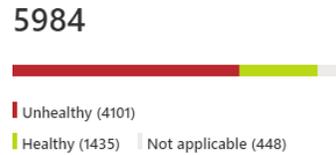
Improve your network security >

Inventory

Unmonitored VMs

134 To better protect your organization, we recommend installing agents

Total Resources



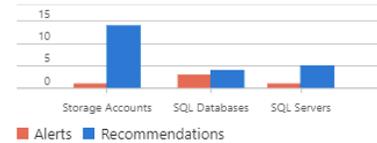
Explore your resources >

Information protection

Resource scan coverage

1% For full coverage scan additional resources

Recommendations & Alerts by classified resources



View classified resources in inventory >



Web Applications

- Attacks

Brute Force

DoS

SQL Injections



- Services

Front Door

Web Application

Gateway

WAF



Demo

<https://blackapp.azurewebsites.net/>

- Burpsuite attack
- Sqlmap attack

REPORT

Website Scanner (Light)

ASSET

<https://blackapp.azurewebsites.net/>

Scan summary

Overall risk level Medium	Scan status Finished	
Risk ratings	Start time 5/12/2023, 11:29:23 AM	Finish time 5/12/2023, 11:29:23 AM
High 0		
Medium 2		
Low 7	Scan duration 13 seconds	Tests performed 19/19
Info 10		



- ⏪
- 🏠 Home
- 📊 Dashboard
- ☰ All services
- ★ FAVORITES
- 🗂️ Resource groups
- 📄 All resources
- 🕒 Recent
- 🌐 App Services
- 🗄️ SQL databases
- 💻 Virtual machines
- ⚙️ Cloud services (classic)
- 🔑 Subscriptions
- 📦 Azure Active Directory
- 🕒 Monitor
- 🛡️ Microsoft Defender for Cloud

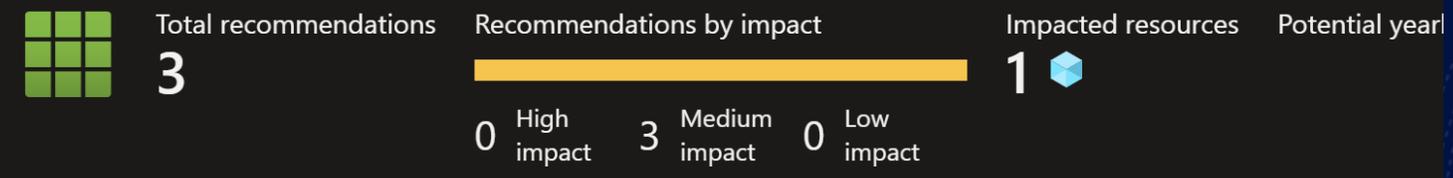
Home >

Advisor recommendations

🗨️ Feedback ⬇️ Download as CSV ⬇️ Download as PDF ⚙️ Configure

Overview 📄 Cost (0) 🛡️ Security (3) 🌐 Reliability (0) 🏆 Operational excellence (0) 📈

📄 All (3)



Impact ↑↓	Description ↑↓	Category ↑↓	Potential benefits ↑↓
Medium	Web apps should request an SSL certificate for all incoming requests	Security	
Medium	Managed identity should be used in web apps	Security	
Medium	Diagnostic logs in App Service should be enabled	Security	



SOC

- Sentinel
- Defender for Cloud
- Microsoft 365 Defender



#GlobalAzureAthens

Thank you 😊



#GlobalAzure



Please evaluate !



A big **thank you** to our sponsors!



Microsoft

InfoQuest
TECHNOLOGIES

Office line
envision . empower . evolve

CUBE

CANDI
ADVANCED BUSINESS AND DIGITAL SOLUTIONS

BlueStream
SOLUTIONS

INFOLAB
Enterprise Training

Code.Hub

SIGNAL

<https://bit.ly/GA23Evaluation>

#GlobalAzureAthens