Microsoft Security

James Graham, PHD

/drjamesgraham

Cloud Solution Architect

CALLING ALL HUNTERS!

Microsoft Defender Masterclass II

17TH MARCH 2021
9AM-1PM GMT

Agenda

9:10 - *Opening Keynote*
9:35 -*Advanced Threat Hunting*
10:30 - *Break I*
10:40 - *Live Response*
11:40 - *Break II*
11:50 - *Power Virtual Agent Lab*
12:55 - *Closing*
13:00 - *End*

Meet the team

Mark Thomas

James Graham

Ally Turnbull

Jack Lewis

Becky Cholerton

Steve Newby

Christos Ventouris

Jaime Lloyd

Rules and Housekeeping

- *Please be patient when asking questions*
- *If it's important, we will post it in the announcements*
- *For lab prerequisites and resources visit aka.ms/defendermasterclass-repo*
- *Feedback – aka.ms/defendermasterclass-feedback*
- *This event is being recorded – further recordings available at aka.ms/defendermasterclass-recordings*
- *Slides will be made available at the repo*

Outcomes

- *Be more proficient at investigating and responding to alerts /incidents using MDE*
- *Learn skills to aid in security solution build and competency attainment*
  - *Security Competency*
  - *Threat Protection – Advanced Specialisation*
  - *SC-200: Microsoft Security Operations Analyst*
  - *SC-900: Microsoft Security, Compliance, and Identity Fundamentals*
- *Understand ways to add efficiencies and automation, by leveraging the Power Platform to integrate MDE with Teams using Power Virtual Agent and Power Automate*

Microsoft Partner Network Program – Security

Security Competency

Advanced Specializations

Silver Status

Individual Certification Requirements
1 Individual in MS-500 (M365 Security Administration)
OR
AZ-500 (Azure Security Technologies)

Demonstrated Customer Performance
1000 Active Users in M365 security workload
OR
US $500/month Security Azure customer consumption within previous 12 months

BENEFITS

Internal use rights for M365
Co-marketing MPN benefits

Gold Status

Individual Certification Requirements
4 individuals in MS-500 (M365 Security Admin)
AND
4 individuals in AZ-500 (Azure Security Technologies) (can also be same person)

Demonstrated Customer Performance
4000 Active Users in M365 security workload
OR
US $1000/month Azure Security customer consumption within previous 12 months

BENEFITS

Internal use rights for M365
Usage incentive eligibility
ECIF* & Customer matching prioritization
Co-marketing MPN benefits

- Threat Protection
- Identity & Access Management
- Information Protection & Governance

*Gold not a requirement for MW EFIC in FY21

Threat Protection advanced specialization

Partners who demonstrate deep knowledge, extensive experience, and proven success deploying Microsoft Threat Protection, Microsoft Cloud App Security, or Azure Sentinel workloads can differentiate their capabilities to customers with the Threat Protection advanced specialization.

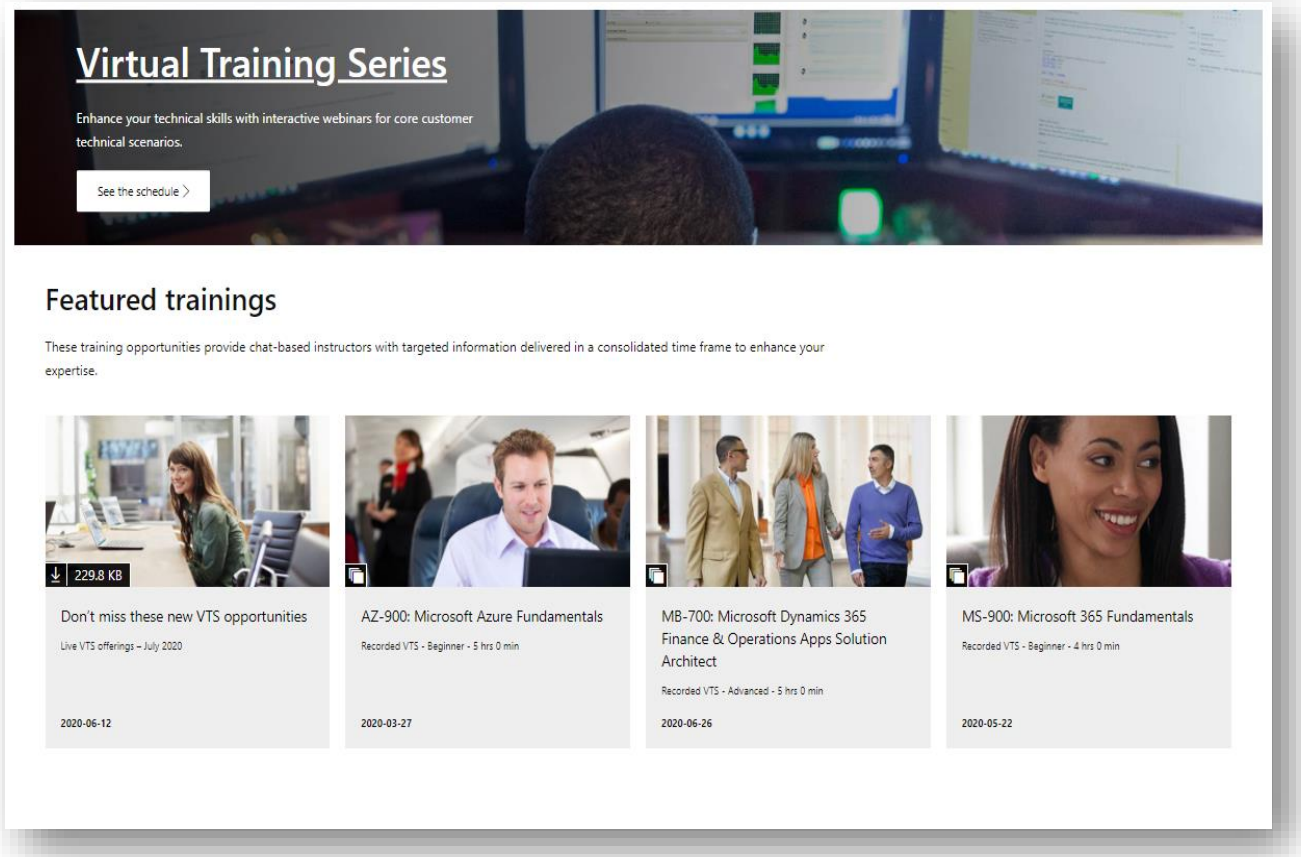
https://aka.ms/PartnerSpecializations

Requirements	Details
Related competency	Maintain an active Gold Security competency.
Performance	Achieve a minimum of 1,000 Monthly Active User (MAU) growth of Azure Advanced Threat Protection (A-ATP) or Microsoft Cloud App Security (MCAS) in a trailing 12-month period (CPOR data) **OR** Achieve a minimum of USD 100,000 in Azure Consumed Revenue (ACR) from Azure Sentinel in a trailing 12-month period (Digital Partner of Record, Partner Admin Link, and Cloud Solution Provider data).
Knowledge	Your organization must have at least six individuals who have passed the MS-500: Microsoft 365 Security Administrator exam.
Customer references	Provide three customer references that demonstrate your organization's ability to deploy Microsoft Threat Protection, Microsoft Cloud App Security, or Azure Sentinel workloads. Review our guidelines for customer references before submitting.
Annual renewal	Your advanced specialization and associated benefits will remain in place for one year but require that you keep your gold competency status in place. If you do not maintain your gold competency, you will lose your advanced specialization status. On your renewal date, you will need to meet the current program requirements which may evolve over time.

Corp Virtual Training Series (VTS)

Interactive, time-zone-friendly webinar series for Microsoft Partners designed to increase your knowledge of incubation and advanced technical scenarios across Microsoft's cloud solutions. These training opportunities offer chat-based instructors, with deep technical knowledge in a consolidated format and time frame.

- Focused on Microsoft core solution areas:
  - Azure
  - Modern Work and Security
  - Business Applications
- Flexible schedules and self-paced options
- Available to all Microsoft Partners

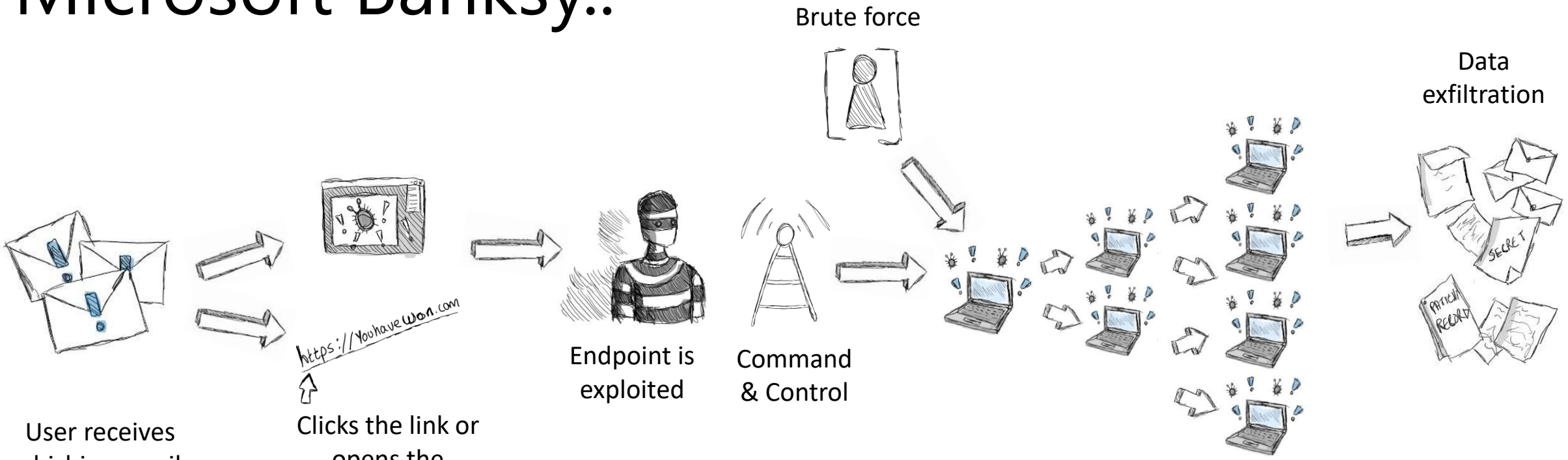


https://aka.ms/enablevts

Ninja Self paced training

- Azure Sentinel ninja training
- Microsoft Defender ATP ninja training
- Azure Security (ASC) ninja training

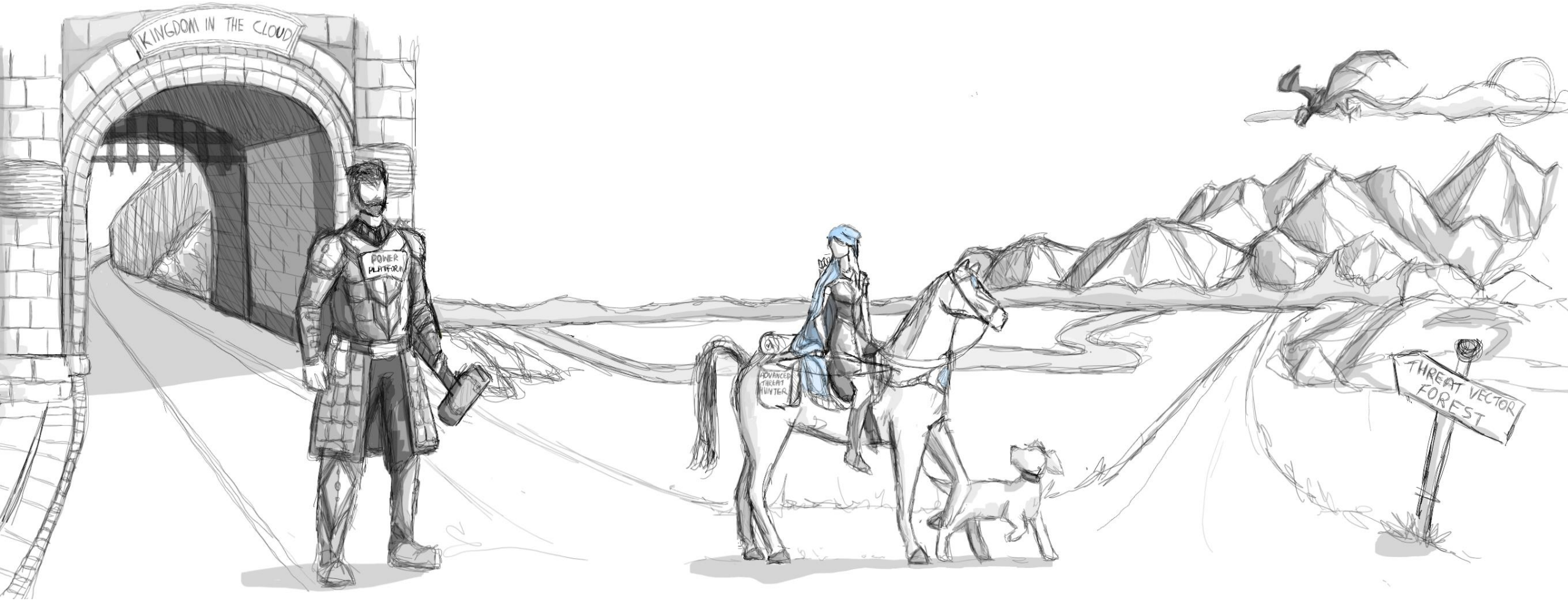
Revealing the Microsoft Banksy..



Microsoft Defender Masterclass II

Microsoft Defender for Endpoint

Endpoint Detection & Response



Navigating a shifting world

Conventional security tools have not kept pace

The nature of business and work have changed

Cost of breaches and regulations are increasing

COVID-19 brought unexpected IT challenges

- Rapidly enabling remote work while protecting corporate resources

Bad actors exploiting COVID-19 themes and VPN vulnerabilities

VPN scalability constraints

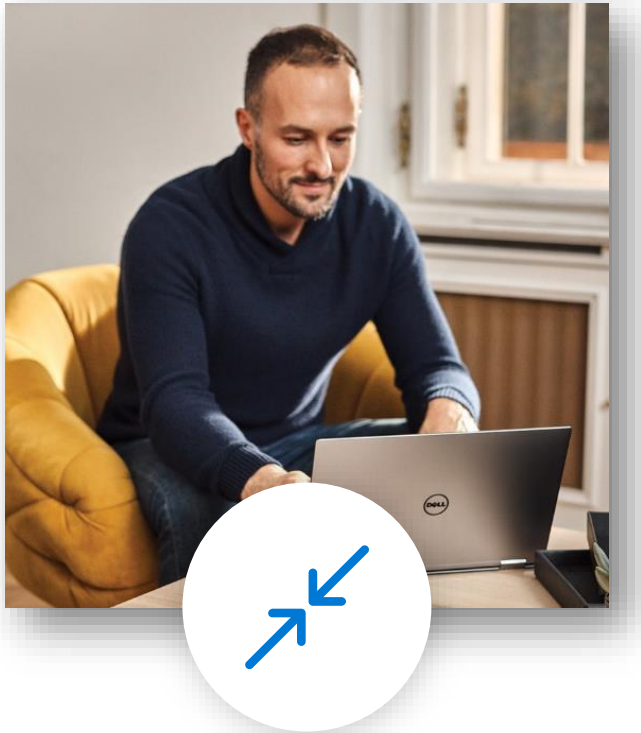
Challenges to onboarding and managing new and personal devices

Sudden spike in the need for remote access to apps

Difficulty rolling out new security controls

A new reality needs new principles

Verify explicitly

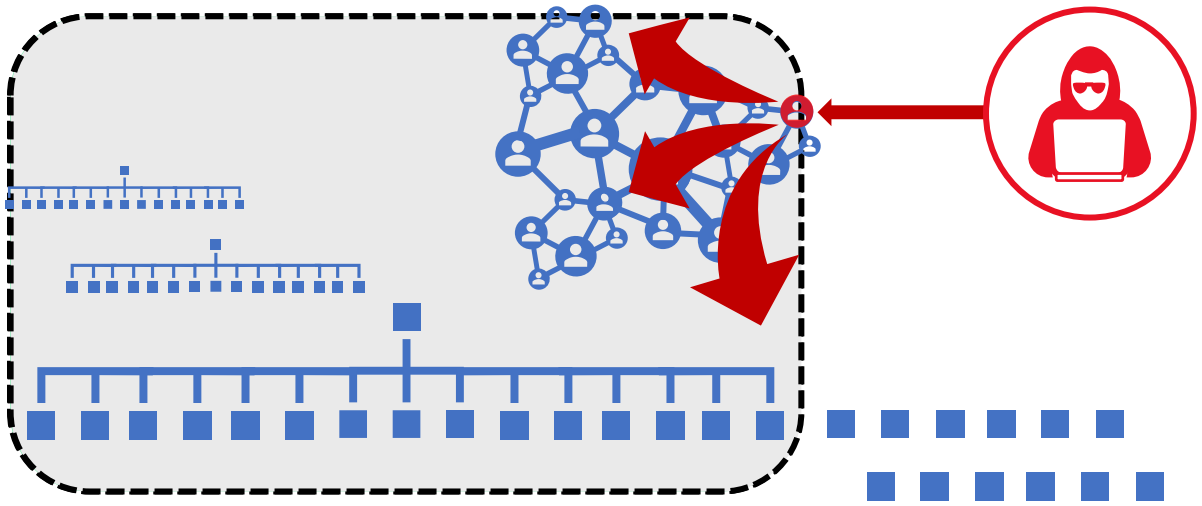


Use least privilege access

Assume compromise

Why are we having a Zero Trust conversation?

Access Control: Keep **Assets** away from **Attackers**

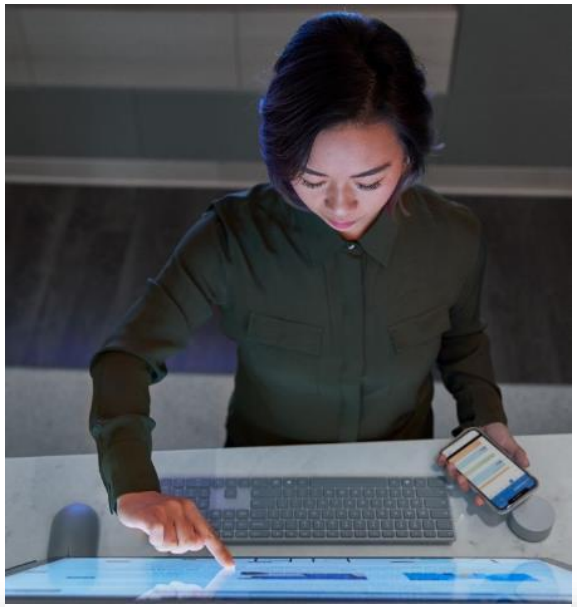


1. **IT Security is complex**
   - Many devices, users & connections
2. **"Trusted network" security strategy**
   - Initial attacks were network based
   - *Seemingly* simple and economical
   - Accepted lower security within the network
3. **Assets increasingly leave the network**
   - BYOD, WFH, Mobile, and SaaS
4. **Attackers shift to identity attacks**
   - Phishing and credential theft
   - Security teams often overwhelmed

Microsoft Security Pillars

Identity and access management

Secure access for a connected world



Threat protection

Stop attacks with integrated and automated SIEM and XDR

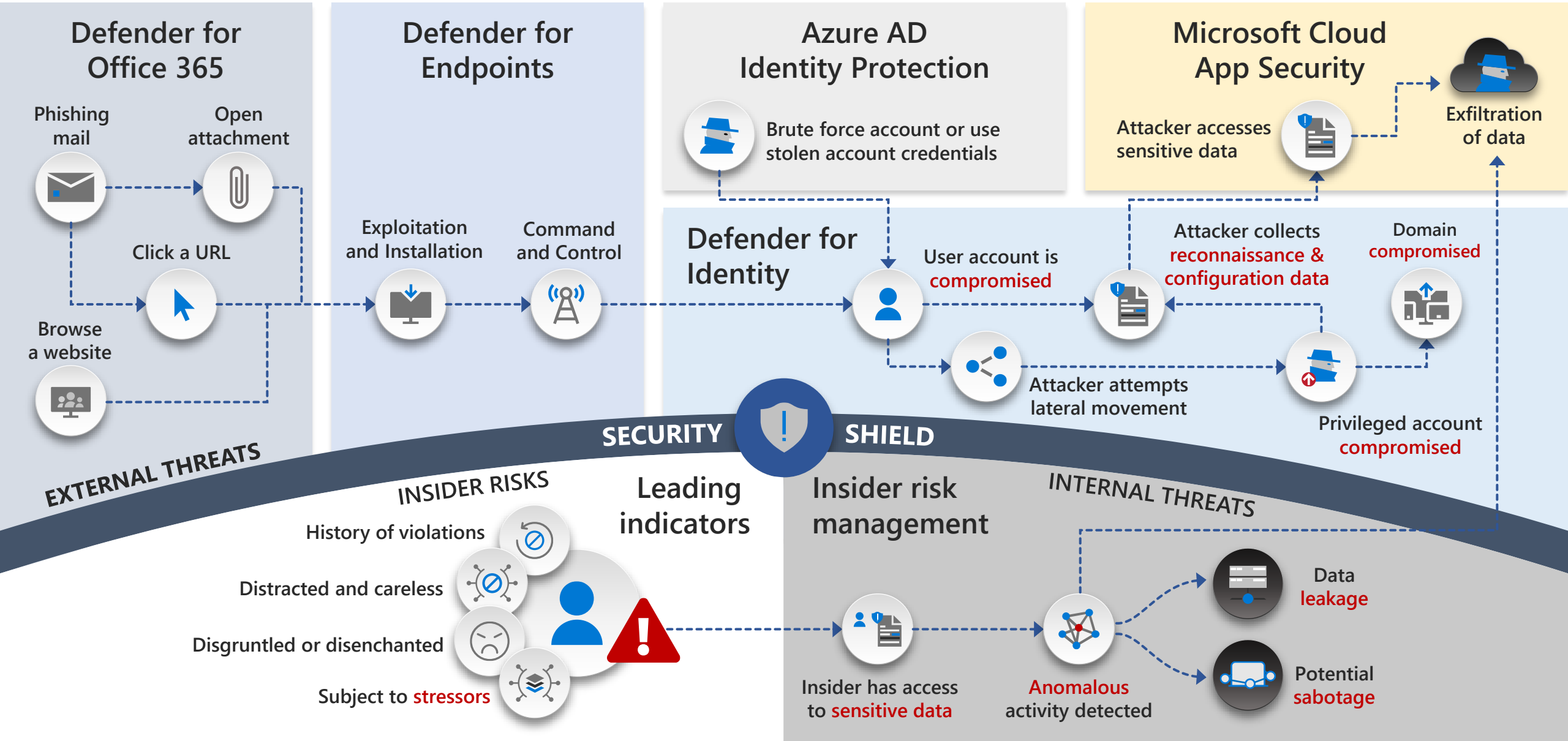
Information protection

Protect sensitive data and manage insider risks with intelligence

Cloud Security & Posture Management

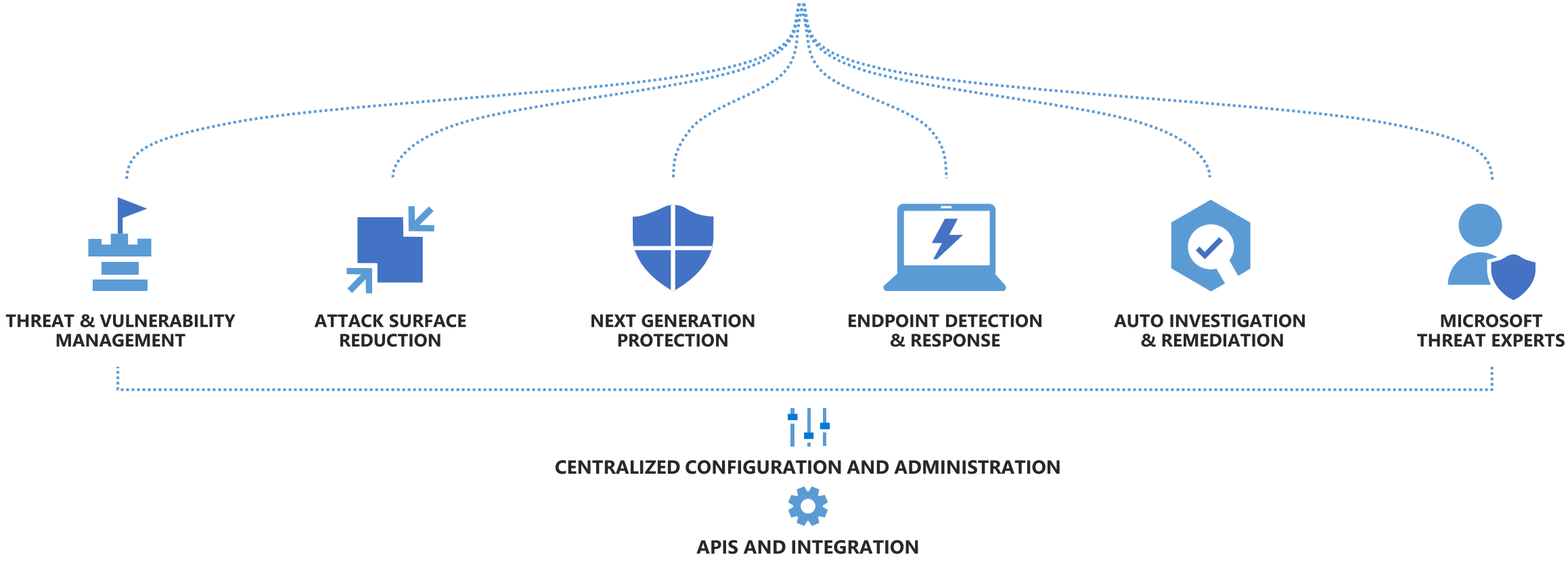
Safeguard your multi-cloud resources with insights and guidance

Internal and external protection across the threat kill chain



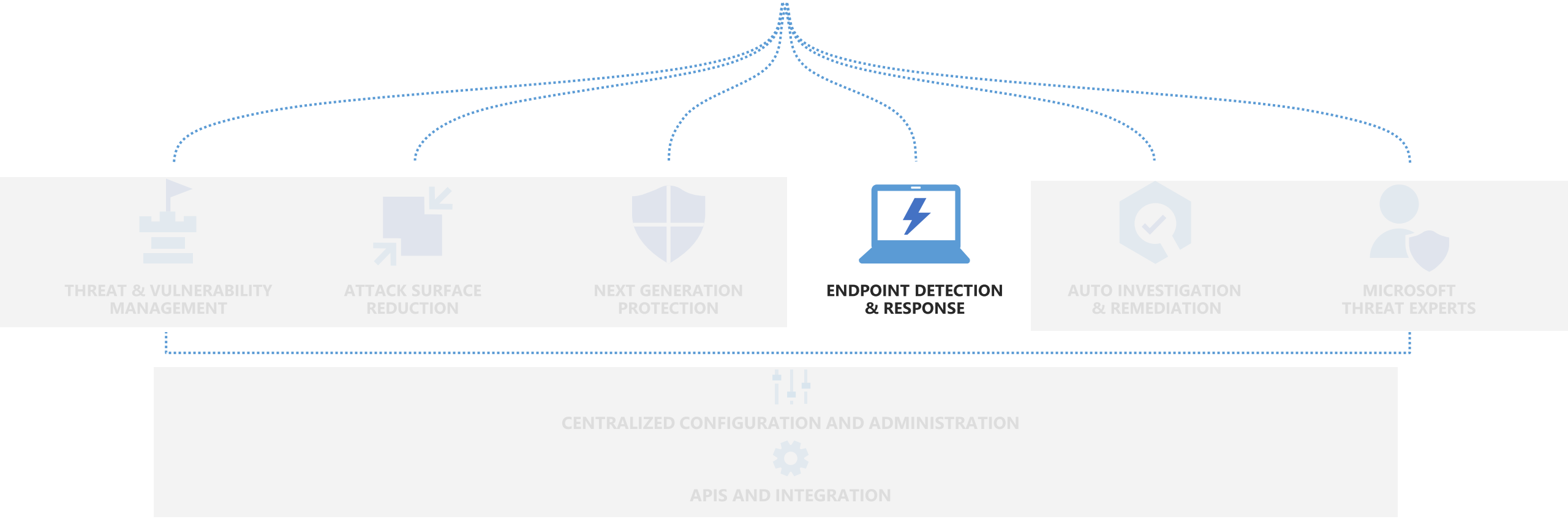
Microsoft Defender
for Endpoint

Built-in. Cloud-powered.



Microsoft Defender
for Endpoint

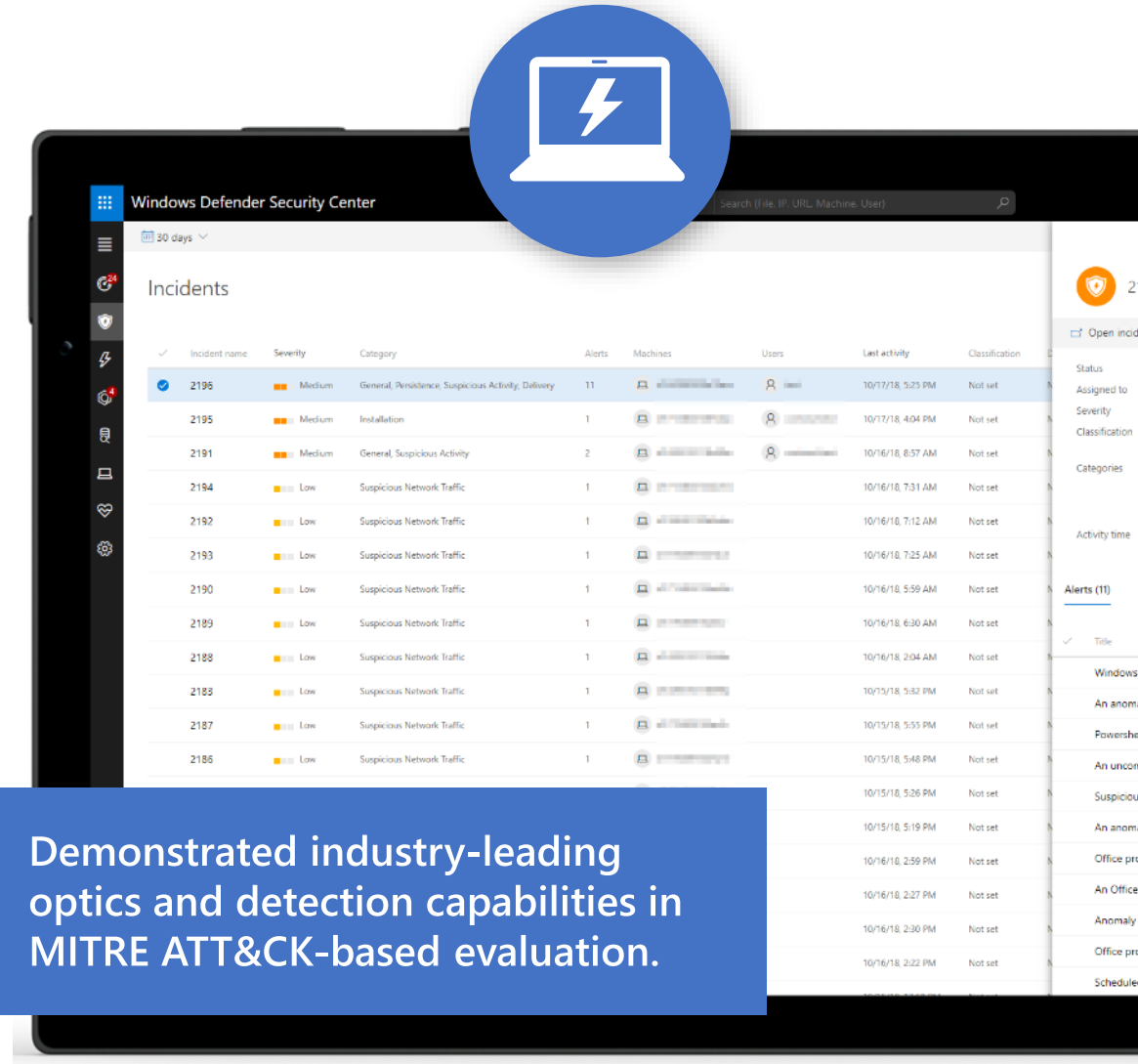
Built-in. Cloud-powered.



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.

Triage & Investigation

Understand what was alerted

Alert investigation experience provides detailed description, rich context, full process execution tree.

Investigate device activity

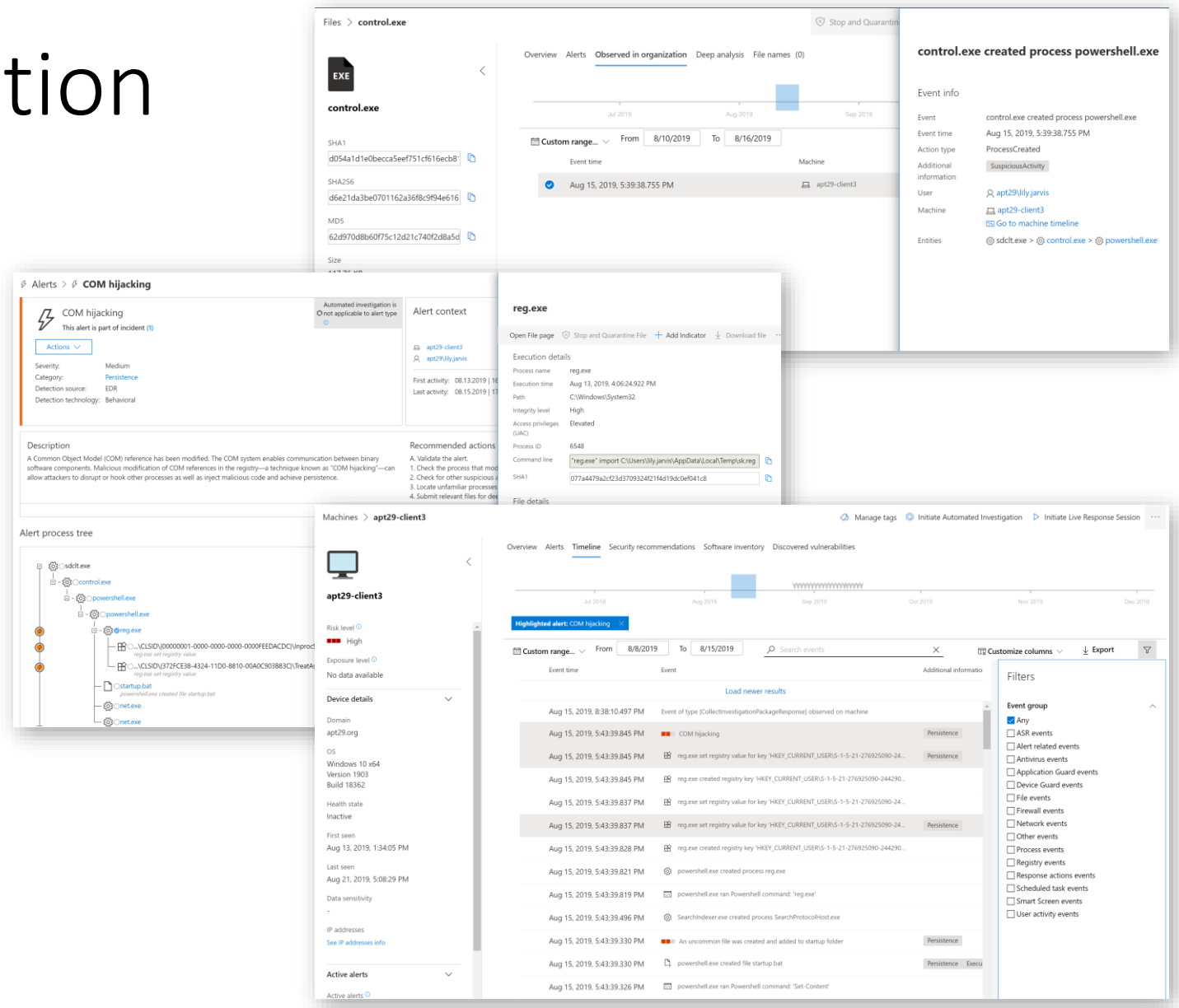
Full machine timeline to drill into activities, filter and search.

Rich supporting data & tools

Supporting profiles for files, IPs, URLs including org & world prevalence, deep analysis sandbox.

Expand scope of breach

In-context pivoting to other affected machines/users.



Incident

Narrates the end-to-end attack story

Reconstructing the story

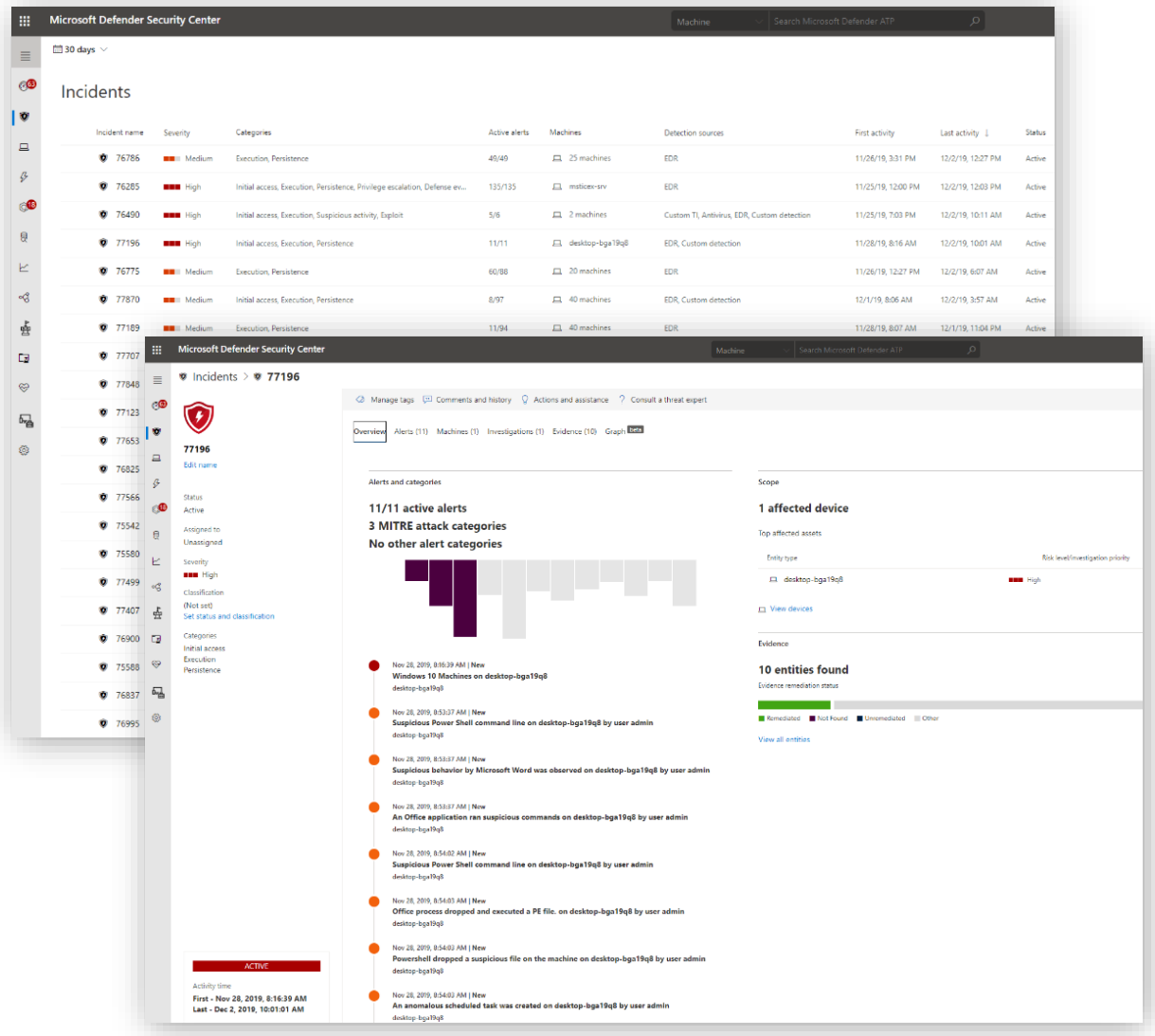
The broader attack story is better described when relevant alerts and related entities are brought together.

Incident scope

Analysts receive better perspective on the purview of complex threats containing multiple entities.

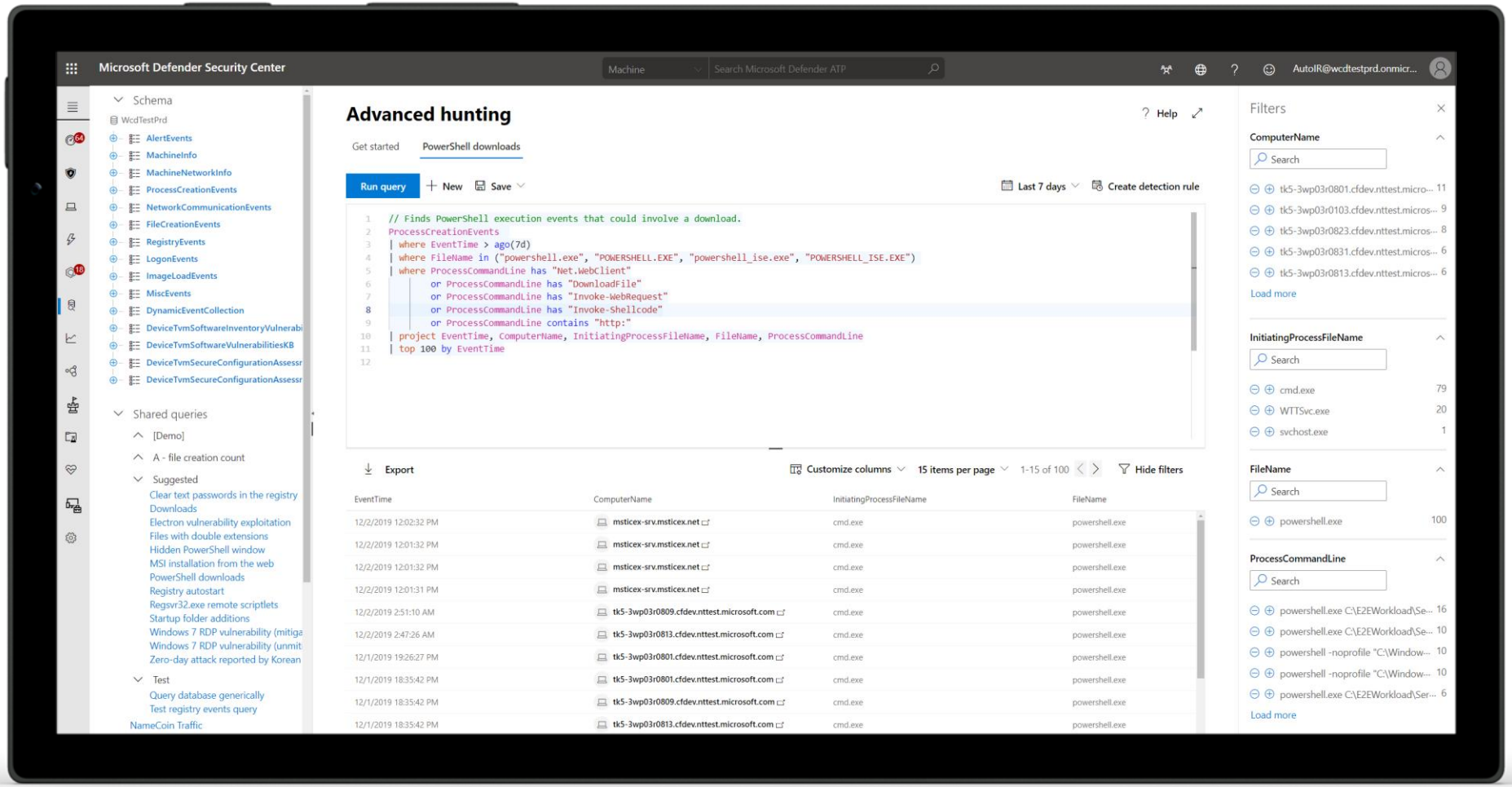
Higher fidelity, lower noise

Effectively reduces the load and effort required to investigate and respond to attacks.



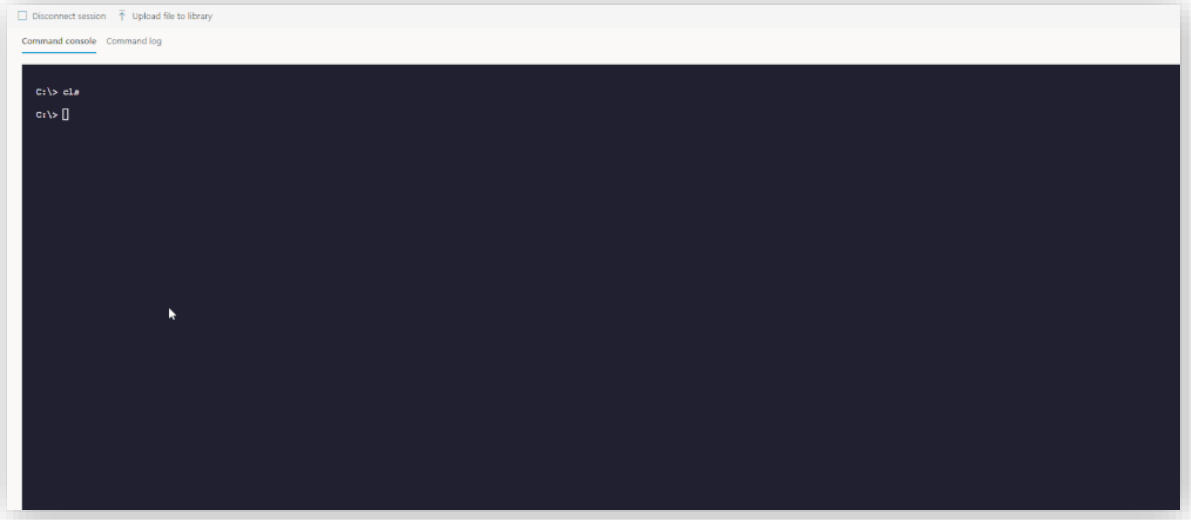
[Announcement blog]

Advanced hunting with custom detection and custom response



Live Response

- Real-time live connection to a remote system
- Leverage Microsoft Defender for Endpoint Auto IR library (memory dump, MFT analysis, raw filesystem access, etc.)
  - Extended remediation command + easy undo
- Full audit
- Extendable (write your own command, build your own tool)
- RBAC+ Permissions
- Git-Repo (share your tools)



Threat Analytics

See how you do against major threats

Threat to posture view

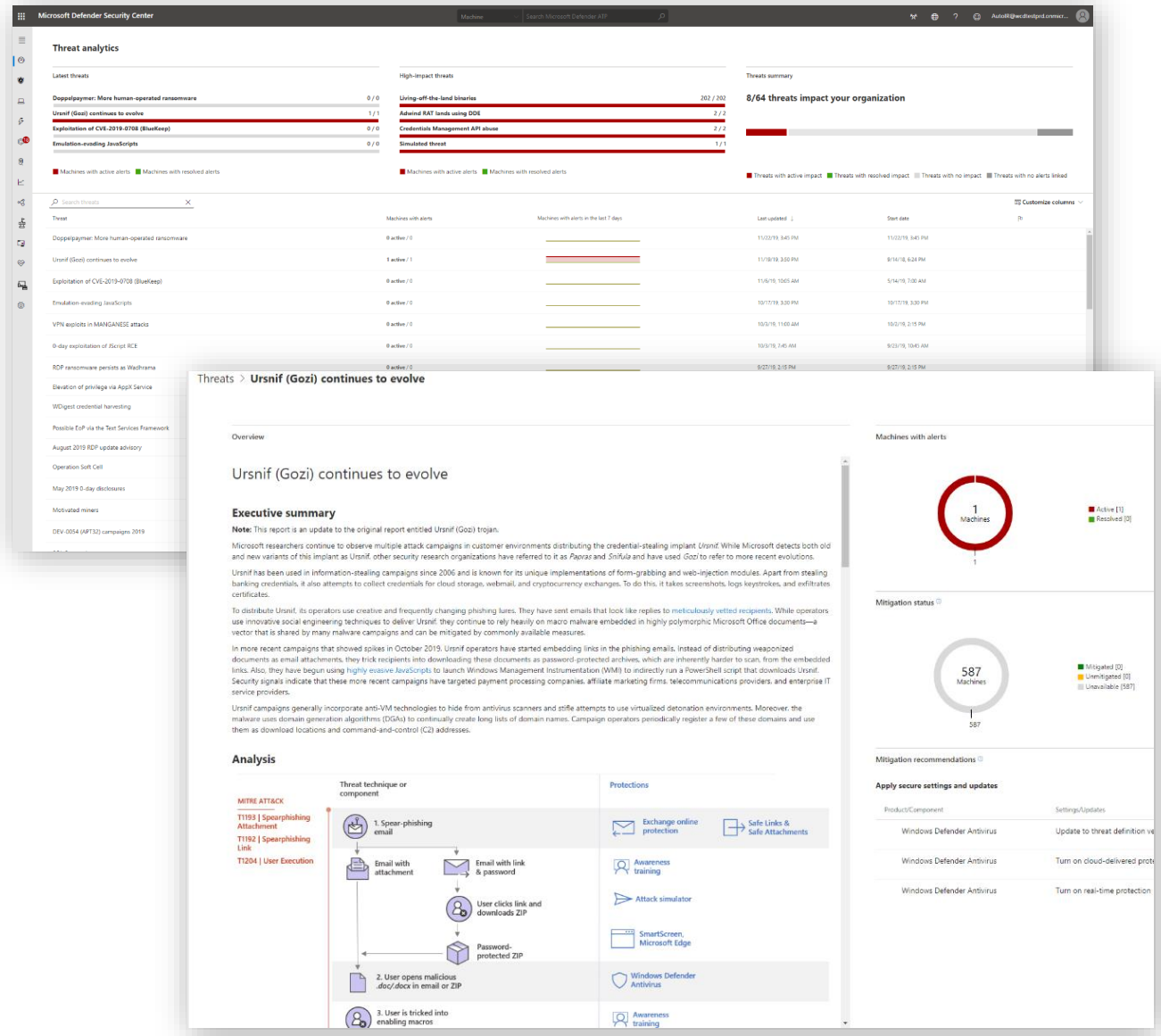
See how you score against significant and emerging campaigns with interactive reports.

Identify unprotected systems

Get real-time insights to assess the impact of the threat on your environment.

Get guidance

Provides recommended actions to increase security resilience, to prevention, or contain the threat.



Break

Lab Preparation

For the next exercise please use your own demo tenant.

Please head over to:

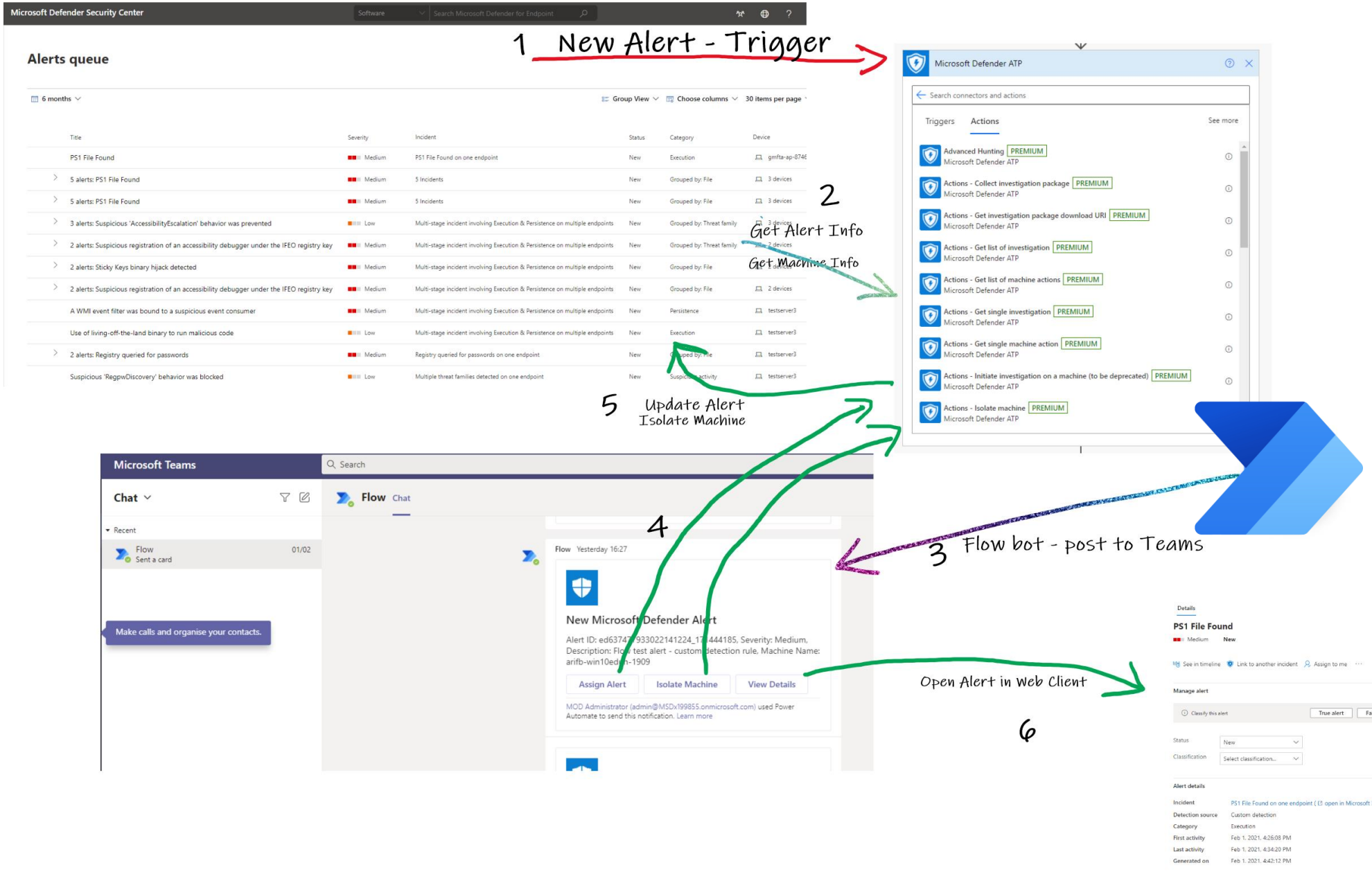
aka.ms/defendermasterclass-repo

You will need:

1. Defender Masterclass – Labs Getting Started
2. Defender Masterclass 2 - Multitenant Teams Bot Microsoft Defender Integration Lab
3. Defender Masterclass 2 - Customer Tenant Credentials

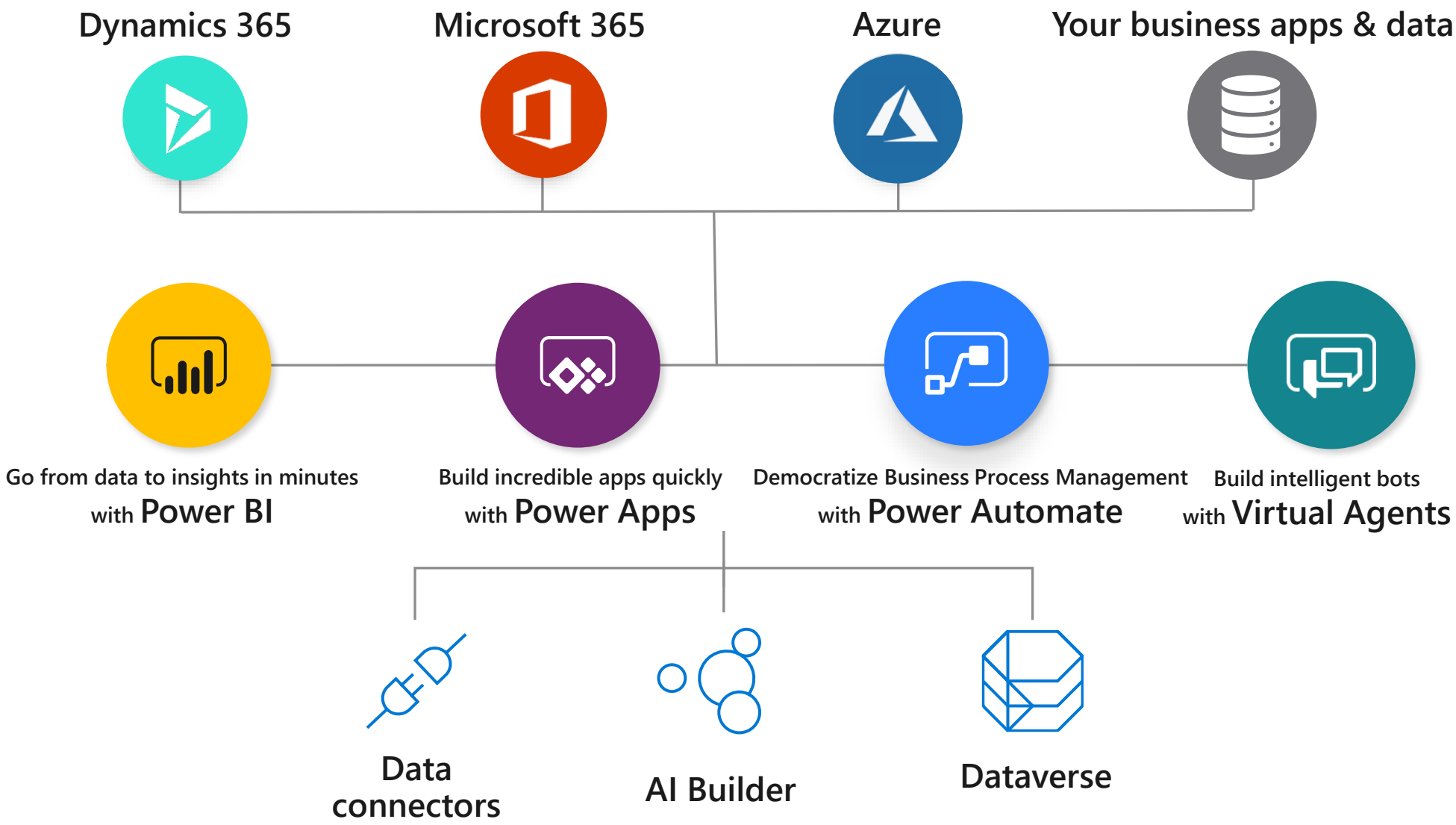
We have a limited number (97) of accounts available from a demo tenant – for those not able to BYO demo tenant.

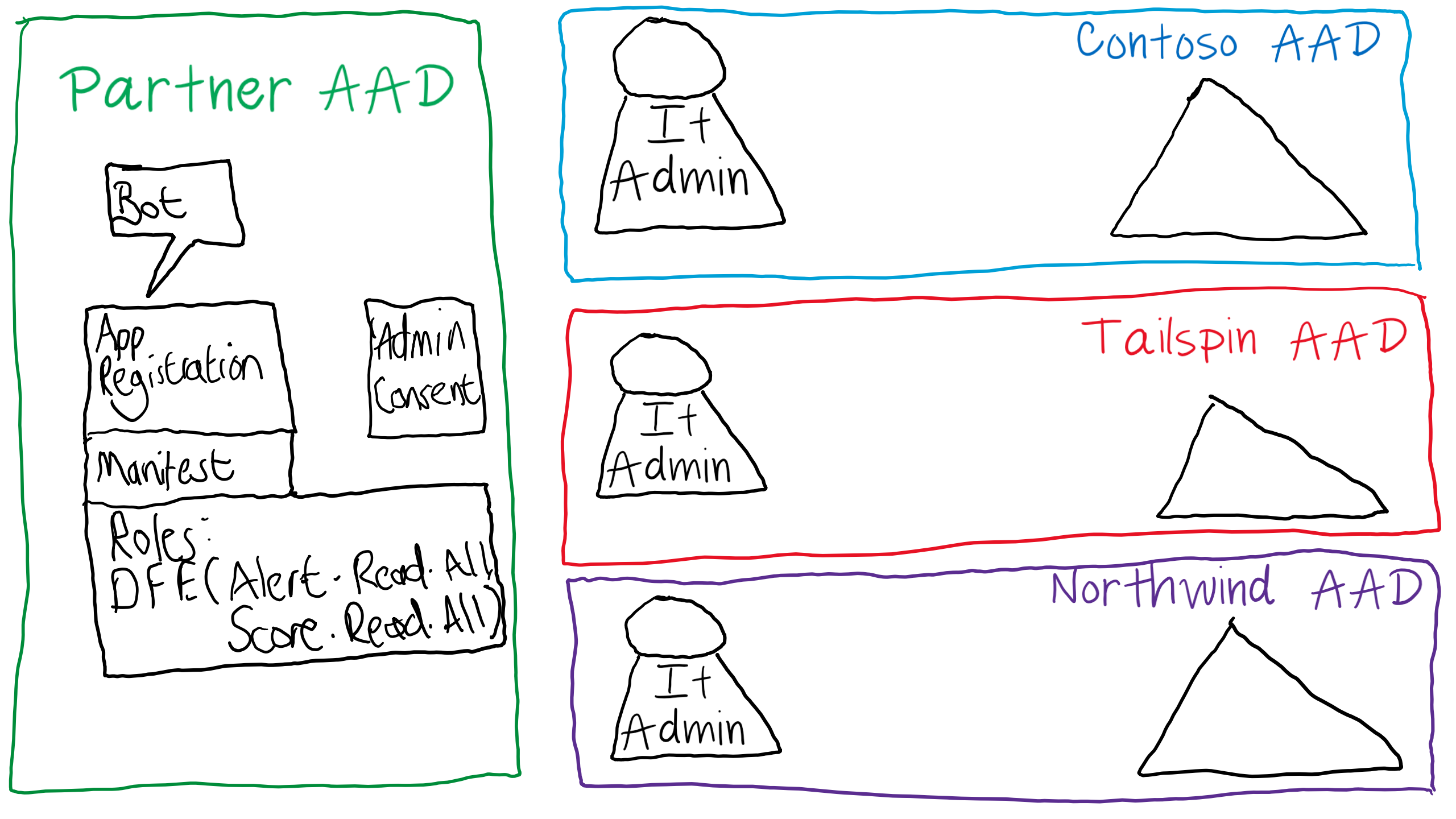
Defender for Endpoint Automation

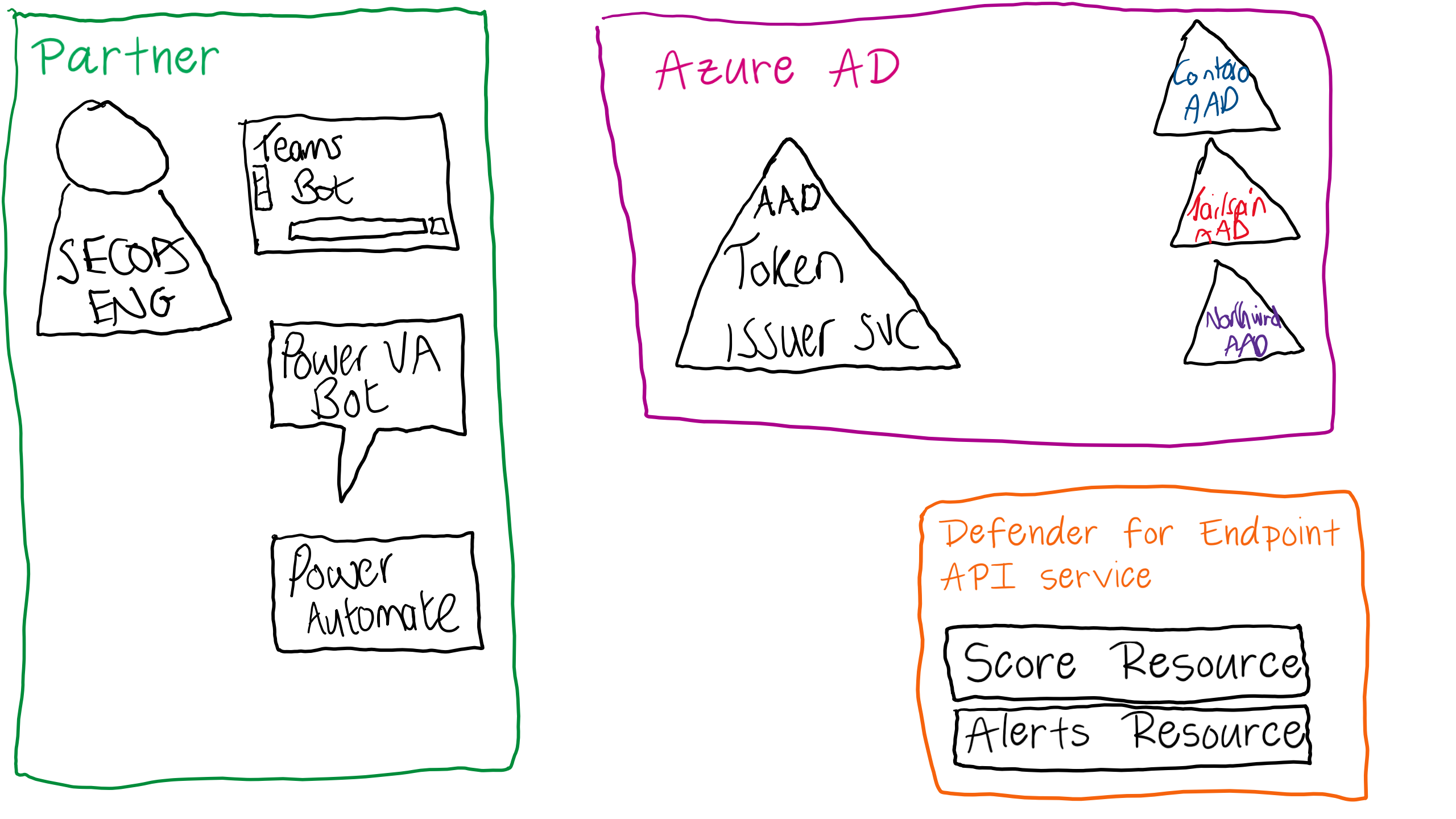


Microsoft Power Platform - Analyse. Act. Automate.

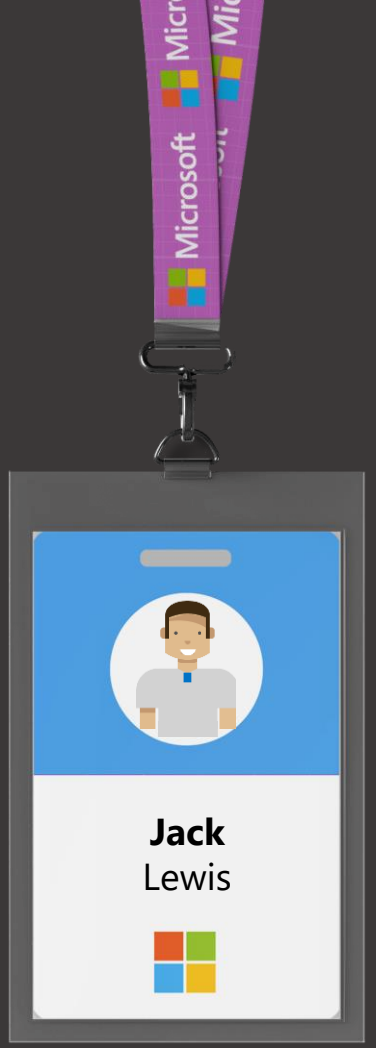
One low-code platform that spans Microsoft 365, Azure, Dynamics 365, and standalone applications – both cloud and on-premises




Partner AAD
Bot
App Registration
Admin Consent
Manifest
Roles:
DFE(Alert.Read.All
Score.Read.All)
IT Admin
Contoso AAD
IT Admin
Tailspin AAD
IT Admin
Northwind AAD

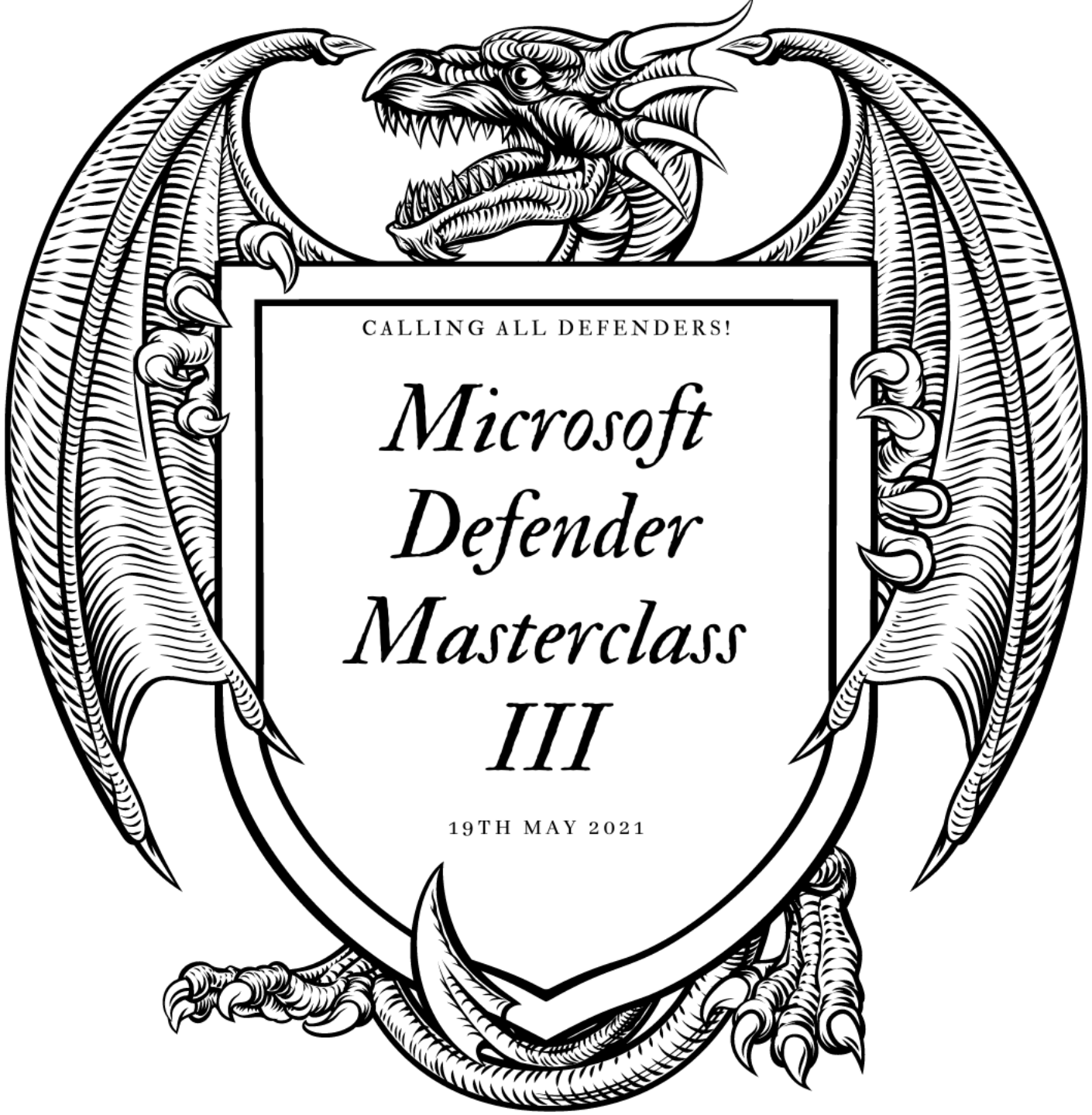

Partner
SECOPS ENG
Teams Bot
Power VA Bot
Power Automate
Azure AD
AAD Token Issuer SVC
Contoso AAD
Fairspin AAD
Northwind AAD
Defender for Endpoint API service
Score Resource
Alerts Resource

Thank you!



aka.ms/jacklewis

Jack Lewis
Jack.Lewis@microsoft.com

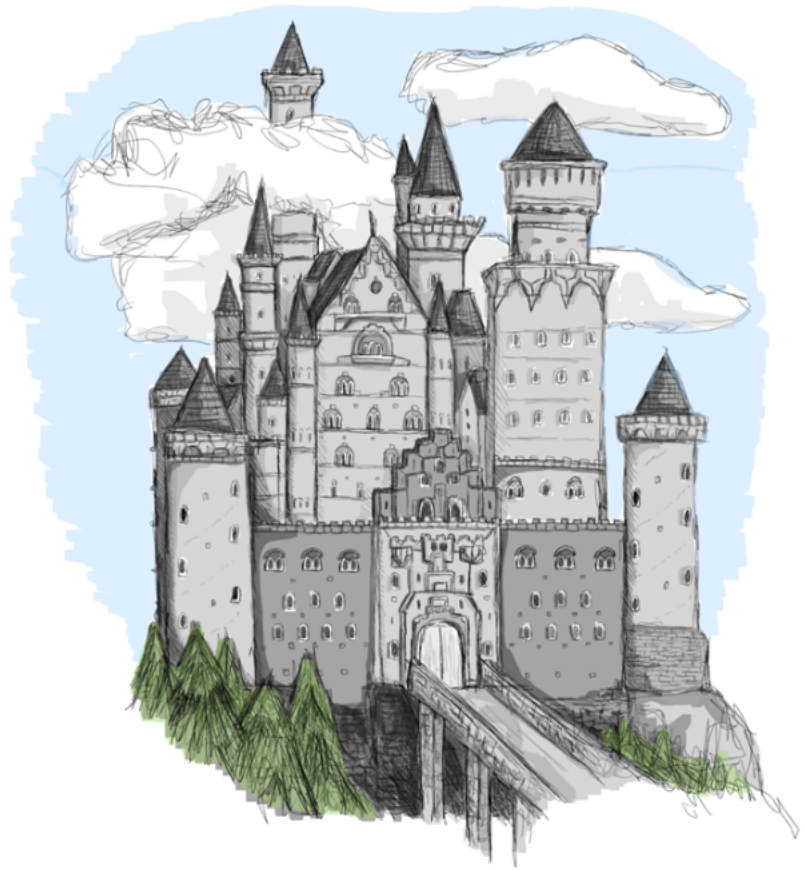


CALLING ALL DEFENDERS!

Microsoft Defender Masterclass III

19TH MAY 2021

Register your bravery at
aka.ms/defendermasterclass3-reg



CALLING ALL DEFENDERS!

Microsoft Defender Masterclass IV

17TH JUNE 2021

Capture the Flag Finale

aka.ms/defendermasterclass4-reg

aka.ms/defendermasterclass-ondemand

aks.ms/defendermasterclass3-reg

aka.ms/defendermasterclass4-reg

aka.ms/defendermasterclass-feedback

Thank you everyone!