Welcome Defenders!

Your journey starts shortly…

CALLING ALL DEFENDERS!

Microsoft Defender Masterclass III

17TH JUNE 2021

Illustration by Becky Cholerton - Microsoft

Microsoft Security

James Graham, PHD

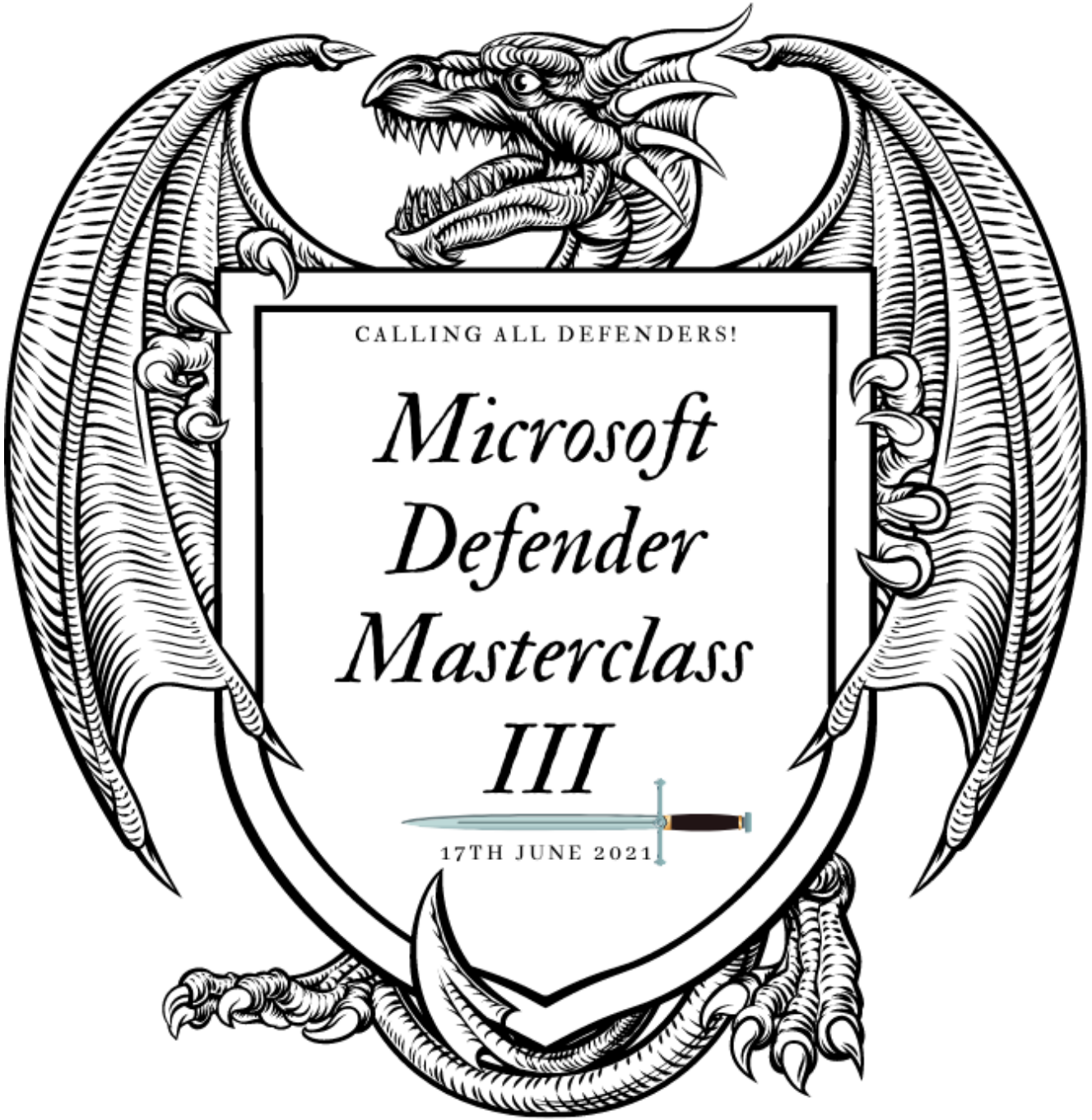
/drjamesgraham

Cloud Solution Architect

Mark Thomas

/themarkthomas

Program Manager



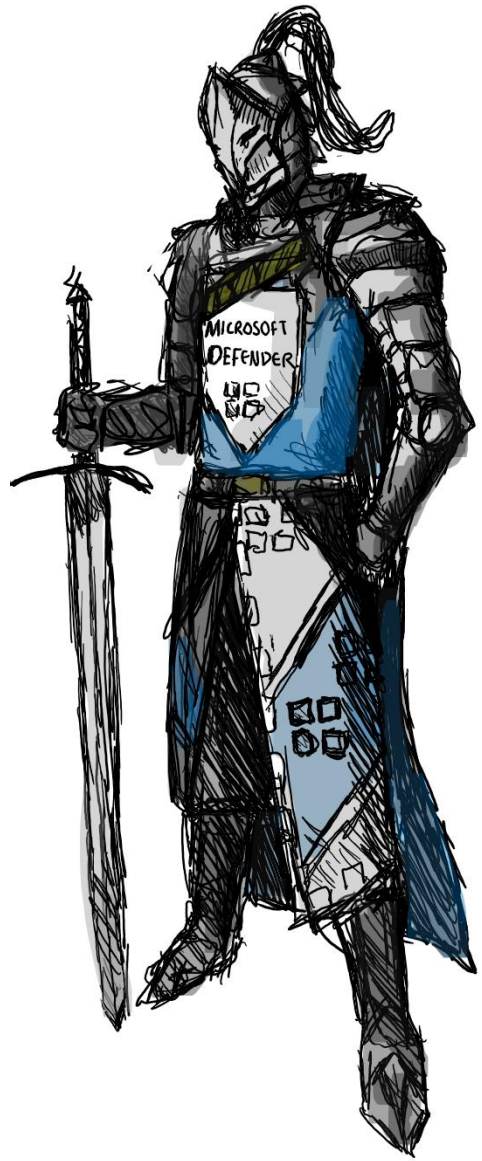
Agenda

9:10am	Opening Keynote	– **Avi Sagiv**
9:35am	Threat Analytics and Attack Surface Reduction Hands-On Exercises	– **Mark Thomas**
10:00am	Break	
10:10am	Threat Analytics and Attack Surface Reduction continued	
11:00am	Break	
11:10am	Azure Virtual Desktop Overview	– **George Wood**
11:30am	Securing Windows 10 Multisession	– **James Graham**
11:50am	Break	
12:00pm	Automated Threat Incident Reports with Microsoft Defender and Power Automate	– **James Graham**
12:55pm	Closing Session	– **James Graham**
1:00pm	Close	

Meet the rest of the team

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 Microsoft 365 Defender*
- *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 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.

Badges – Requirements and How to claim

- **Silver** – Completed skills challenge or Completed MS-500 MS Learn Collection + registered for at least one Masterclass Event.
- **Gold** – Completed Ultimate Skills Challenge or Silver + MS-500 pass + registered for at least two Masterclass Events,

- Email: james.graham@microsoft.com
- Subject: Defender Masterclass Badge Claim
- Body: Provide proof of completing the skills challenge (aka.ms/defendermasterclass-skillschallenge or aka.ms/defendermasterclass-ultimatechallenge – now closed) or completed modules – screenshots will suffice, with proof that it's you. MS-500 – proof of certification (screenshot will suffice).

- Qualified submissions will receive Badge via email

aka.ms/defendermasterclass-feedback

Microsoft

Master Class: Opening Session

Avi Sagiv - Principal PM- Security Partners

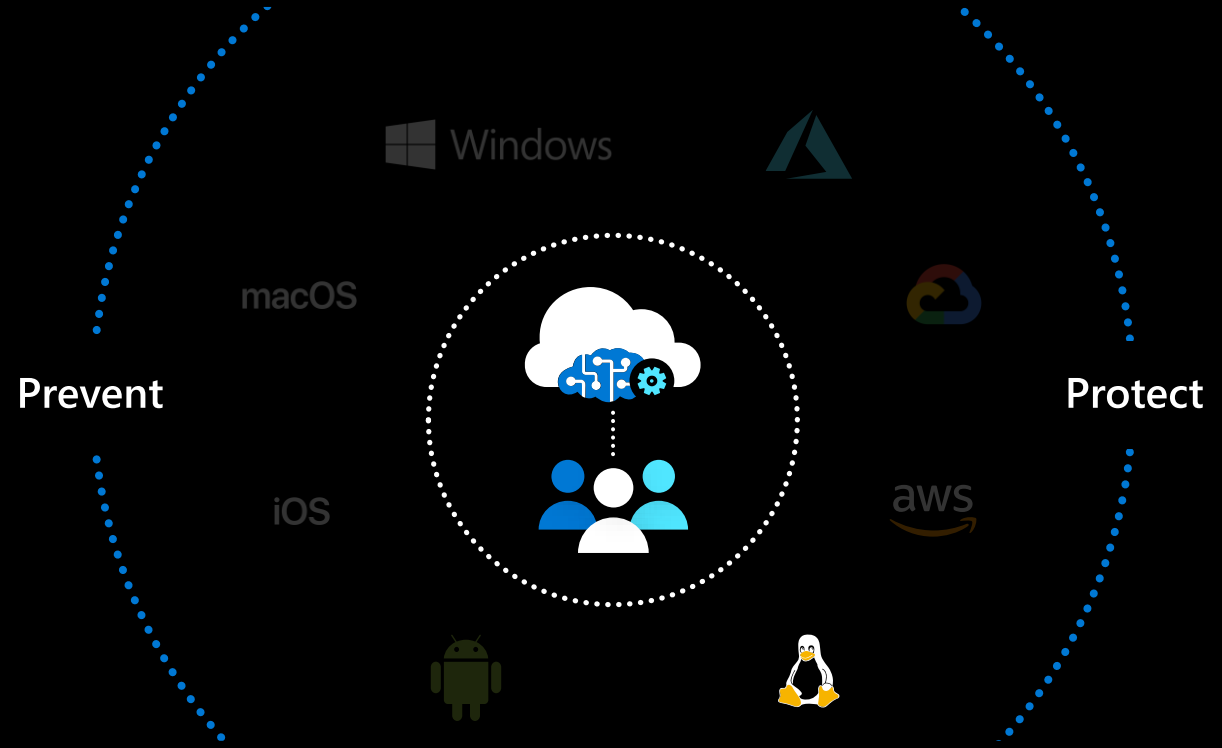
Agenda

- Our Security Vision
- XDR Overview & Roadmap
- Partner Opportunities & Resources

SIEM

Azure Sentinel

Visibility across your entire organization



Microsoft 365 Defender

Secure your end users

Azure Defender

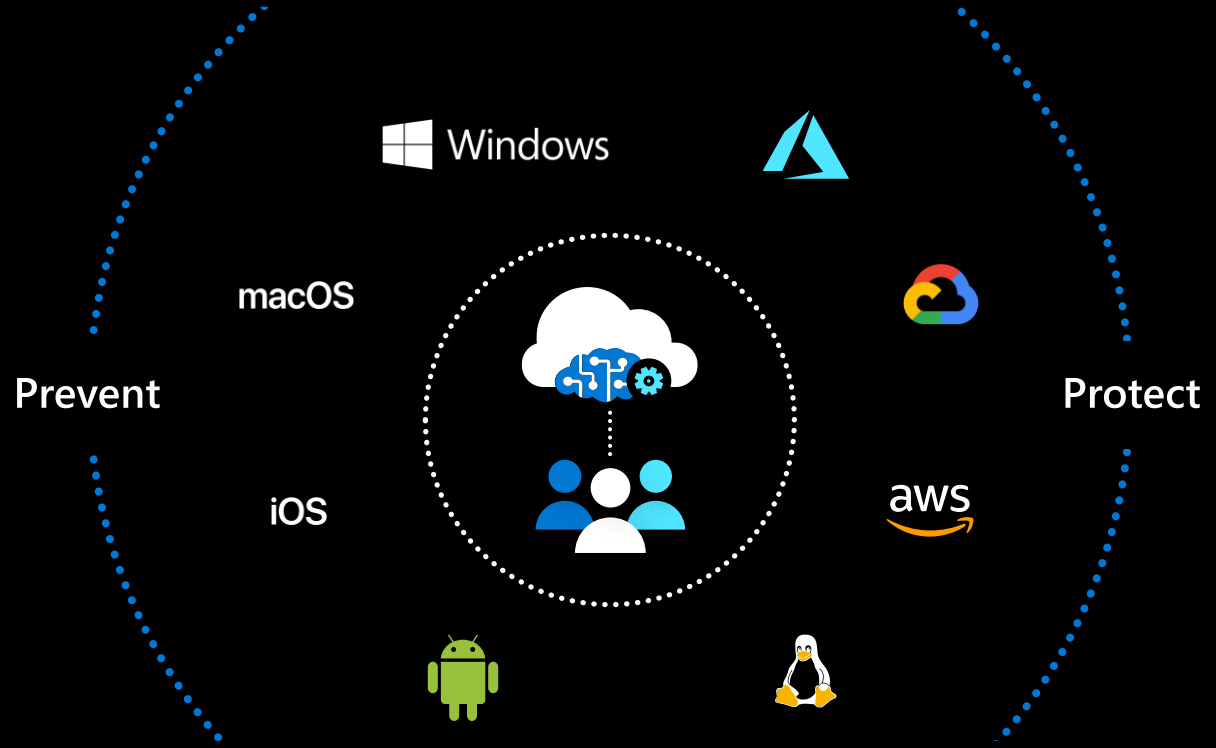
Secure your infrastructure

XDR

SIEM

Azure Sentinel

Visibility across your entire organization



Microsoft 365 Defender

Secure your end users

Azure Defender

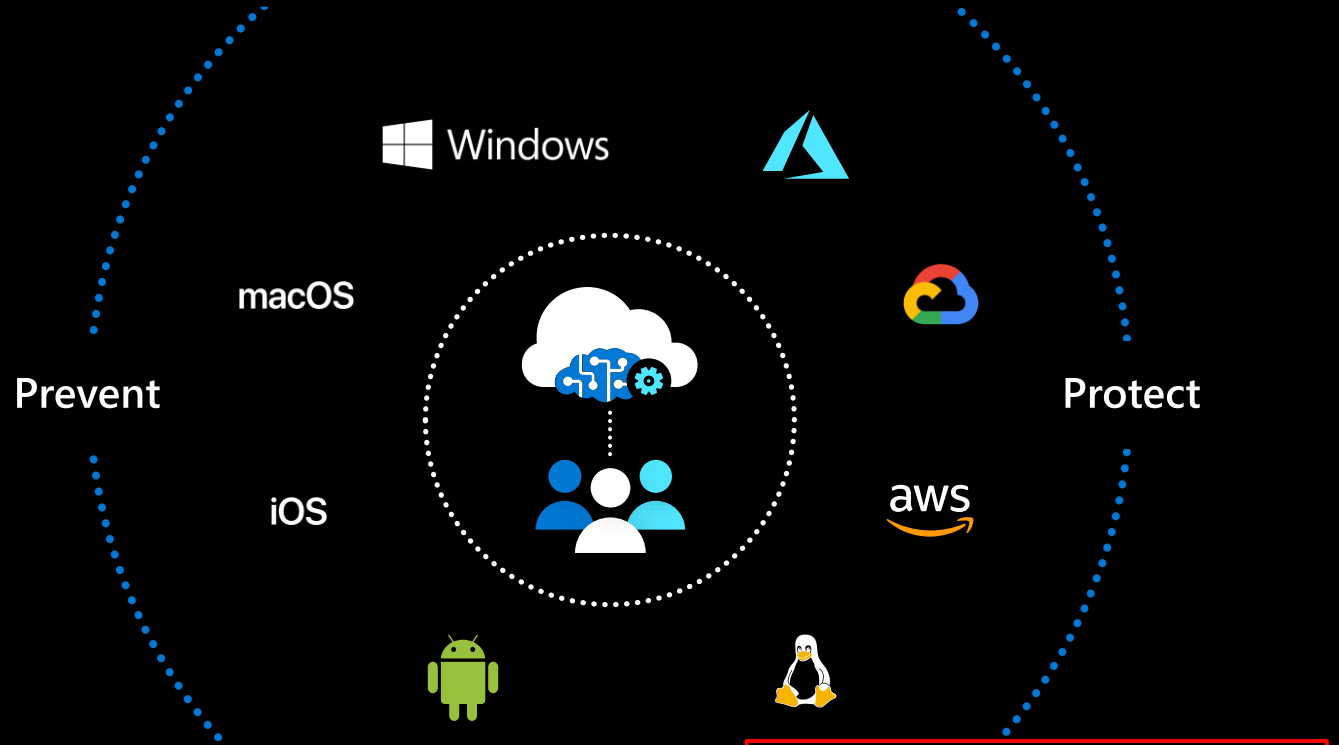
Secure your infrastructure

XDR

SIEM

Azure Sentinel

Visibility across your entire organization



Microsoft 365 Defender

Secure your end users

Azure Defender

Secure your infrastructure

XDR

Azure Defender

Protect your hybrid-cloud workloads

Servers | SQL & Storage | Container Registries and Kubernetes | Key Vault, DNS and Resource Manager | App services | IoT

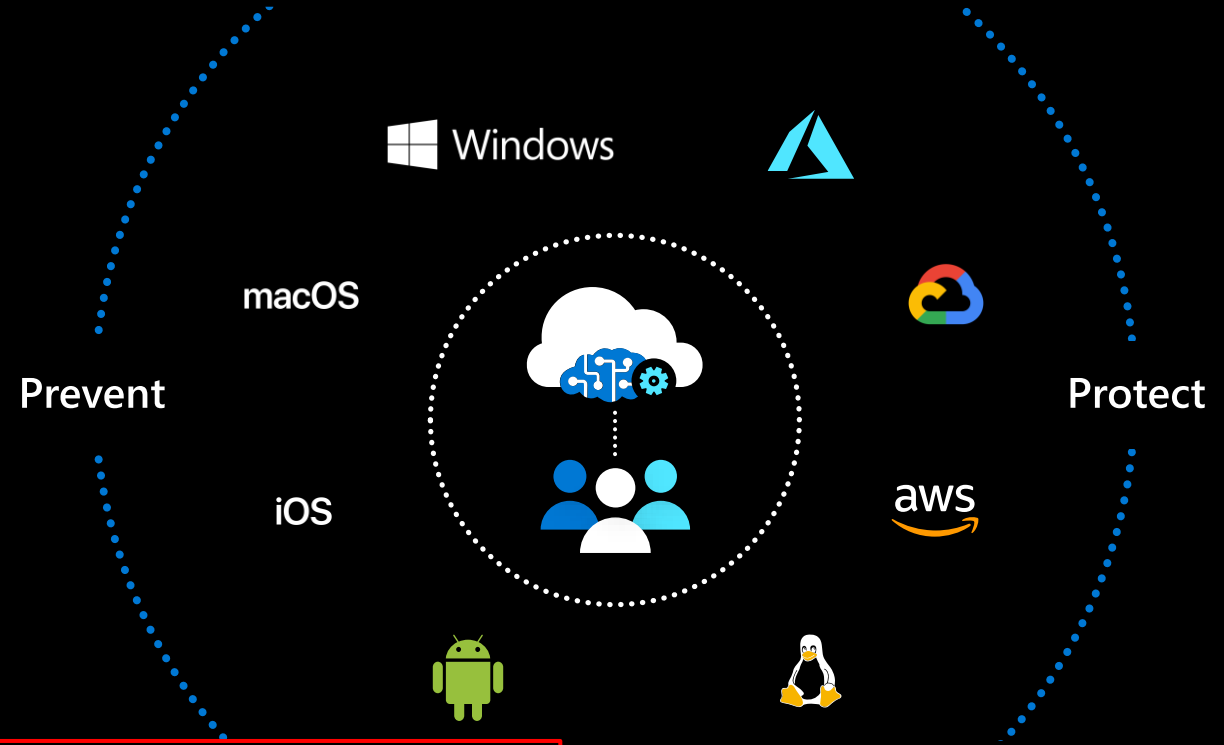
Multi-cloud coverage

aws Amazon Web Services | Microsoft Azure | Google Cloud

SIEM

Azure Sentinel

Visibility across your entire organization



Microsoft 365 Defender

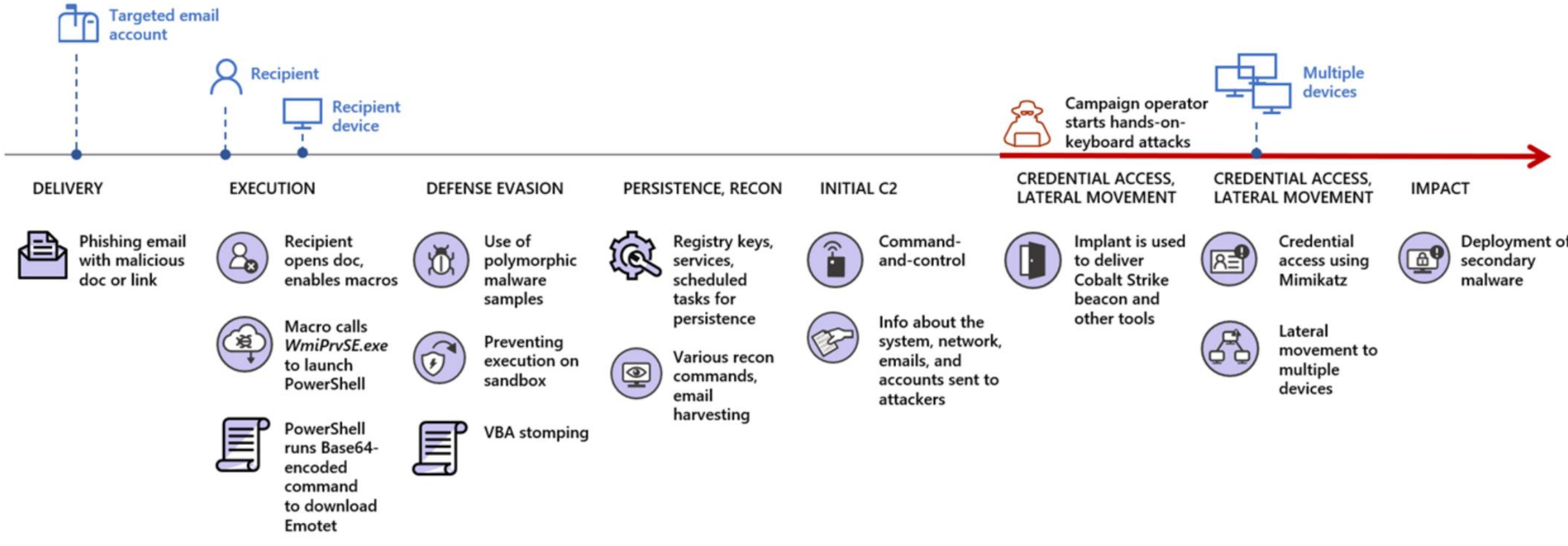
Secure your end users

Azure Defender

Secure your infrastructure

XDR

M365D motivation: attacks are crossing modalities



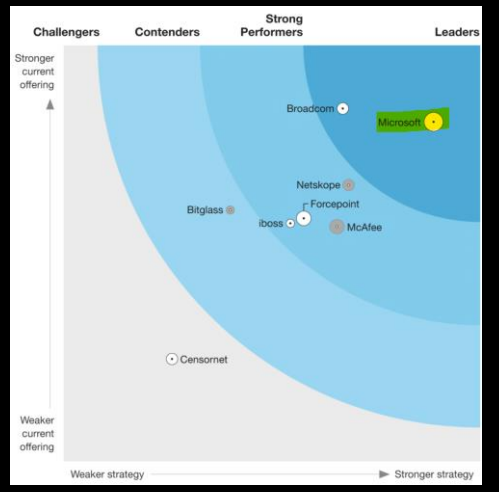
Emotet/Ryuk Ransomware campaign

Microsoft is Uniquely Positioned as Leader

Endpoint Security

Email Security

Access Mgmt.



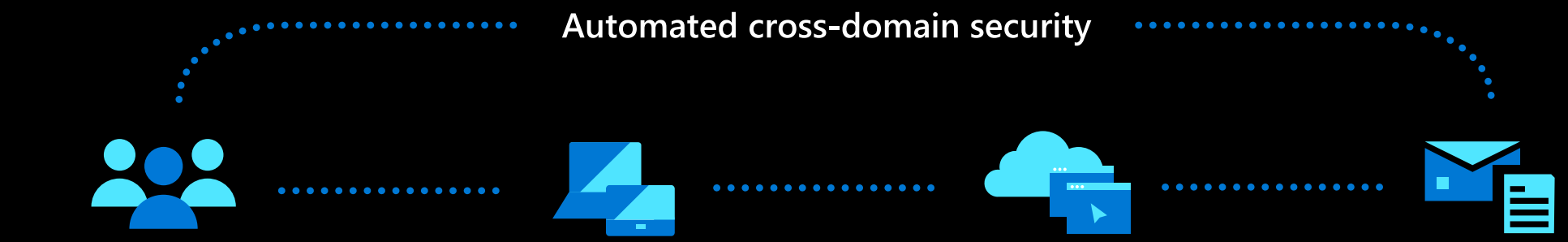
Cloud Security

Endpoint Mgmt.

Gartner

FORRESTER®

Microsoft 365 Defender



Shift from individual silos to coordinated cross-domain security

Microsoft 365 Defender

Automated cross-domain security

One portal
- unified entities

Coordinated active protection from threats

Automatic healing of affected assets

Unified threat intelligence and analytics

Cross-domain threat hunting

Management · APIs · Connectors

Learn more: http://aka.ms/m365d

Try it today: http://security.microsoft.com

Microsoft 365 Defender

Automated cross-domain security

One portal
- unified entities

Coordinated active protection from threats

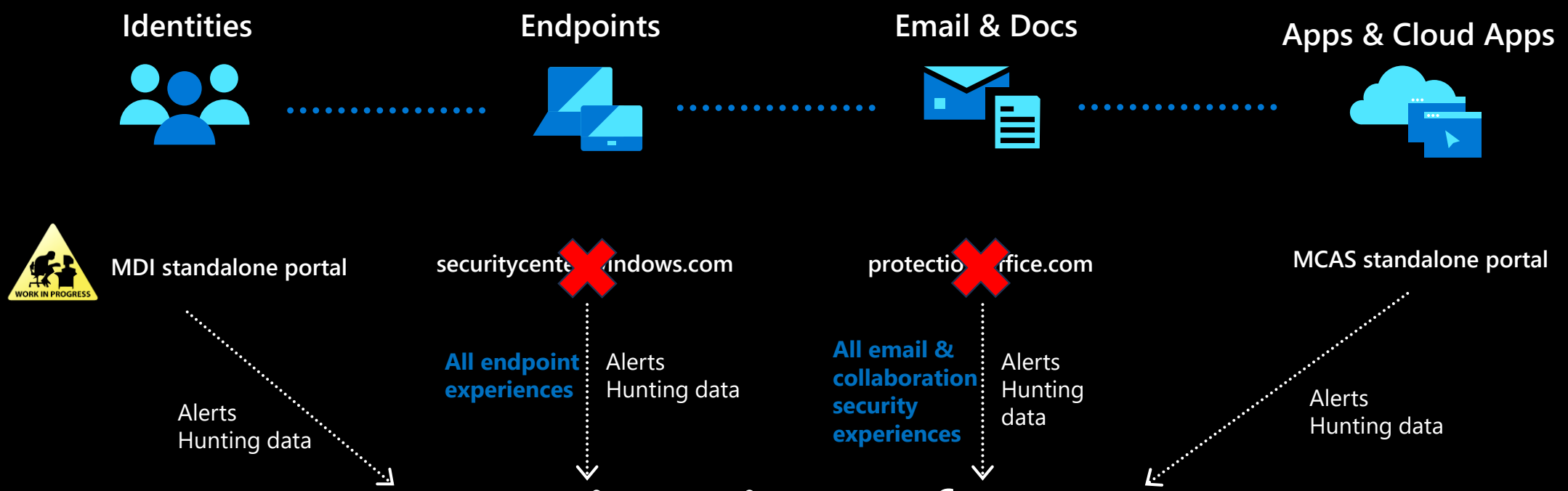
Automatic healing of affected assets

Unified threat intelligence and analytics

Cross-domain threat hunting

Management · APIs · Connectors

M365D One Portal:
a journey from multiple to a single portal



Demo: Portal Overview

Microsoft 365 Defender

Automated cross-domain security

One portal
- unified entities

Coordinated active protection from threats

Automatic healing of affected assets

Unified threat intelligence and analytics

Cross-domain threat hunting

Management · APIs · Connectors

Demo: Incident

Microsoft 365 Defender

Automated cross-domain security

One portal
- unified entities

Coordinated active protection from threats

Automatic healing of affected assets

Unified threat intelligence and analytics

Cross-domain threat hunting

Management · APIs · Connectors

Demo: Action Center

Microsoft 365 Defender

Automated cross-domain security

One portal
- unified entities

Coordinated active protection from threats

Automatic healing of affected assets

Unified threat intelligence and analytics

Cross-domain threat hunting

Management · APIs · Connectors

Learn more: http://aka.ms/m365d

Try it today: http://security.microsoft.com

Demo: Threat Analytics

Microsoft 365 Defender

Automated cross-domain security

One portal
- unified entities

Coordinated active protection from threats

Automatic healing of affected assets

Unified threat intelligence and analytics

Cross-domain threat hunting

Management · APIs · Connectors

Learn more: http://aka.ms/m365d

Try it today: http://security.microsoft.com

Demo: Advanced Hunting

What’s coming?

What's coming?

Threat protection is built-in to all Microsoft-owned assets

M365 Defender is a full orchestrated protection stack (not just post-breach)

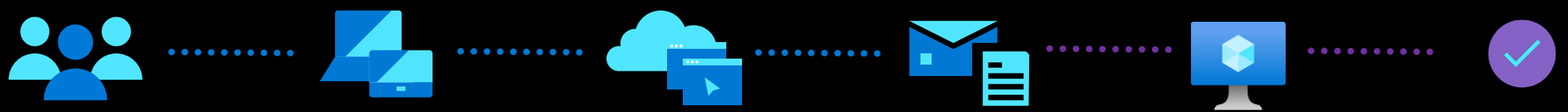
Remediation & prevention are built-in

From multiple to one unified product –

Across infrastructure and user experience

Microsoft 365 Defender Future

Cross-domain security



Identities

Azure Active Directory Identity Protection
+
Microsoft Defender for Identity

Endpoints

Microsoft Defender for Endpoint

Cloud Apps

Microsoft Cloud App Security
+
Office API Protection (MAPG)

User Data

Microsoft Defender for Office 365

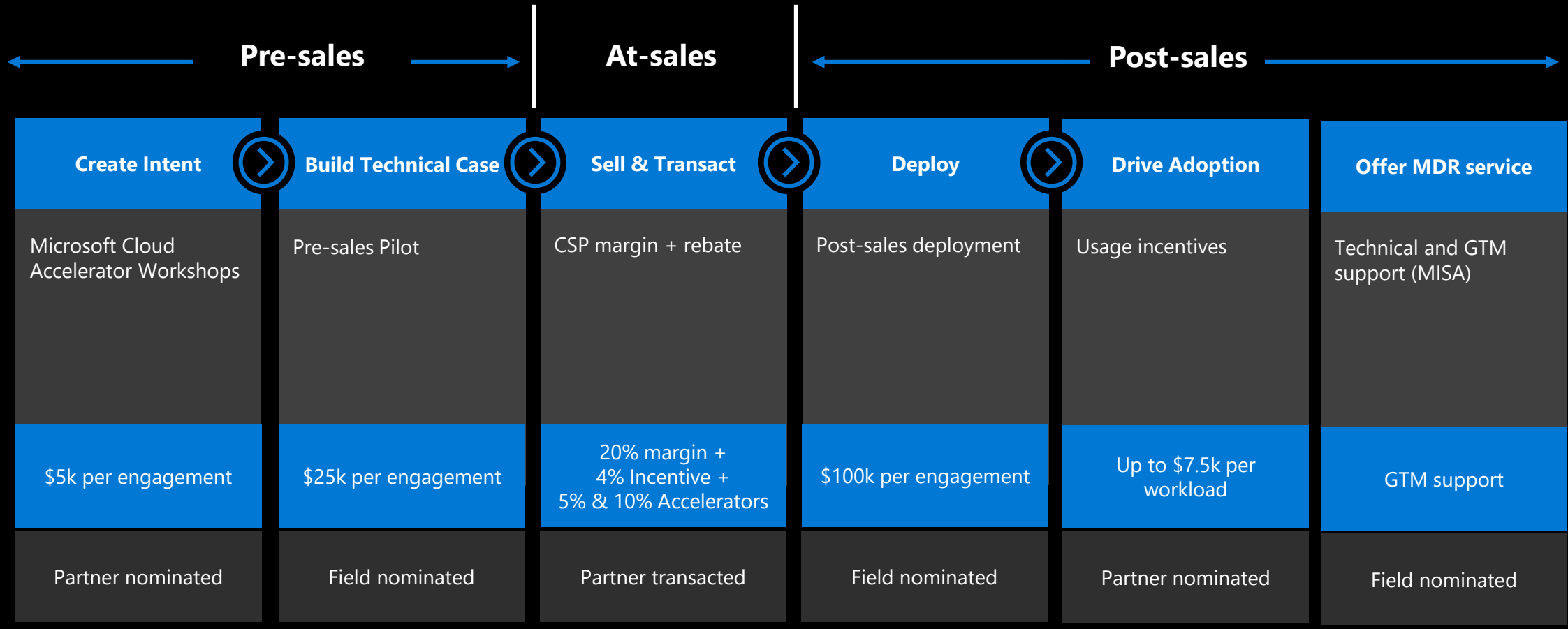
Cloud Workloads

Azure Defender

Compliance

Microsoft Information Protection
+
Insider Risk

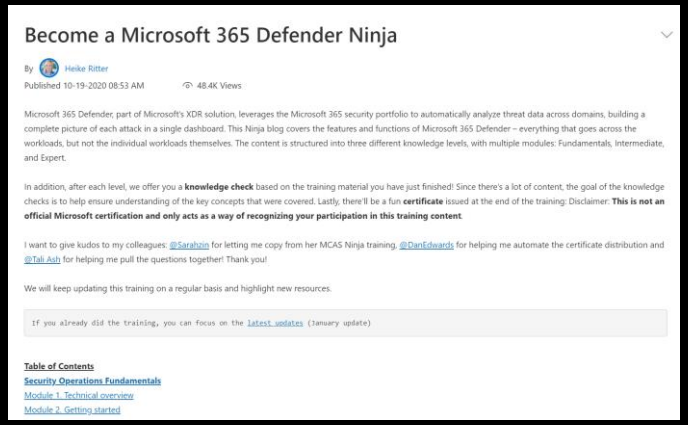
Partner Opportunities



Key Resources to help you get started

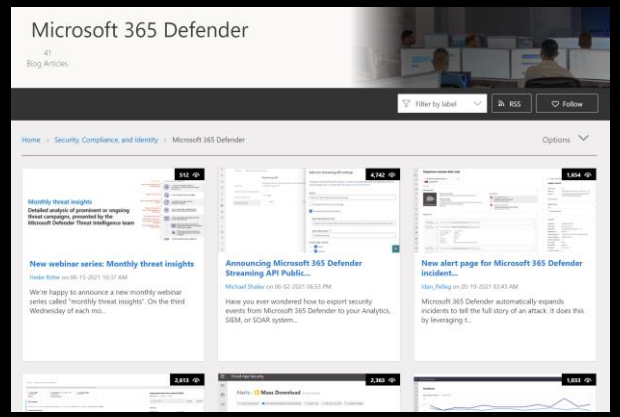
M365D Ninja Training

Product training material for SecOps and SecAdmins structured in expertise levels with knowledge check



Product blog announcements

Check out new feature releases and updates directly from the product group

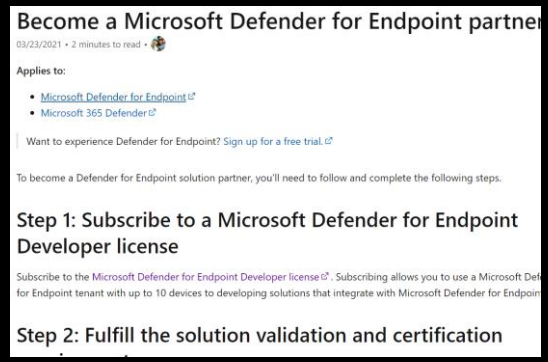


Product Documentation

Deep “How to?” product documentation across all feature areas

Become MSSP partner

From “get lab license” to “get listed in catalog” in 4 simple steps



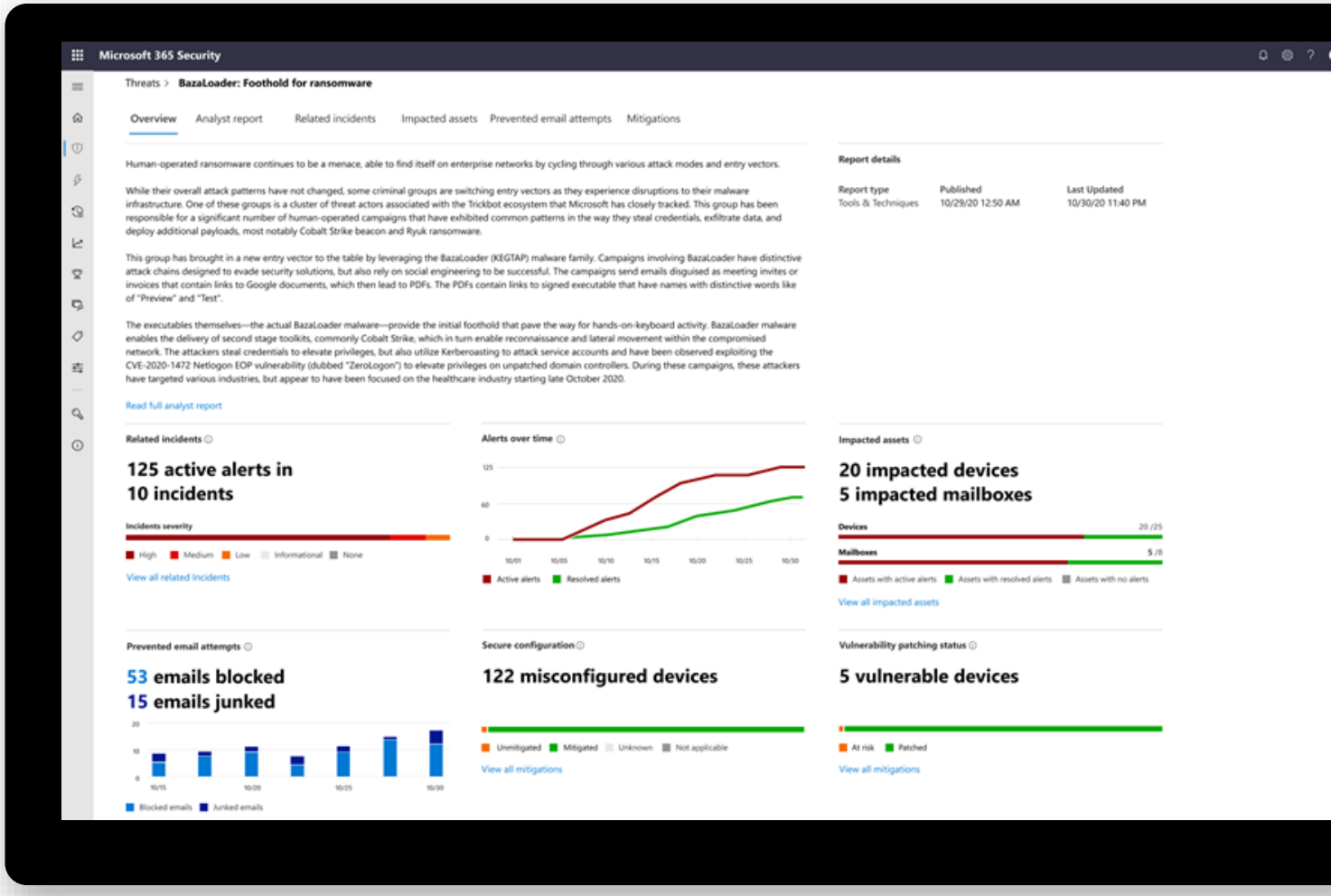

Microsoft
Thank you

Microsoft

Microsoft Defender for Endpoint Threat Analytics

Threat Analytics

- How bad is the threat?
- Does it affect me?
- What can we do about it?



What's new with threat analytics?

- **Threat analytics expanded across Microsoft 365 Defender domains**

  To be available for all customers with E5 for Microsoft Defender for Office 365, Defender for Endpoint

- **Email threat intelligence into threat analytics**

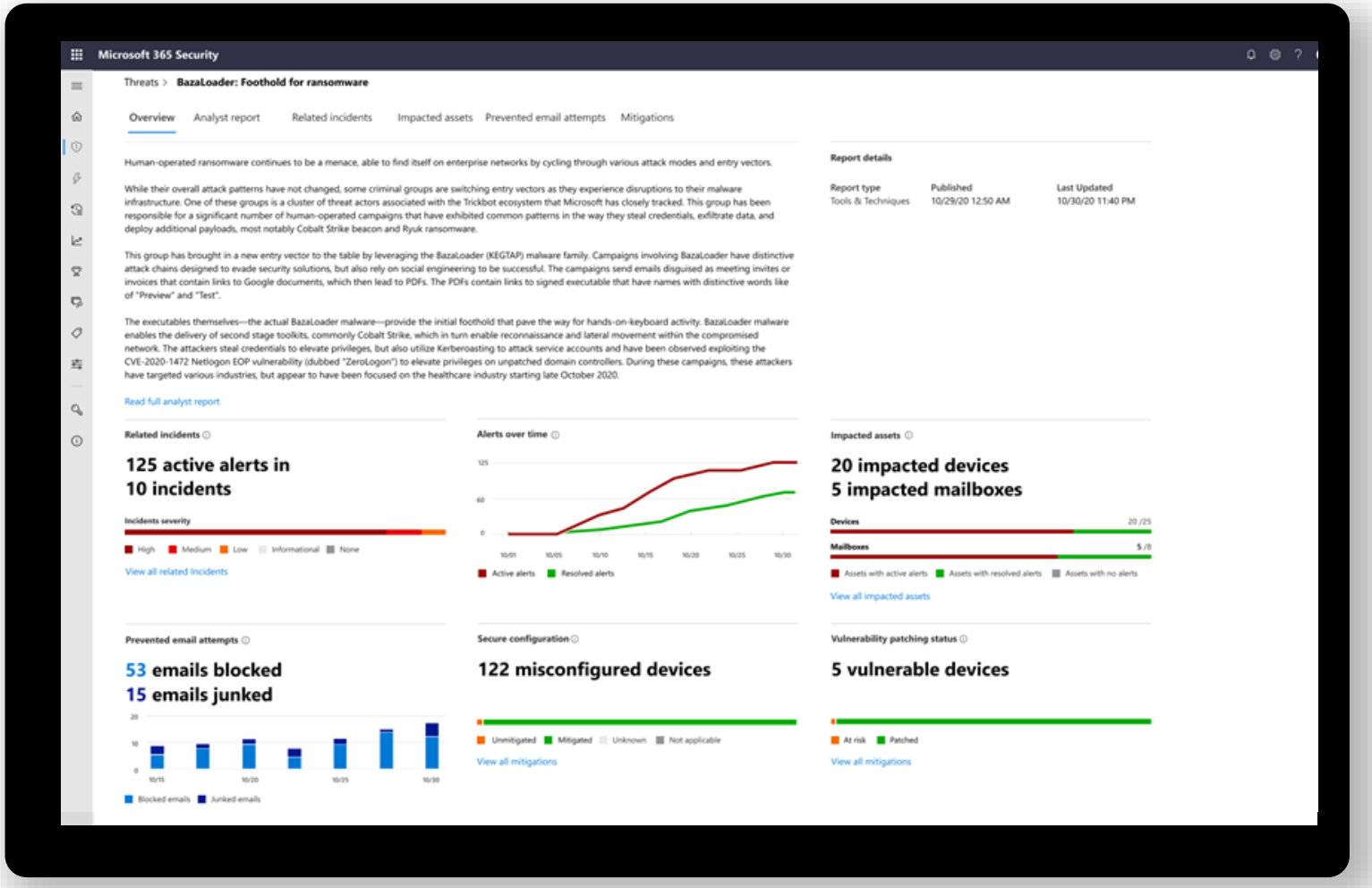
  Email-related detections and mitigations from Defender for Office 365

- **Related incidents**

  Continue the investigation using threat related incidents

- **New experience**

  Enhanced design for quickly identifying and leveraging actionable information



Leverage threat analytics

Review the analyst report

Deep-dive analysis

MITRE techniques

Detection details

Recommended mitigations

Advance hunting queries

Monitor your org state

Active alerts and incidents

Impacted assets—devices and mailboxes

Prevented email attempts

Exposure score and recommended mitigations

Take action

Handle active incidents

Remediate impacted assets

Apply policy changes

Implement Threat & Vulnerability Management mitigations

Microsoft

Masterclass III – Threat Analytics Lab

Demo Tenant – Backup Option

Grab Credentials – https://aka.ms/idonthaveatenant

Break

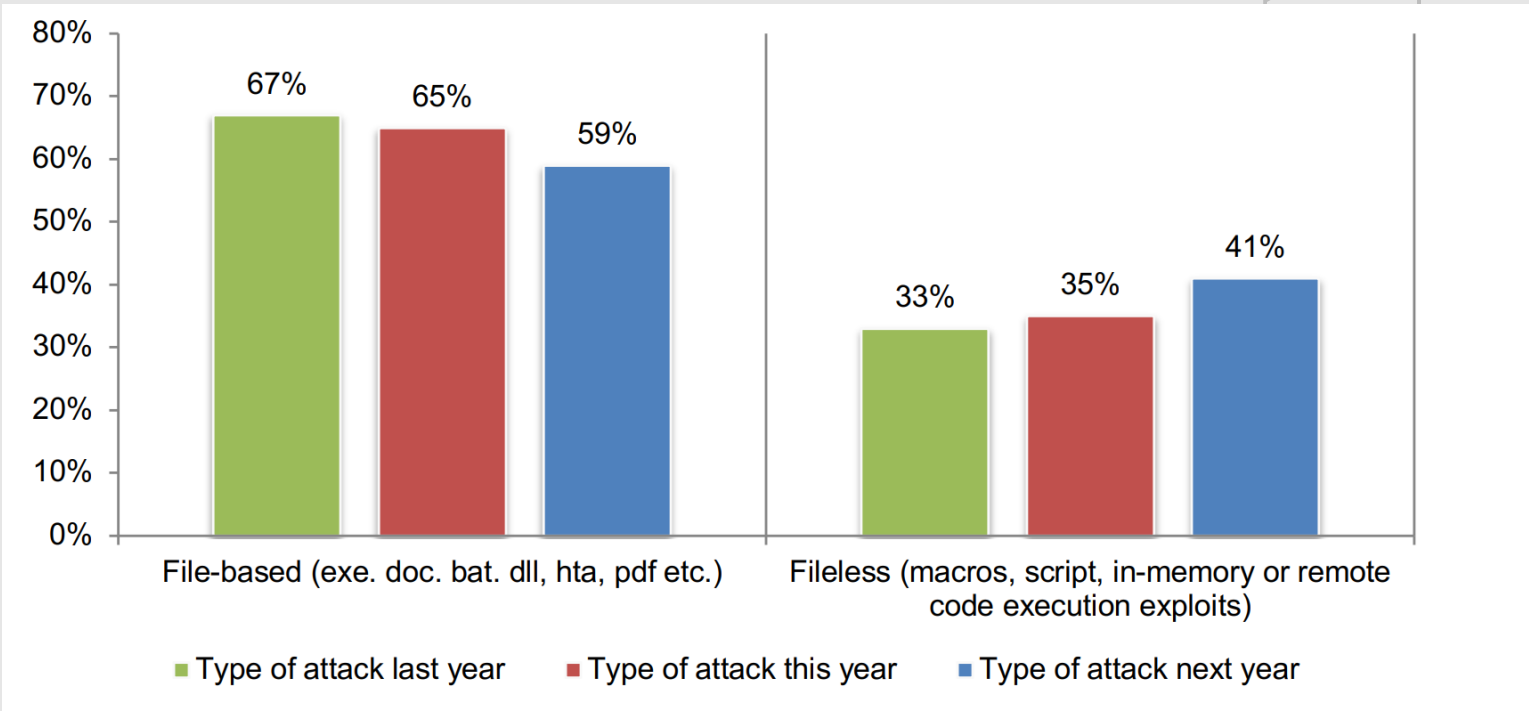
Back at 10:10am (UTC+1)

Microsoft

Microsoft Defender for Endpoint Attack Surface Reduction

Evolving Threat Landscape: Fileless Attacks

- **Fileless attacks are growing!**
- **Why? Because they are effective**



[2020 Ponemon Study on the State of Endpoint Security Risk]

Fileless Attacks: What *are* they? Why fileless?

- Classes of **malware** that **indirectly use files**
- Fileless threats often "**live off the land**", by abusing native platform capabilities (e.g. scripting languages, and management repositories)

Stealth

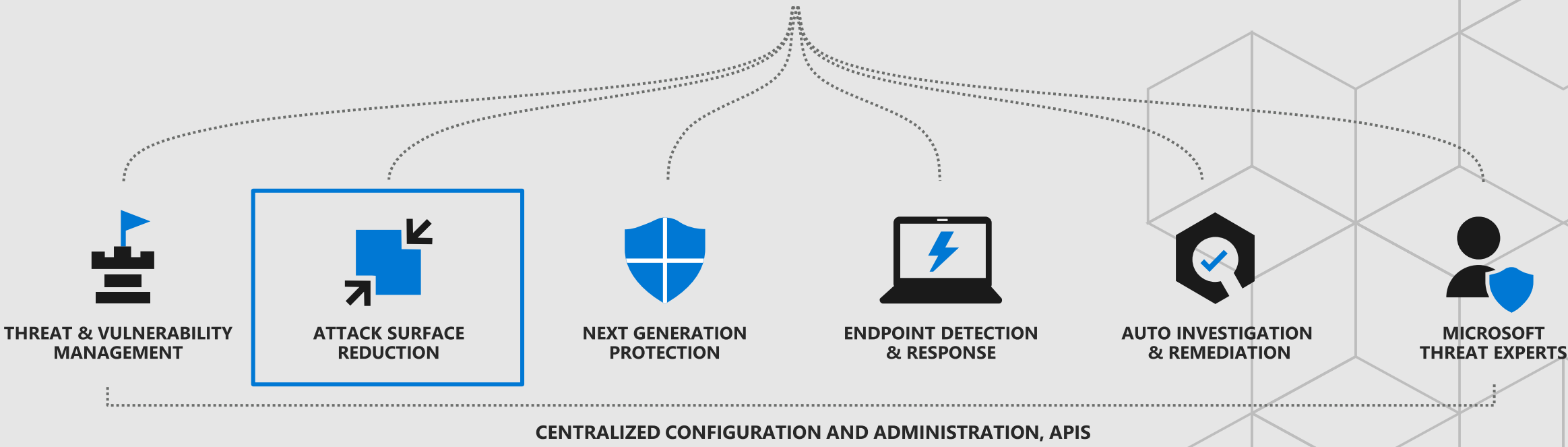
- The filesystem is heavily scrutinized
- Use of built-in tools allows malware to blend in as legitimate
- Fewer events are generated
- Harder to investigate in retrospect

Flexibility

- Many attack vectors (Registry, WMI, scripting languages, etc.)
- Versatile built-in tools at attacker's disposal
- Attacks can be easily staged

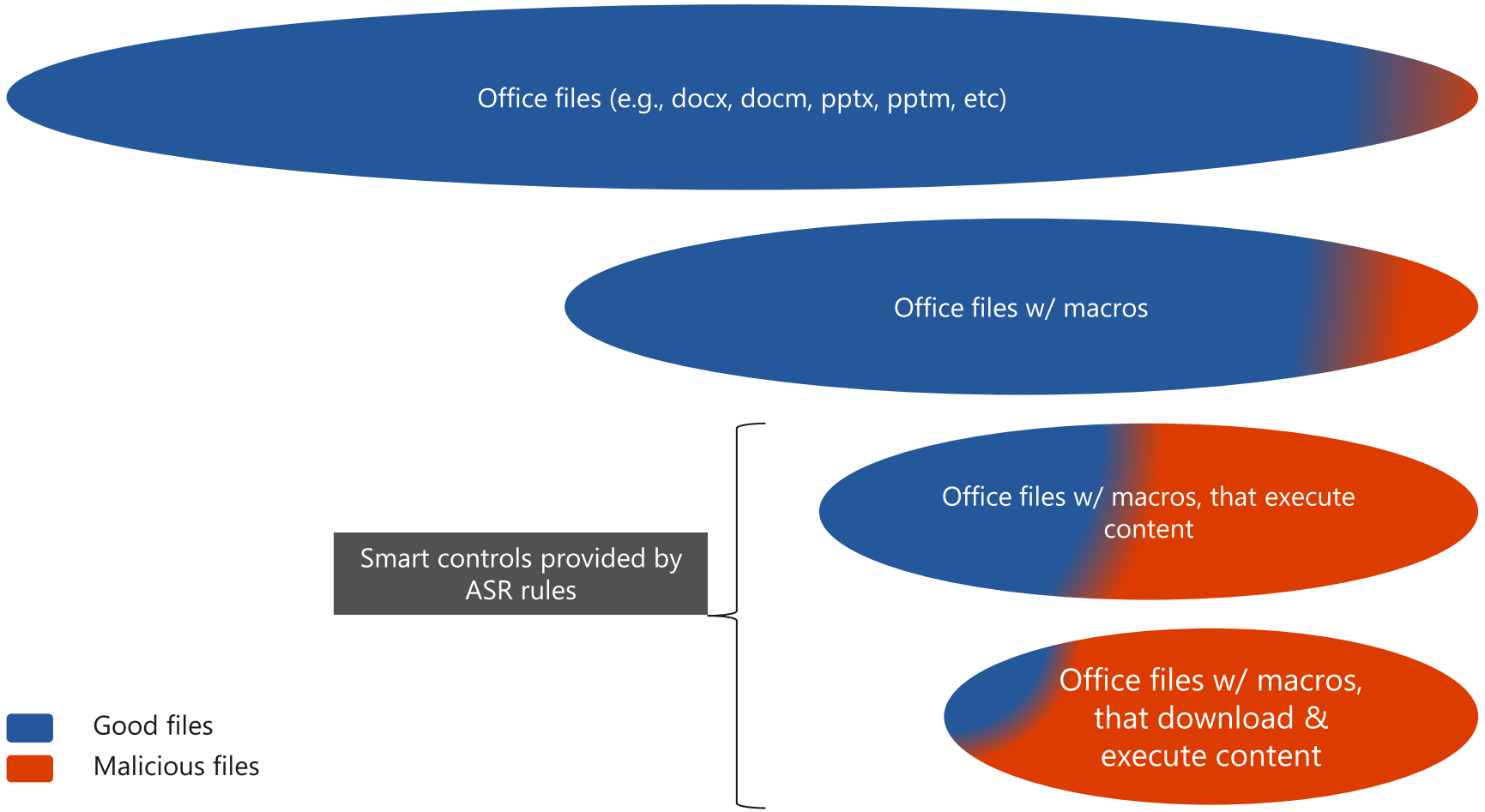
Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.



ASR rules – Office Macros example

Smart-ASR control provides the ability to block behavior that balances security and productivity



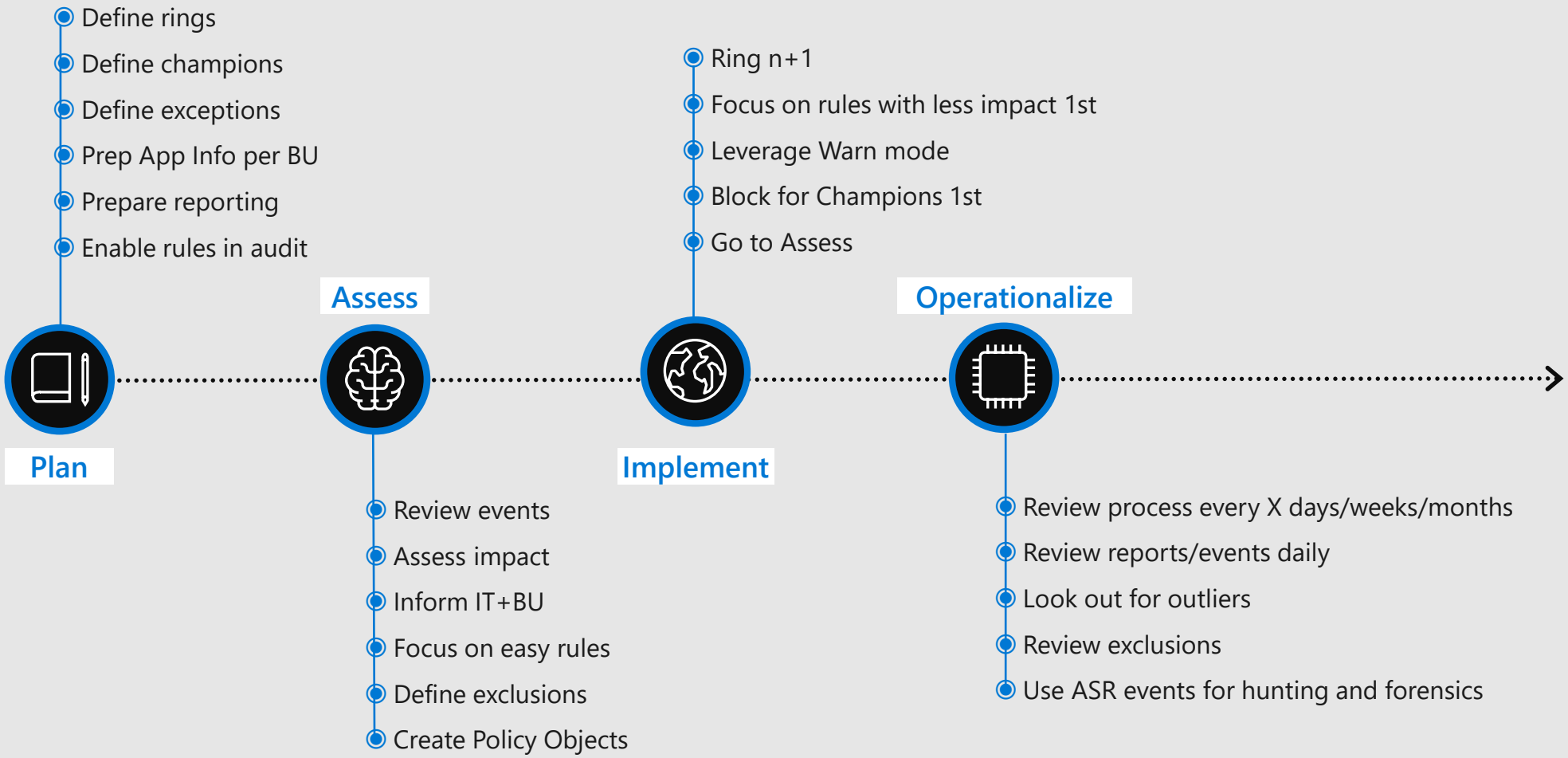
Blocking Office files, severely impacts productivity (as there are way more good files than malicious files)

Blocking Office files w/ macros, still impacts productivity (as there might be the occasional use for legit macro)

Blocking Office files w/ macros that execute content, is far less impactful on legit productivity, while dramatically improving security

Blocking Office files w/ macros that download and execute content, is almost exclusive behavior of bad files. Thus negligent impact on productivity, with dramatic security benefit

ASR rules – High-level Adoption Plan



Microsoft

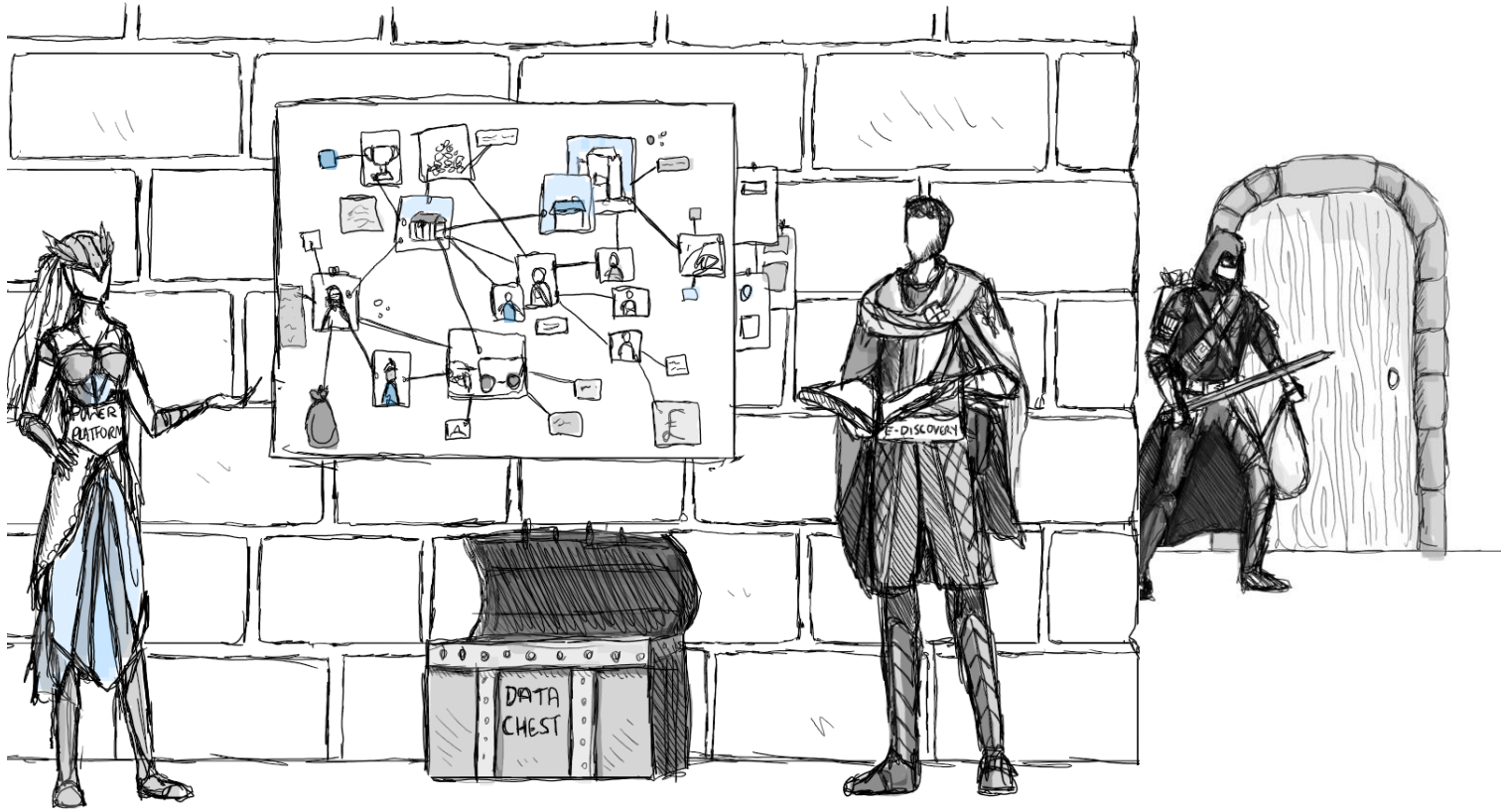
Masterclass III – Attack Surface Reduction Lab

Azure Sentinel Technical Playbook for MSSP's

How to deploy Azure Sentinel as a managed security services provider

http://aka.ms/azsentinelmssp

Compliance @ Speed Part 3 The Finale – 23rd June, 2021 9:30am – 1pm (British Summer Time)



Join the Microsoft Protectors for Part III at Speed. A 3.5 hour event, where we will build on what you learnt in Part I . More Compliance Platform demos across Microsoft 365 and Azure including:
eDiscovery , Azure Sentinel, Conditional Access, AIP Scanner, more Power Platform integrations+ API Intergrations

Illustrations by Becky Cholerton

Microsoft

Protectors.. .Register your bravery at aka.ms/complianceatspeed3-reg

Break

Back at 11:13am

Microsoft

Azure Virtual Desktop Overview

June 2021

George Wood – Microsoft CSA

When is virtualization useful?

Security and regulation

Financial services

Health care

Government

Elastic workforce

Mergers and acquisition

Short-term employees

Contractors and partners

Remote employees

BYOD and mobile

Call centers

Branch workers

Specialized workloads

Design and engineering

Legacy apps

Software dev test

Windows server and desktop offerings today

Windows Server Desktop Experience	Windows 10 Enterprise
Scalable multi-session **legacy** Windows environment	Native single-session **modern** Windows experience
Windows Server	Windows 10
Multiple sessions	Single session
Win32	Win32, UWP
Office Perpetual	Microsoft 365 Apps for enterprise
Long-term servicing channel	Semi-annual channel

Extending the opportunities for virtualization

Windows Server RD Session Host

Scalable multi-session **legacy** Windows environment

Windows Server

Multiple sessions

Win32*

Office 2019 Perpetual

Long-term servicing channel

Windows 10 Enterprise multi-session

Scalable **multi-session** modern Windows user experience with Windows 10 Enterprise security

Windows 10

Multiple sessions

Win32*, UWP

Microsoft 365 Apps for enterprise

Semi-annual channel

Windows 10 Enterprise

Native **single-session** modern Windows experience

Windows 10

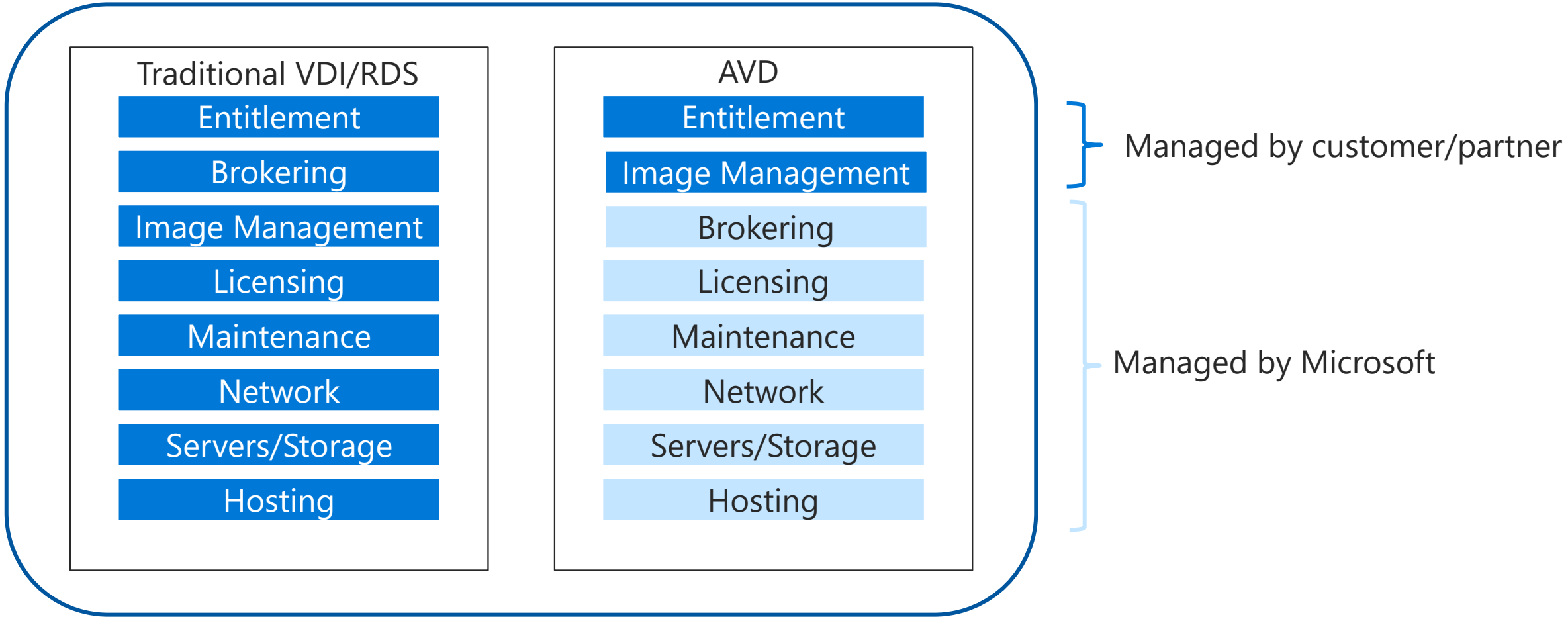
Single session

Win32, UWP

Microsoft 365 Apps for enterprise

Semi-annual channel

Where to make the difference between traditional VDI/RDS and AVD



**Gartner, Inc., When Midsize Organizations Should Select Desktop as a Service, Nathan Hill, Refreshed: July 19, 2018

Native Azure Virtual Desktop

High Level Architecture

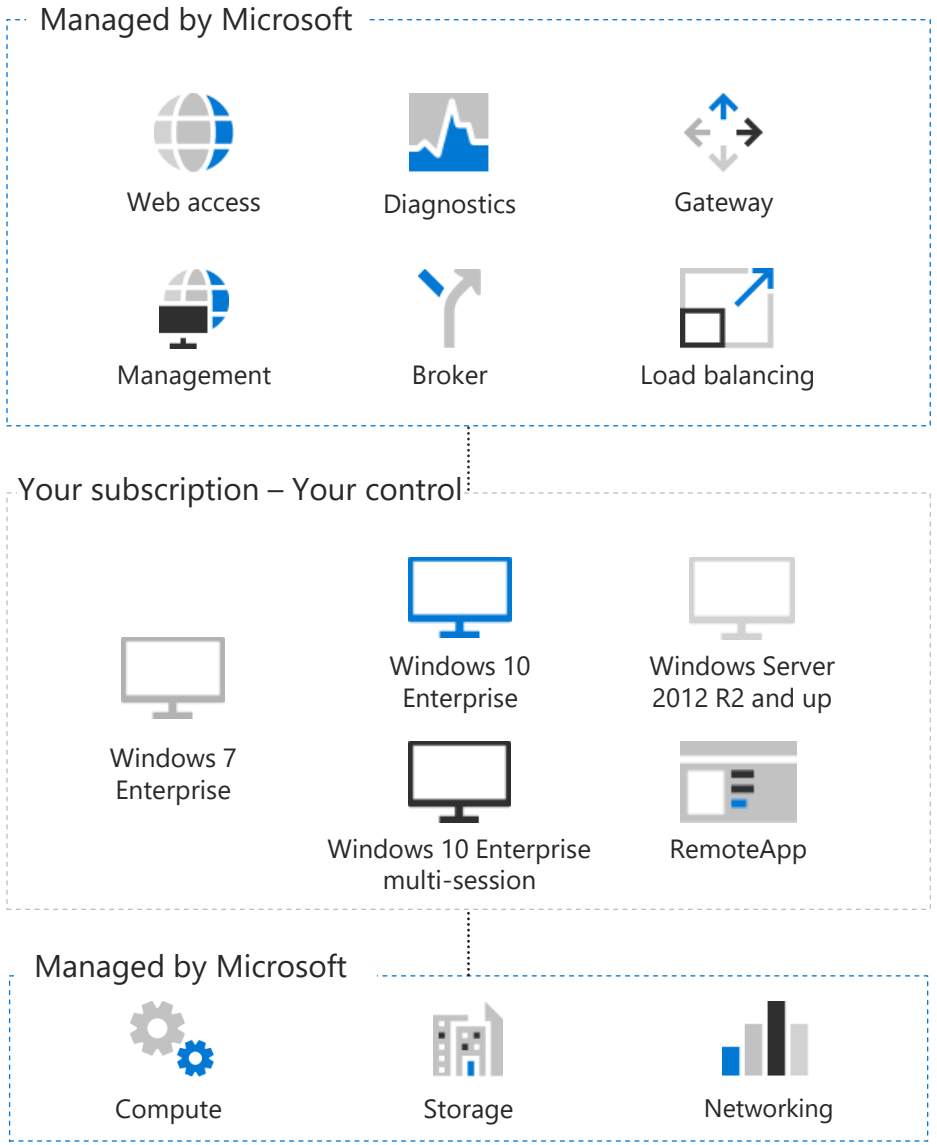
Use Azure Active Directory identity management service

Provide virtualization infrastructure as a managed service

Deploy and manage virtual machines in Azure subscription

Manage using existing tools like Configuration Manager or Microsoft Intune

Connect easily to on-premises resources



Many customers are already eligible for Azure Virtual Desktop

Azure Virtual Desktop Licensing Requirements

Client

Customers are eligible to access Windows 10 single and multi-session and Windows 7 with Azure Virtual Desktop if they have one of the following licenses:*

- **Microsoft 365 E3/E5**
- **Microsoft 365 A3/A5/Student Use Benefits**
- **Microsoft 365 F1**
- **Microsoft 365 Business Premium**
- **Windows 10 Enterprise E3/E5**
- **Windows 10 Education A3/A5**
- **Windows 10 VDA per user**

Server

Customers are eligible to access server workloads with Azure Virtual Desktop if they have one of the following licenses:

- **RDS CAL license with active Software Assurance**.

* Customers can access Azure Virtual Desktop from their non-Windows Pro endpoints if they have a Microsoft 365 E3/E5/F1, Microsoft 365 A3/A5, or Windows 10 VDA per user license.

Making Office 365 ProPlus the best experience in Azure Virtual Desktop with FSLogix

With the acquisition of FSLogix, WVD will provide three core pieces of technology

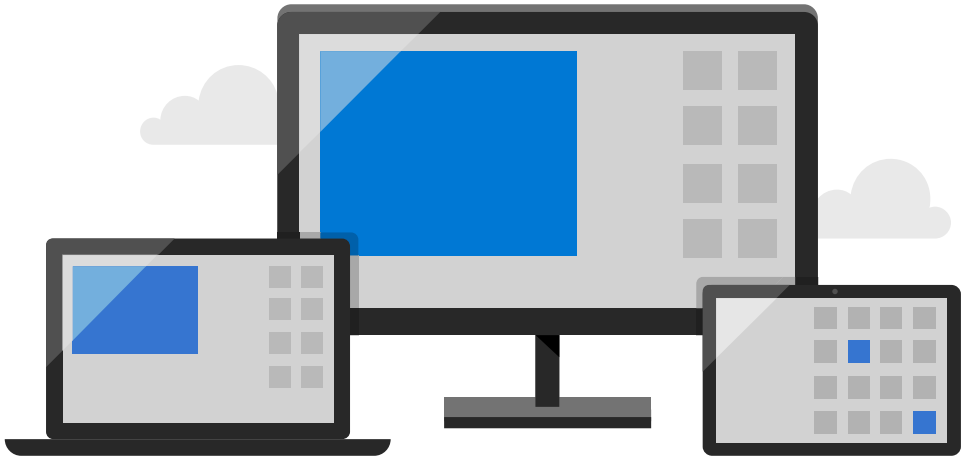
- **Profile Containers:** Dramatically speeds up logon and application launch times
- **Office 365 Containers:** Making Office much more performant in multi-user virtual environments.

  Eg: Outlook OST file, OneDrive cache, Windows Search DB and Skype for Business GAL.

- **App Masking:** Helps minimize the number of images to be maintained and hence reduces costs for large organizations.

  Allows enterprises to have a single OS image for all pools of VM's with all apps installed

- **Java Redirection:** Pins apps and websites to specific versions of Java co-existing on same machine



Blending security across the Microsoft ecosystem

Microsoft 365

Conditional Access

Multi-Factor Authentication

Role-based Access Control (RBAC)

Defender for Endpoint

Azure

>90 compliance offerings

>3,500 global cybersecurity experts

6.5 trillion global signals daily

$1 billion annual cybersecurity investment

Azure Virtual Desktop

Reverse Connect (No inbound ports need be opened to the customer environment)

Azure AD authentication

AD-joined virtual machines

Azure Virtual Desktop is available worldwide

Empower IT to transform the workplace

Provide a full-desktop, authenticated experience for users at every level

Reduce the costs and time spent managing on-premises infrastructure

Simplify management, provisioning, and access to corporate data and apps

Deploy and scale in minutes

Upcoming features and next steps

- Support for Azure Active Directory Join
- Manage Win 10 multi-session with Microsoft Endpoint Manager
- AVD Quickstart
- Support for external user access rights

To continue learning, visit aka.ms/wvd-learn

Get certified! Exam AZ-140: Configuring and Operating Microsoft Azure Virtual Desktop

Microsoft Security

~~Windows~~ Azure Virtual Desktop Endpoint Security

Lab Preparation – come back at 12:12pm

For the next exercise please use your own demo tenant.

Please head over to:

aka.ms/defendermasterclass-repo

OR

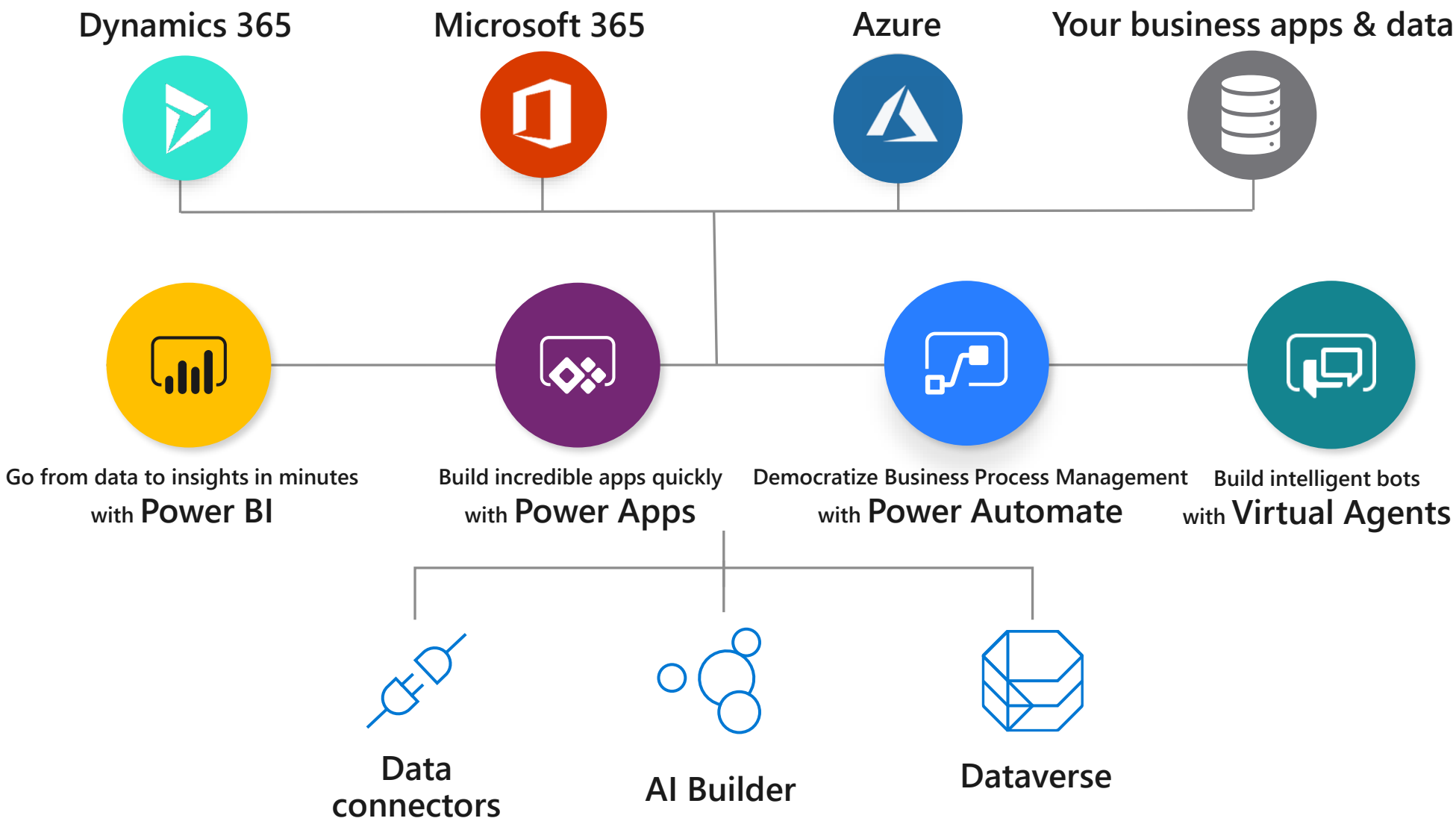
aka.ms/icantaccessgithub

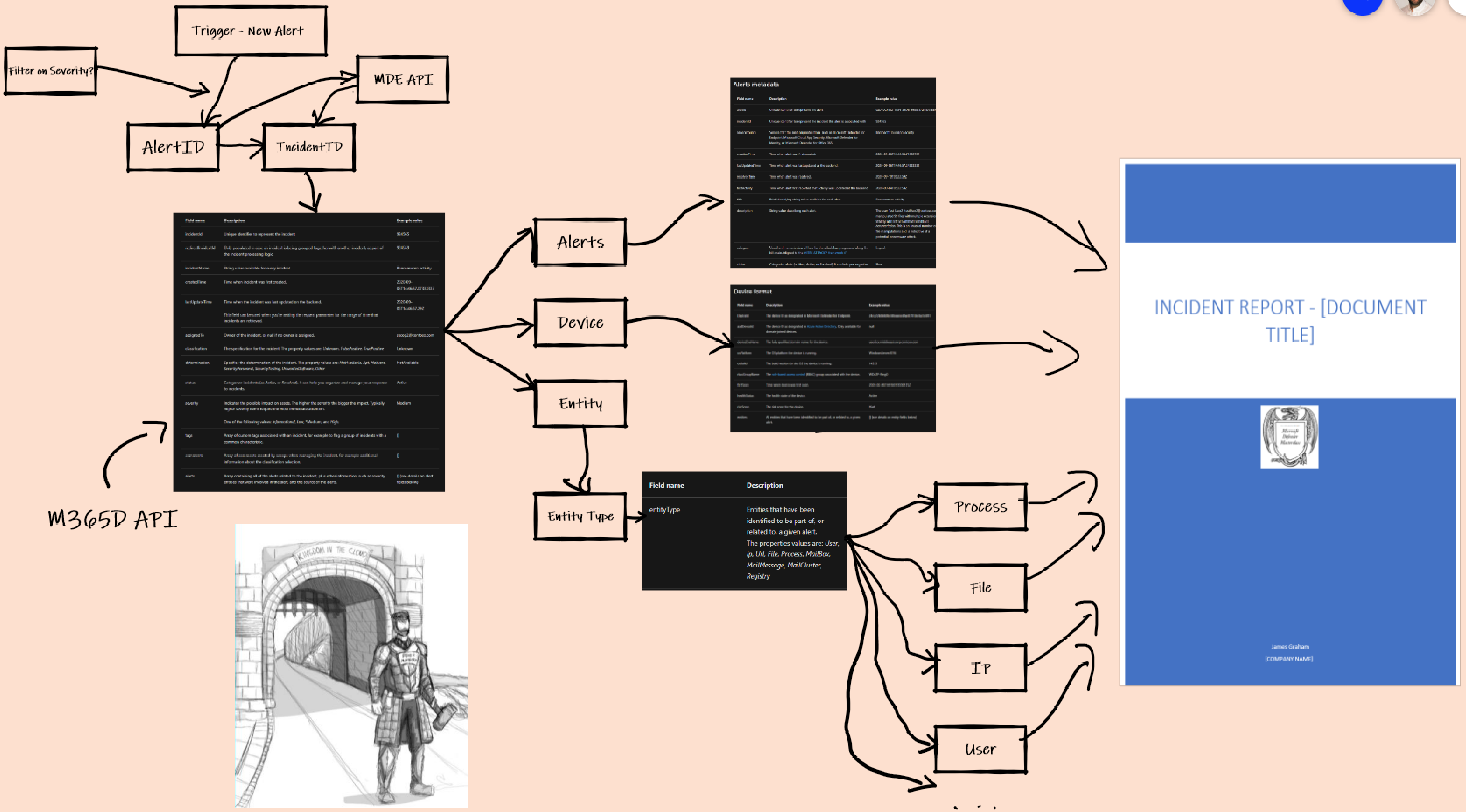
You will need:

1. Demo Tenant Access
2. Defender Masterclass 3 - Automated Incident Report Lab Guide

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




Trigger - New Alert
Filter on Severity?
MDE API
AlertID
IncidentID
M365D API
Alerts
Device
Entity
Entity Type
Alerts metadata
Device format
Field name
Description
entity type
Entities that have been identified to be part of, or related to, a given alert.
The properties values are: User, Ip, Url, File, Process, MailBox, MailMessage, MailCluster, Registry
Process
File
IP
User
INCIDENT REPORT - [DOCUMENT TITLE]
James Graham
[COMPANY NAME]
KINGDOM IN THE CLOUD

The Final Battle! Do you have the courage to Capture the Flag!

aka.ms/defendermasterclass4-reg

CALLING ALL DEFENDERS!

Microsoft Defender Masterclass IV

30TH JUNE 2021

SOLD OUT

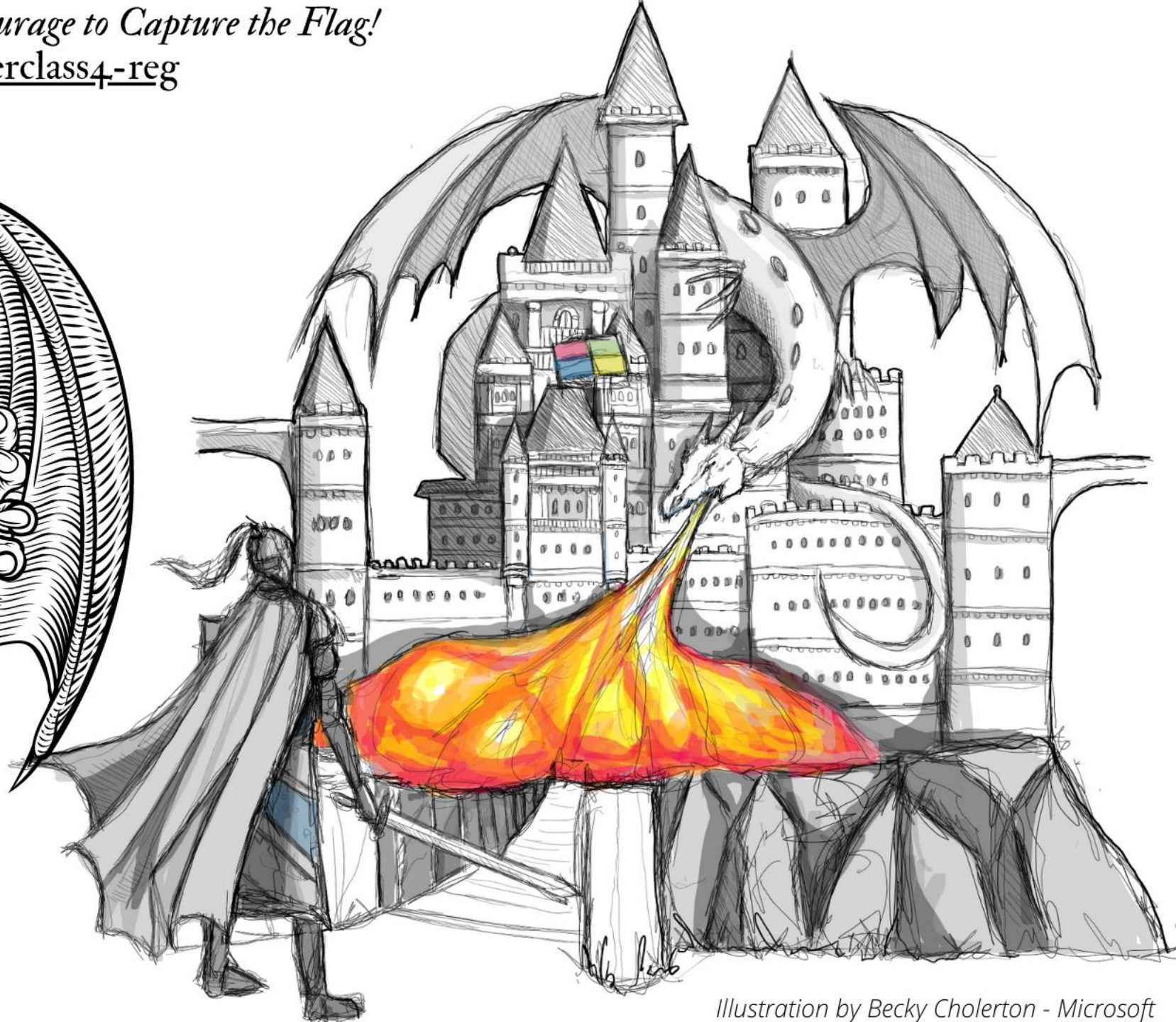
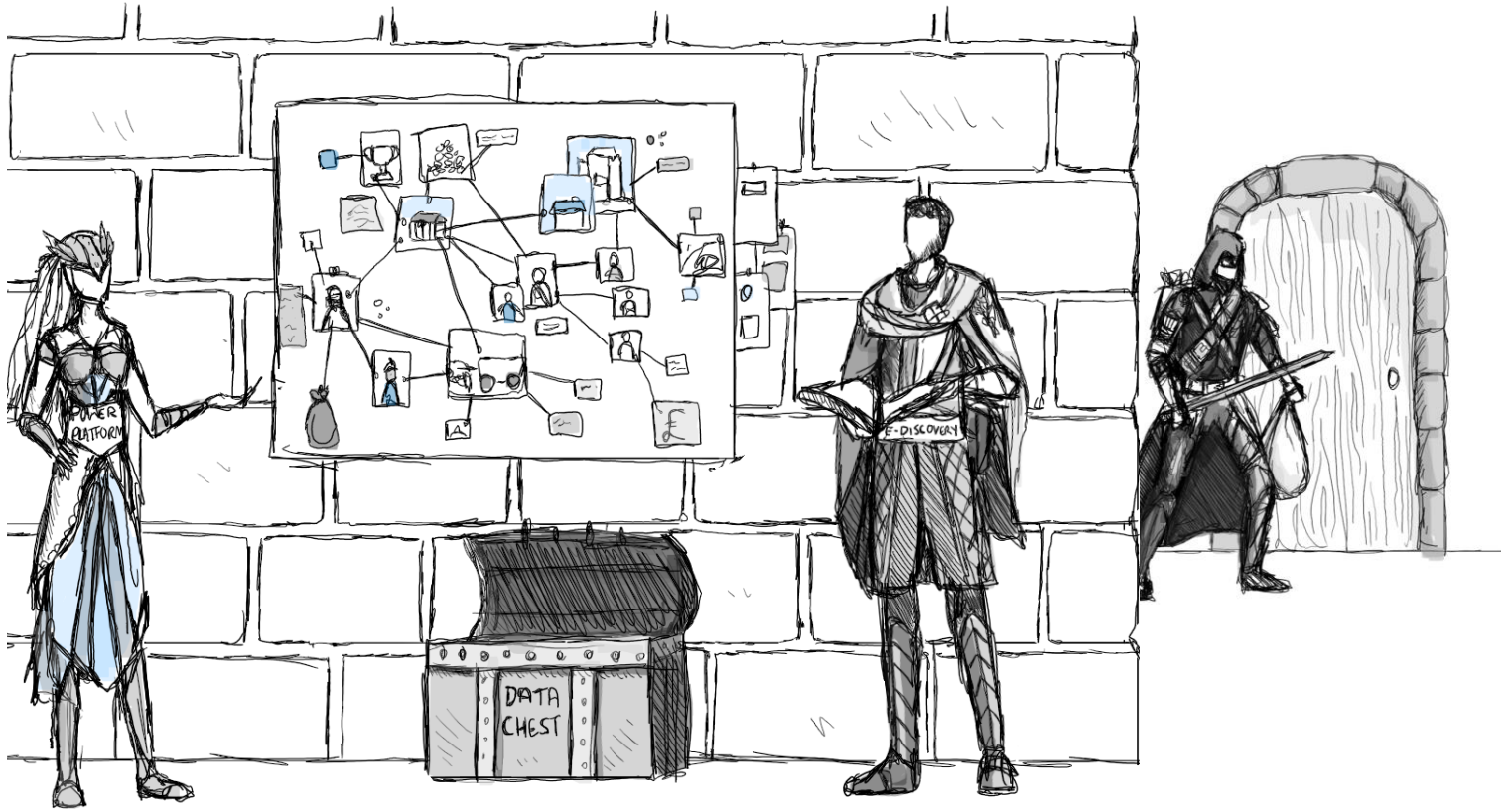


Illustration by Becky Cholerton - Microsoft

Compliance @ Speed Part 3 The Finale – 23rd June, 2021 9:30am – 1pm (British Summer Time)



Join the Microsoft Protectors for Part III at Speed. A 3.5 hour event, where we will build on what you learnt in Part I . More Compliance Platform demos across Microsoft 365 and Azure including:
eDiscovery , Azure Sentinel, Conditional Access, AIP Scanner, more Power Platform integrations+ API Intergrations

Illustrations by Becky Cholerton

Microsoft

Protectors.. .Register your bravery at aka.ms/complianceatspeed3-reg

aka.ms/defendermasterclass-ondemand

aka.ms/defendermasterclass-feedback

Thank you everyone!