Threat hunting with the Microsoft cloud

Tom Janetscheck

AZURE SATURDAY SPONSORS

SUPERADMINS

Microsoft | Development Center Serbia

atc | Admin Training Center

BEOtech

Payoneer GO BEYOND

EUROPEAN CLOUD SUMMIT

ITradar

NETOKRACIJA

C:\> CMD IT Solutions

AZUG SRBIJA

Coca-Cola

grand KAFA

about me.

Tom Janetscheck

Principal Cloud Security Architect with Devoteam Alegri

Focused on Cloud Security, IaaS, Azure Identity, and Governance

Microsoft® MVP Most Valuable Professional

Community Lead of Azure Meetup Saarbrücken

Co-founder and co-organizer of Azure Saturday

Tech blogger and book author

@azureandbeyond

https://blog.azureandbeyond.com

Agenda at a glance

- Cloud security challenges

  Why is cloud security so difficult and identity security so important?

- Azure Security Center

  Improve your hybrid cloud security posture

- Microsoft Intelligent Security Graph

  Unique insights, informed by trillions of signals

- Azure Sentinel

  SIEM/SOAR solution from the cloud

- Demo

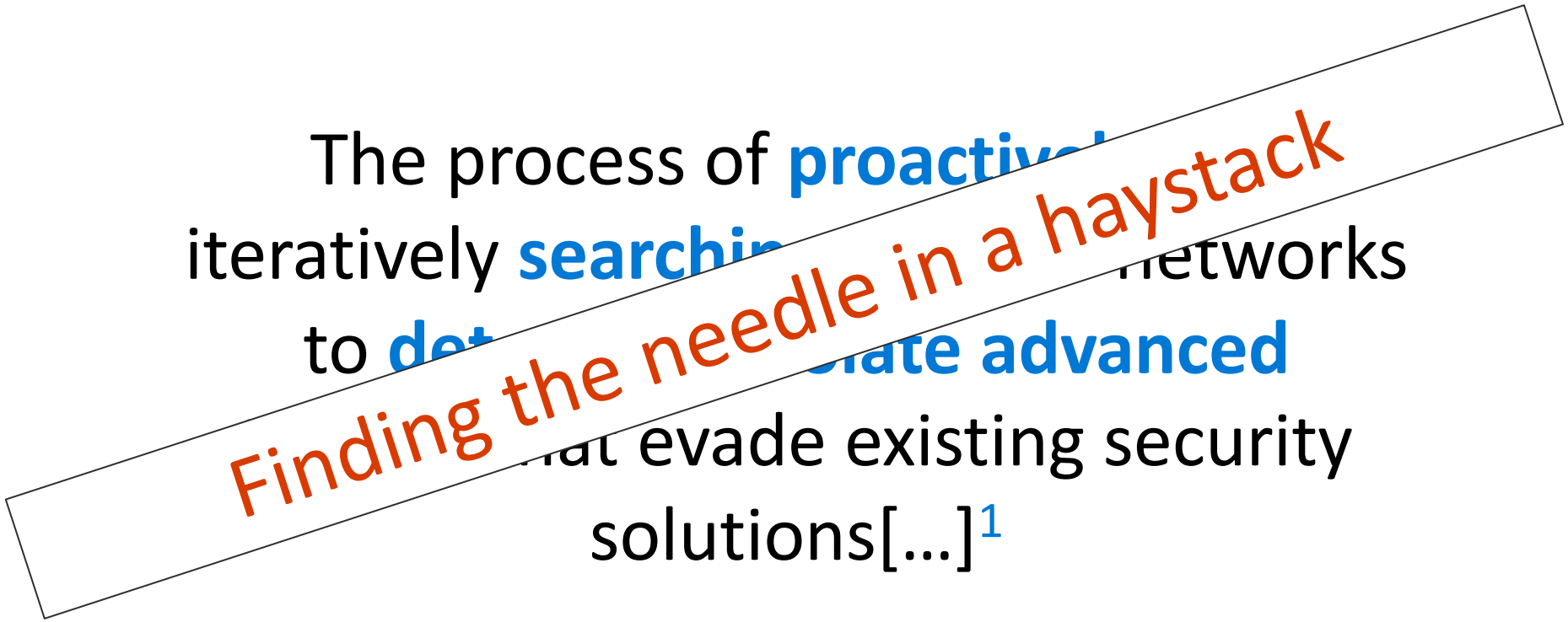
Governance – a definition

Establishment of **policies**, and continuous **monitoring** of their proper **implementation**, by the members of the governing body of an organization[…][1]

[1]Source: BusinessDictionary

Cyber Threat Hunting – a definition

The process of **proactiv** iteratively **searchin** networks to **det** **iate advanced** that evade existing security solutions[…][1]



[1]Source: TechRepublic

German federal criminal agency – 2018 cybercrime situation report

87.000 cases of cybercrime in 2018[1]

60.000.000 € amount of damage
with an immense dark figure[1]

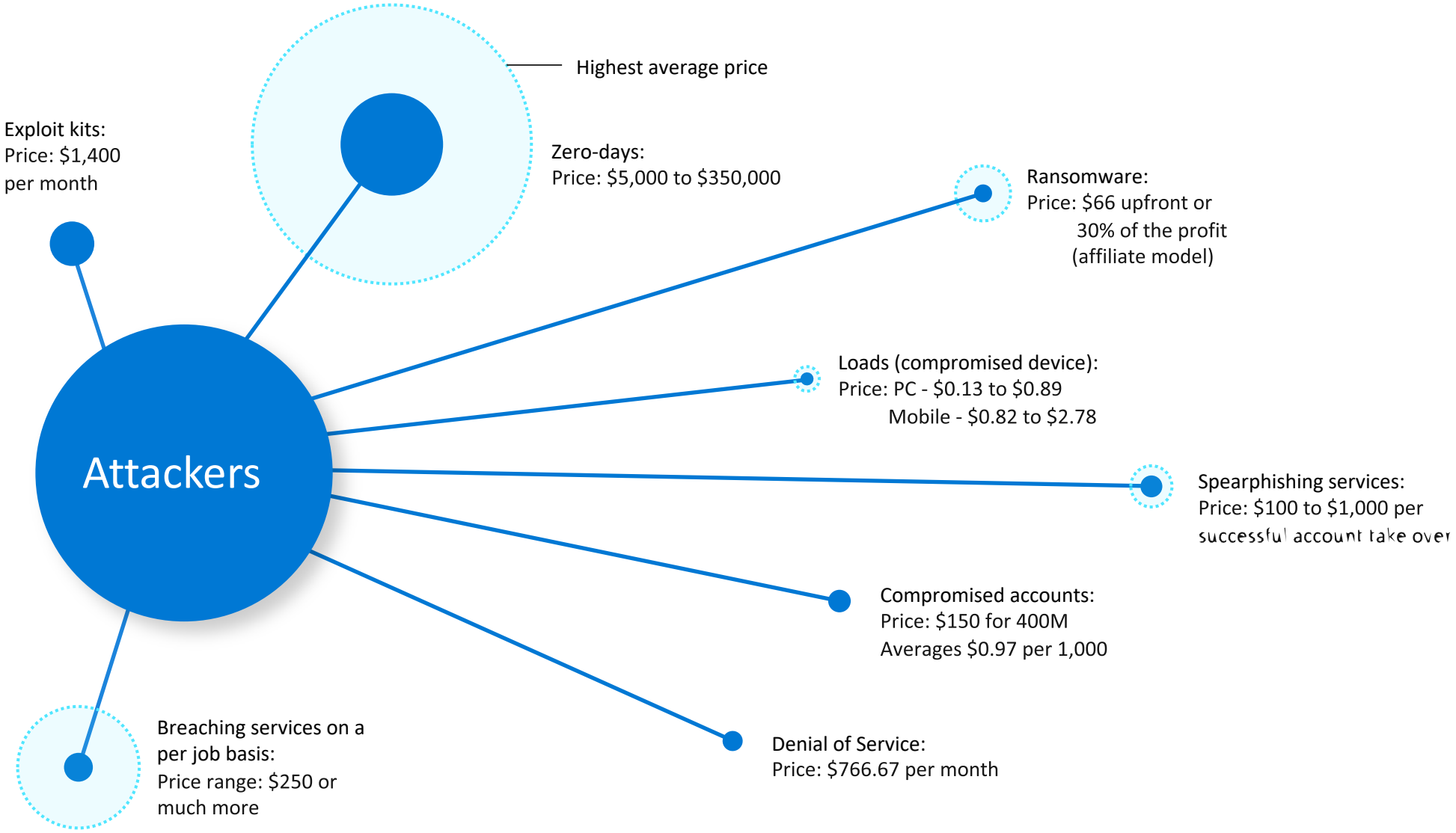
Estimated amount of damage according to
Bitkom: 43.300.000.000 (!) € per year[2]

[1] Source: BKA - 2018 Cybercrime situation report

[2] Source: Bitkom press release Oct 11, 2018

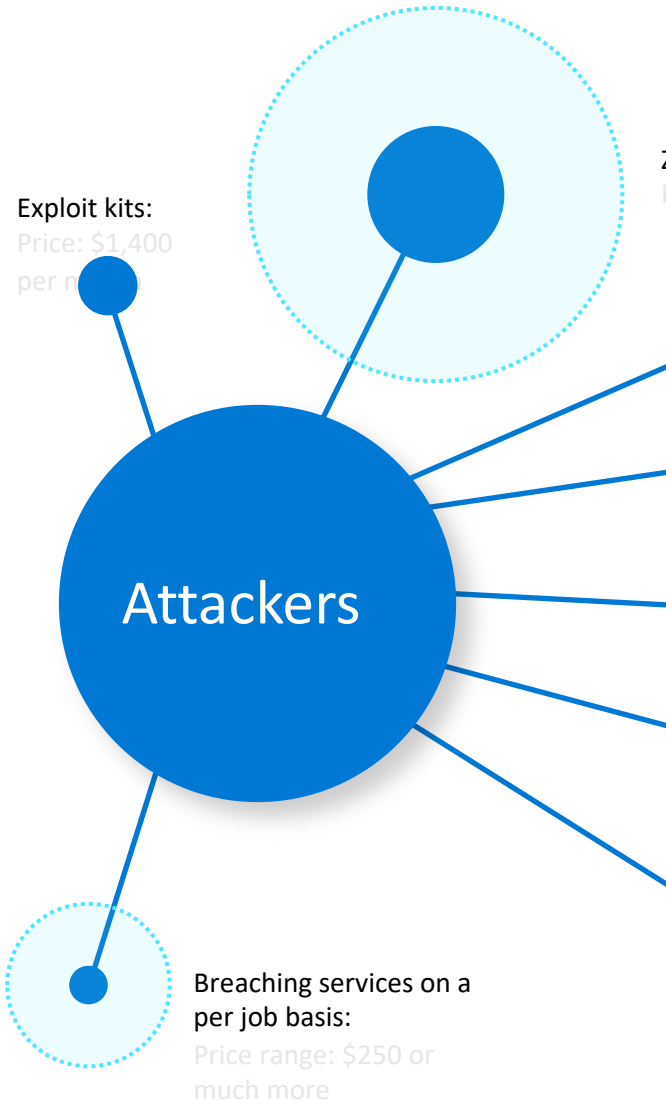
Attack services are cheap

More details at https://aka.ms/CISOWorkshop



Attack services are cheap

More details at https://aka.ms/CISOWorkshop



Zero-days:
Price: $5,000 to $350,000

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

Loads (compromised device):
Price: PC - $0.13 to $0.89
Mobile - $0.82 to $2.78

Spearphishing services:
Price: $100 to $1,000 per
successful account take over

Compromised accounts:

Denial of Service:
Price: $766.67 per month

FOCUS ON HYGIENE (NOT ZERO DAYS)

Zero day vulnerabilities are expensive and impractical for many attacks. https://aka.ms/CyberHygiene has guidance from Microsoft + NIST, the Center for Internet Security (CIS), and US DHS NCCIC (formerly US-CERT)

FOCUS ON MFA/PASSWORDLESS & ZERO TRUST

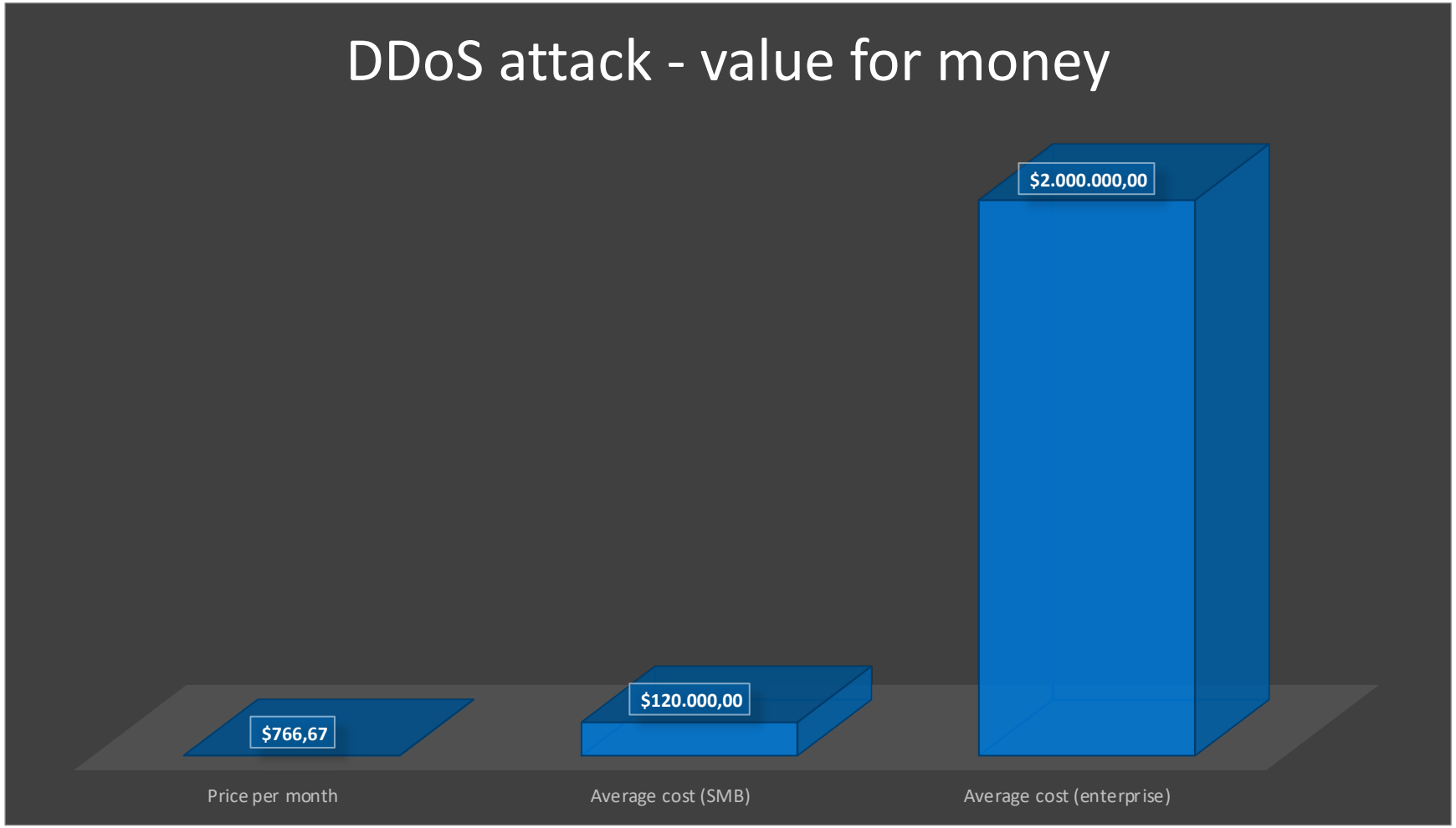
Attackers have moved to identity attacks like phishing and cred theft (which easily evade traditional network defenses)

Increase cost of these attacks starting with administrative privileges and other business critical assets

ENABLE DDoS PROTECTION FOR CRITICAL SERVICES

Ensure that your business-critical services have DDoS protection from Azure platform or a capable 3rd parties

DDoS Attacks – value for money



Source: Kaspersky Lab Research Report 02/2018

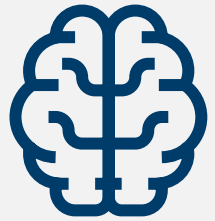
Today‘s cloud security challenges

Rapidly changing workloads

It’s both, a strength and a challenge of the cloud. How do you make sure that ever-changing services are up to your security standards?

Increasingly sophisticated attacks

Attack automation and evasion techniques are evolving along multiple dimensions



Security skills are on short supply

We need human expertise, adaptability, and creativity to combat human threat actors.

Identity protection is essential!

Use passphrases rather than (complex) passwords or go password-less

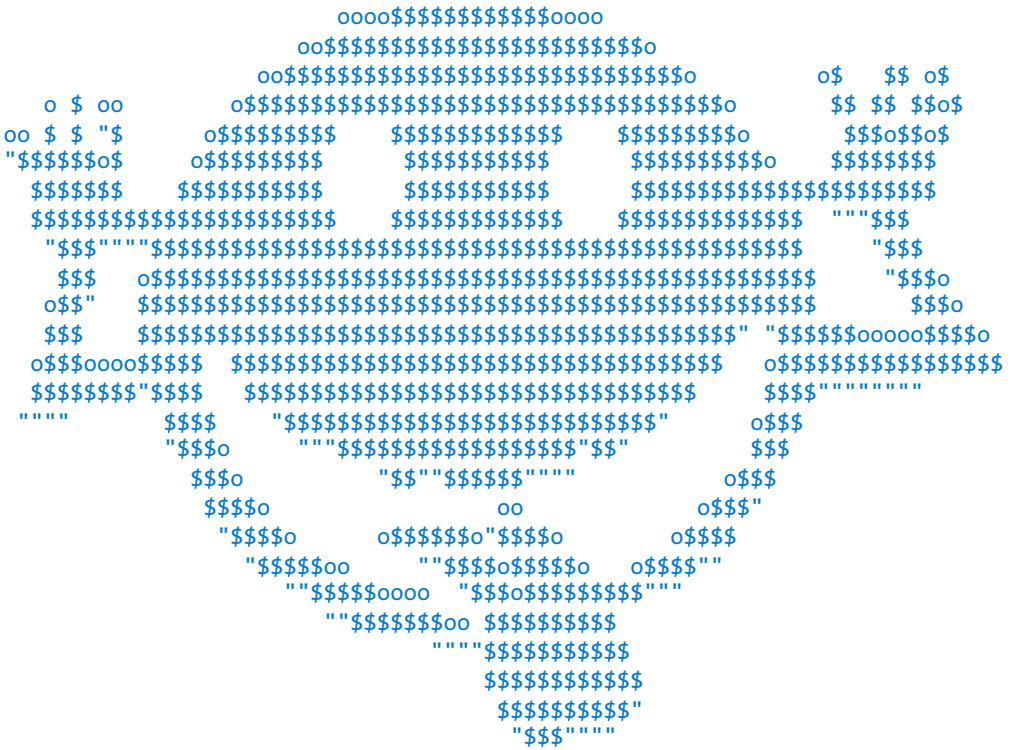
Implement multi-factor authentication

Adhere to the principle of least privilege

Establish privileged identity/access management (PIM/PAM)

Enable conditional access policies

Identity protection is essential!



Microsoft Azure Security Center

Strengthen hybrid security posture

Security Center assesses your environment and enables you to understand the status of your resources, and whether they are secure.

Adaptive threat prevention

Enable actionable, adaptive protections that identify and mitigate risk to reduce exposure to attacks

Intelligent detection and response

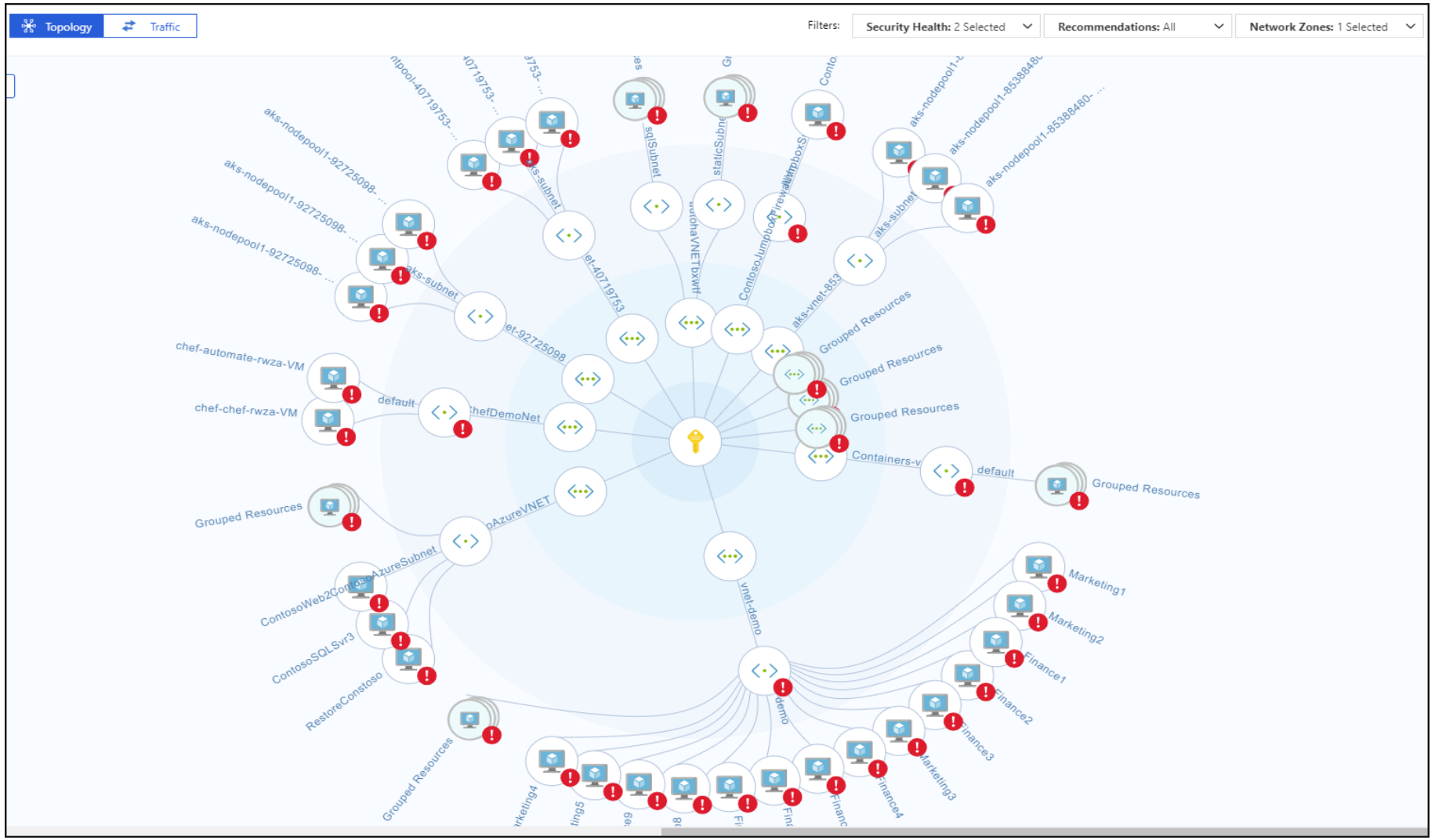
Use advanced analytics and Microsoft Intelligent Security Graph to rapidly detect and respond to evolving cyber threats

Strengthen your security posture

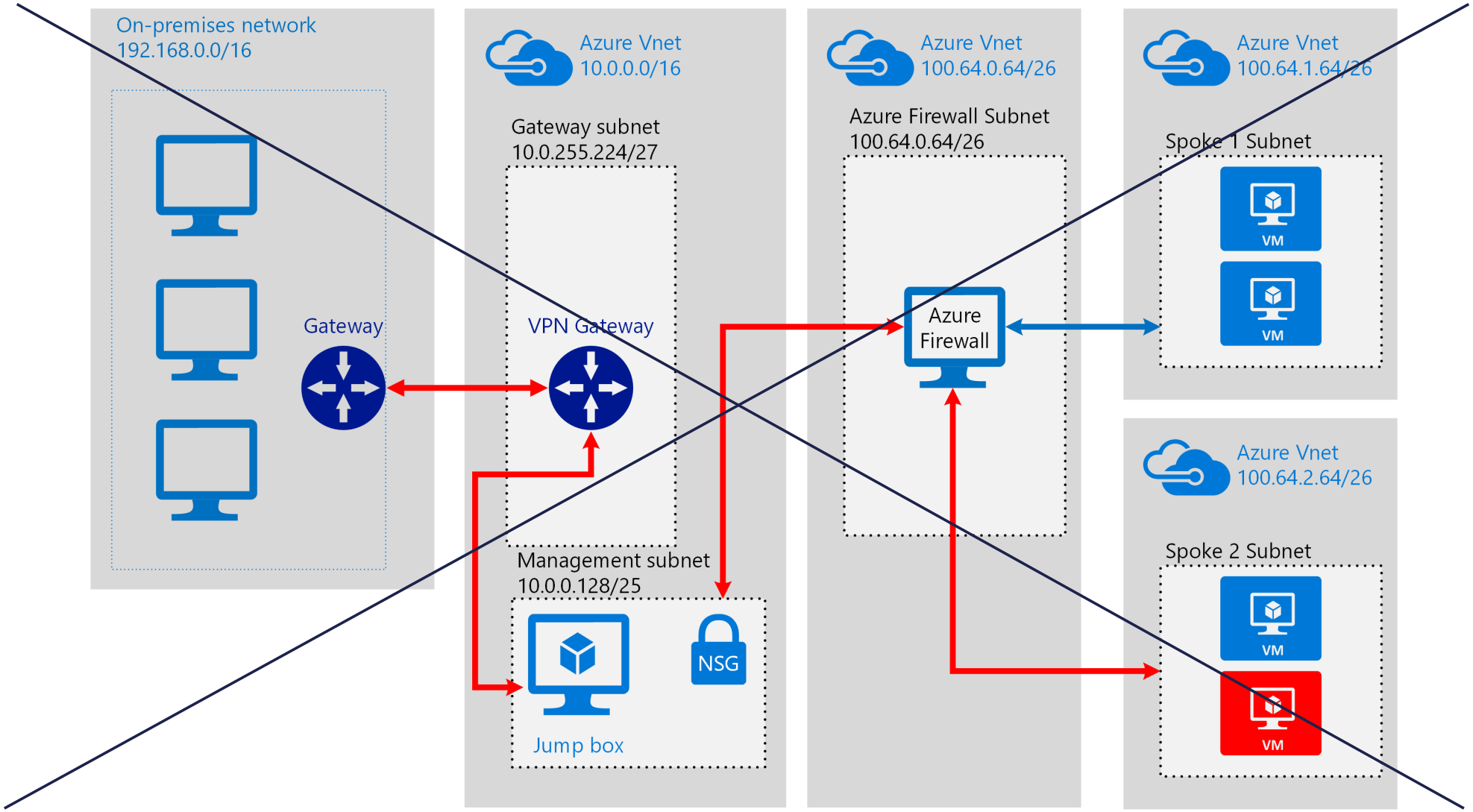
Identify shadow IT subscriptions

Optimize and improve resource security

Continous assessments



Recognize configuration issues



Microsoft Azure Security Center

Strengthen hybrid security posture

Security Center assesses your environment and enables you to understand the status of your resources, and whether they are secure.

Adaptive threat prevention

Enable actionable, adaptive protections that identify and mitigate risk to reduce exposure to attacks

Intelligent detection and response

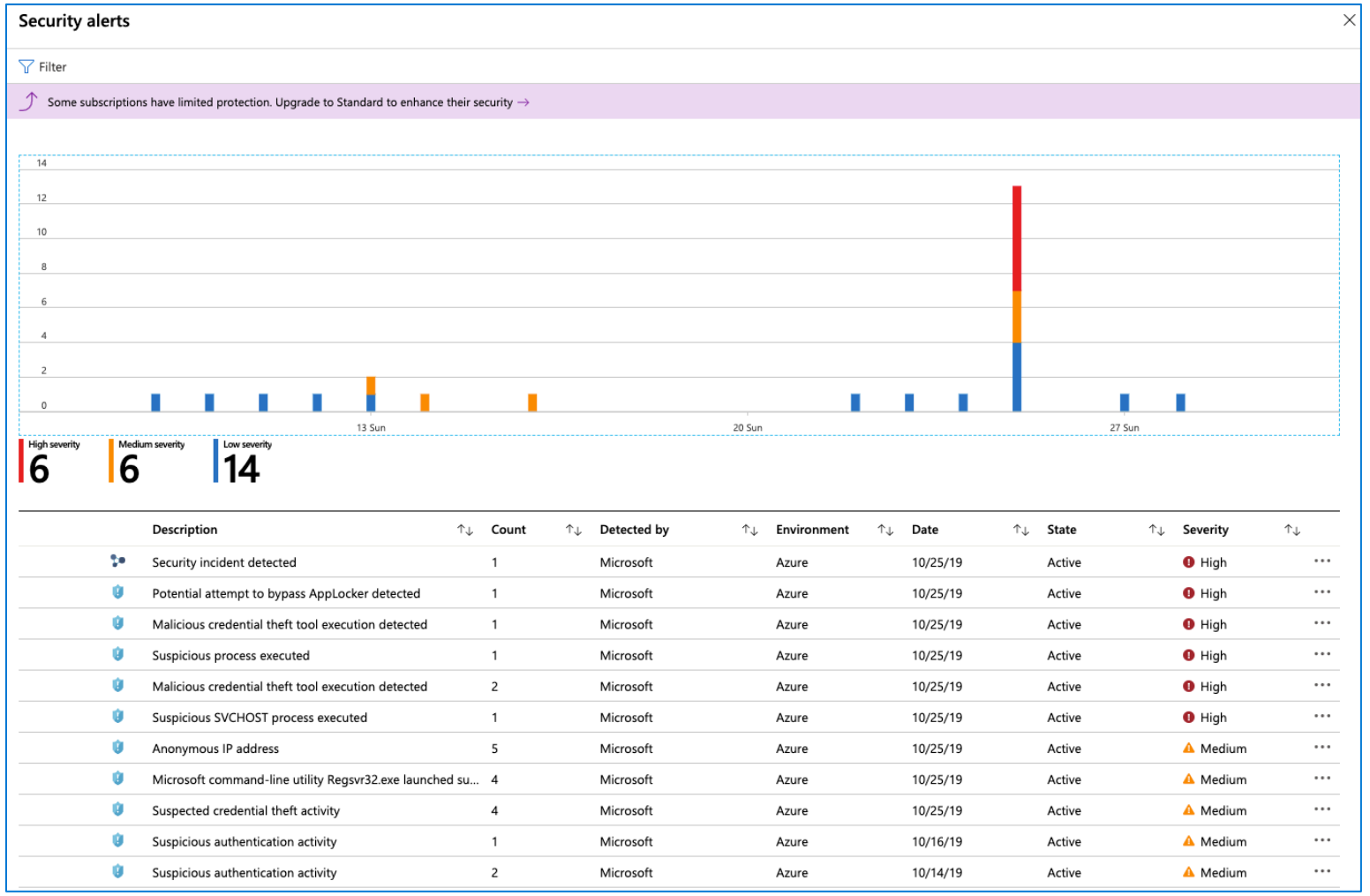
Use advanced analytics and Microsoft Intelligent Security Graph to rapidly detect and respond to evolving cyber threats

Adaptive threat prevention

Advanced Threat Protection

Native integration with Microsoft Defender ATP for Windows machines

Advanced Thread Detection for Linux machines



Microsoft Azure Security Center

Strengthen hybrid security posture

Security Center assesses your environment and enables you to understand the status of your resources, and whether they are secure.

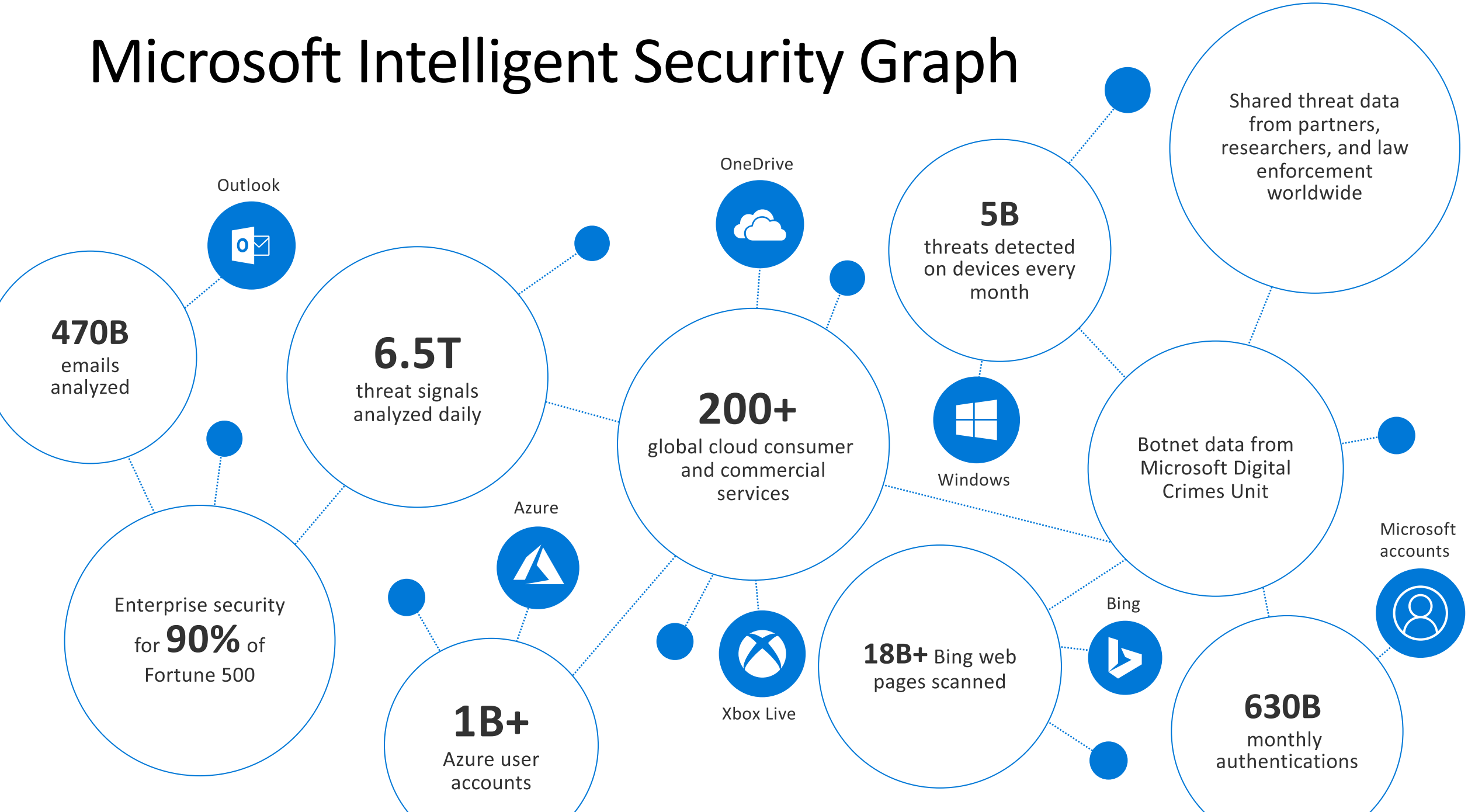
Adaptive threat prevention

Enable actionable, adaptive protections that identify and mitigate risk to reduce exposure to attacks

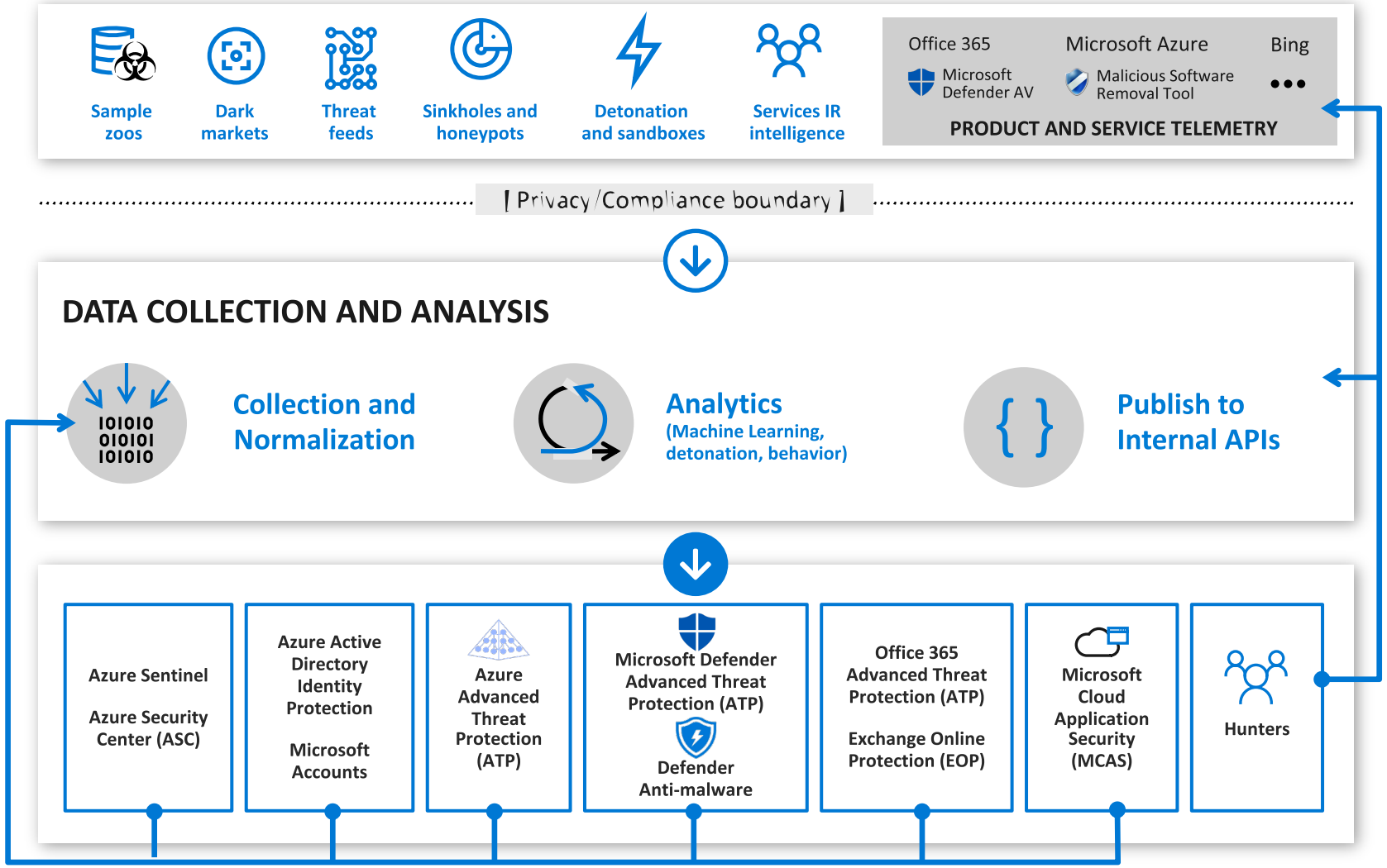
Intelligent detection and response

Use advanced analytics and Microsoft Intelligent Security Graph to rapidly detect and respond to evolving cyber threats

Microsoft Intelligent Security Graph



Inside the Intelligent Security Graph



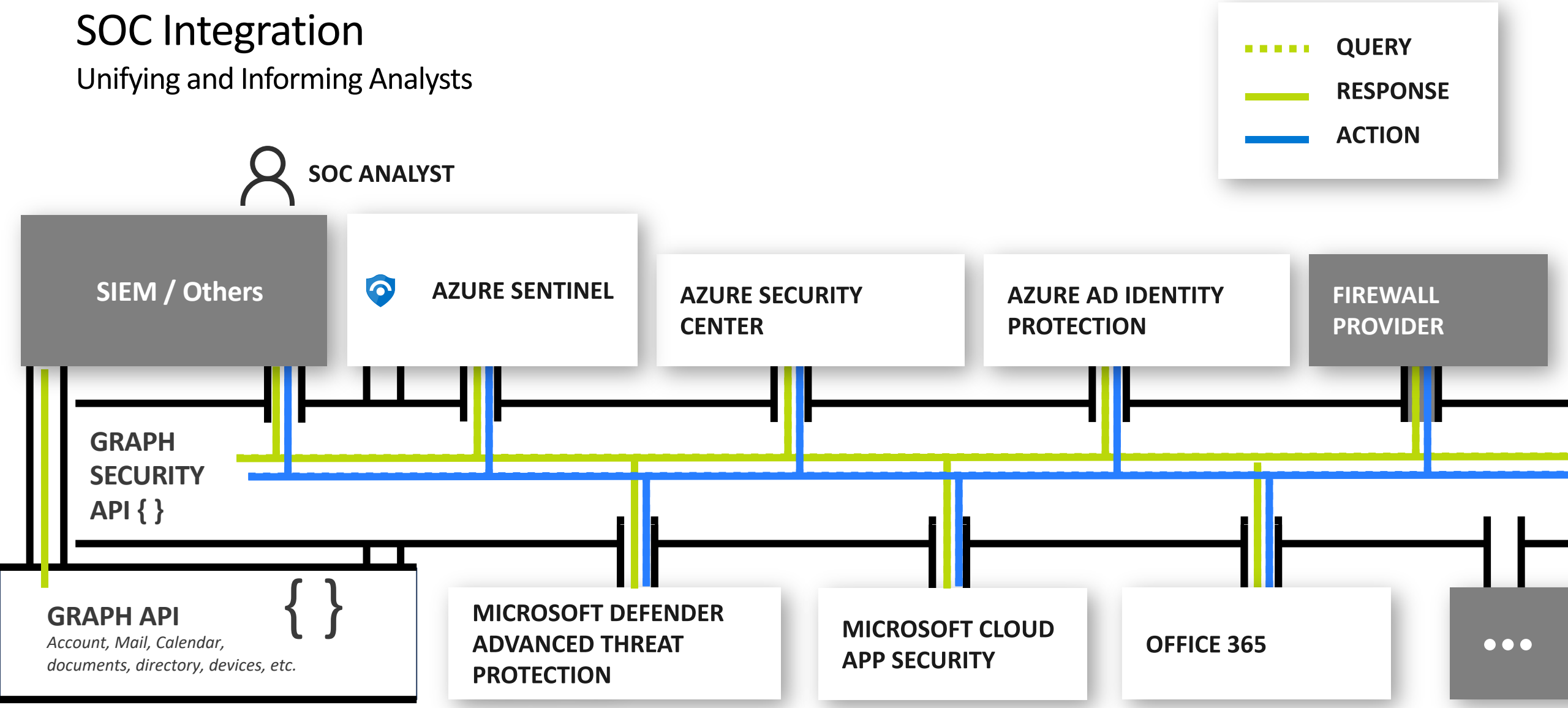
- Products instrumented to strict privacy/compliance standards

  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

SOC Integration

Unifying and Informing Analysts



http://aka.ms/graphsecurityapi | https://aka.ms/graphsecuritydocs

AZURE SENTINEL

Core capabilities

Collect

Microsoft Services

Apps, users, infrastructure

Public Clouds

Security solutions

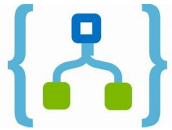
Analyze & detect threats

Machine learning, UEBA

Investigate & hunt suspicious activities

Interactive Attack Visualization, Azure Notebooks

Automate & orchestrate response



Playbooks

Enrichment with Intelligence (Geo location, IP Reputation)

Data Ingestion

Data Repository

Data Search

Azure Monitor (Log Analytics)

Integrate

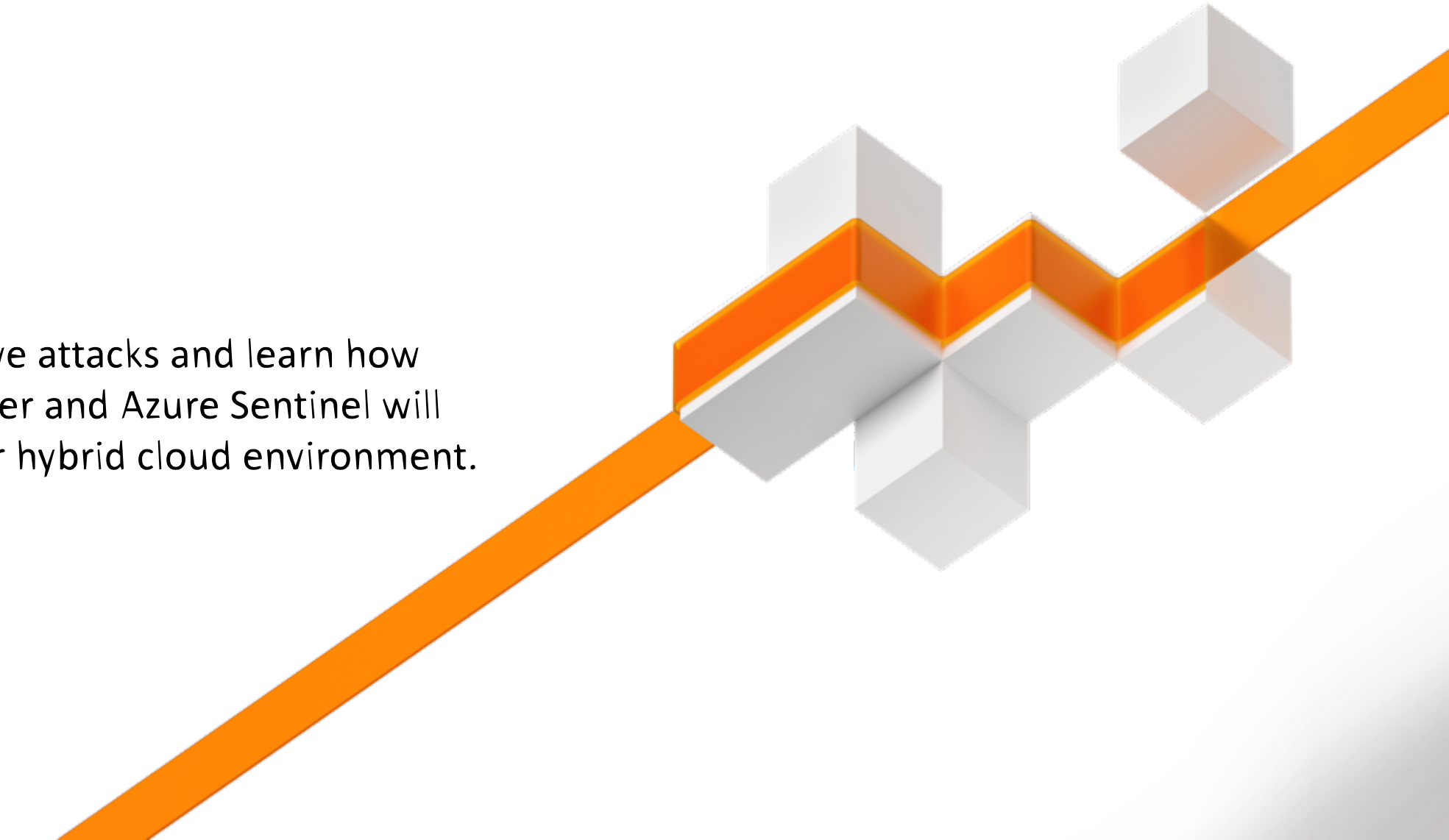
ServiceNow

Other tools

Community

Demo

Witness on-stage live attacks and learn how Azure Security Center and Azure Sentinel will help to protect your hybrid cloud environment.



Take aways

1

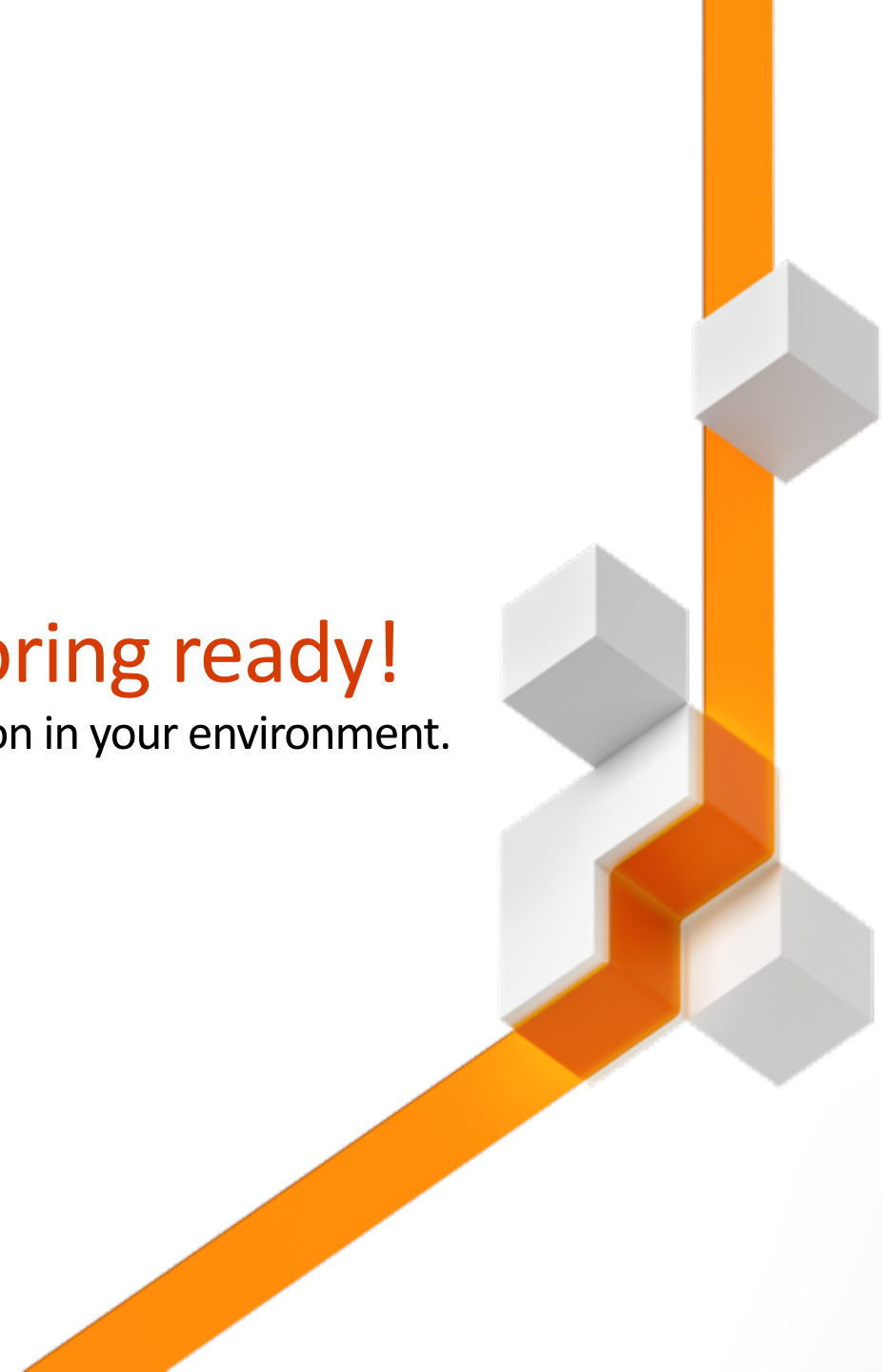
Assume breach!

It’s not a question about the “if”, but about the “when”!

2

Have your monitoring ready!

You need to know what's going on in your environment.
Massive telemetry is necessary!



3

Leverage AI/ML-based security tools!

Human security skills are on short supply so make sure you rely on an intelligent cloud service!

Microsoft