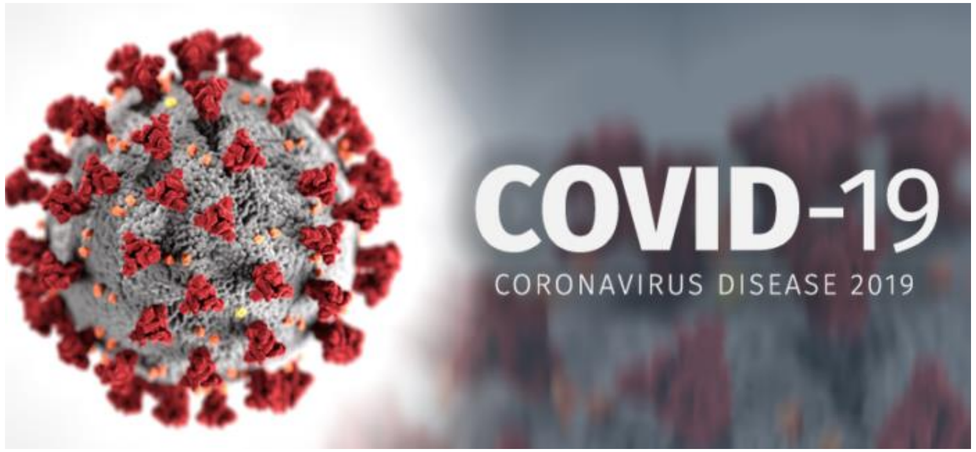
Microsoft Security HKT Enterprise Solutions

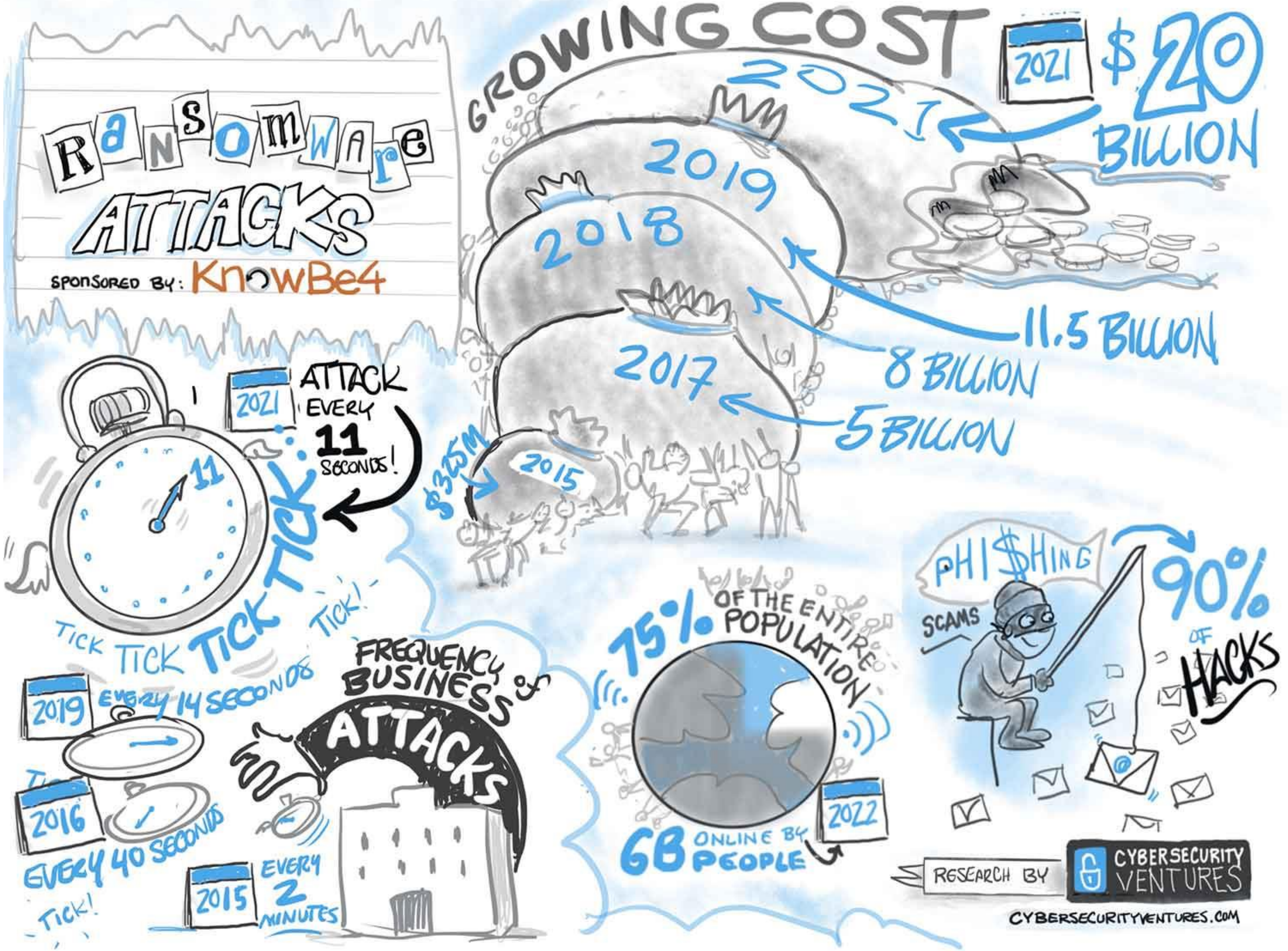
MODERNIZE SECURITY AND DEFEND AGAINST THREATS

Speaker:

Patric Wu – Microsoft Cloud Solution Architect (Security)
Ken Lam – Assistant Vice President (Security Business, HKT)

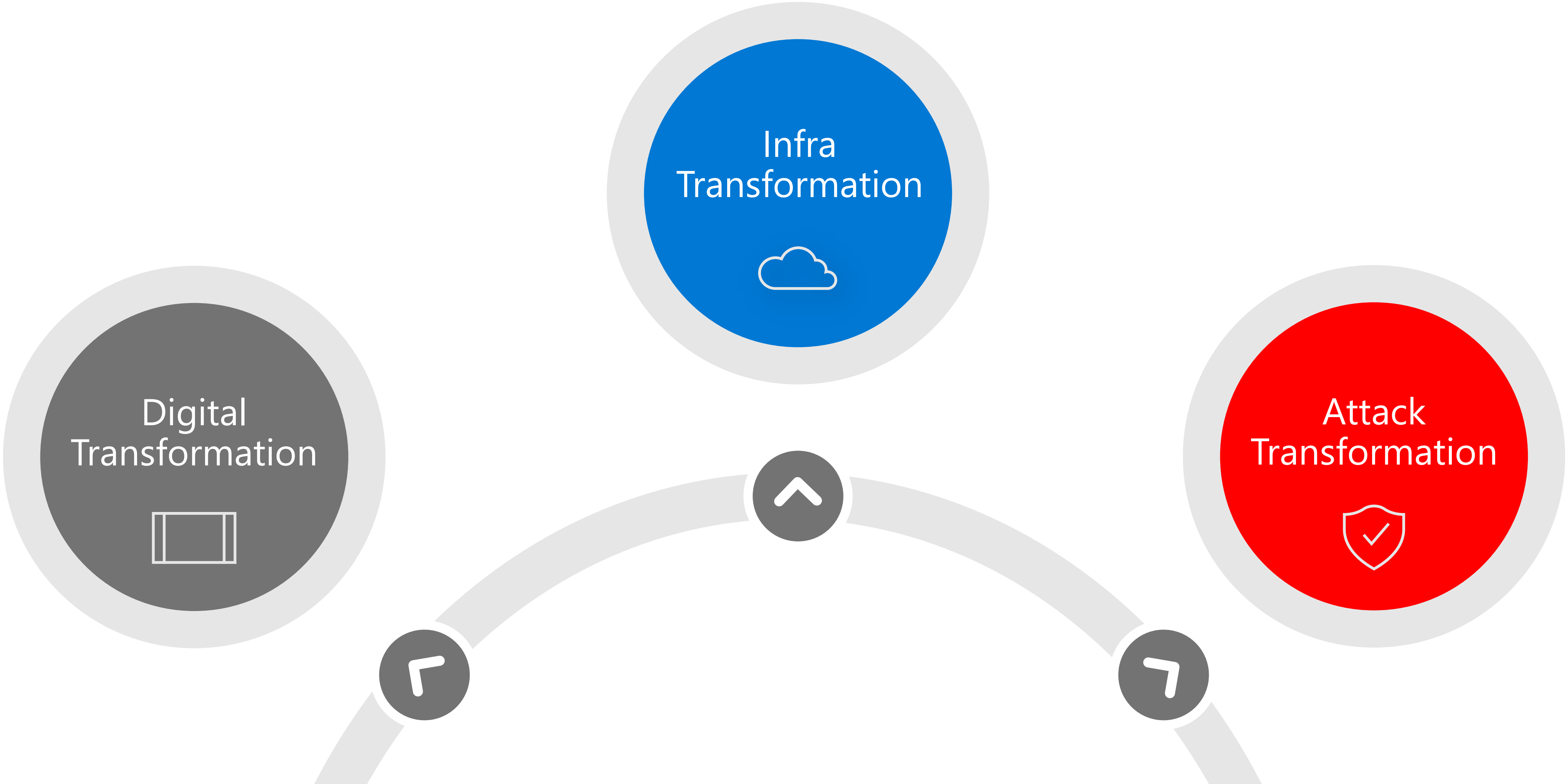
Questions before we start




RANSOMWARE
ATTACKS
SPONSORED BY: KnowBe4
GROWING COST
2021 $20 BILLION
2021
2019
2018
2017
2015
$325M
11.5 BILLION
8 BILLION
5 BILLION
2021 ATTACK EVERY 11 SECONDS!
11
TICK TICK TICK TICK TICK! TICK!
2019 EVERY 14 SECONDS
2016 EVERY 40 SECONDS
2015 EVERY 2 MINUTES
FREQUENCY of BUSINESS ATTACKS
75% OF THE ENTIRE POPULATION
6B ONLINE BY PEOPLE
2022
PHI$HING
SCAMS
90% OF HACKS
RESEARCH BY CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

NOW
HIRING!
PETSMART
PETSMART
PETSMART
PETSMART
PETSMART

The era of transformation



Infra Transformation

Digital Transformation

Attack Transformation

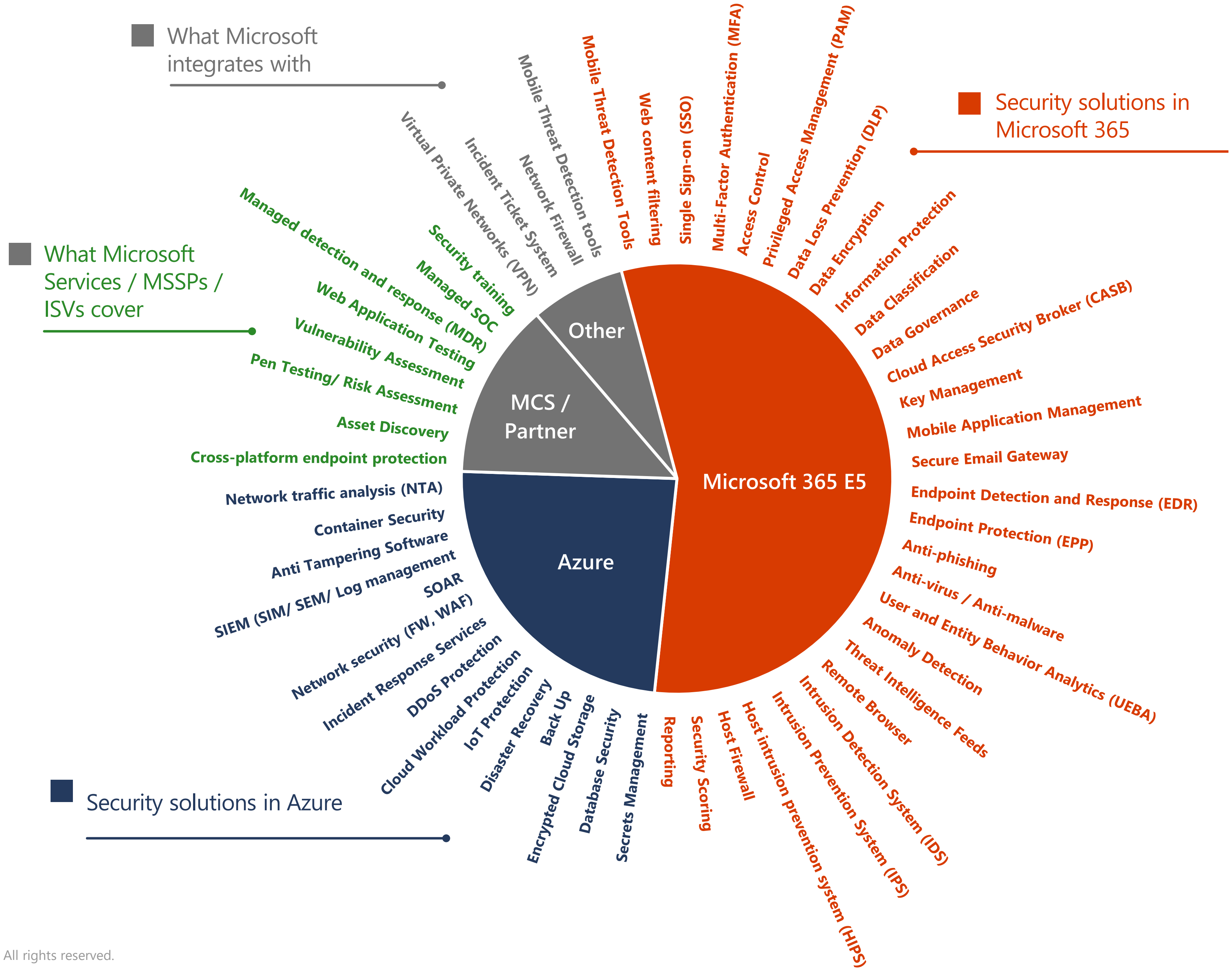
Security Tsunami Is Coming

Attacks are increasing in **impact and sophistication**

Existing security tools are not designed for **multi-cloud and hybrid**

Volume of signal and tooling complexity is **overwhelming**

Microsoft
Security



■ What Microsoft integrates with

Virtual Private Networks (VPN)
Incident Ticket System
Network Firewall
Mobile Threat Detection tools

■ Security solutions in Microsoft 365

Mobile Threat Detection Tools
Web content filtering
Single Sign-on (SSO)
Multi-Factor Authentication (MFA)
Access Control
Privileged Access Management (PAM)
Data Loss Prevention (DLP)
Data Encryption
Information Protection
Data Classification
Data Governance
Cloud Access Security Broker (CASB)
Key Management
Mobile Application Management
Secure Email Gateway
Endpoint Detection and Response (EDR)
Endpoint Protection (EPP)
Anti-phishing
Anti-virus / Anti-malware
User and Entity Behavior Analytics (UEBA)
Anomaly Detection
Threat Intelligence Feeds
Remote Browser
Intrusion Detection System (IDS)
Intrusion Prevention System (IPS)
Host intrusion prevention system (HIPS)
Host Firewall
Security Scoring
Reporting

■ Security solutions in Azure

Secrets Management
Database Security
Encrypted Cloud Storage
Back Up
Disaster Recovery
IoT Protection
Cloud Workload Protection
DDoS Protection
Incident Response Services
Network security (FW, WAF)
SOAR
SIEM (SIM/ SEM/ Log management
Anti Tampering Software
Container Security
Network traffic analysis (NTA)

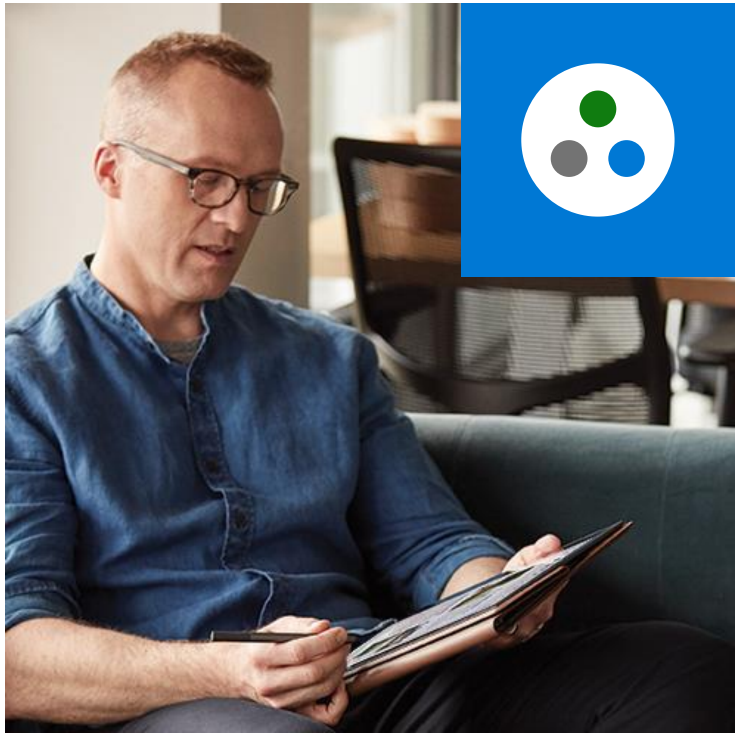
■ What Microsoft Services / MSSPs / ISVs cover

Cross-platform endpoint protection
Asset Discovery
Pen Testing/ Risk Assessment
Vulnerability Assessment
Web Application Testing
Managed detection and response (MDR)
Managed SOC
Security training

Transforming security: the Microsoft approach

Deliver rapid, intelligent results

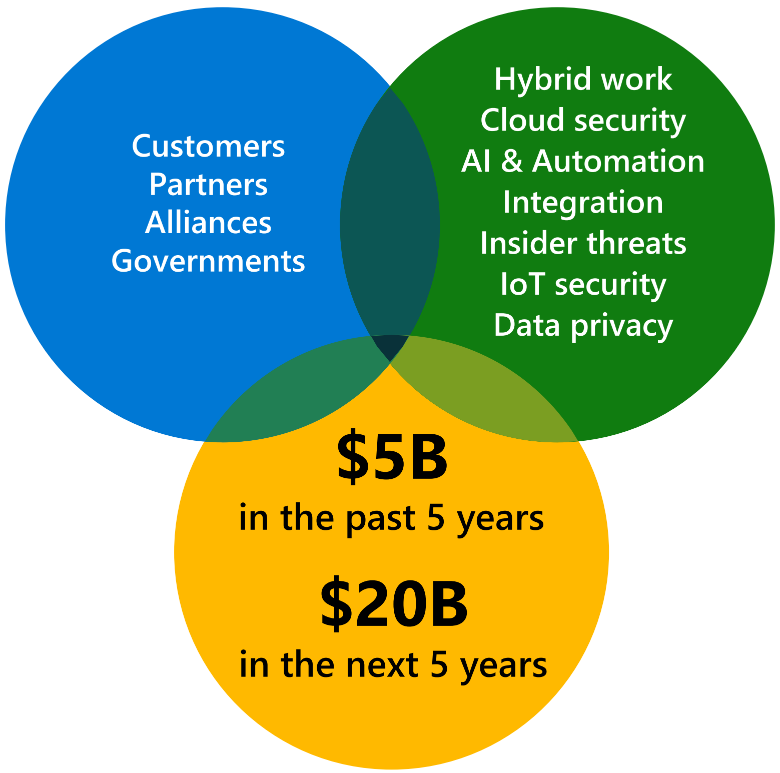
Integrate your security tools



Secure all clouds, all platforms

We’re investing where security is going

To help you keep pace with change



Our world

Customers
Partners
Alliances
Governments

Trends

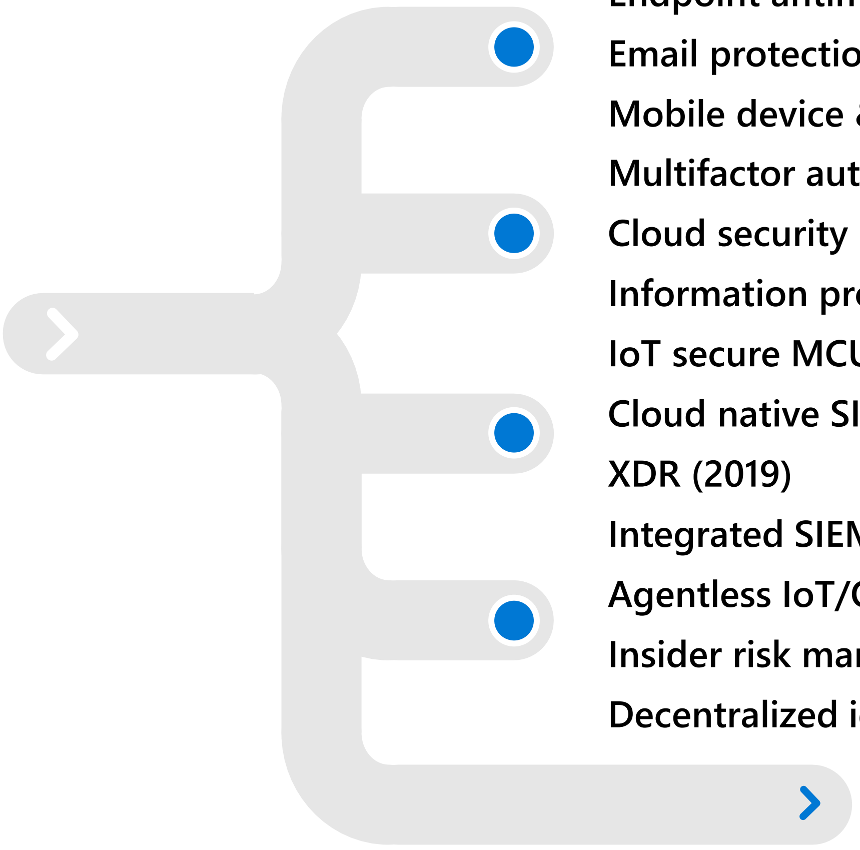
Hybrid work
Cloud security
AI & Automation
Integration
Insider threats
IoT security
Data privacy

$5B
in the past 5 years

$20B
in the next 5 years

R&D Investment

Continual innovation



- Endpoint antimalware (2004)
- Email protection (2005)
- Mobile device & application management (2010)
- Multifactor authentication (2013)
- Cloud security (2015)
- Information protection and governance (2015)
- IoT secure MCU (2018)
- Cloud native SIEM (2019)
- XDR (2019)
- Integrated SIEM and XDR (2020)
- Agentless IoT/OT security monitoring (2020)
- Insider risk management (2020)
- Decentralized identity (2021)

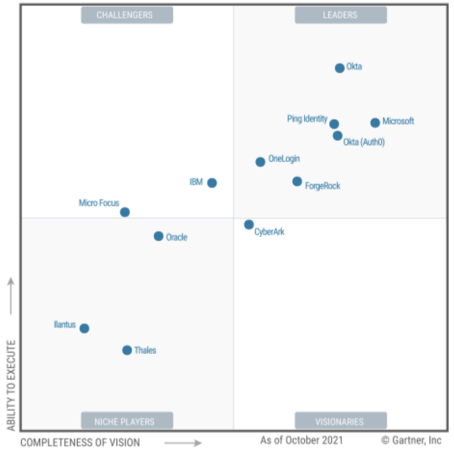
many more to come…

Gartner®

Microsoft Security— a Leader in 5 Gartner Magic Quadrant reports

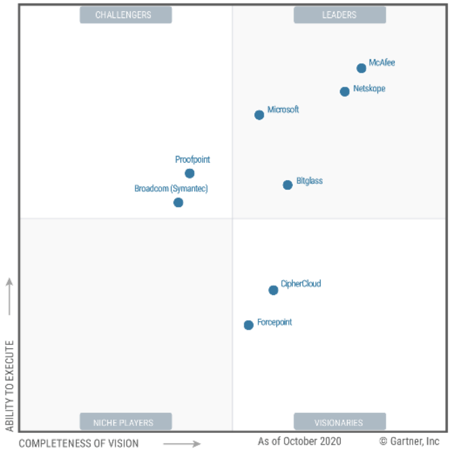
*Gartner "Magic Quadrant for Access Management," by Henrique Teixeira, Abhyuday Data, Michael Kelley, November 2021
*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Craig Lawson, Steve Riley, October 2020
*Gartner "Magic Quadrant for Enterprise Information Archiving," by Michael Hoech, Jeff Vogel, October 2020
*Gartner "Magic Quadrant for Endpoint Protection Platforms," by Paul Webber, Rob Smith, Prateek Bhajanka, Mark Harris, Peter Firstbrook, May 2021
*Gartner "Magic Quadrant for Unified Endpoint Management," by Dan Wilson, Chris Silva, Tom Cipolla, August 2021

These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

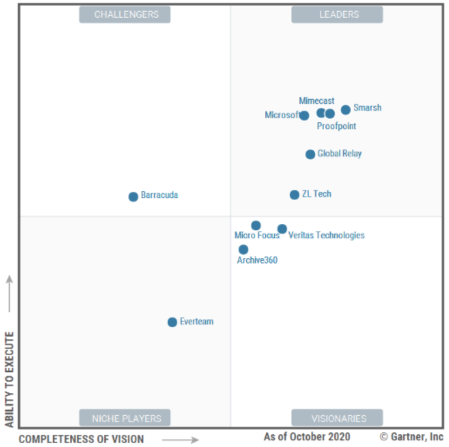


Source: Gartner (November 2021)

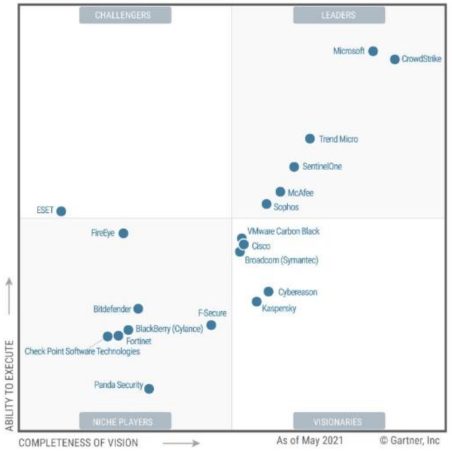
Access Management



Cloud Access Security Brokers

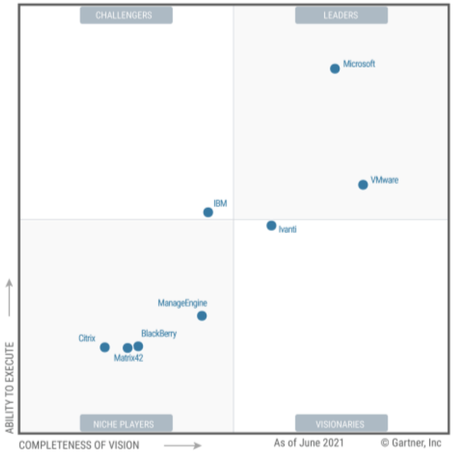


Enterprise Information Archiving



Source: Gartner (May 2021)

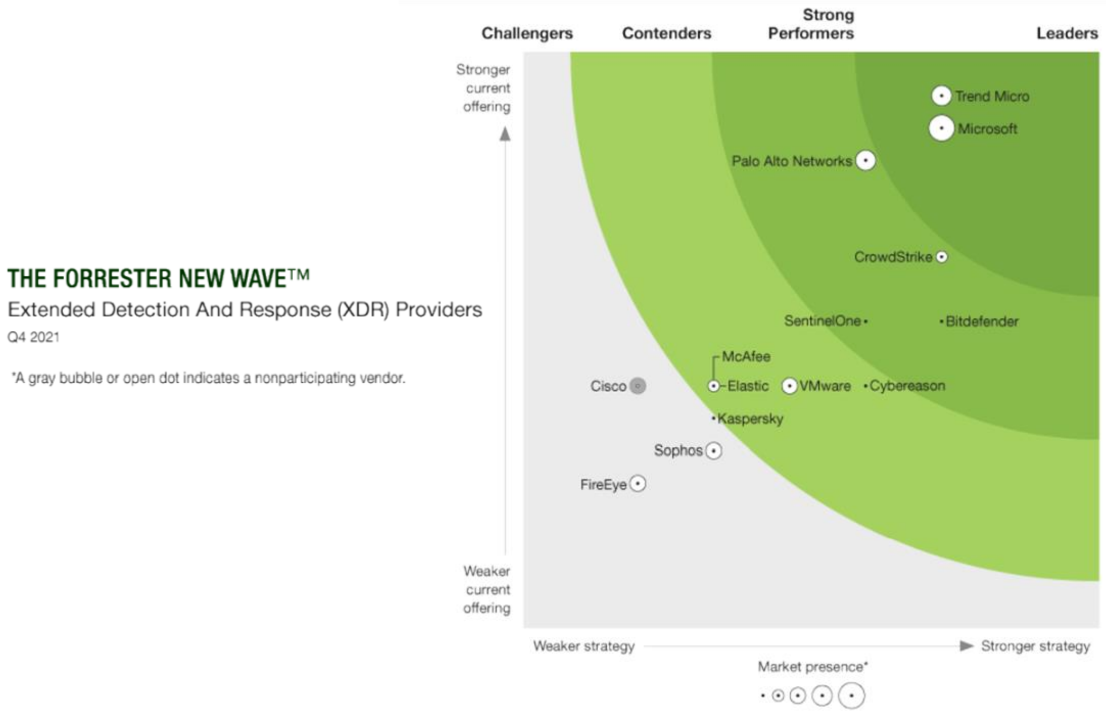
Endpoint Protection Platforms



Source: Gartner (August 2021)

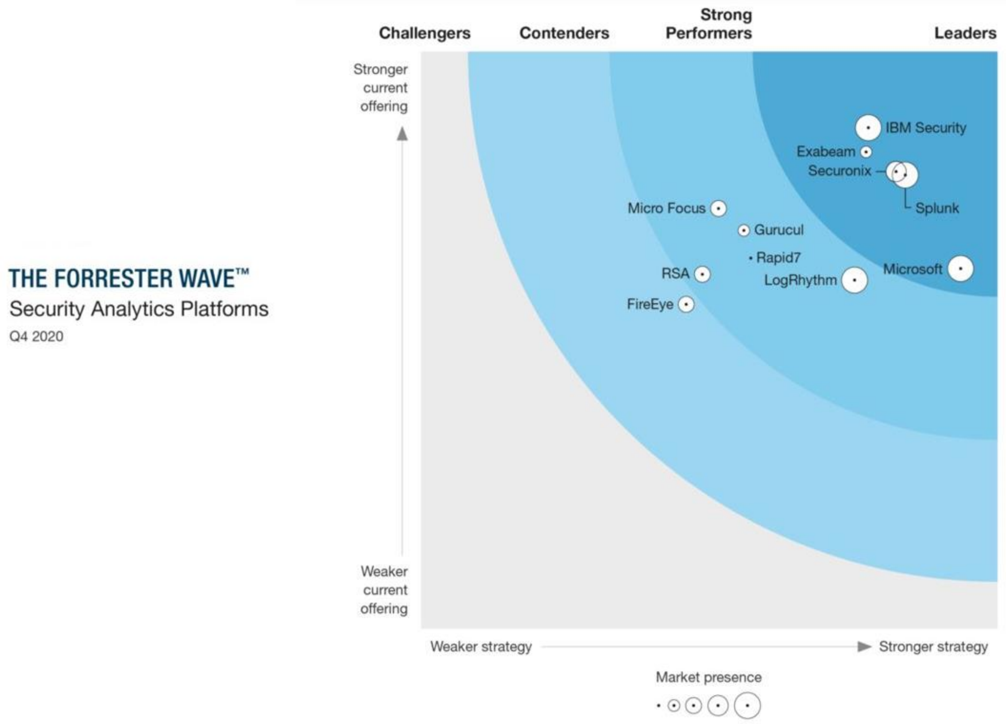
Unified Endpoint Management

Industry recognition for SIEM and XDR solution



Microsoft achieves a Leader placement in the Forrester New Wave, Extended Detection and Response (XDR) Providers

The Forrester New Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of Forrester's call on a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester New Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.



Azure Sentinel achieves a Leader placement in The Forrester Wave™: Security Analytics Platform Providers, Q4 2020

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Protection aligned to where you're going

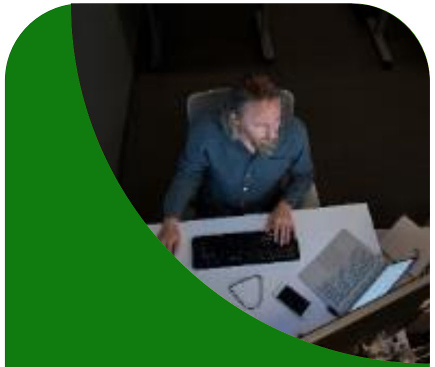
Solutions to support your digital journey

Identity and access management

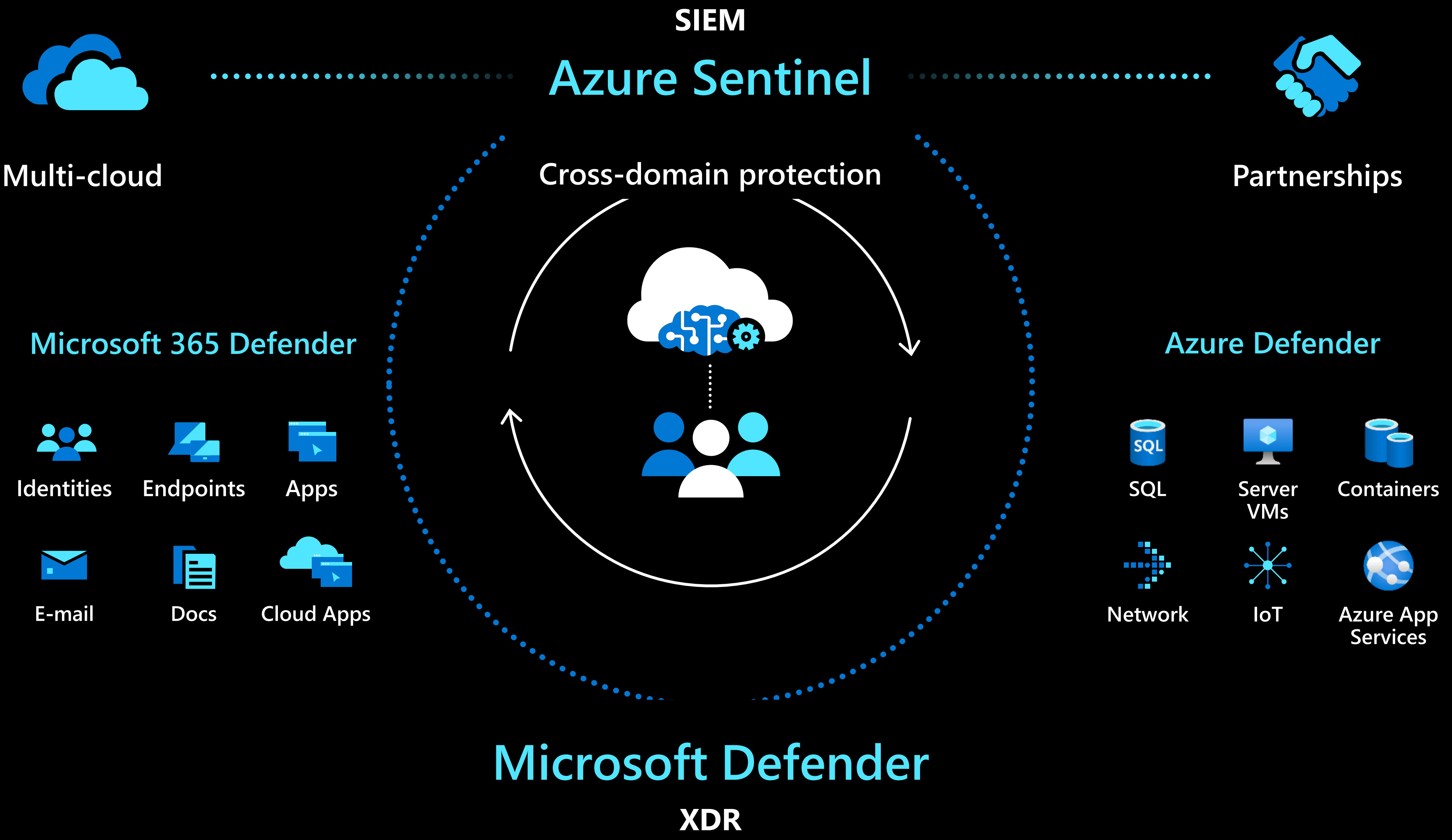
Threat protection

Cloud security

Information protection and governance



Risk management



SIEM

Azure Sentinel

Multi-cloud

Partnerships

Cross-domain protection

Microsoft 365 Defender

Identities

Endpoints

Apps

E-mail

Docs

Cloud Apps

Azure Defender

SQL

Server VMs

Containers

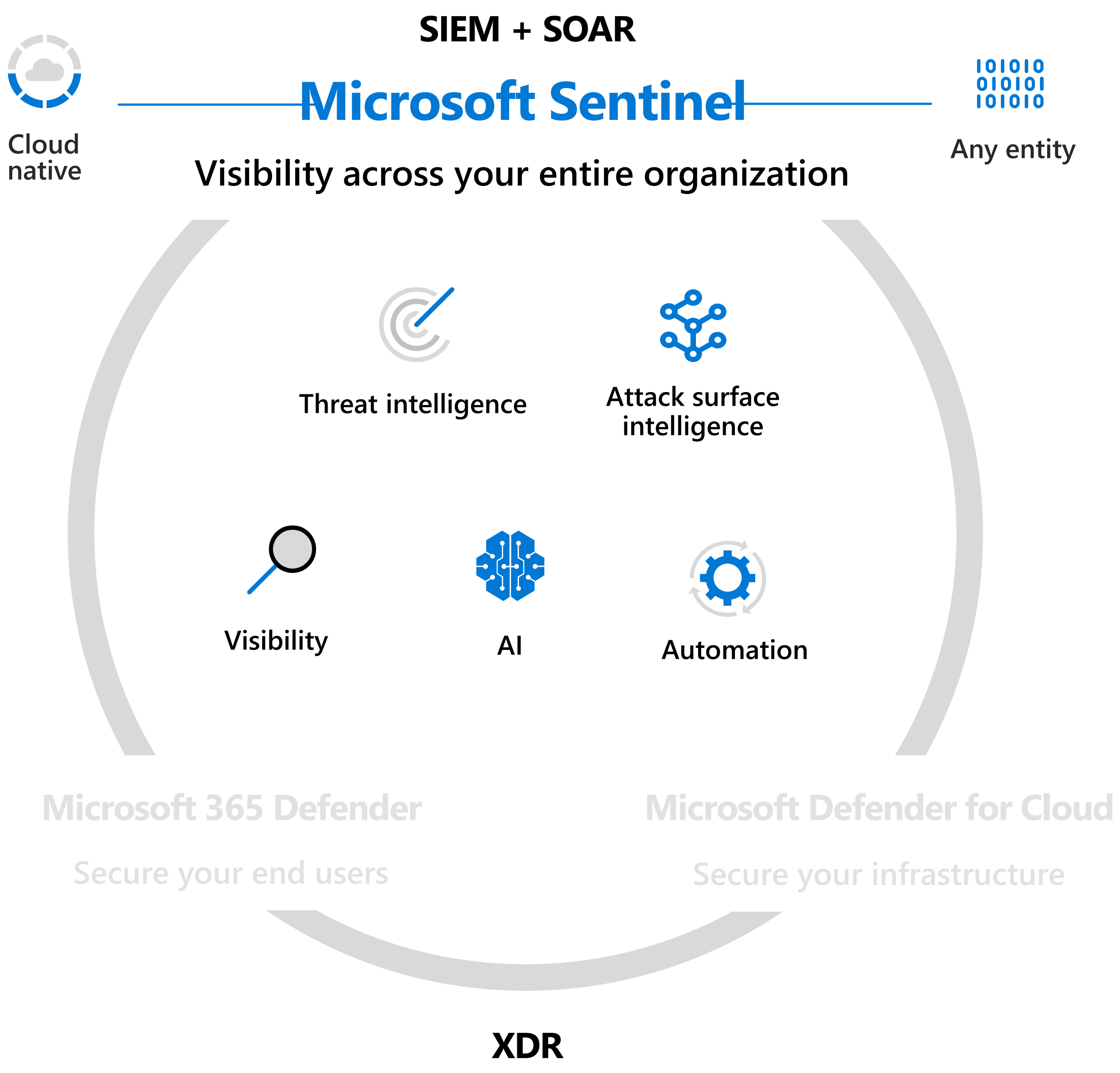
Network

IoT

Azure App Services

Microsoft Defender

XDR



SIEM + SOAR

Cloud native

Microsoft Sentinel

Any entity

Visibility across your entire organization

Threat intelligence

Attack surface intelligence

Visibility

AI

Automation

Microsoft 365 Defender

Secure your end users

Microsoft Defender for Cloud

Secure your infrastructure

XDR

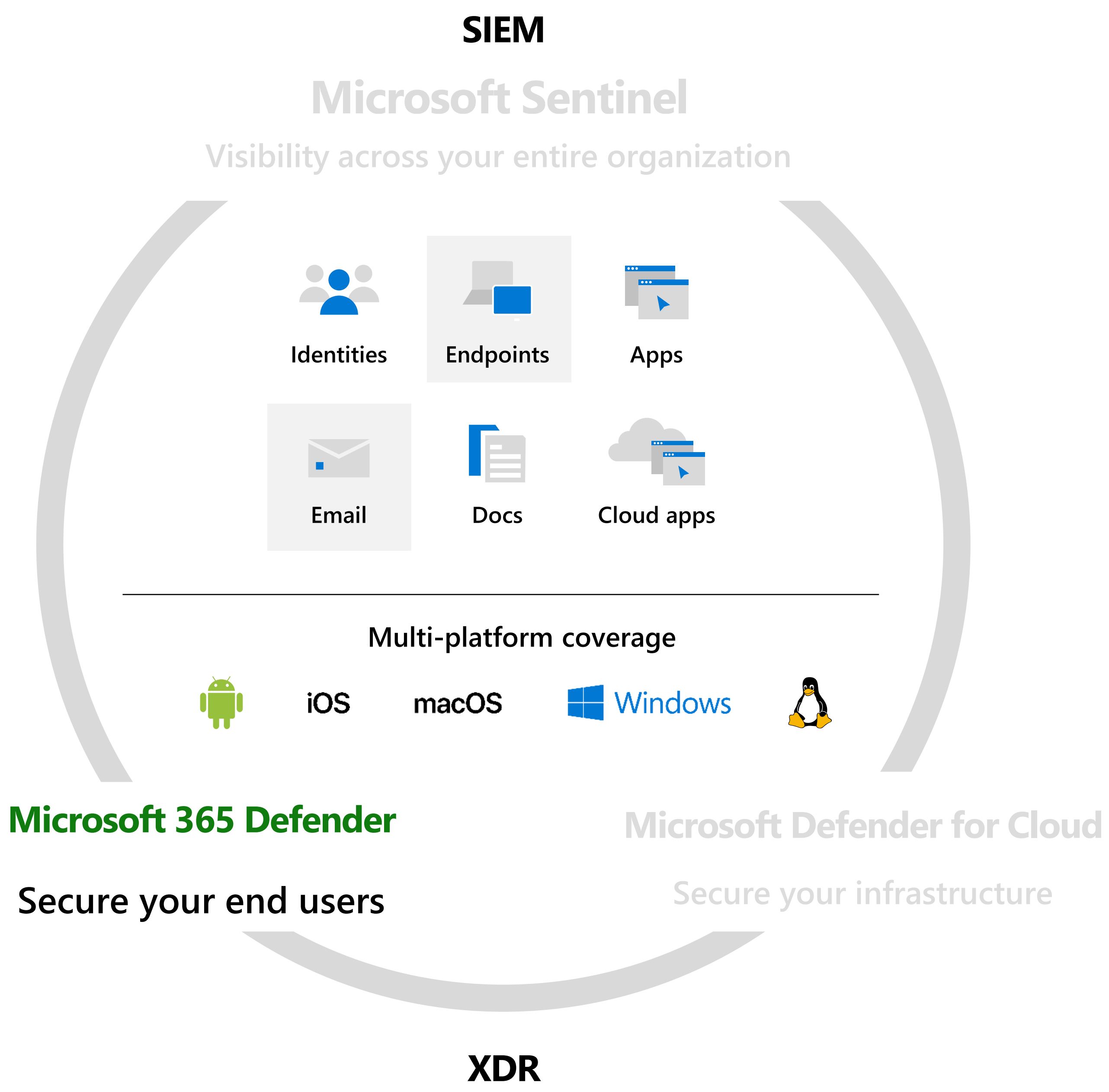
→ Collect security data at cloud scale and integrate with your existing tools.

→ Pinpoint your external attack surface exposed to real-world threats

→ Leverage AI to detect emergent threats, reducing false positives by 79% over three years.[1]

→ Respond rapidly with built-in orchestration and automation.

[1] The Total Economic Impact™ of Microsoft Microsoft Sentinel from Forrester Consulting.



→ Stop attacks before they occur with out-of-the-box, best-in-class protection capabilities.

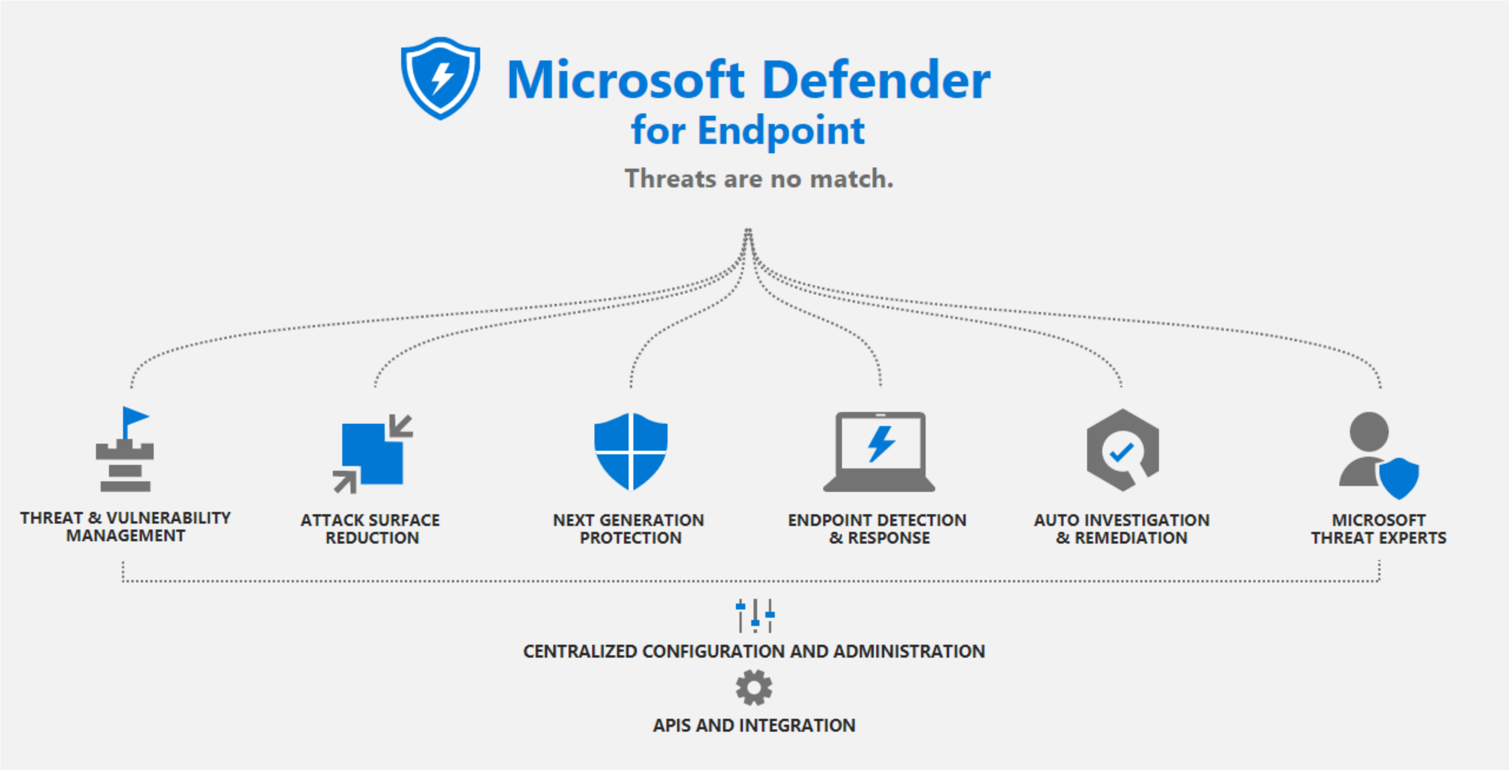
→ Detect and automate across siloes, integrating threat data for rapid response.

→ Hunt across all your Microsoft 365 data and apply your unique expertise.

→ View alerts and remediate across your Microsoft 365 environment in a single dashboard.

Comprehensive endpoint protection

Endpoints


Microsoft Defender
for Endpoint
Threats are no match.
THREAT & VULNERABILITY MANAGEMENT
ATTACK SURFACE REDUCTION
NEXT GENERATION PROTECTION
ENDPOINT DETECTION & RESPONSE
AUTO INVESTIGATION & REMEDIATION
MICROSOFT THREAT EXPERTS
CENTRALIZED CONFIGURATION AND ADMINISTRATION
APIS AND INTEGRATION

→ Industry-leading capabilities in MITRE ATT&CK evaluation and AV tests.

→ Multi-platform support including iOS, Android, Linux, MacOS, and Windows.

→ AI-based automatic investigation and remediation reduces threat volume.

An industry leader in endpoint security

Gartner

Gartner names Microsoft a Leader in 2019 Endpoint Protection Platforms Magic Quadrant.

FORRESTER®

Forrester names Microsoft a Leader in 2020 Enterprise Detection and Response Wave.

MITRE | ATT&CK™

Microsoft Threat Protection leads in real-world detection in MITRE ATT&CK evaluation.

Our antimalware capabilities consistently achieve high scores in independent tests.

SC MEDIA
THE CYBERSECURITY SOURCE

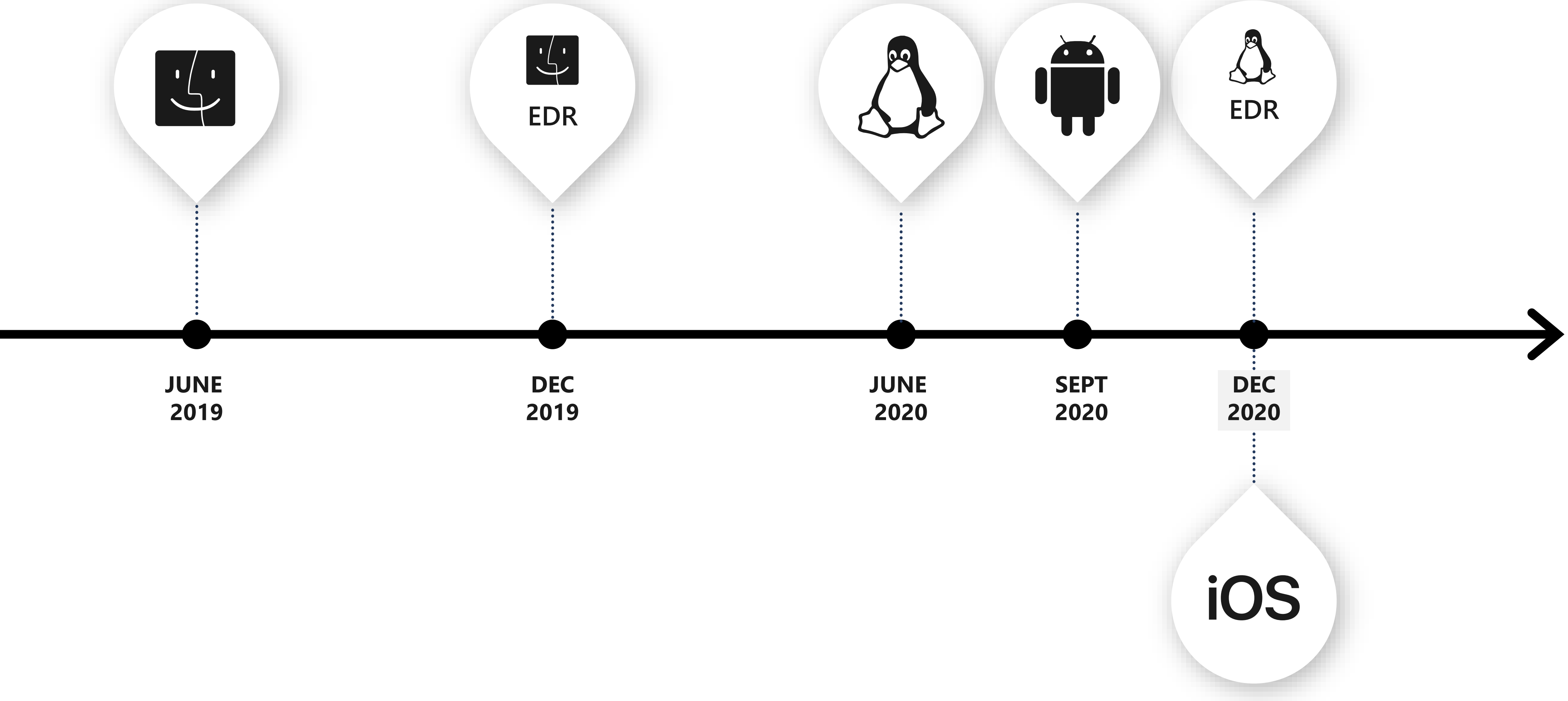
Microsoft Defender for Endpoint awarded a perfect 5-star rating by SC Media in 2020 Endpoint Security Review

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2020

Microsoft won six security awards with Cyber Defense Magazine at RSAC 2020:

- ✓ Application Isolation – Next Gen
- ✓ Endpoint Security – Editor's Choice
- ✓ Threat and Vulnerability Management – Most Innovative
- ✓ Malware Detection – Best Product
- ✓ Managed Detection and Response – Market Leader
- ✓ Enterprise Threat Protection – Hot Company

Delivering industry leading endpoint security across platforms



General availability dates

Why we're different

Agentless, cloud powered

No additional deployment or infrastructure. No delays or update compatibility issues. Always up to date.

Unparalleled optics

Built on the industry's deepest insight into threats and shared signals across devices, identities, and information.

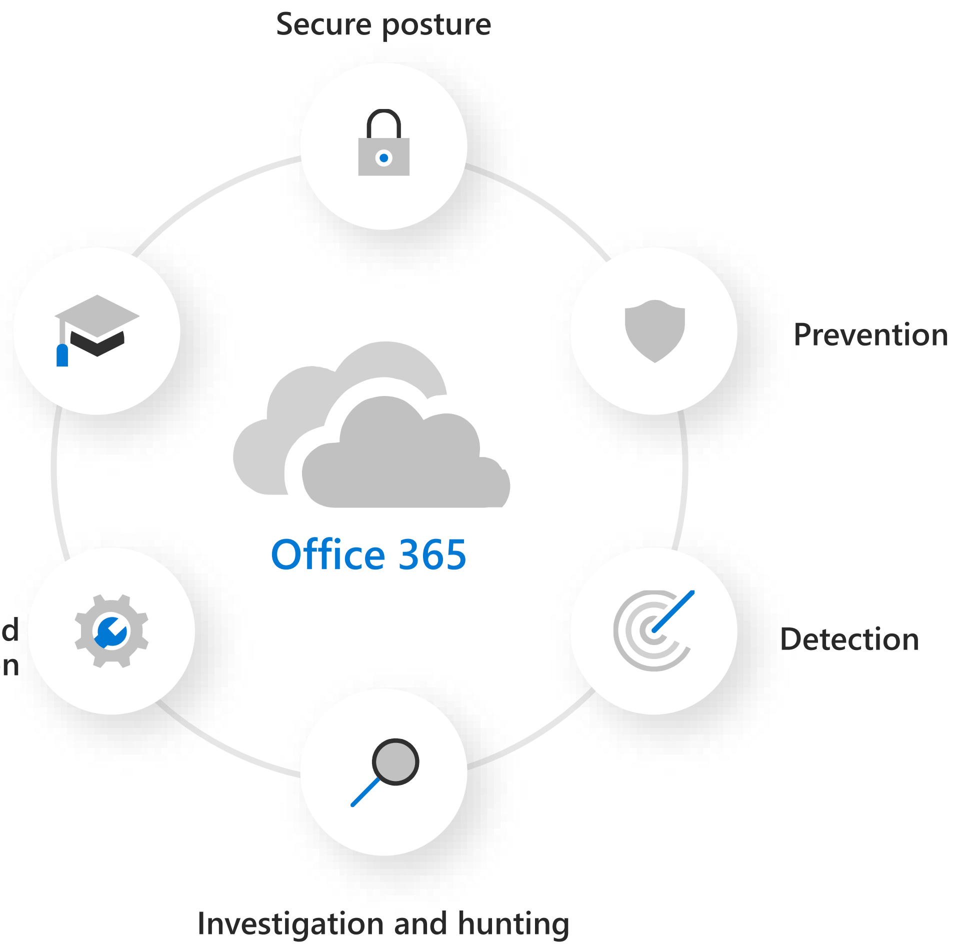
Automated security

Take your security to a new level by going from alert to remediation in minutes—at scale.

Comprehensive phishing and email protection

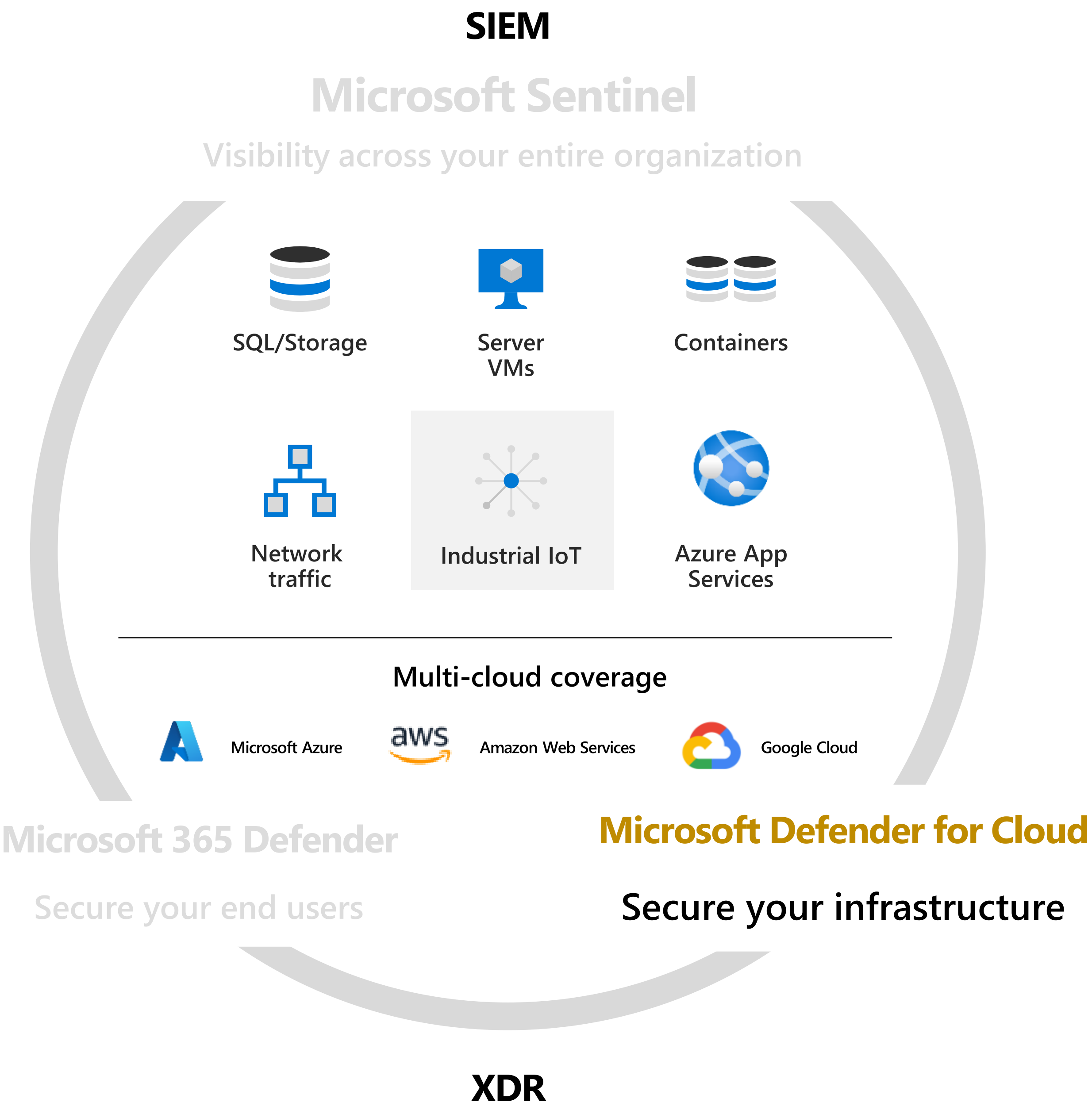
E-mail

Microsoft Defender for Office 365



- Natively integrated into Office 365 with simpler administration and lower TCO.
- Utilize powerful automation for email and collaboration tools with a single, natively integrated solution.
- Reduce the time for investigation and remediation by 89.3%.[1]

[1] Forrester "The Total Economic Impact™ of Microsoft Office 365 Threat Intelligence.



SIEM

Microsoft Sentinel

Visibility across your entire organization

Multi-cloud coverage

Microsoft 365 Defender

Secure your end users

Microsoft Defender for Cloud

Secure your infrastructure

XDR

- → Protect data services, cloud native services, Windows and Linux servers, and IoT from threats.
- → Extend protection to on-premises and multi-cloud for virtual machines and SQL databases using Azure Arc.
- → With prioritized alerts, focus on what matters the most.

Agentless security for IoT and Operational Technology (OT)

Microsoft Defender for IoT

PLCs and DCUs

HMIs

Engineering workstations

Historians

Enterprise IoT

Building automation

Secure both legacy and greenfield devices

Rockwell Automation · SIEMENS · GE · EMERSON · Windows 10 IoT

Schneider Electric · ABB · YOKOGAWA · TOSHIBA · Microsoft Windows xp

hp · Johnson Controls · CISCO

→ Prevent safety incidents, revenue impact from production downtime & theft of sensitive IP

→ Discover & classify unmanaged devices, prioritize vulnerabilities, and detect threats with IoT/OT-aware behavioral analytics.

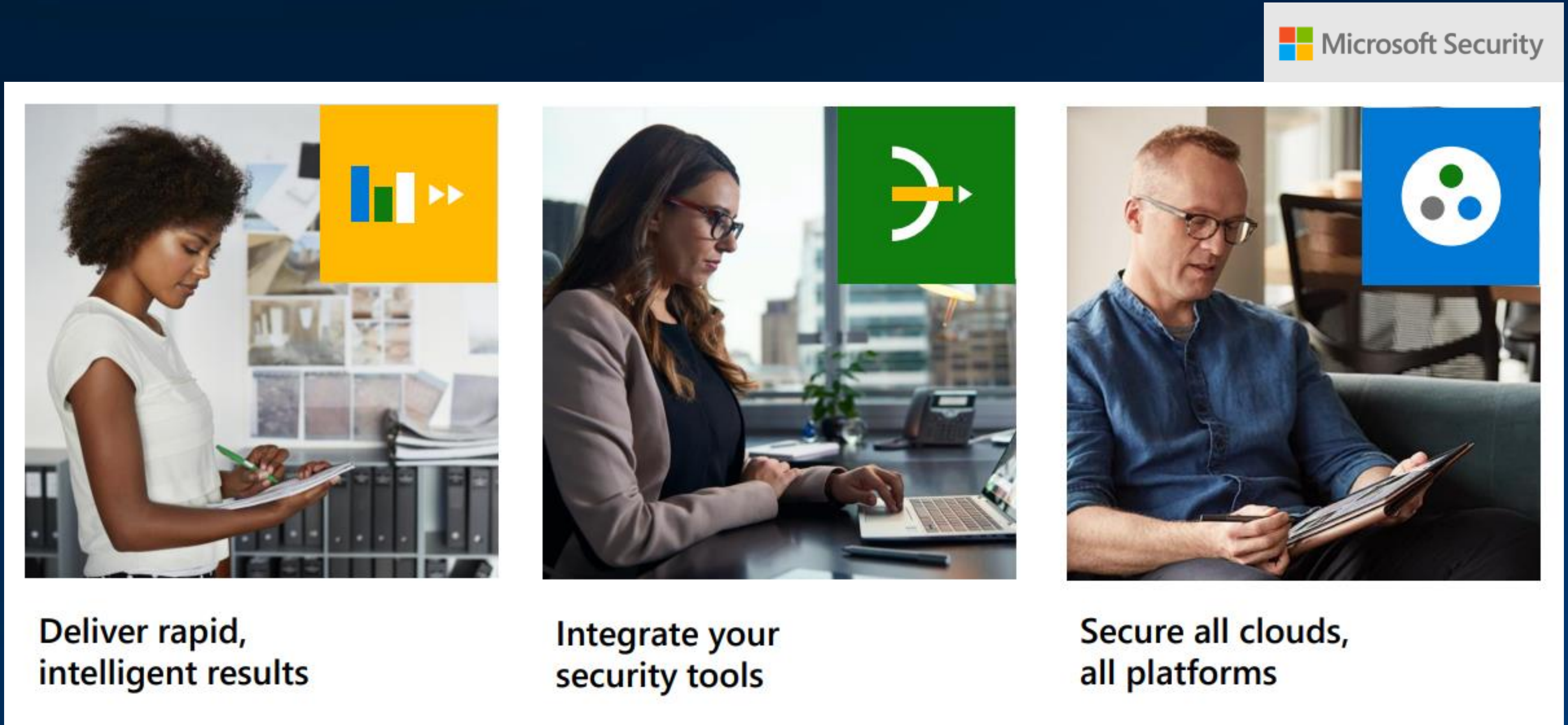
→ Fast, frictionless deployment (<1 day per site).

→ Integrated with Microsoft Sentinel and 365 Defender for unified IT/OT monitoring and governance.

→ Supports on-premises or cloud-connected deployments

Managing Cybersecurity Needs when Talent is Scarce and Alerts are in overload

Let's start our Journey
with Security Transformation



Microsoft Security

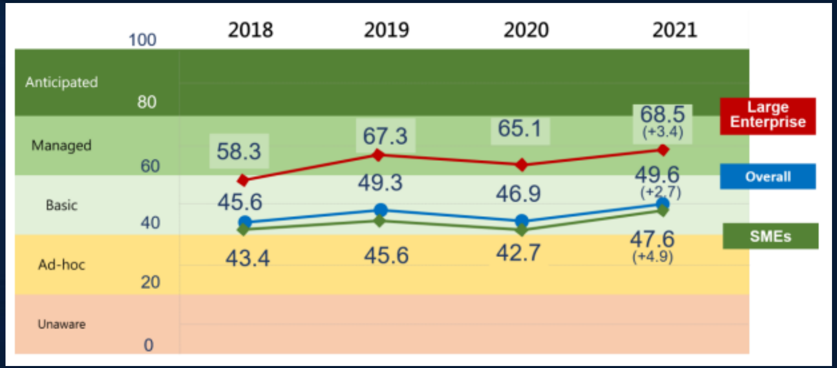
Deliver rapid, intelligent results

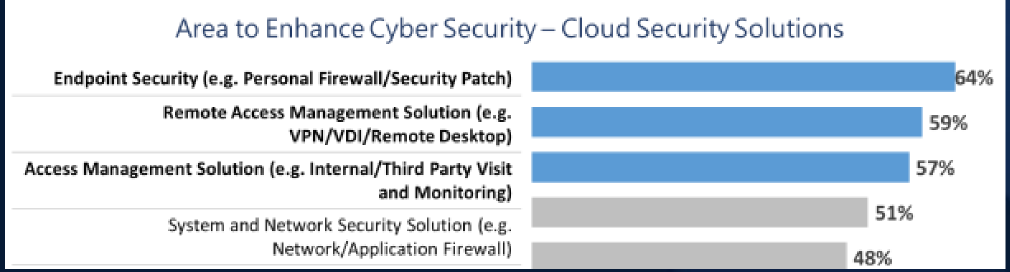
Integrate your security tools

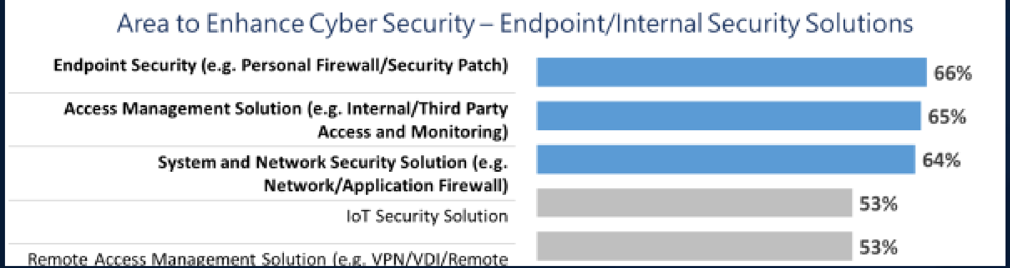
Secure all clouds, all platforms

Are you ready to Kick-start?
especially in Hong Kong Enterprises

HKT香港企業網絡保安準備指數 2021
HKT Hong Kong Enterprise Cyber Security Readiness Index



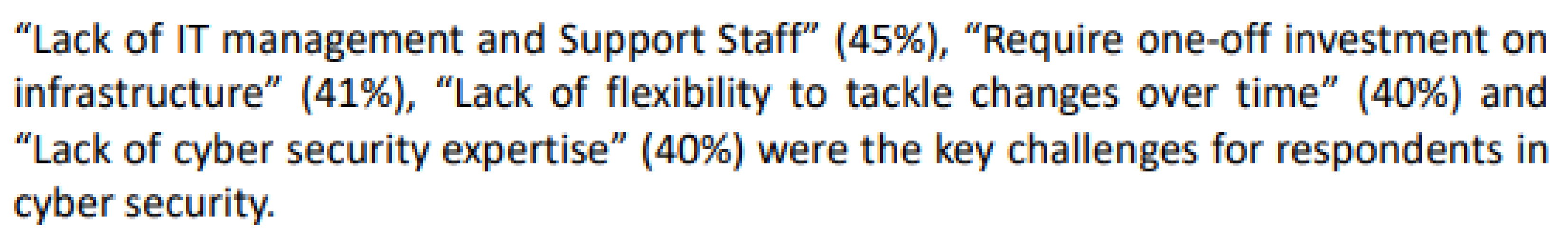




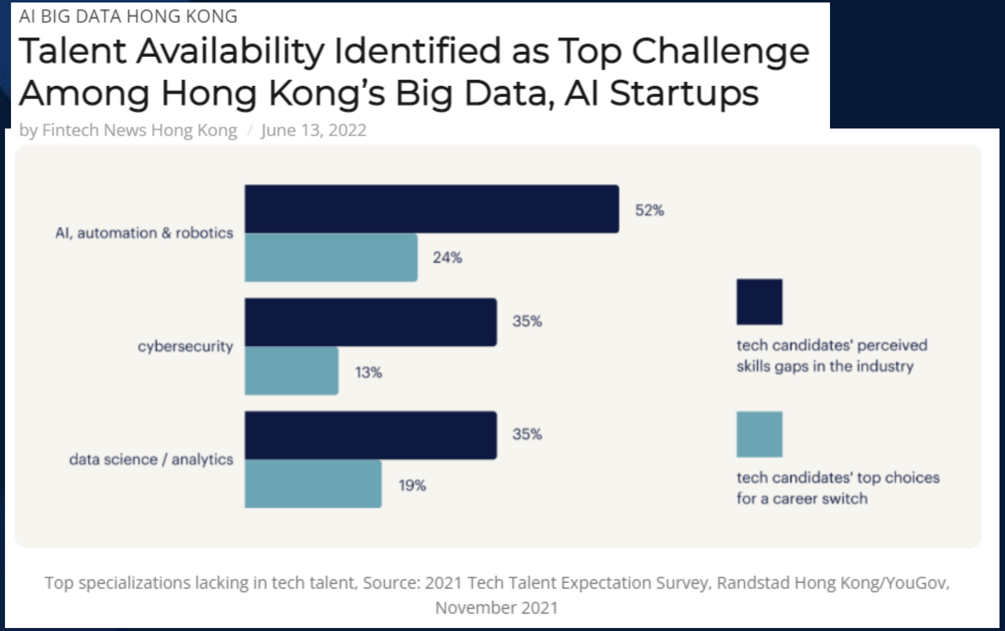
Enterprises got its own priority for enhancement

Key Challenges

- Talent Shortage
- Budget Constraints



"Lack of IT management and Support Staff" (45%), "Require one-off investment on infrastructure" (41%), "Lack of flexibility to tackle changes over time" (40%) and "Lack of cyber security expertise" (40%) were the key challenges for respondents in cyber security.



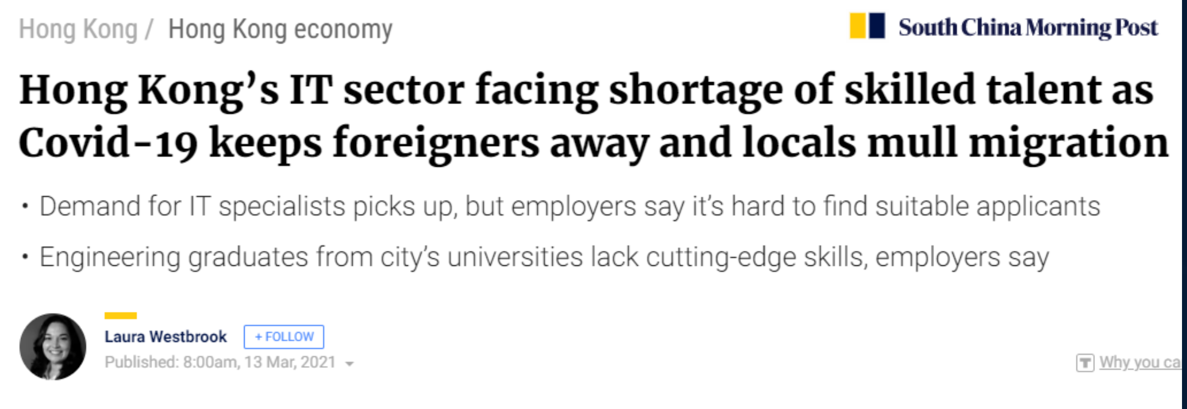
AI BIG DATA HONG KONG

Talent Availability Identified as Top Challenge Among Hong Kong's Big Data, AI Startups

by Fintech News Hong Kong / June 13, 2022

AI, automation & robotics
52%
24%
cybersecurity
35%
13%
data science / analytics
35%
19%
tech candidates' perceived skills gaps in the industry
tech candidates' top choices for a career switch

Top specializations lacking in tech talent, Source: 2021 Tech Talent Expectation Survey, Randstad Hong Kong/YouGov, November 2021



Hong Kong / Hong Kong economy

South China Morning Post

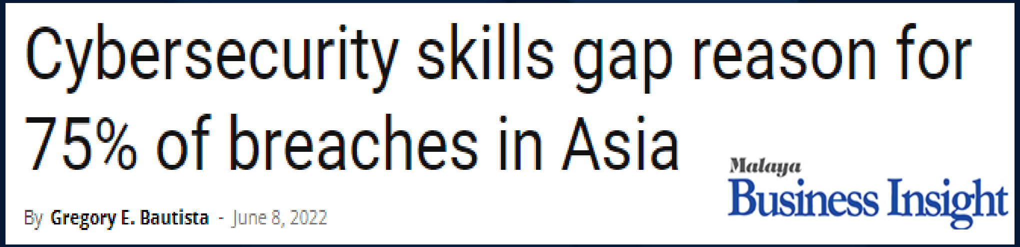
Hong Kong's IT sector facing shortage of skilled talent as Covid-19 keeps foreigners away and locals mull migration

- Demand for IT specialists picks up, but employers say it's hard to find suitable applicants
- Engineering graduates from city's universities lack cutting-edge skills, employers say

Laura Westbrook + FOLLOW

Published: 8:00am, 13 Mar, 2021

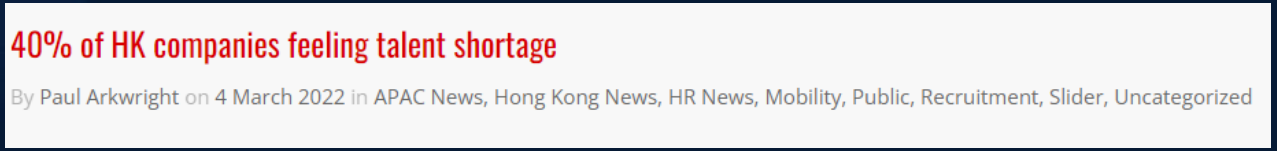
Why you ca



Cybersecurity skills gap reason for 75% of breaches in Asia

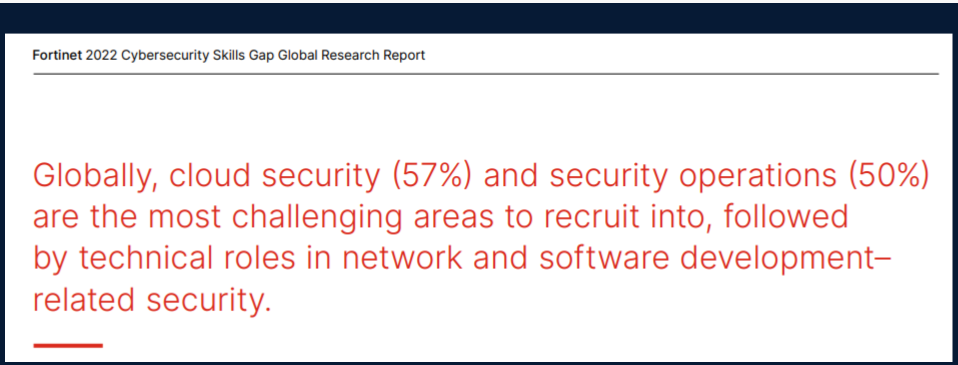
By Gregory E. Bautista - June 8, 2022

Malaya Business Insight



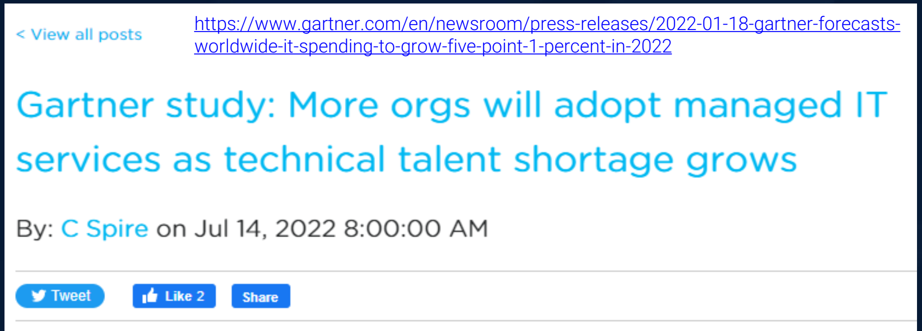
40% of HK companies feeling talent shortage

By Paul Arkwright on 4 March 2022 in APAC News, Hong Kong News, HR News, Mobility, Public, Recruitment, Slider, Uncategorized



Fortinet 2022 Cybersecurity Skills Gap Global Research Report

Globally, cloud security (57%) and security operations (50%) are the most challenging areas to recruit into, followed by technical roles in network and software development–related security.



< View all posts

https://www.gartner.com/en/newsroom/press-releases/2022-01-18-gartner-forecasts-worldwide-it-spending-to-grow-five-point-1-percent-in-2022

Gartner study: More orgs will adopt managed IT services as technical talent shortage grows

By: C Spire on Jul 14, 2022 8:00:00 AM

Stop Talent War!
Re-think the Strategy with Managed Security Services (MSS)

Optimal Solution to secure organizations as attack surfaces continue to expand, talent is limited, and companies are facing more threats than ever before

Managed Security Service Providers (MSSP) offer outsourced management of tools and a security operations center (SOC)

- Managed Technology or Devices (Firewall, SIEM)
- Security Scanning or Assessment
- Managed Detect & Response (MDR)

Ensure up-to-date state of Security

Faster Deployment , Improved Time-to-Value

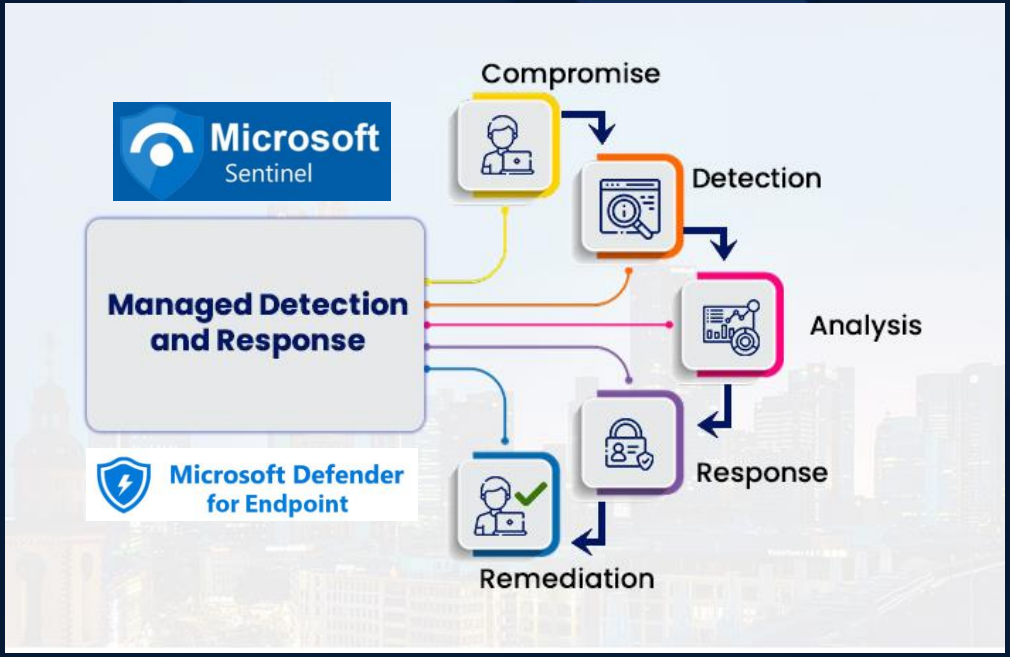
Managed Detect & Response (MDR)
Handling Cyber Risk Better

Experts working 24x7, acting as virtual extension of your in-house team

- Telemetry & Intelligence
- Detection & Enrichment
- Investigation & Hunting
- Response & Containment

Partnered with Microsoft

More than just forwarding alerts & notifications



Embracing Digital Transformation with MSSP

Important points to consider

Multiple Technical Dimensions

Ability to deliver different solutions in Cloud and Security

Emerging Technologies

Leveraging exponential technologies such as Artificial Intelligence (AI), Automation, data analytics and IoT

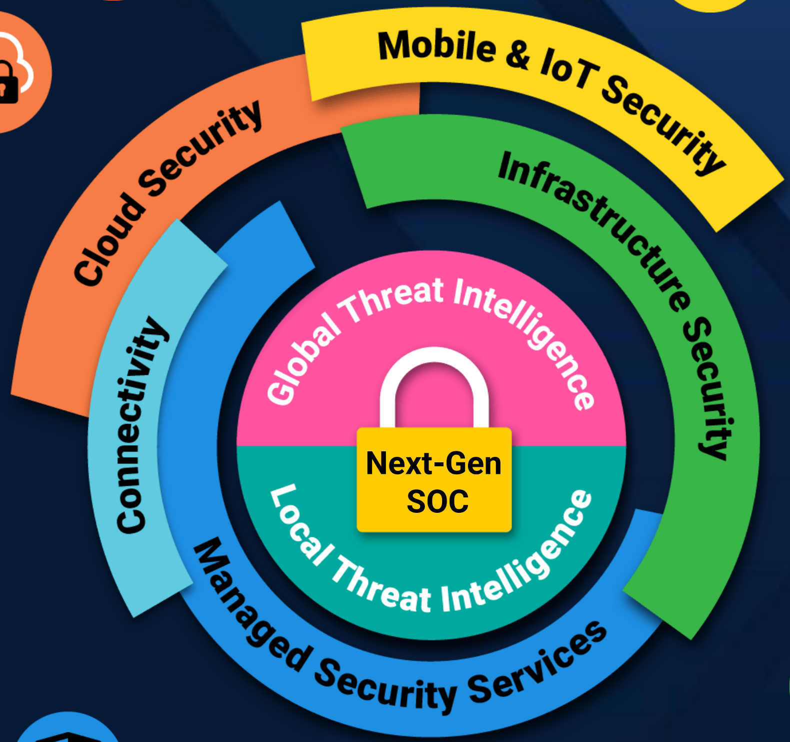
Managed Services Capability

Optimizing operational efficiency and free up resources back to Business

Real World transformation story

Having technology consulting expertise and solid experience in Digital Transformations

All round Cybersecurity Solutions



Next-Gen SOC

Global Threat Intelligence

Local Threat Intelligence

Managed Security Services

Connectivity

Cloud Security

Mobile & IoT Security

Infrastructure Security

Secure Access Service Edge (SASE)

5G Security

Unified Endpoint Management

IoT Security

Zero-Trust Architecture

Application & Data Protection

Security Workflow & Automation

Threat Analytics

Technology Management (XDR / Firewall / WAF / SASE / PAM)

Consultancy & Skill Development

Incident Response

Threat Management Services

DNS Security & Services

DDoS Protection

DevSecOps

Hybrid & Multi-Cloud Security

150+

Cybersecurity Certifications

SANS GIAC (ISC)² ISACA CompTIA

HKT Enterprise Solutions

Thank you.