Microsoft Security

Challenges & Opportunities of the Modern CISO

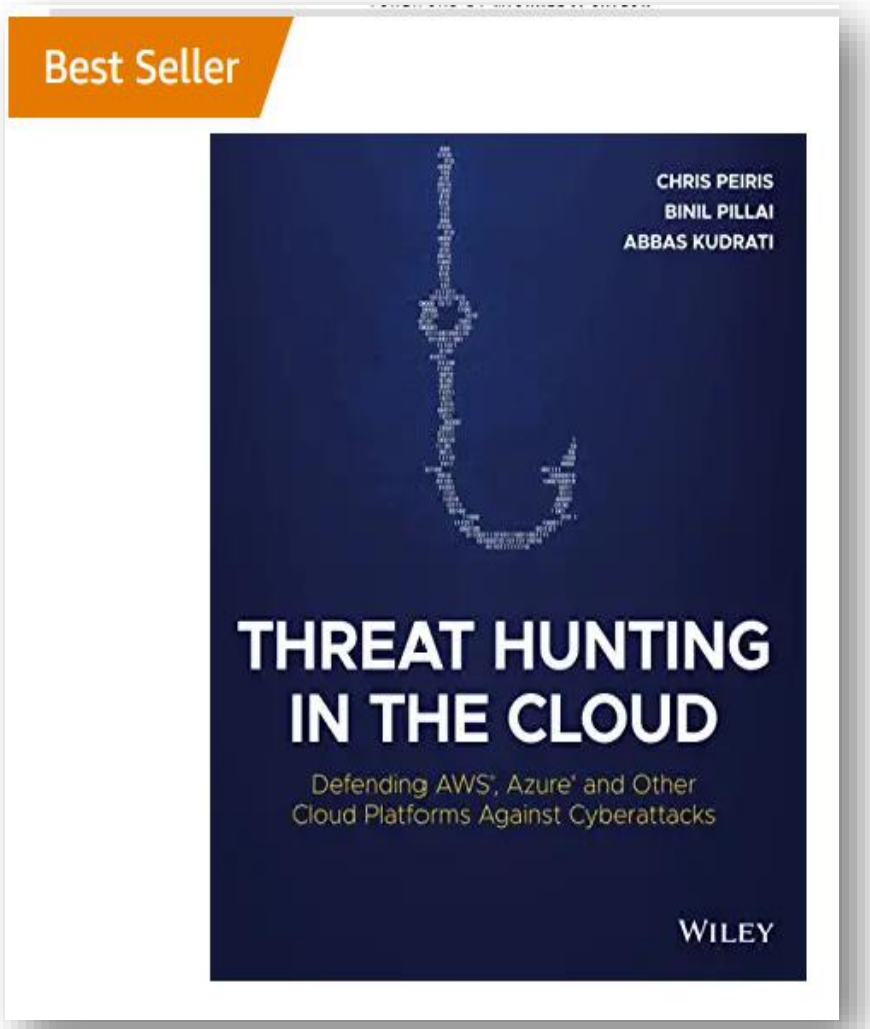
Abbas Kudrati
APAC Chief Cybersecurity Advisor
Abbas.Kudrati@Microsoft.Com
https://aka.ms/abbas

About me

"You join Microsoft, not to be cool
but to make others cool"
Satya Nadella

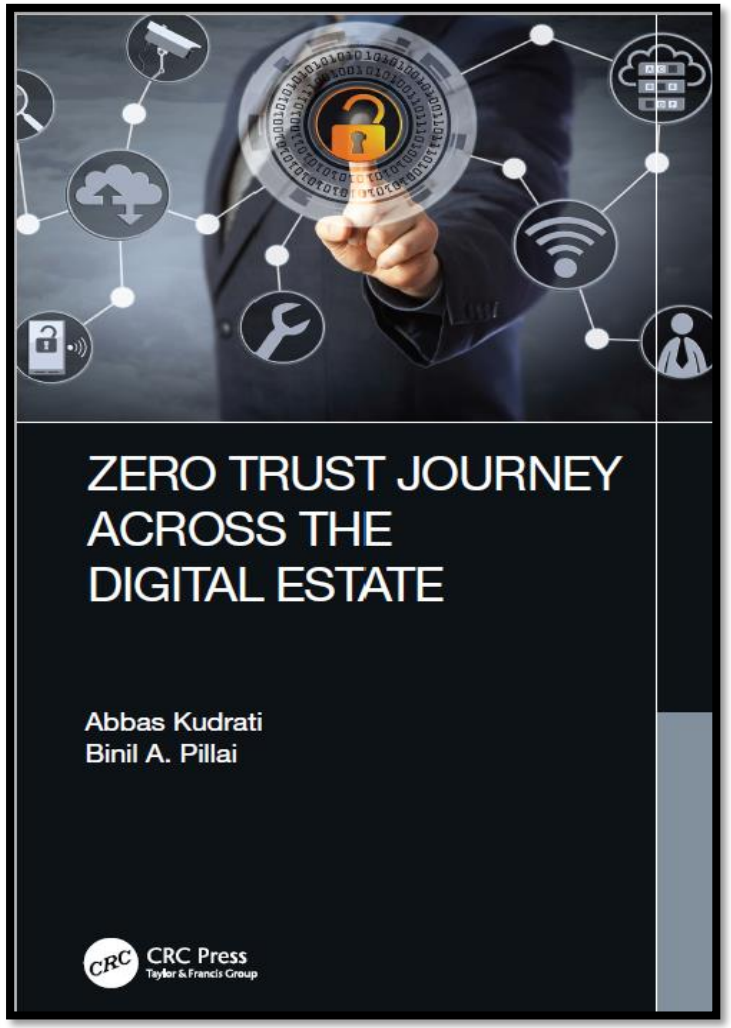
- **Cybersecurity practitioner and CISO with 25 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**

My Publications

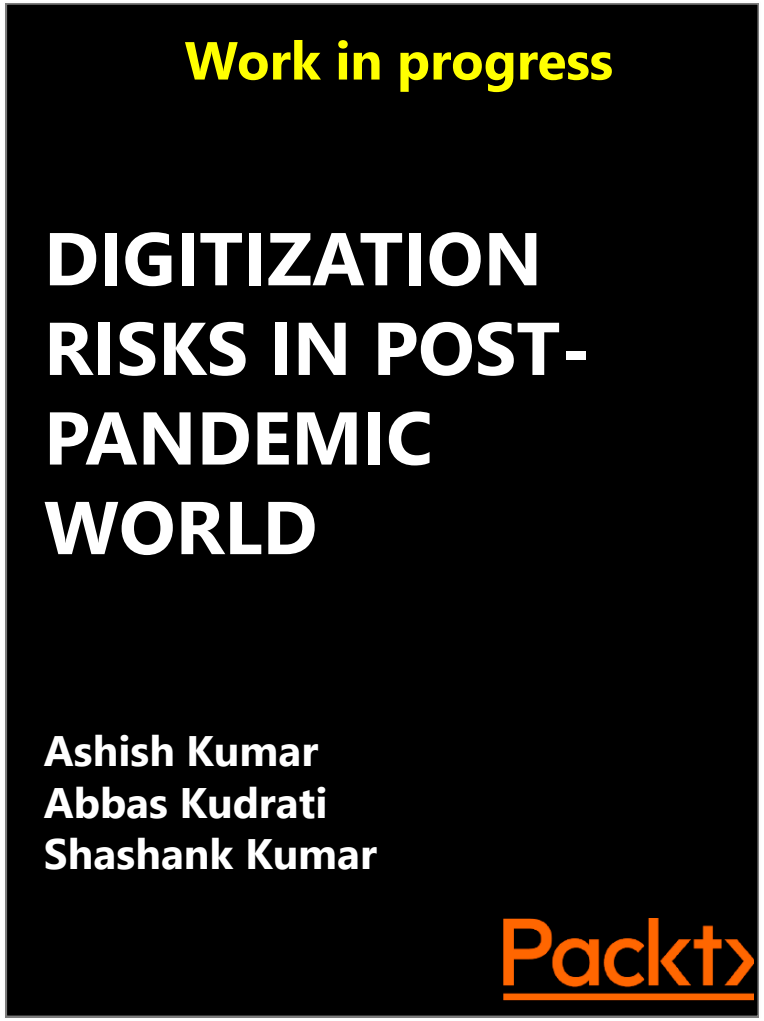


[Get it on Amazon](#)

Or send me a request for a free copy

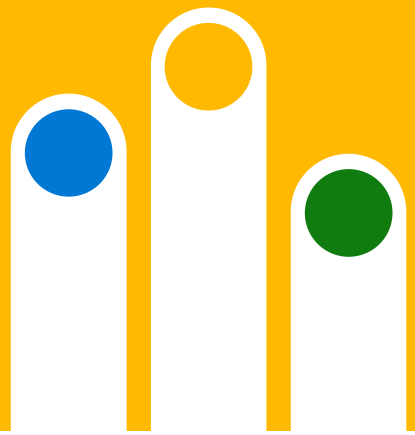


[Pre order on Amazon](#)



Releasing soon by July 2022

Security has never been more critical



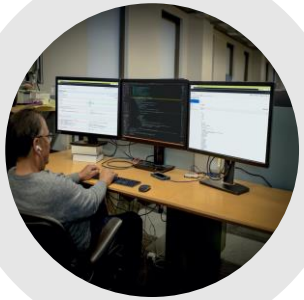
Remote and hybrid work has **increased 300%**[1]

Cyber attacks are becoming **more sophisticated**

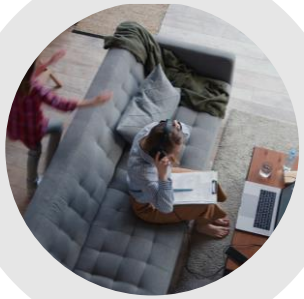
Pressures of **rising costs** and growing concerns around **investment return**

Source: Predictions 2021: Remote Work, Automation, And HR Tech Will Flourish, Forrester

Today's reality | Distributed and hybrid



The tools we use
are varied, from corporate to BYOD, cloud-based, or on-prem apps.



Where we work
has continued to rapidly evolve to a mix of locations.

How we do our work
is an evolving mix of virtual, physical, collaborative, and data-driven styles.

Evolving risks
Increasing volume and sophistication of threats, and a wider, more distributed attack surface.

Challenges

Old World vs. New World

~~Users are employees~~	→	Employees, partners, customers, bots
~~Corporate managed devices~~	→	Bring your own devices and IoT
~~On-premises apps~~	→	Explosion of cloud apps
~~Monolithic apps~~	→	Composite apps & public restful APIs
~~Corp network and firewall~~	→	Expanding Perimeters
~~Local packet tracking and logs~~	→	Explosion of signal

COVID and the future of Hybrid Work has proven that traditional perimeter security controls are no longer adequate…. a new approach is needed

Traditional CISO Challenges

Common Enterprise Challenges

Technology and business silos, lifecycle debt, skills shortages and an explosion of data

Threat actors have rapidly increased in sophistication over the past year, using techniques that make them harder to spot.

The 2020 State of Security Operations, Forrester, April 2020

17%

of Security decision makers indicate only 17% of them leverage automation to address threats.

Thomson Reuters Financial Risk, "The Cost of Compliance"

49%

of organisations agree their various security tools are well integrated and over a third indicate that their staff wastes time chasing false leads.

Microsoft Compliance Tracker H1 FY21

EXTERNAL THREATS

INTERNAL THREATS

#1

Protecting and governing sensitive data is the biggest concern in complying with regulations

Microsoft GDPR research, 2017

63%

of organizations fear data leak/spillage during and after the pandemic

Microsoft COVID Security Priorities Survey 2020

88%

of organizations no longer have confidence to detect and prevent loss of sensitive data[3]

Forrester. Security Concerns, Approaches and Technology Adoption. December 2018

Modern CISO Challenges

Empower your security teams to protect employees and resources

How CISOs are navigating the challenges of COVID-19

82%

feel pressured to lower costs.

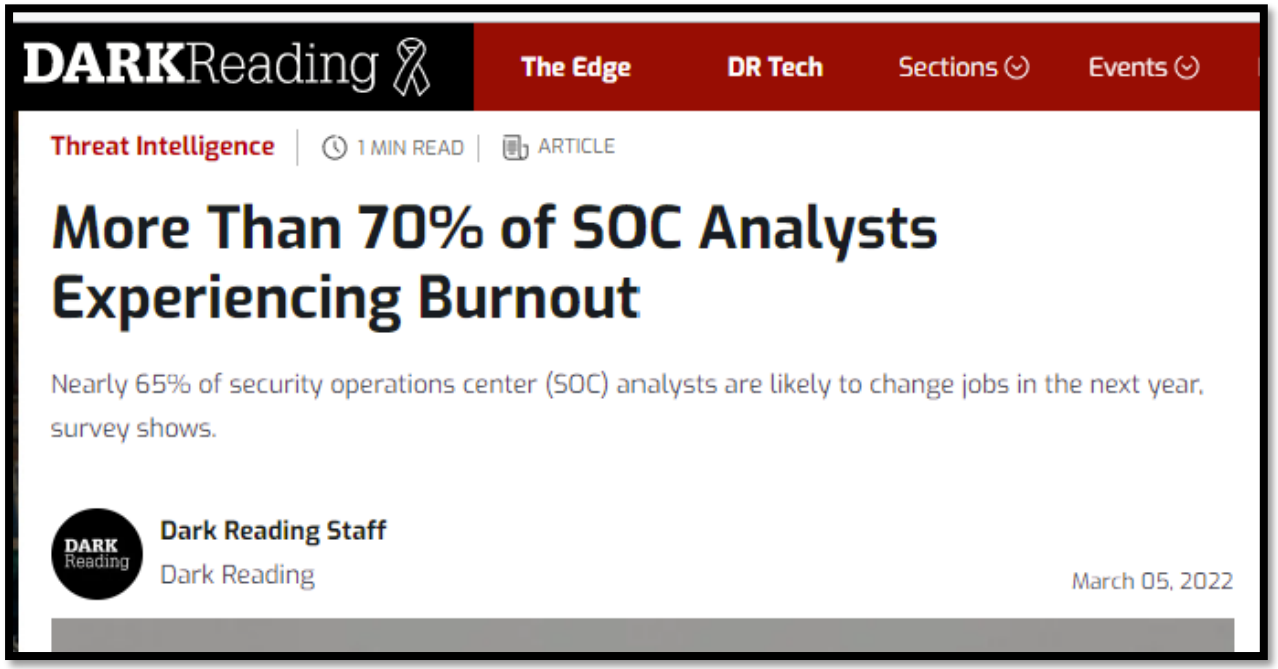
67%

identified pandemic-themed phishing attacks.

#1

priority to reduce cost is improved threat protection.

Source: "Microsoft Pandemic CISO Survey" 2020



DARKReading

The Edge | DR Tech | Sections | Events

Threat Intelligence | 1 MIN READ | ARTICLE

More Than 70% of SOC Analysts Experiencing Burnout

Nearly 65% of security operations center (SOC) analysts are likely to change jobs in the next year, survey shows.

Dark Reading Staff
Dark Reading

March 05, 2022

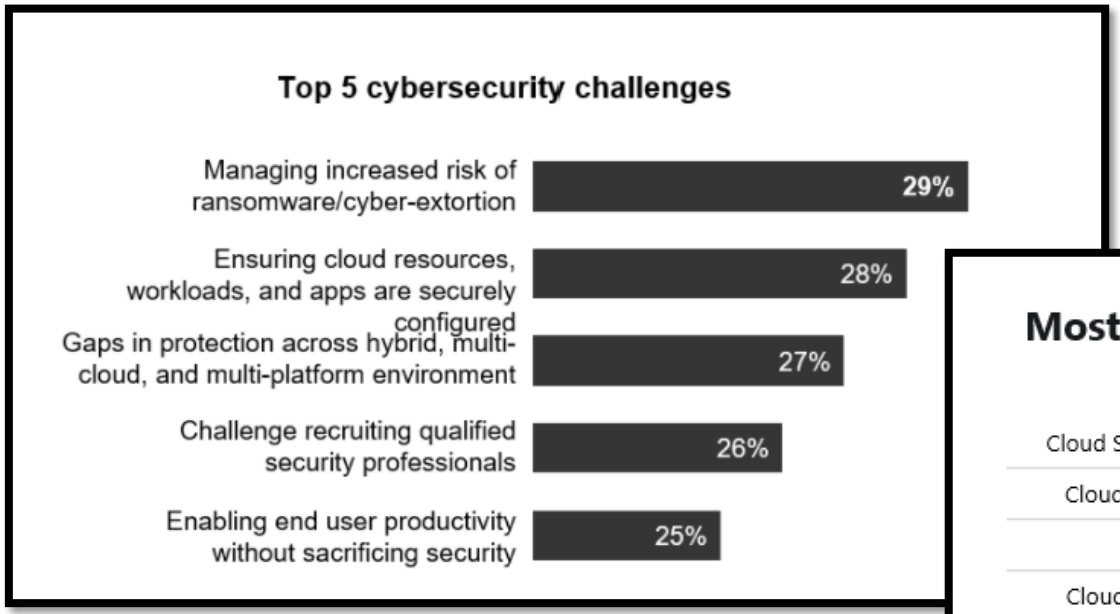
Stress and frustration continue to plague the security operations center (SOC):

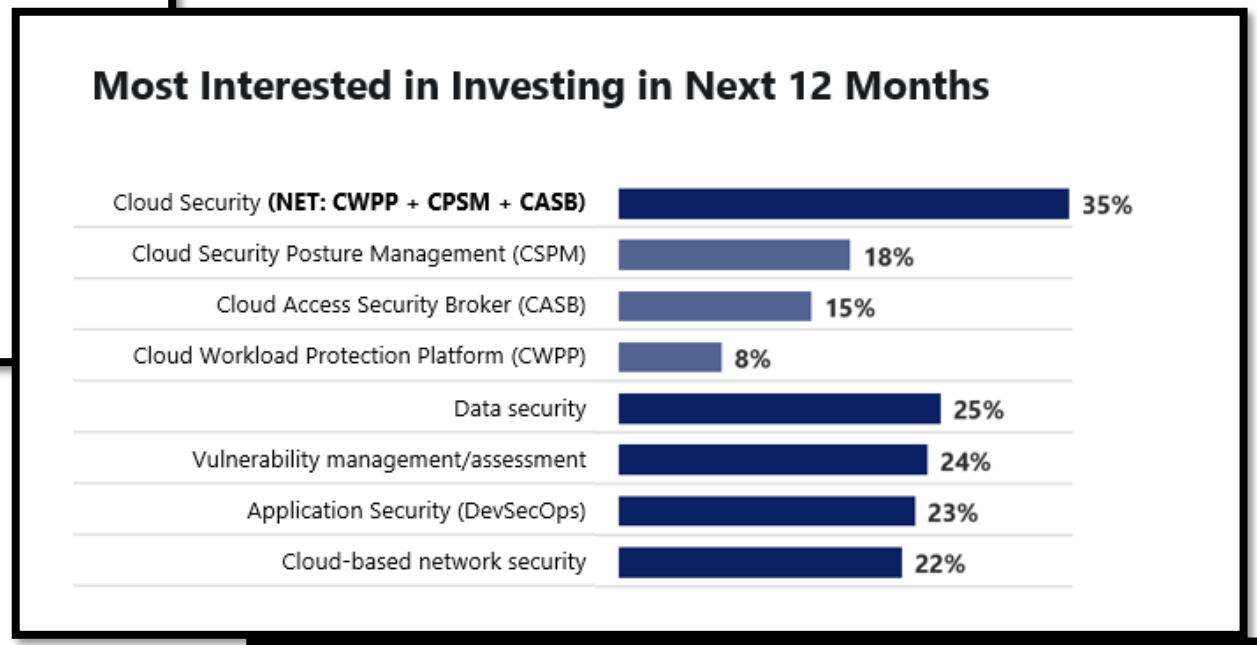
nearly 70% report understaffed teams, and 60% say their workloads have spiked over the past year.

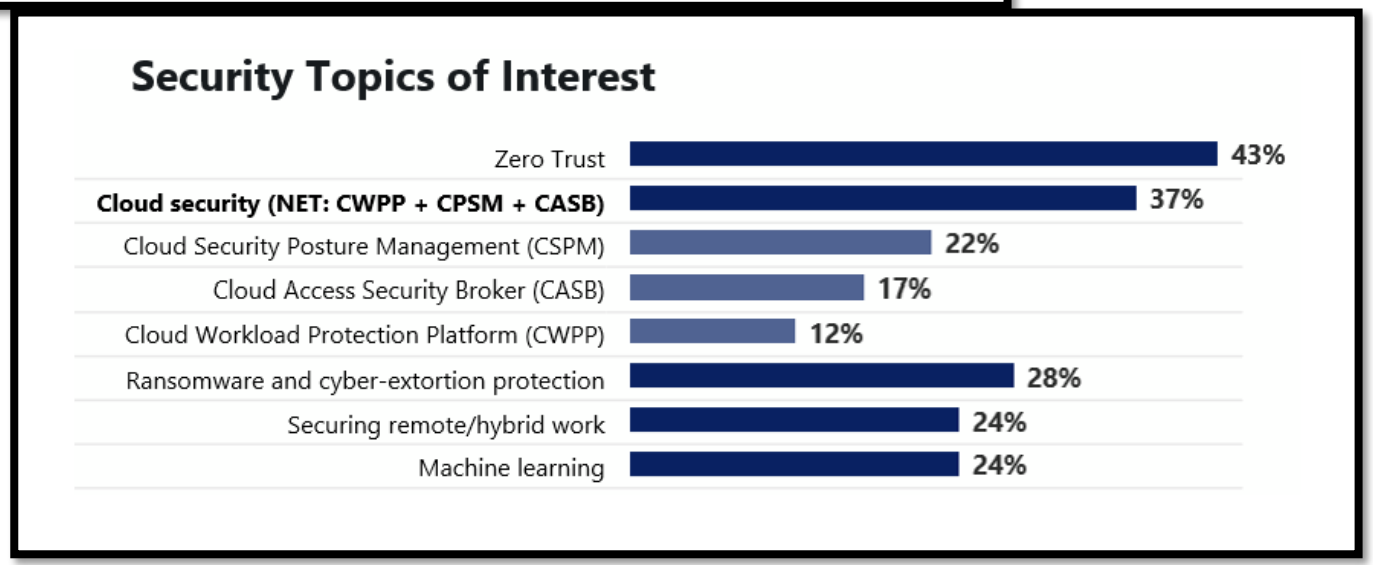
Some 64% of SOC analysts say manual work eats up more than half of their time, and reporting and monitoring are their least favorite parts of the job.

More than 65% say half of their security tasks could be automated, leaving them time to do deeper security work.

And 64% are considering leaving the organization for a new position somewhere else.







[How CISOs are preparing to tackle 2022 - Microsoft Security Blog]

Opportunities

Gartner Cybersecurity Prediction 2021-2022

1. By the end of 2023, modern privacy laws will cover the personal information of 75% of the world's population – strong need to automate Privacy Mgt
2. By 2024, 30% of enterprises will adopt cloud-delivered Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA) and Firewall As A Service (FWaaS) capabilities **from the same vendor**. – tools consolidation
3. By 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements. – Cyber readiness becoming a KPI

[The Top 8 Cybersecurity Predictions for 2021-2022 (gartner.com)]

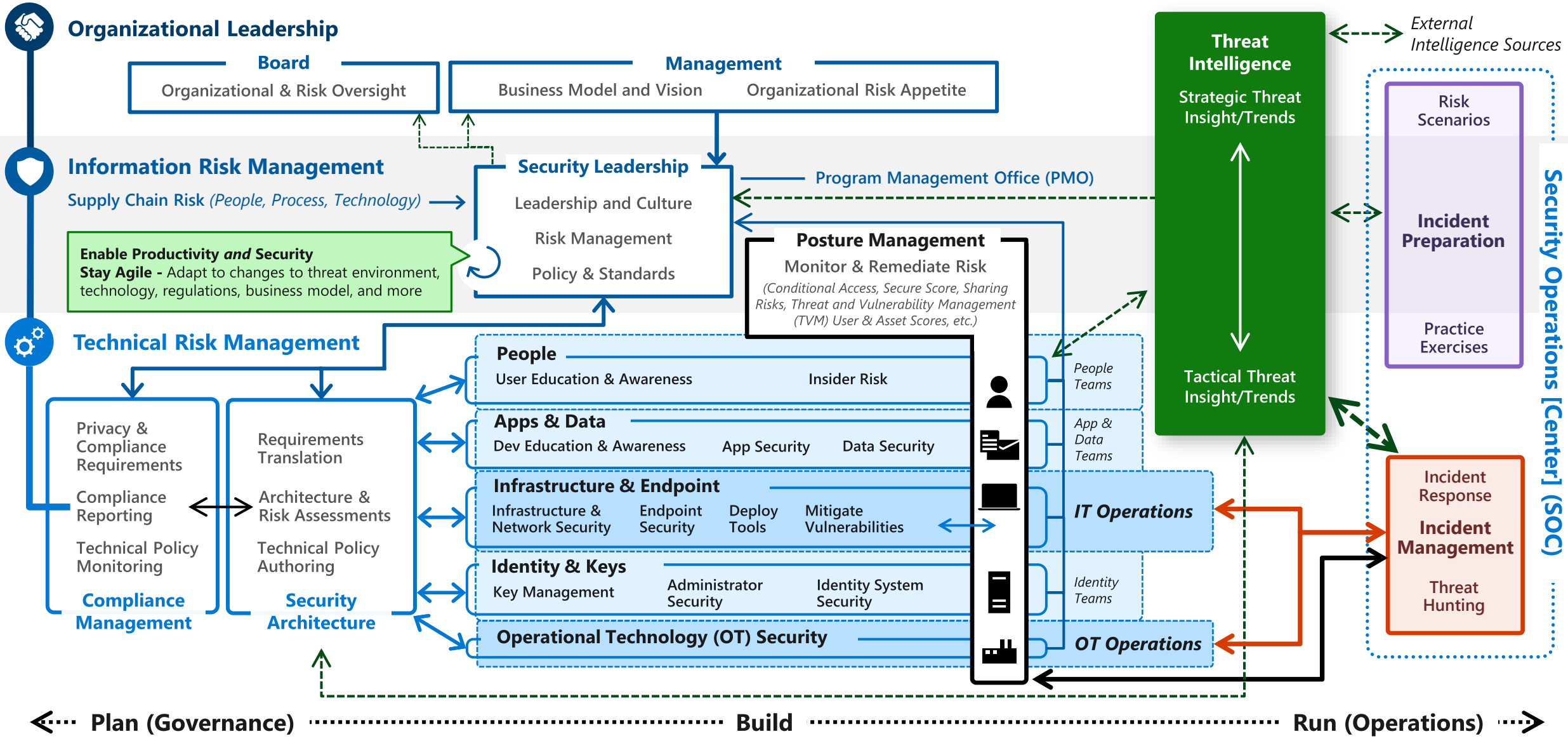
[Gartner Top Security and Risk Trends for 2021]

Managing Information\Cyber Risk

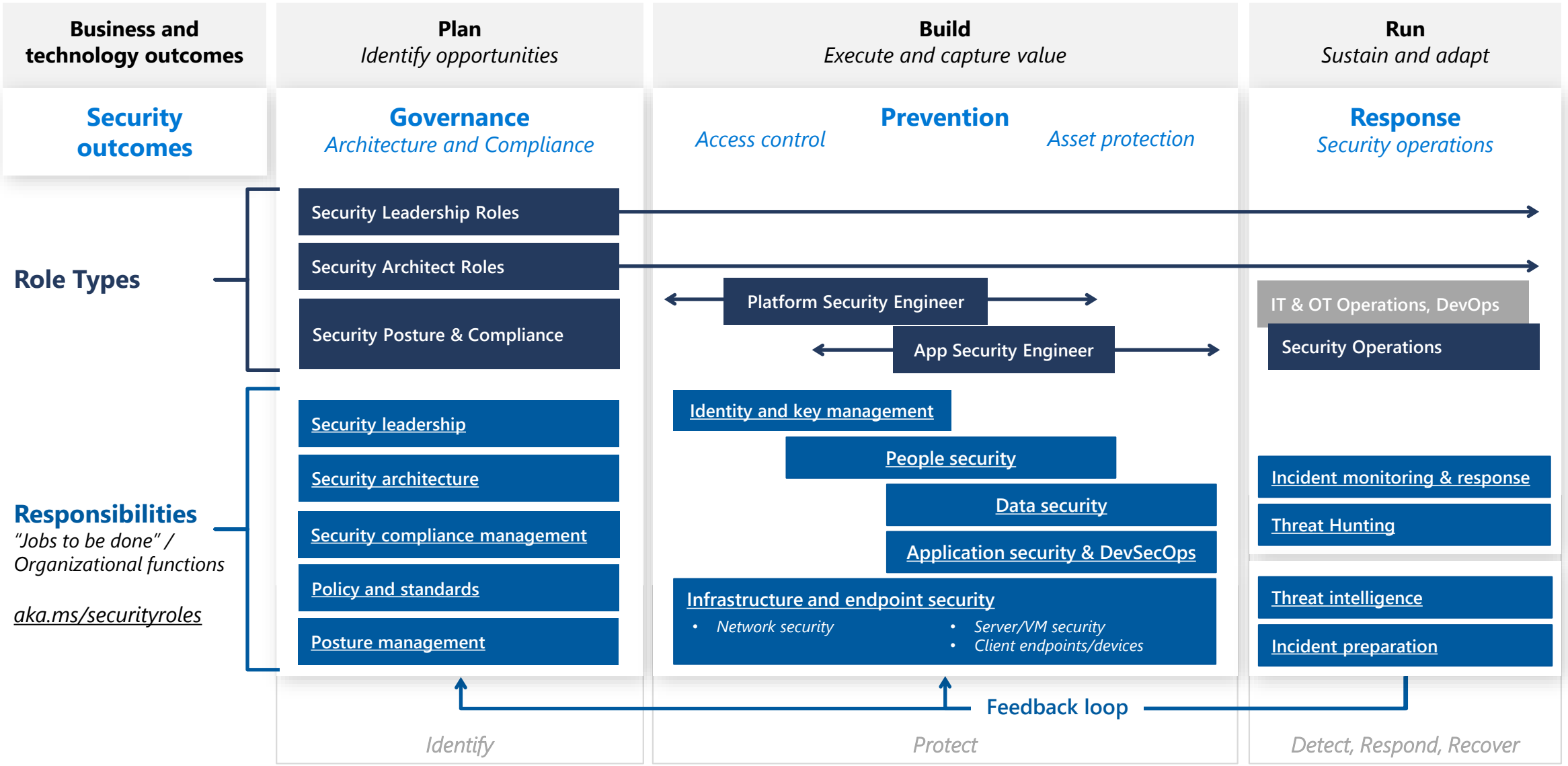
Security responsibilities or "jobs to be done"

December 2021 - https://aka.ms/SecurityRoles

Microsoft



Security Roles and Responsibilities



Zero Trust

- Simplify
- Integrate
- Automate
- Consolidate

Security Strategy for

- **business assets** (data, applications, devices)
- **everywhere** (private & public networks)

Leads to Technical Initiatives

User Access

Dynamic access control that **explicitly validates trust** before providing access

Modern SecOps

Pervasive detection and rapid response to attacks **anywhere**

OT and Datacenter

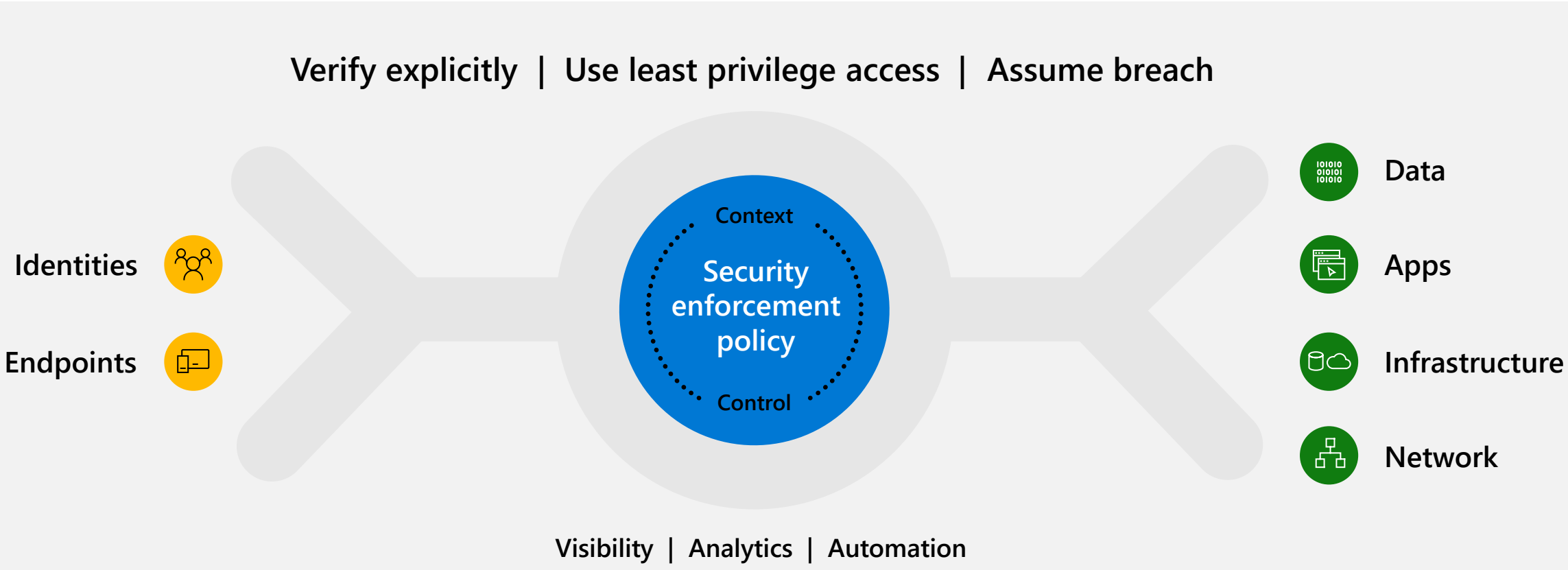
Monitor and protect existing and new assets by **business risk**

Increases security

Increases productivity

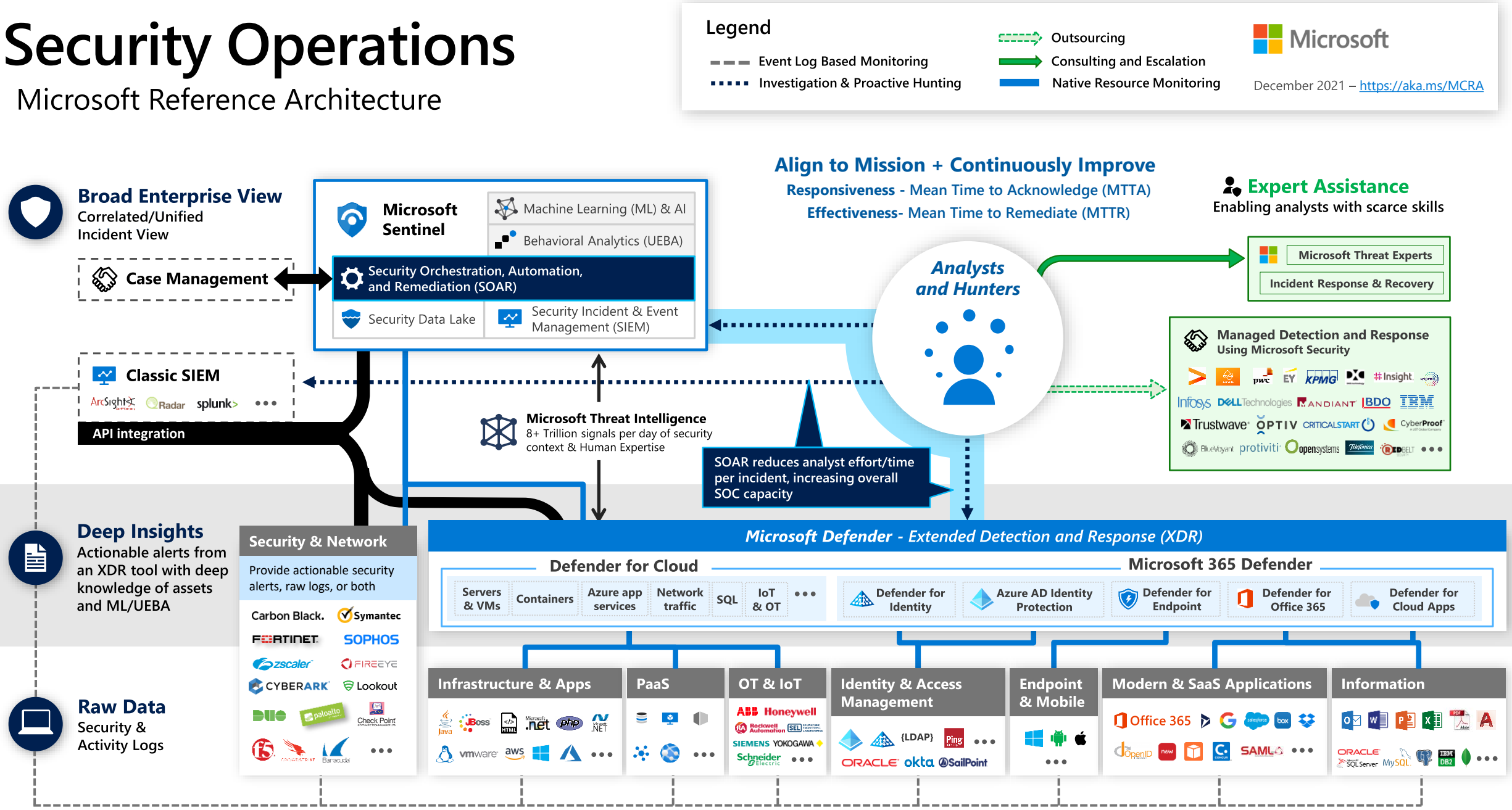
Start with a Zero Trust Approach

Increase security assurances for your critical business assets

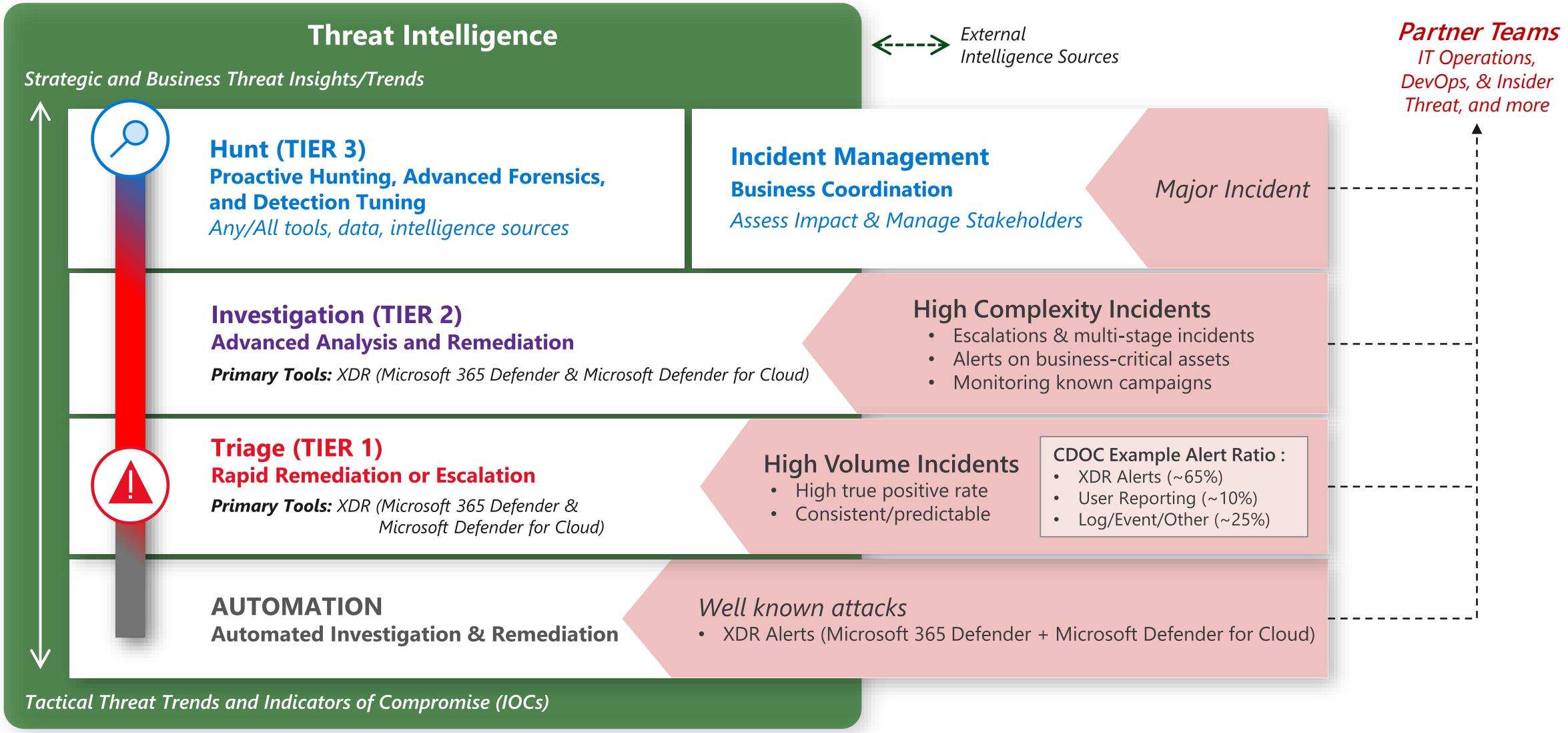


Security Operations

Microsoft Reference Architecture

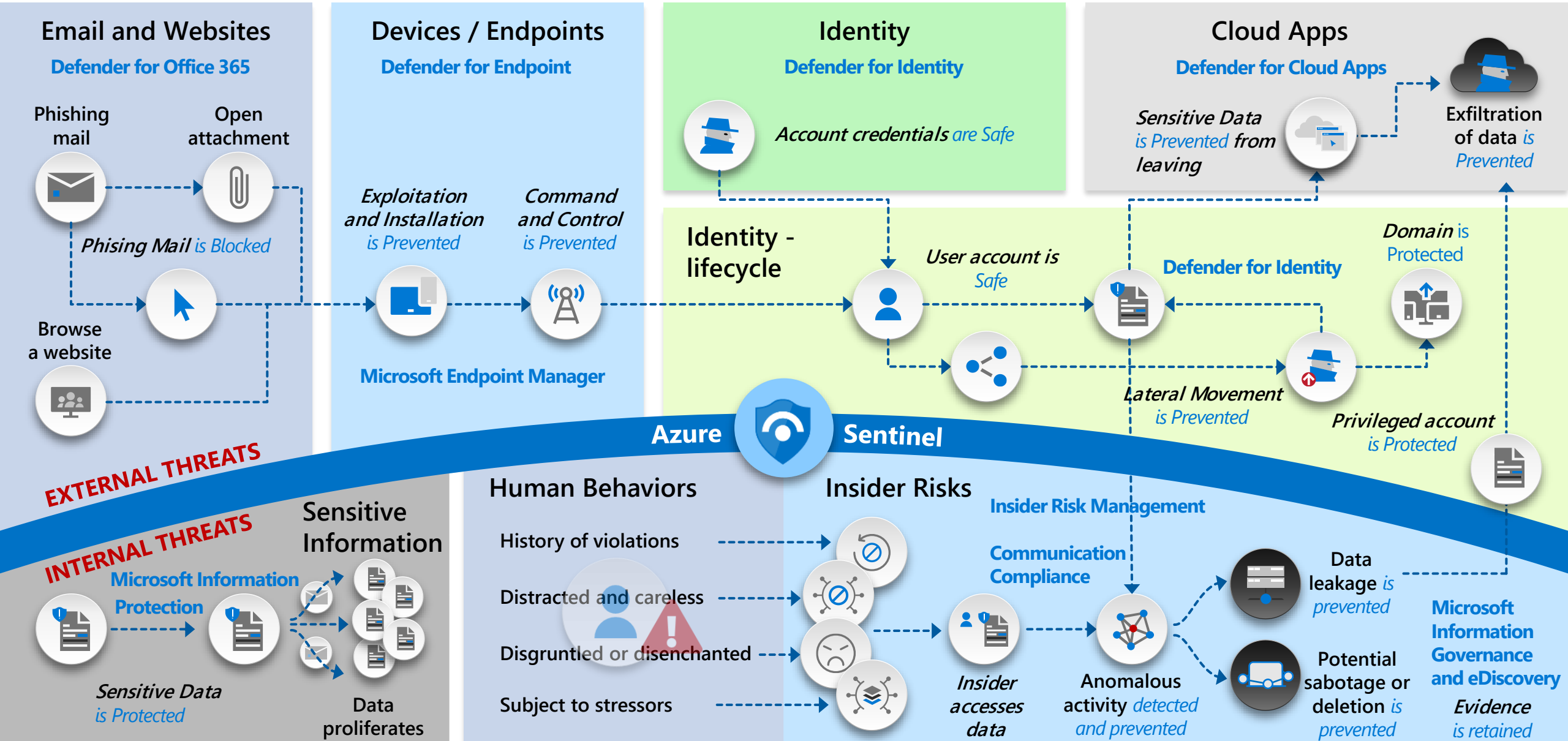


Security Operations Model – Functions and Tools



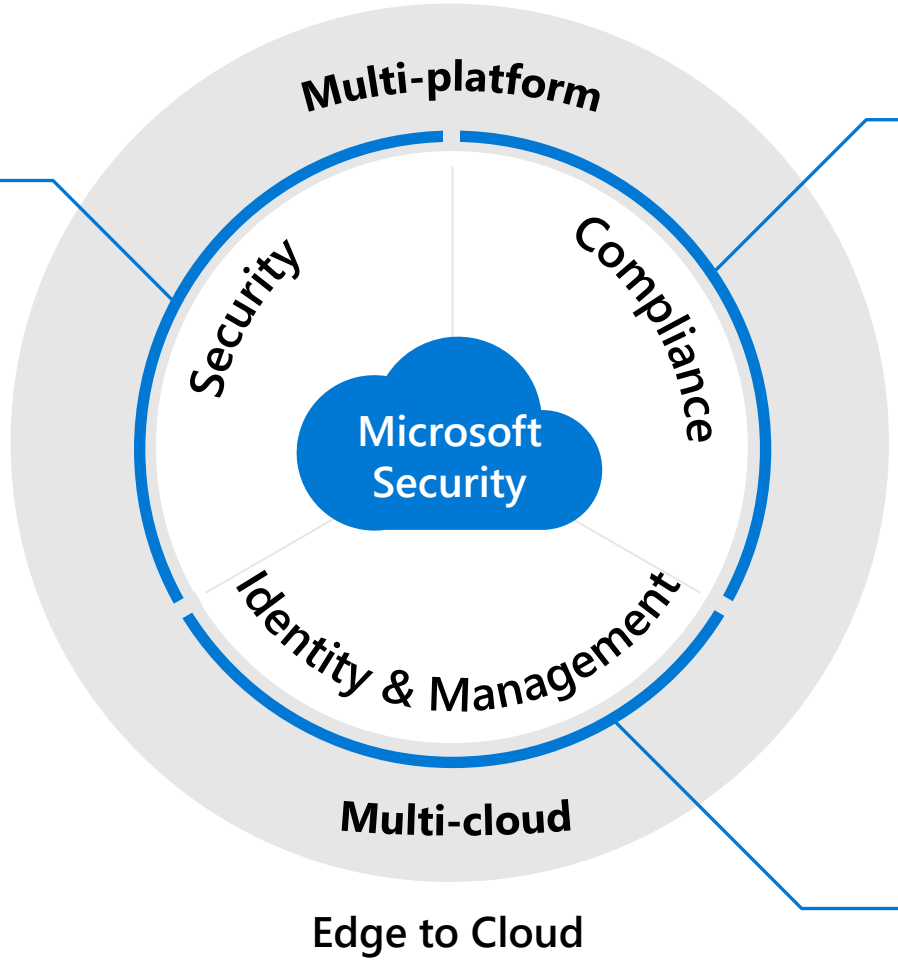
Proactive Services: Respond to threats in a sustainable way

Protect against internal and external threats using an integrated and automated platform approach



We integrate over 50 security categories

Endpoint detection and response
Endpoint protection platform
Forensic tools
Intrusion prevention system
Threat vulnerability management
Anti-phishing
User and entity behavior analytics
Threat intelligence feeds
App and browser isolation
Attachment sandboxing
Application control
End-user training
Network firewall (URL detonation)
Host firewall
Secure email gateway
Security assessment
SIEM
SOAR
Cloud access security broker
Cloud workload protection platform
Cloud security posture management
Incident response services
DDOS protection
IoT protection



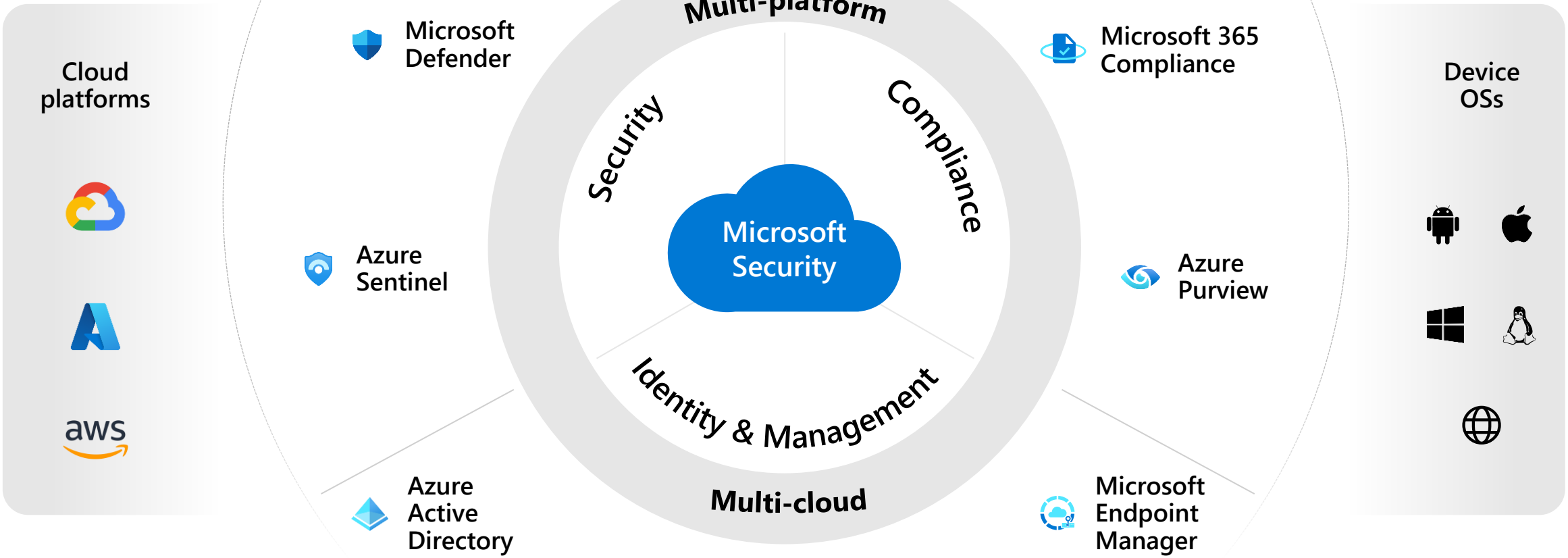
Data discovery
Data classification
Data loss prevention
Insider risk management
Data retention
Data deletion
Records management
eDiscovery
Audit
Risk assessments
Privileged access management
Compliance management
Information and messaging encryption
Device encryption
Encrypted cloud storage

Identity and access management
Single sign-on
User provisioning and lifecycle
User Directory
Multi-factor authentication
Passwordless authentication
Conditional access
Identity protection
Self-service password reset
Identity for Customers and Partners
Identity governance
Priviledged identity management

Endpoint management
Mobile application management
Mobile device management

And deliver them through six product families

Working together as one comprehensive solution



Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

December 2021 – https://aka.ms/MCRA

Security Operations / SOC

Threat Experts | *Detection and Response Team (DART)* | MSSP/MDR

Microsoft Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

Microsoft Defender – *Extended Detection and Response (XDR)*

Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting

- **Cloud** – *Azure, AWS, GCP, On Premises & other 3rd party clouds*
- **Endpoint** – *& Server/VM*
- **Office 365** – *Email and Apps*
- **Identity** – *Cloud & On-Premises*
- **SaaS** – *Cloud Apps*
- ***+ More*** – *OT, IoT, SQL, and more*
- *Other Tools, Logs, & Data Sources*

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. Security Documentation
2. Microsoft Best Practices
3. Azure Security Top 10 | Benchmarks | CAF | WAF

Software as a Service (SaaS)

Microsoft Defender for Cloud Apps

- *App Discovery & Risk Scoring (Shadow IT)*
- *Threat Detection & Response*
- *Policy Audit & Enforcement*
- *Session monitoring & control*
- *Information Protection & Data Loss Prevention (DLP)*

Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

Endpoints & Devices

Microsoft Endpoint Manager

Unified Endpoint Management (UEM)

Intune | Configuration Manager

Microsoft Defender for Endpoint

Unified Endpoint Security

- Endpoint Detection & Response (EDR)
- Web Content Filtering
- Threat & Vuln Management
- Endpoint Data Loss Protection (DLP)

Hybrid Infrastructure – IaaS, PaaS, On-Premises

Defender for Cloud – Cross-Platform Cloud Security Posture Management (CSPM)

Secure Score | Compliance Dashboard

On Premises Datacenter(s) | *3rd party IaaS & PaaS* | Microsoft Azure

Extranet: NGFW | Edge DLP | IPS/IDS | Azure AD App Proxy *Beyond User VPN*

Intranet: Azure Arc | Azure Stack

Express Route | Private Link

Azure Marketplace

- Azure Firewall & Firewall Manager
- Azure WAF
- DDoS Protection
- Azure Key Vault
- Azure Bastion
- Azure Lighthouse
- Azure Backup
- *Security & Other Services*

Information Protection

Classification Labels

- Azure Purview
- Microsoft Information Protection (MIP) – Discover, Classify, Protect, Monitor
- File Scanner *(on-premises and cloud)*
- Data Governance
- Advanced eDiscovery

Compliance Manager

Azure Active Directory

- Passwordless & MFA – Hello for Business, Authenticator App, FIDO2 Keys
- Identity Protection – Leaked cred protection, Behavioral Analytics
- Azure AD PIM
- Identity Governance
- Azure AD B2B & B2C

Defender for Identity

Active Directory

Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users

Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance

Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls

Windows 10 & 11 Security

- *Network protection*
- *Credential protection*
- *Full Disk Encryption*
- *Attack surface reduction*
- *App control*
- *Exploit protection*
- *Behavior monitoring*
- *Next-generation protection*

IoT and Operational Technology (OT)

Azure Sphere

Microsoft Defender for IoT

- *ICS, SCADA, OT*
- *Internet of Things (IoT)*
- *Industrial IoT (IIoT)*
- *Asset & Vulnerability management*
- *Threat Detection & Response*

Defender for Cloud – Cross-Platform, Cross-Cloud XDR

Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses

People Security

Attack Simulator | Insider Risk Management | Communication Compliance

GitHub Advanced Security – Secure development and software supply chain

Threat Intelligence – 8+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

The way forward path

The Future of the CISO - A view from Gartner

More companies are appointing a CISO with *"decreasing responsibility for day-to-day security operations, and a greater level of participation in strategic business decisions"*

http://www.iweek.co.za/training-and-recruitment/new-security-order

Gartner says:

"CISOs must be leaders for digital transformation"

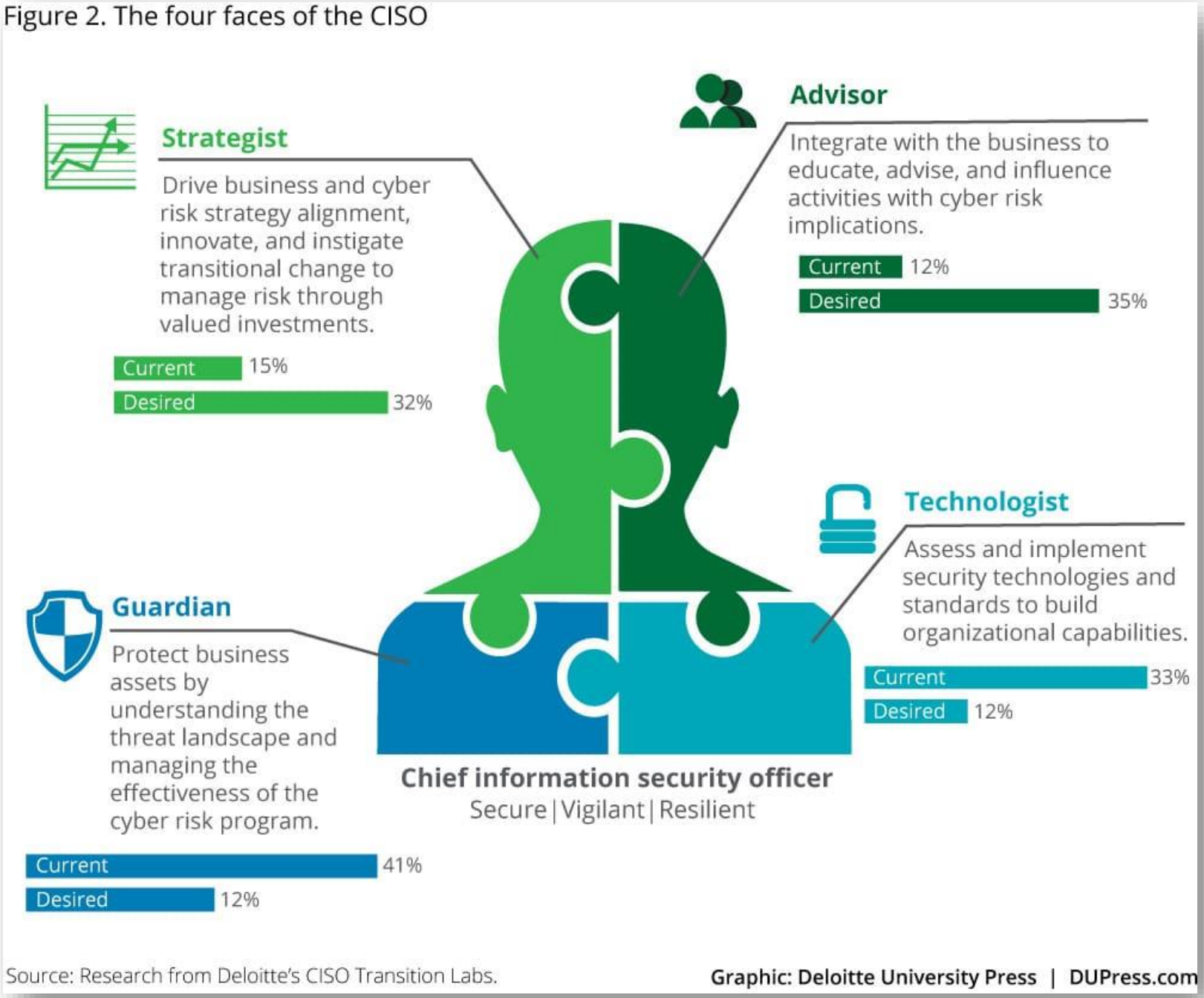
https://www.gartner.com/en/information-technology/role/security-risk-management-leaders

"By proactively assessing risk appetite and the value of the desired business outcome, CIOs and chief information security officers (CISOs) can transform digital risk management into a competitive advantage."

John A. Wheeler
Director, Gartner Research & Advisory

The four faces of The Modern CISO

Figure 2. The four faces of the CISO



Source: Research from Deloitte's CISO Transition Labs.

Graphic: Deloitte University Press | DUPress.com

Summary and End Note

- The CISO role will grow and gain respect, will become an **ENABLER** rather then a **DISABLER**.
- Develop a **communications strategy and plan** for continuation stakeholder engagement and education.
- Focus on your most important mission i.e. **Preserve customer/user trust**, **Prevent damage to your environment** and **Ensure compliance**.
- Reduce operational complexity will result in the **consolidation of IT security vendors** and **tools**.

Way Ahead

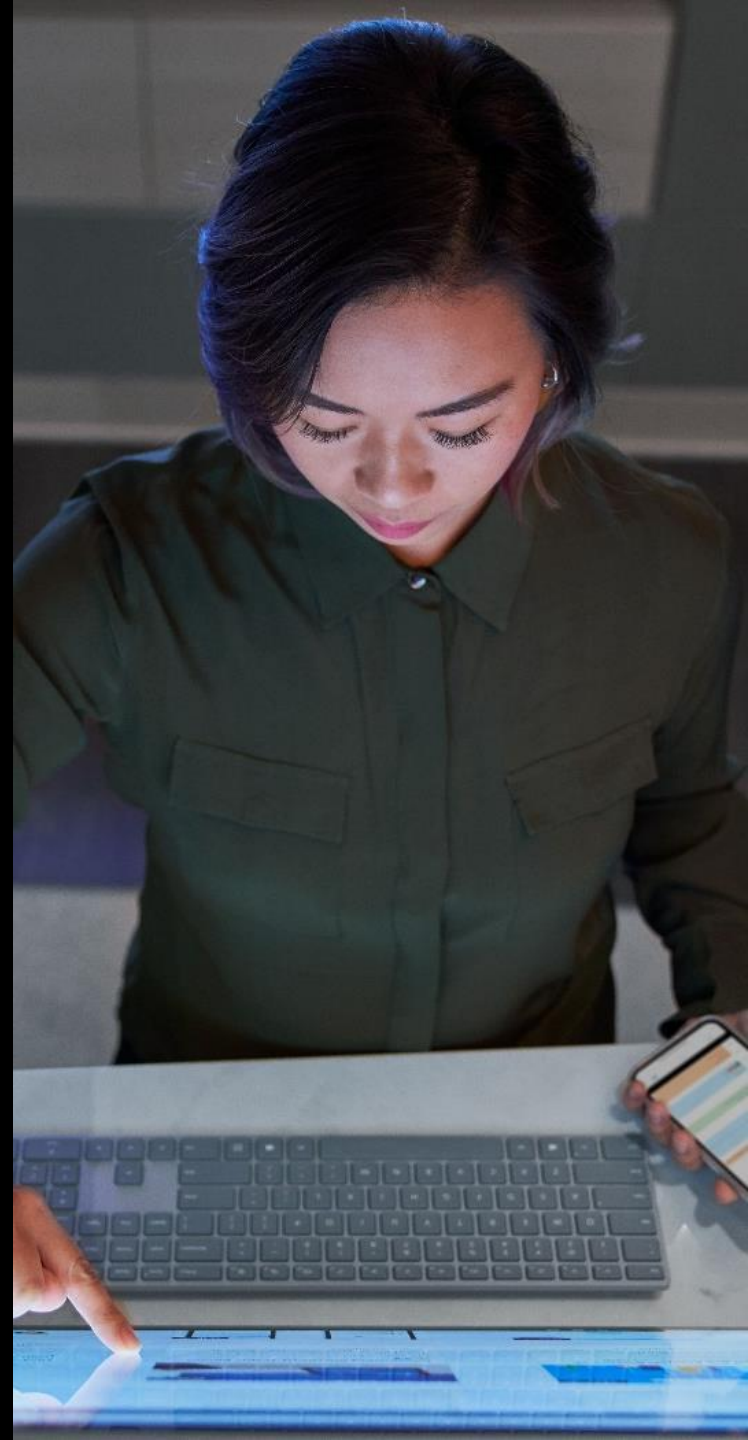
Delivering a seamless and secure experience for every employee in a hybrid world

Managing costs and where to consolidate

Modernizing security operations for faster resolution and risk remediation

Developing a compliance posture to address growing privacy concerns and complex regulations

Establishing a strategy to acquire and develop security talent in a competitive and scare skills market



Microsoft Security

Bonus slides

Board communication tips from Microsoft's CISO

- Updates and Discussion, have discussion as and when needed and updates 2 or 3 times a year.
- 5 questions CISOs need to ask themselves before presenting to the board
  1. Can you demonstrate a good governance process ?
  2. Do you have the right talent in place ?
  3. What are you doing to ensure a culture of cybersecurity ?
  4. How are you dealing with Technical Debt
  5. How are you and what are you doing to Future Proofing the company?

https://www.microsoft.com/en-us/videoplayer/embed/RE30ldv?autoplay=true

Further reading and learning resources

- Microsoft Security: What cybersecurity skills do I need to become a CISO? - Microsoft Security Blog
- Curiosity is key for a career in cybersecurity - Microsoft News Centre Europe
- CISO Stressbusters: 7 tips for weathering the cybersecurity storms - Microsoft Security Blog
- CISO Workshop Slides/Videos
- CISO series - Microsoft Security Blog
- How CISOs are preparing to tackle 2022 - Microsoft Security Blog
- Microsoft CISO Bret Arsenault provides practical advice to secure your hybrid workspace - Inside Track Blog
- Security | Managing Cyber Risk | Microsoft
- Zero Trust: Security Through a Clearer Lens session (Recording | Slides)
- Microsoft's IT Learnings from (ongoing) Zero Trust journey

Thank you

https://aka.ms/abbas