

Mastering Microsoft

Streamlined
Security for
On-Prem,
Multi-Cloud
& Workspaces



Anna Barkvall

Director Strategic Programs Global Portfolio Management

Orange Cyberdefense Group



Cyberdefense

Security is a team sport

Microsoft Intelligent Security Association

Microsoft Intelligent Security Association

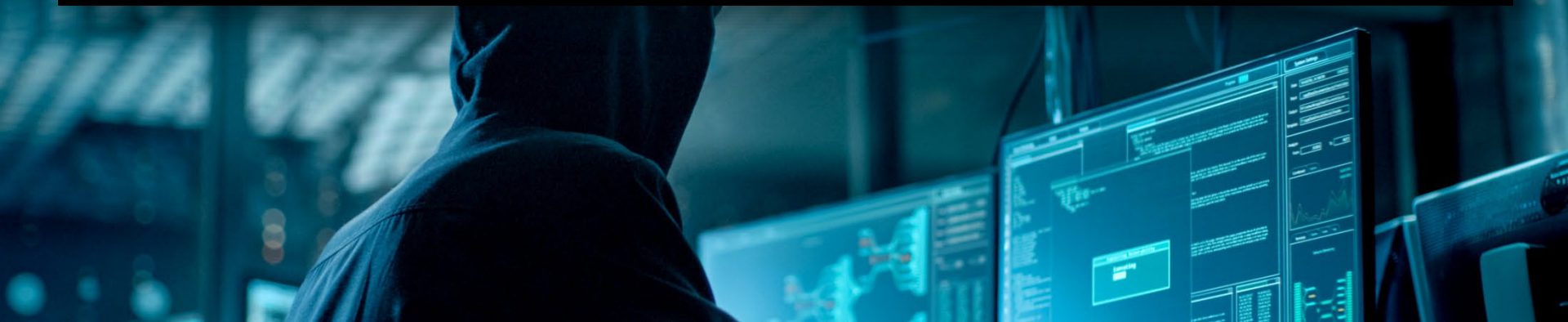


Microsoft teams up with security partners to build an ecosystem of intelligent security solutions to better defend our joint customers.



Attacker realities

Attackers have access to cheap and readily available resources to unleash creative assaults on your organization that don't align with your mission, tech, or tools.



New ways of working, emerging threats



Navigating a shifting world

**Conventional security
tools have not kept
pace**



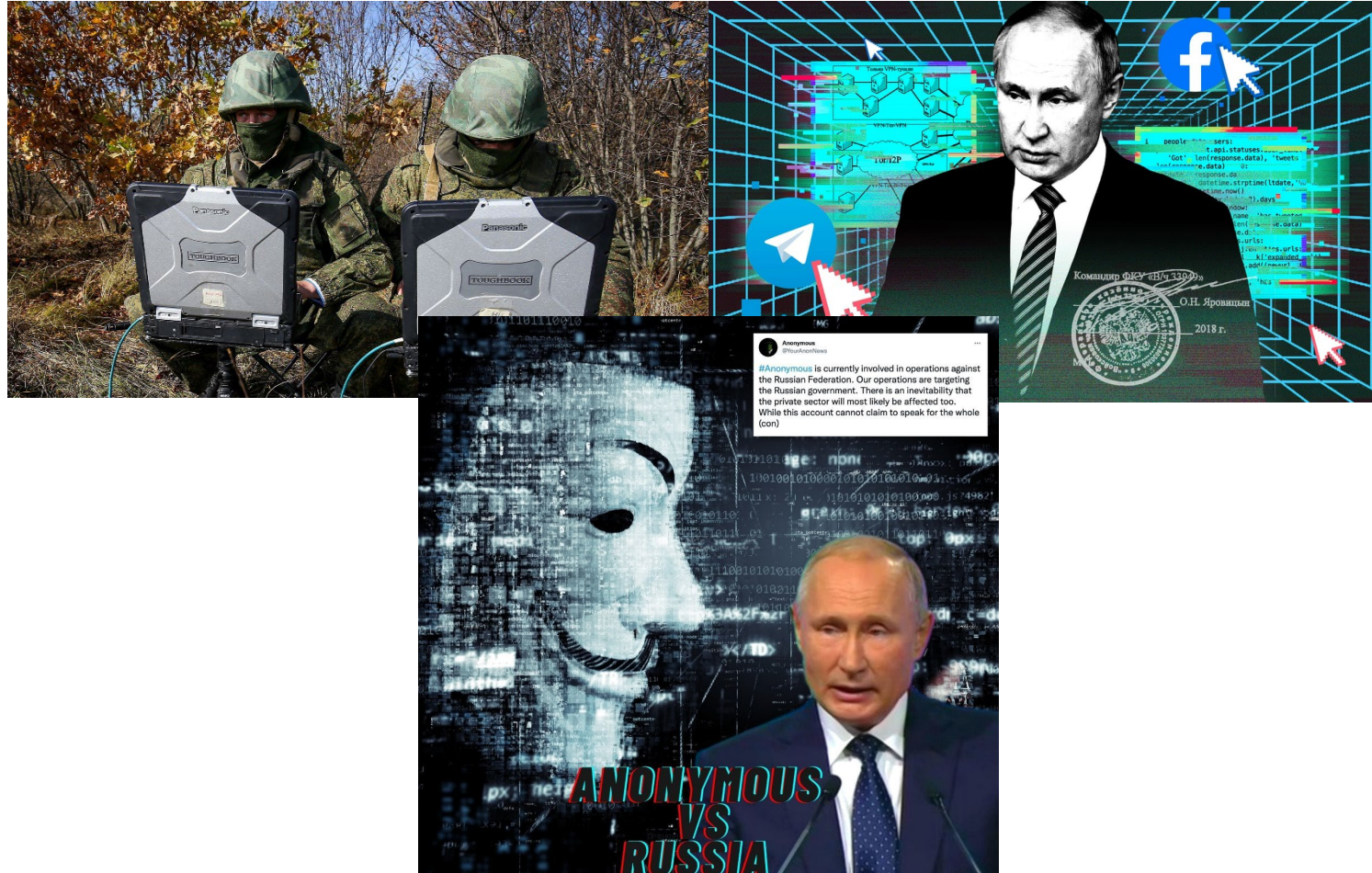
**Attacks growing
more sophisticated**



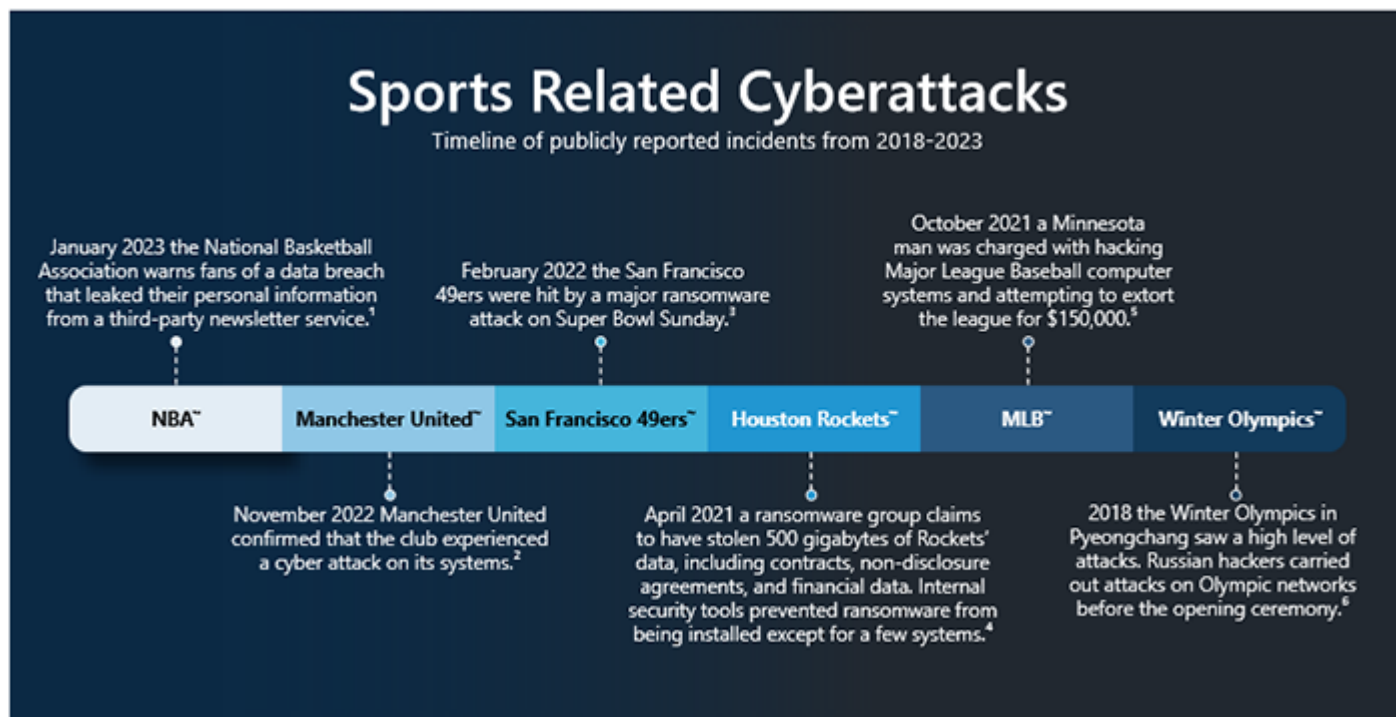
**Regulatory landscape
becoming more complex**



War



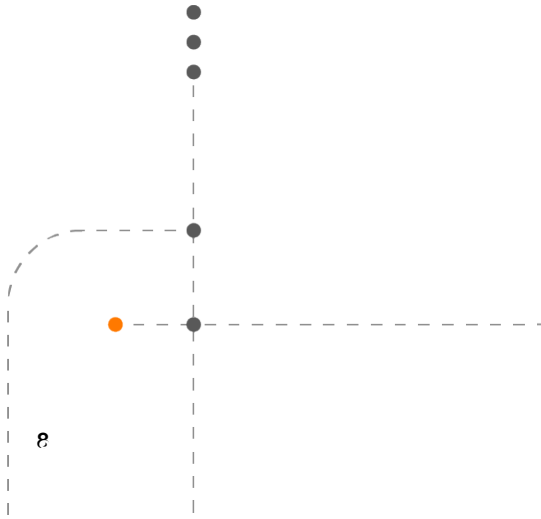
And even at sports



**98% basic security
protects against
+90% of attacks**



- MFA
- Zero trust
- Endpoint Detection and Response solution
- Patch
- Protect Data



Unstructured data is becoming the backbone

Organizations are increasingly relying on unstructured data, It accounts for 80 % of the data that an organization process daily



And it growing, and this trend is not going away because it's becoming the backbone of how business operate



Challenges of securing your cloud estate

1,181 different cloud services are used by enterprises on average

81% of orgs use two or more public cloud providers

27% increase in cloud and SaaS threats over the last year alone

52% cite data security concerns as a barrier to cloud expansion

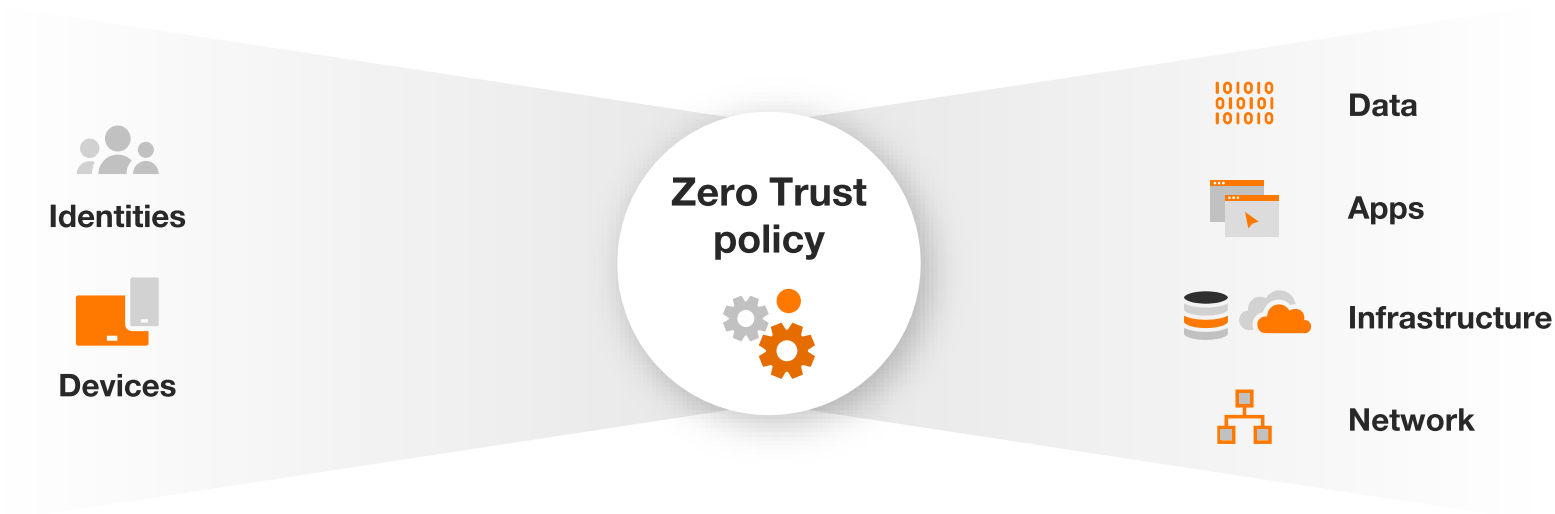


What formula

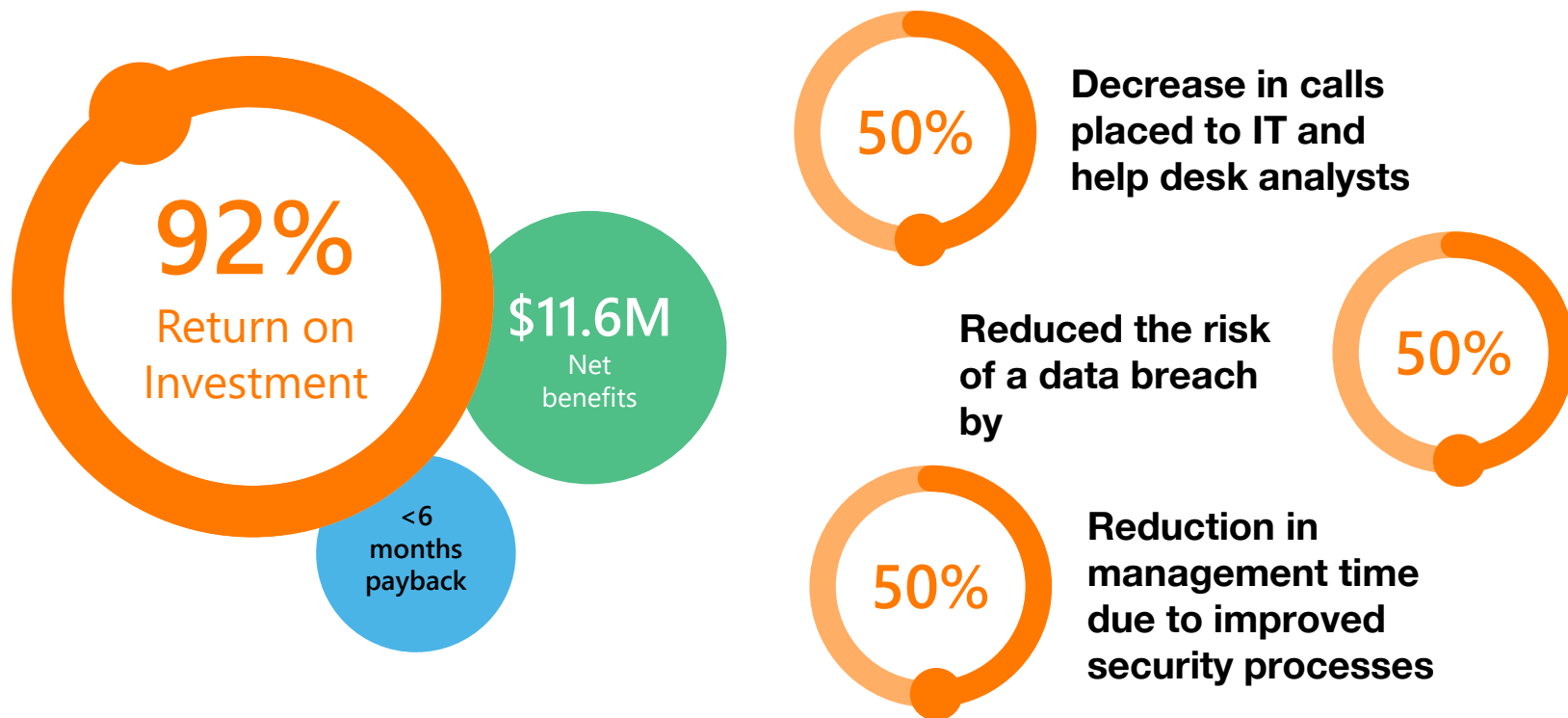


Securing your organization with Zero Trust

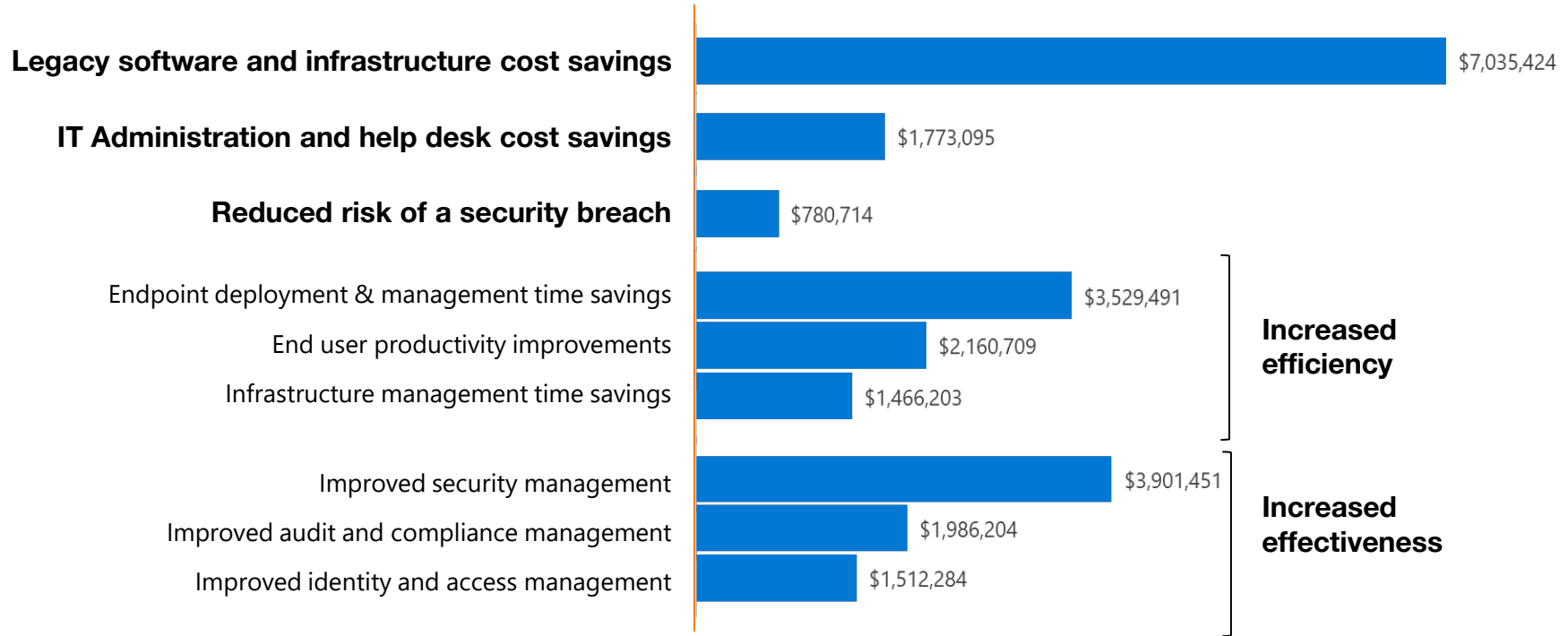
Verify explicitly | Use least-privileged access | Assume breach



Total Economic Impact™ of Zero Trust solutions from Microsoft

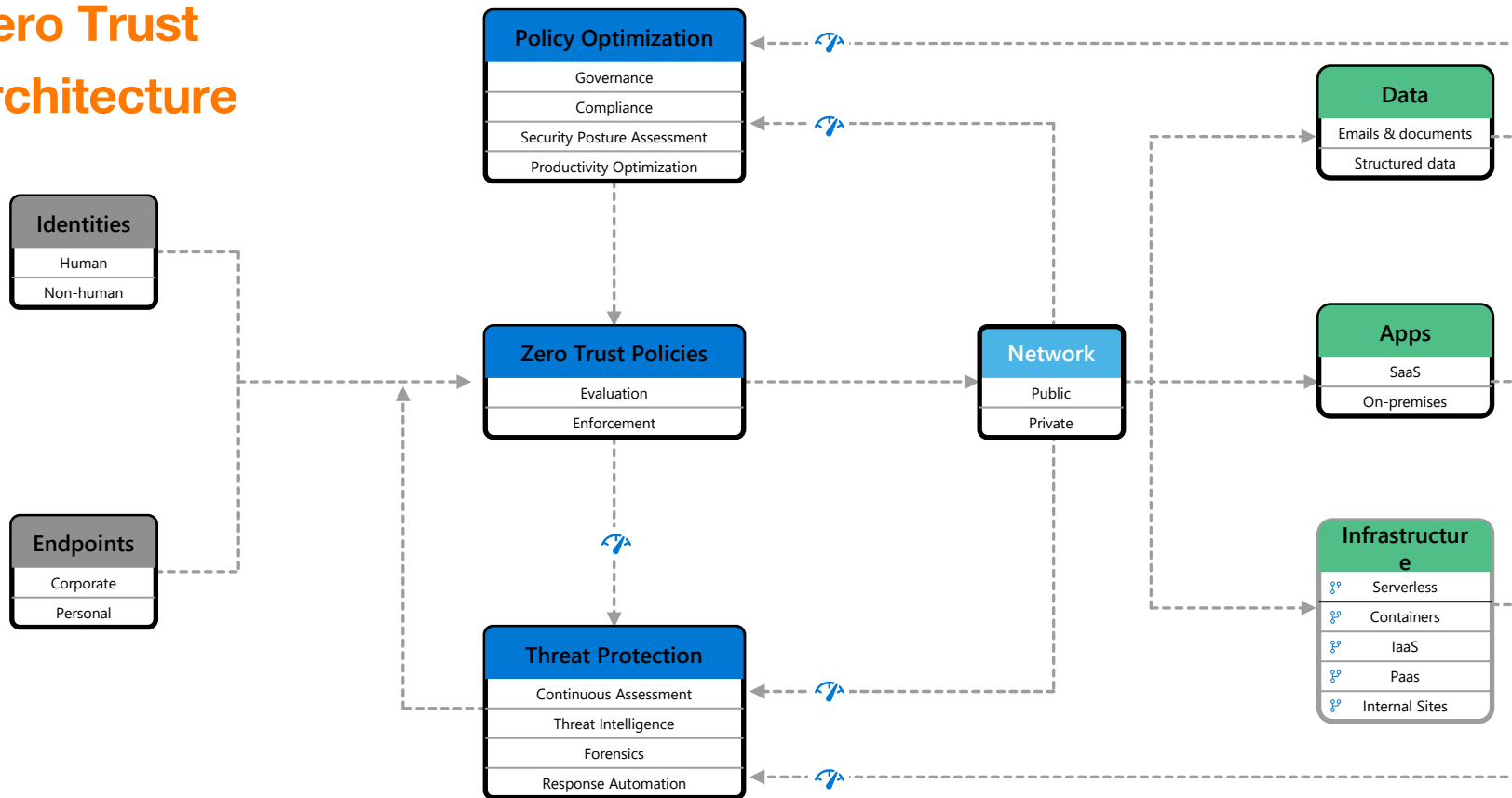


Benefits Value of Zero Trust solutions from Microsoft

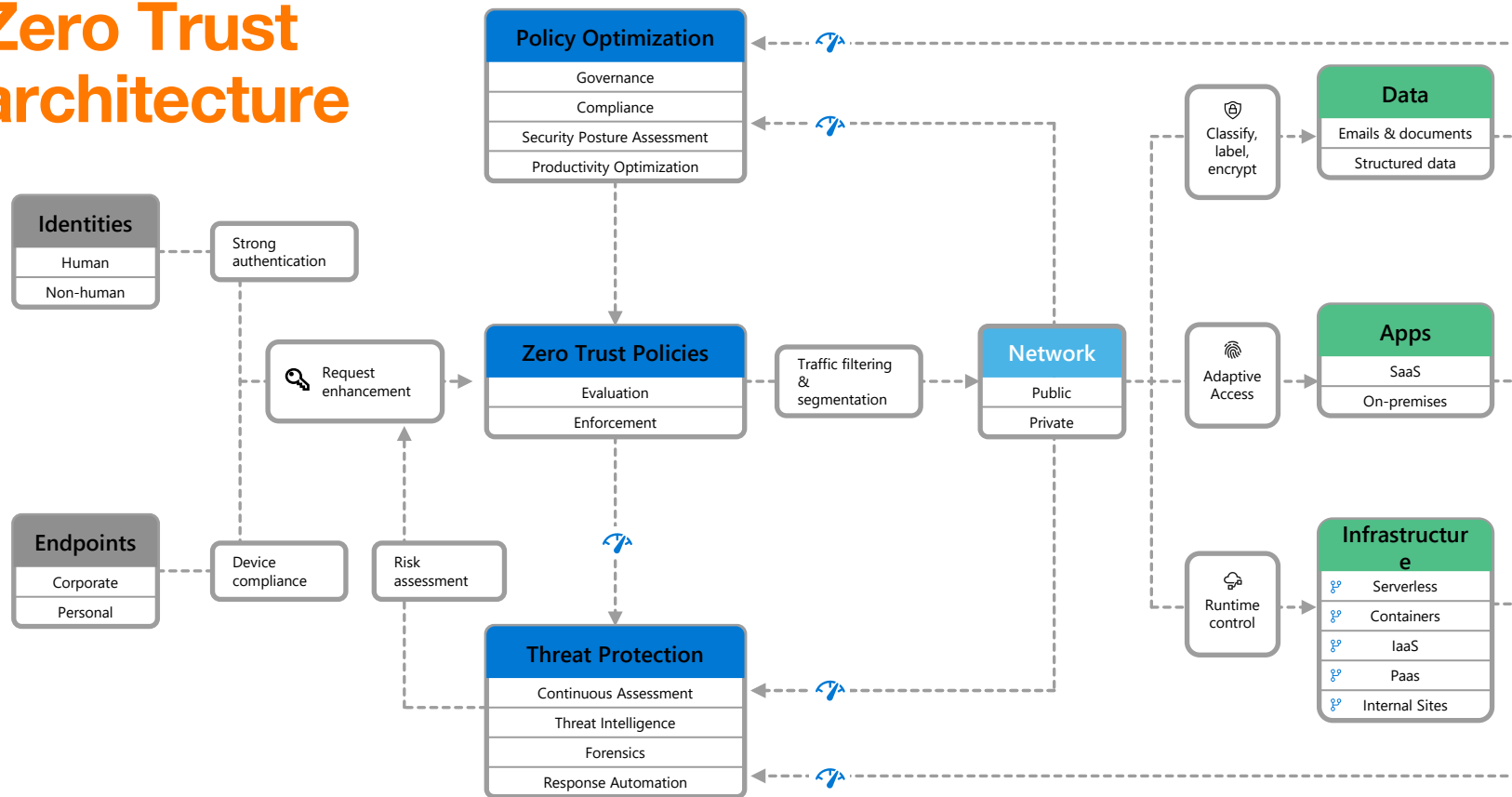


Three-year Present Value, risk adjusted, based on composite organization of 10,000 people: 5,000 knowledge workers with M365 E5 licenses and 5,000 frontline workers with M365 E3 licenses.

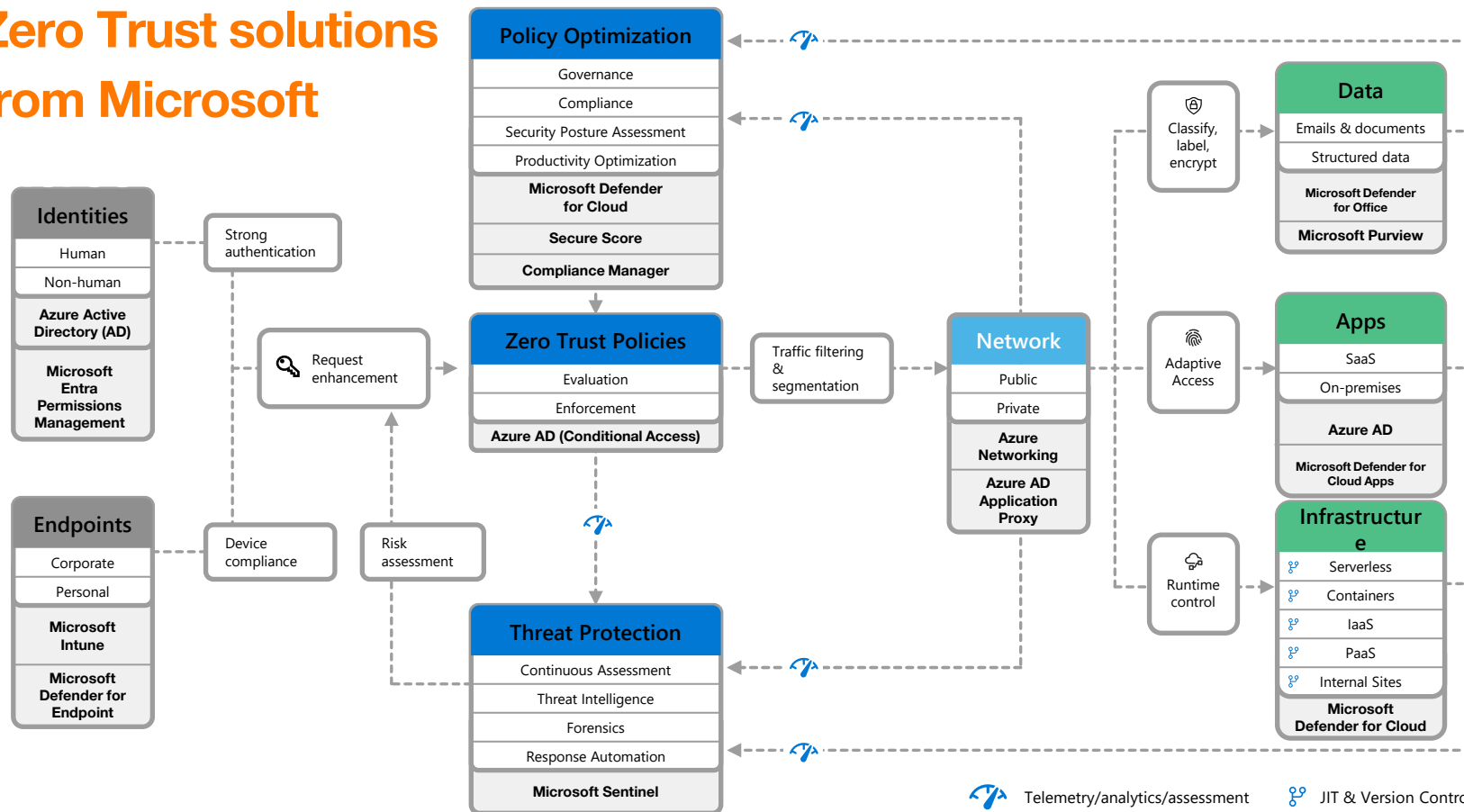
Zero Trust architecture



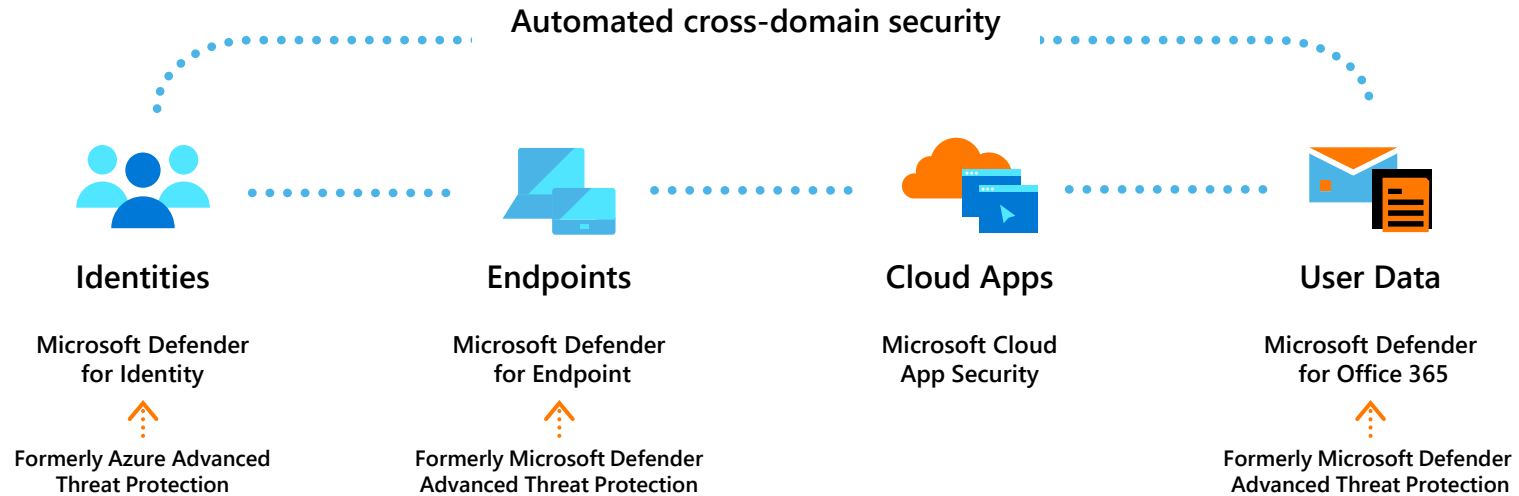
Zero Trust architecture



Zero Trust solutions from Microsoft



Microsoft 365 Defender

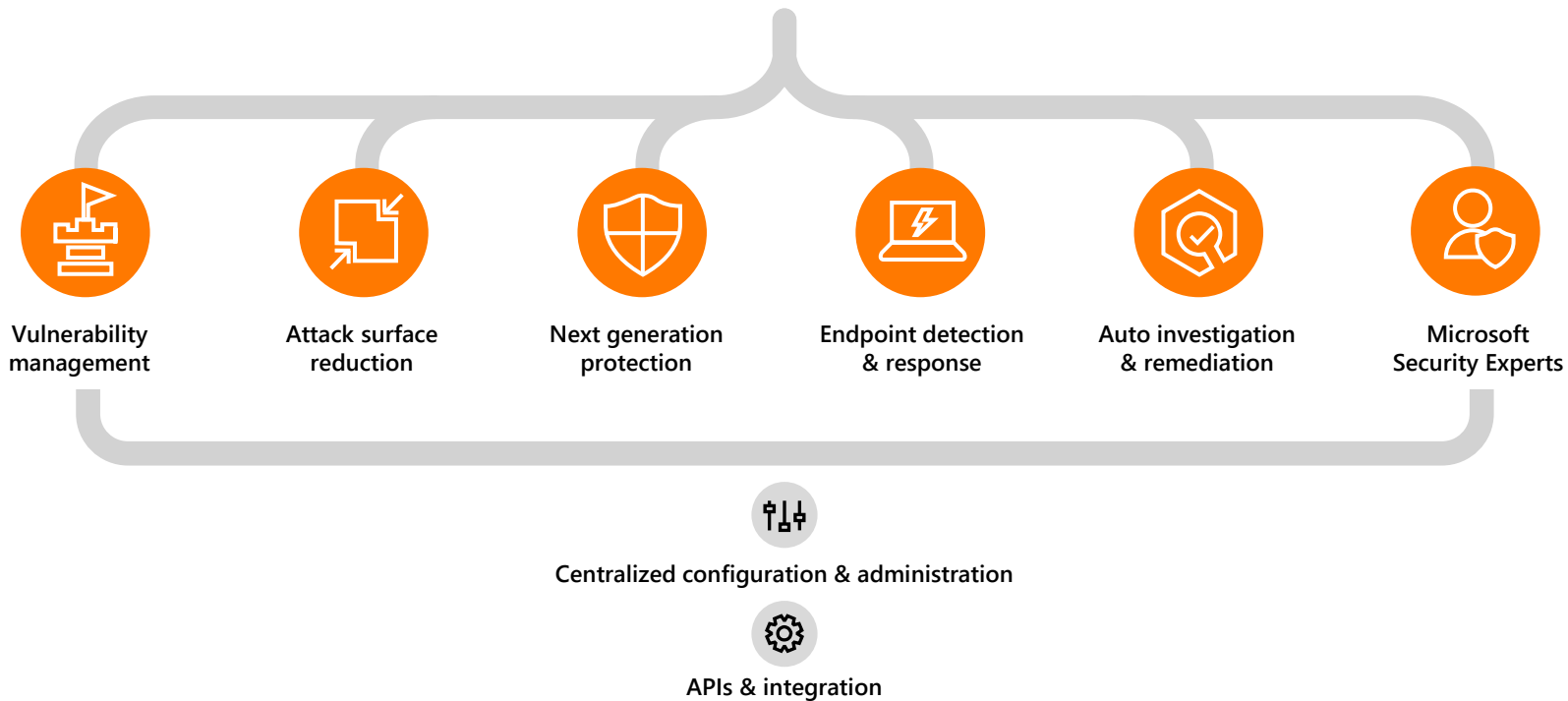


Shift from individual silos to coordinated cross-domain security

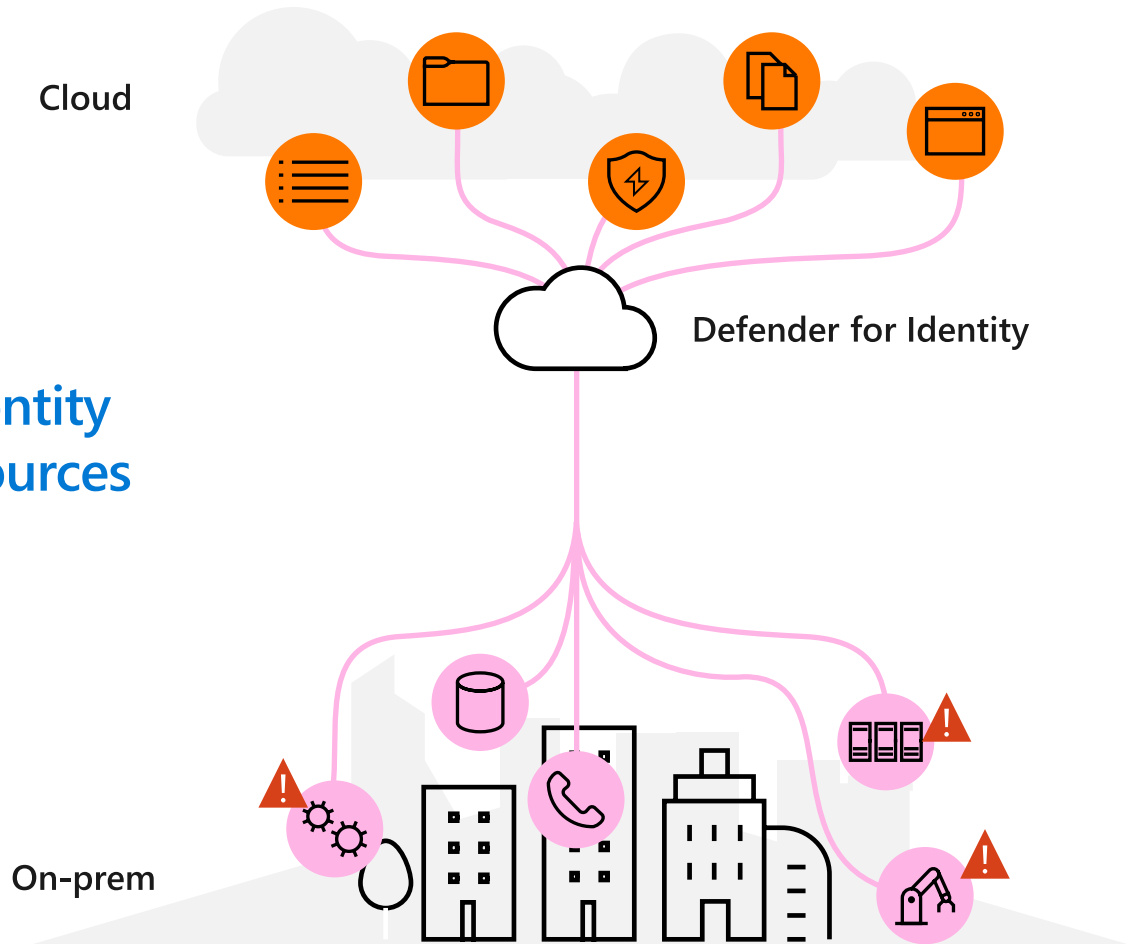


Microsoft Defender for Endpoint

Threats are no match.

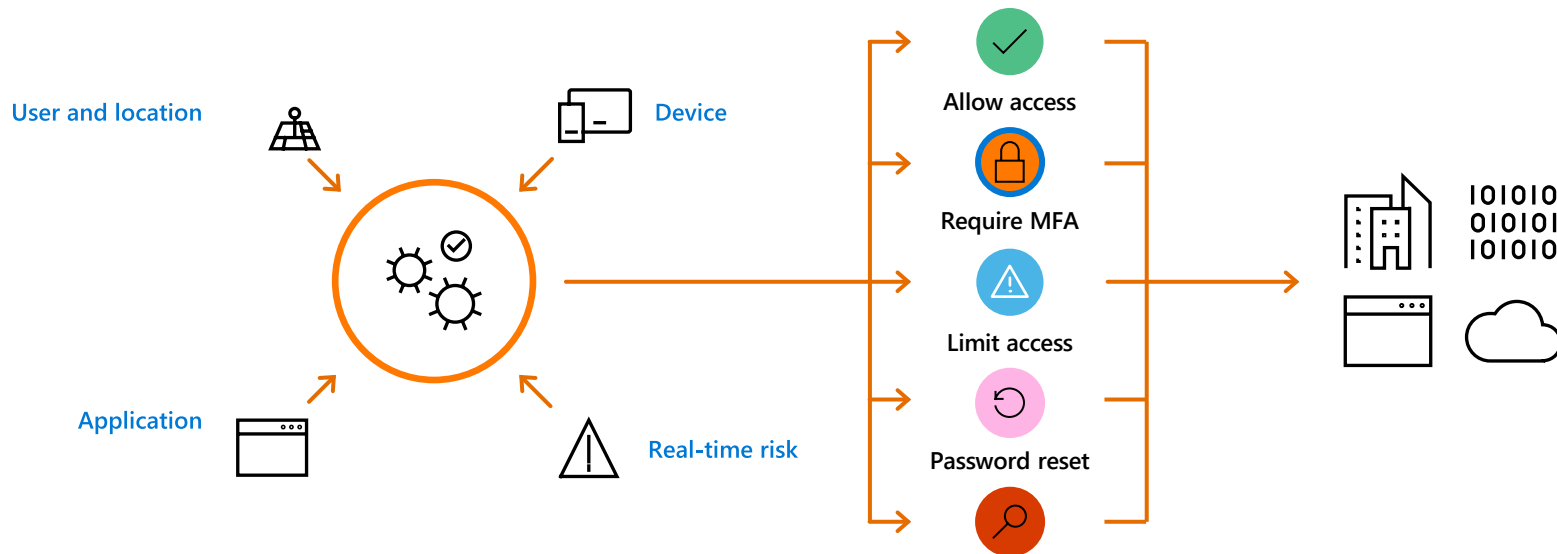


Microsoft Defender for Identity
monitors on-premises resources
and integrates with cloud
security solutions



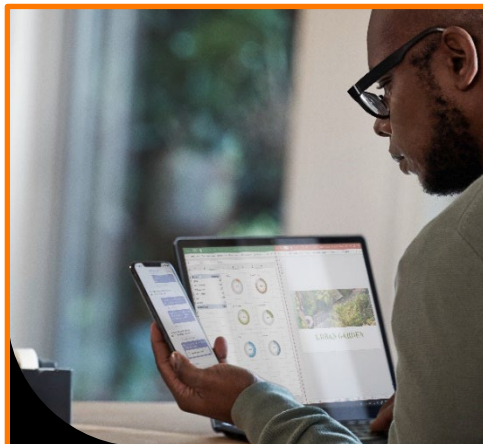
Protect resources with Conditional Access

Enable Zero Trust with strong authentication and adaptive policies



Multi-factor authentication

Verify user identities with strong authentication



We support a broad range of multi-factor authentication options

Including passwordless technology



Microsoft Authenticator



Windows Hello



FIDO2 Security key



Biometrics



Push Notification



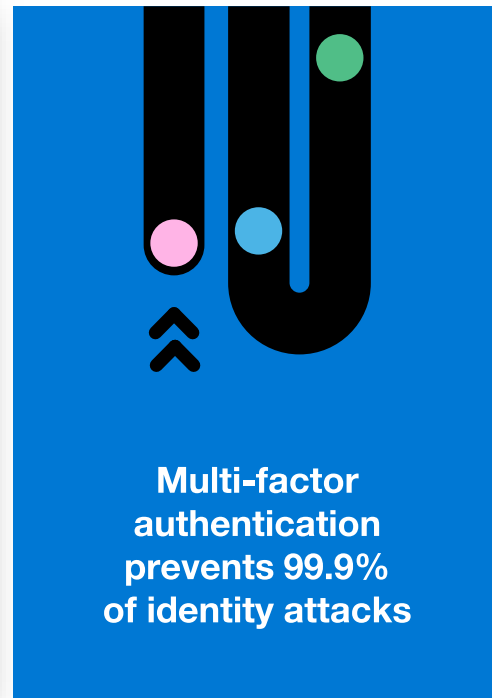
Soft Tokens OTP



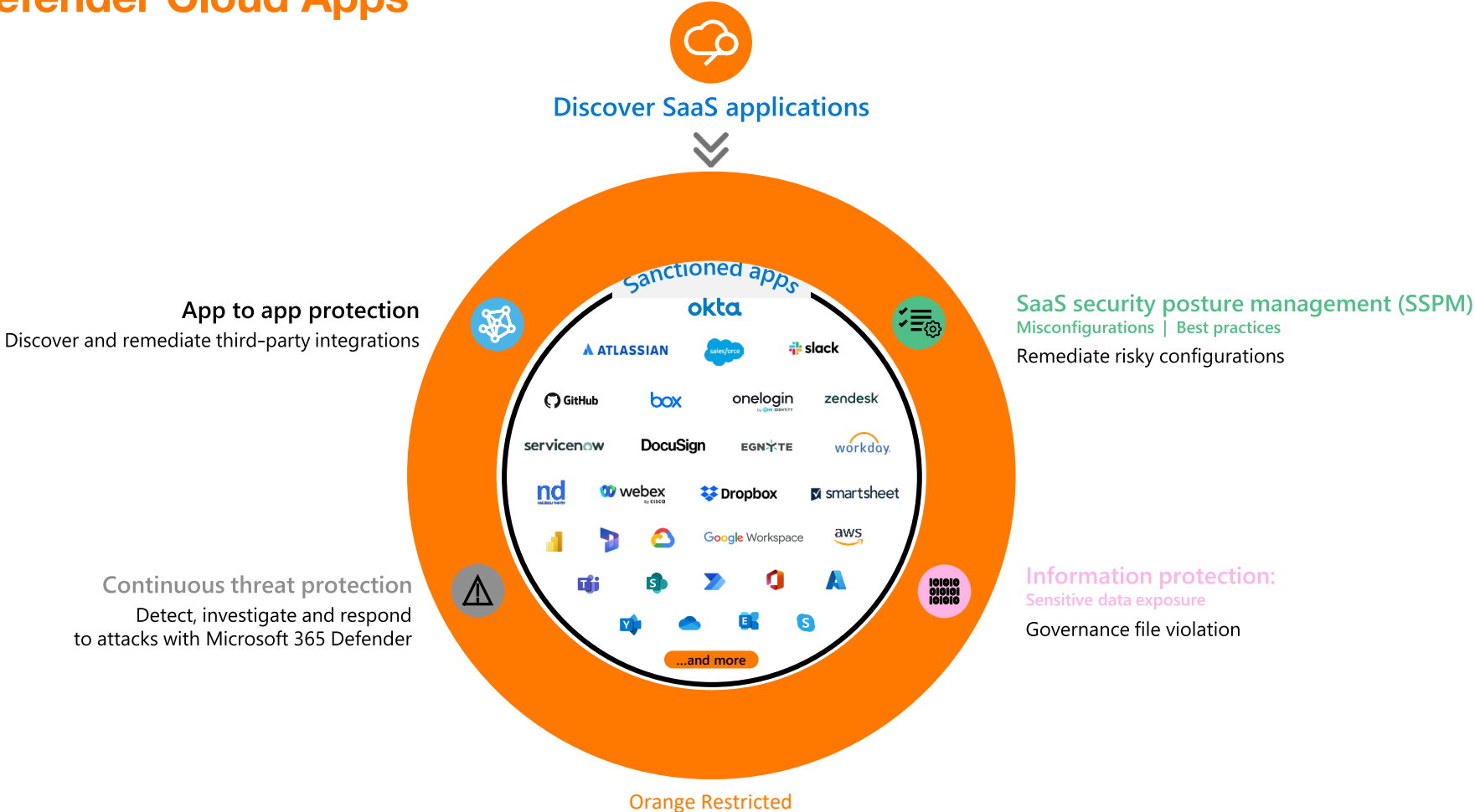
Hard Tokens OTP



SMS, Voice

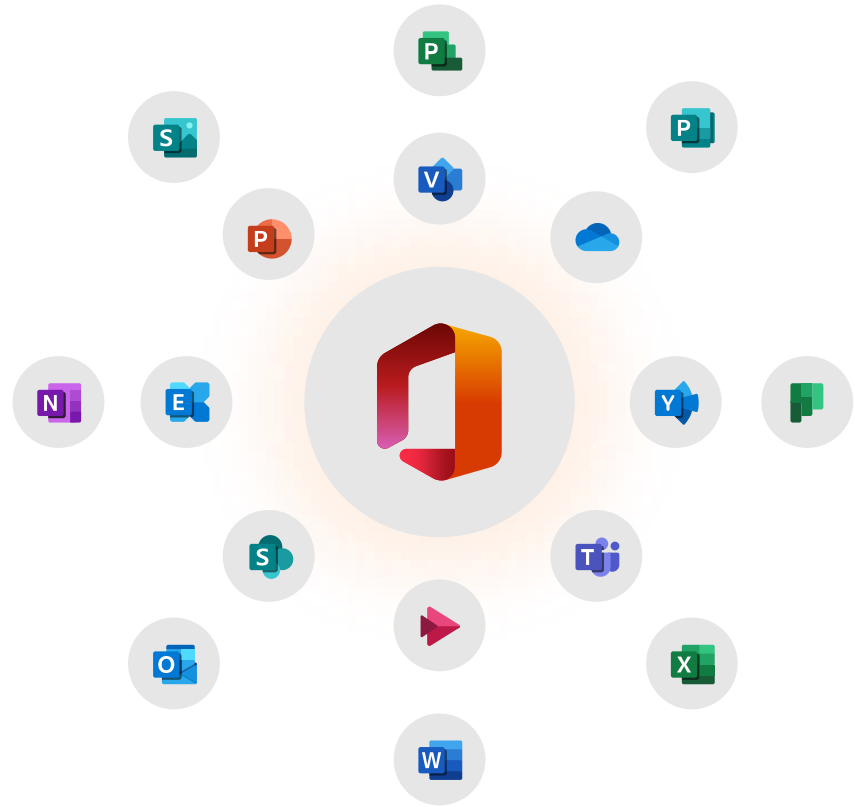


Defender Cloud Apps





Native protection for Office 365





What formula



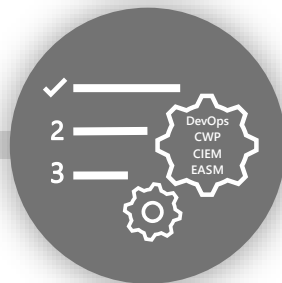
Defender for Cloud

Microsoft Defender for Cloud

Unify your DevOps
Security Management



Strengthen and manage your
cloud security posture



Protect your cloud
workloads



Microsoft Defender For Cloud

Cloud-native application protection across clouds and on-premises environments

Unify your DevOps
security management



DevOps posture
visibility across
pipelines



Infrastructure as
Code security



Code to cloud
contextualization



Integrated
workflows & pull
request annotations

Strengthen and manage
your security posture



Full visibility with
agentless and agent-
based scanning



Integrated insights
across DevOps, EASM,
CIEM, and workloads



Attack
path-based
prioritization



At-scale
governance
& automated
remediation



Security
compliance
management

Detect threats and
protect your workloads



Full-stack
threat protection



Vulnerability assessment
& management

Automate with the tools
of your choice



aws

Amazon Web Services



Microsoft Azure



Google Cloud Platform



On-premises

Free foundational CSPM

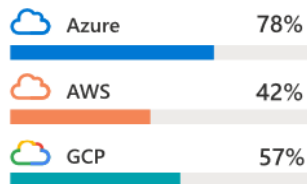
Secure Score

- » Strengthen security posture across all critical cloud resources including network, access, compute, databases, your service layer, and more
- » 450+ out-of-the-box recommendations
- » Create custom recommendations to meet organizational requirements

Multicloud security benchmark for security compliance

- Manage cloud security compliance with continuous assessment of cloud resources across Amazon Web Services, Microsoft Azure, and Google Cloud Platform in a single, integrated dashboard
- Use industry standards, regulatory compliance frameworks, and cloud-specific benchmarks to implement best practices (CIS, PCI, NIST, SOC, ISO HIPAA, etc.)
- Create custom recommendations to meet unique organizational needs

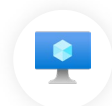
Secure score



Evaluated categories



Access



Compute



SQL server



IoT



Network

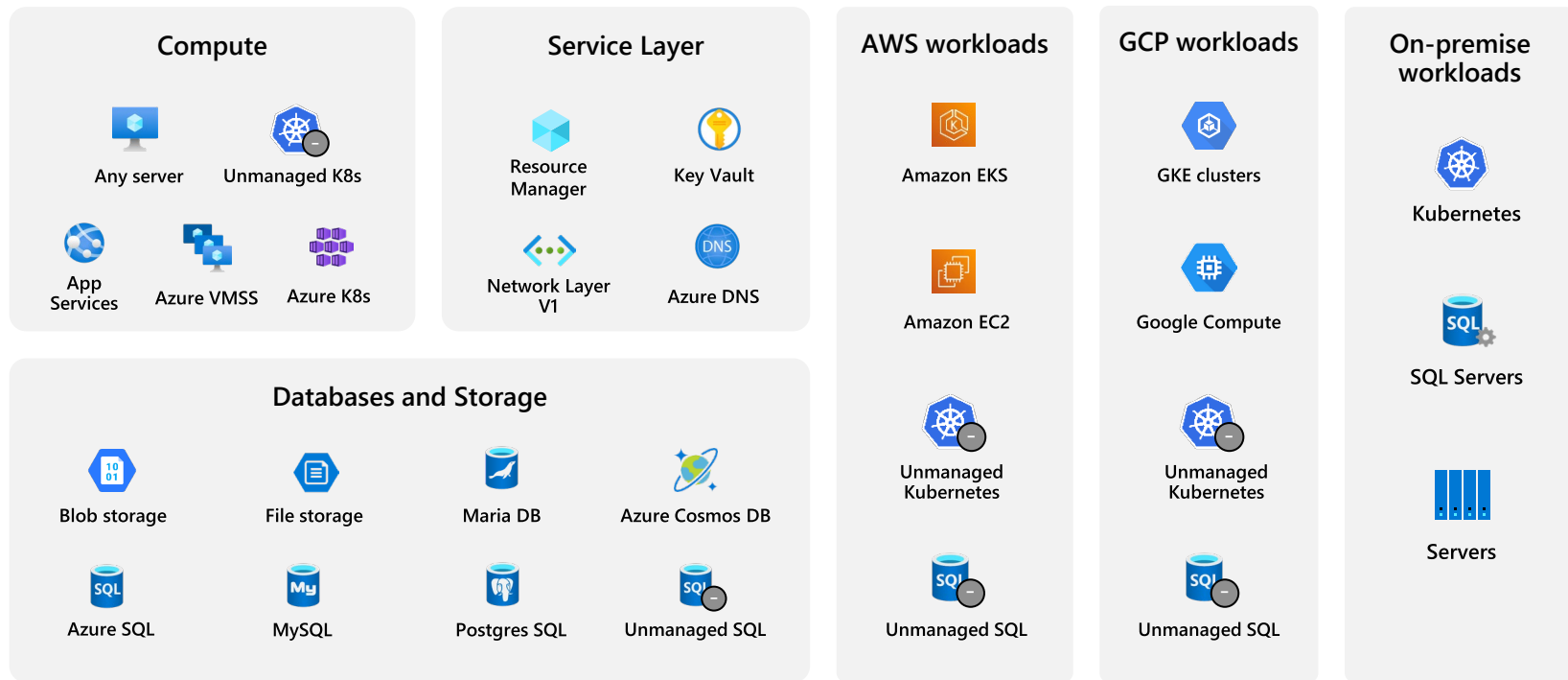


App Services



Containers

Full-stack coverage with dedicated detections



Dipped a toe in the water

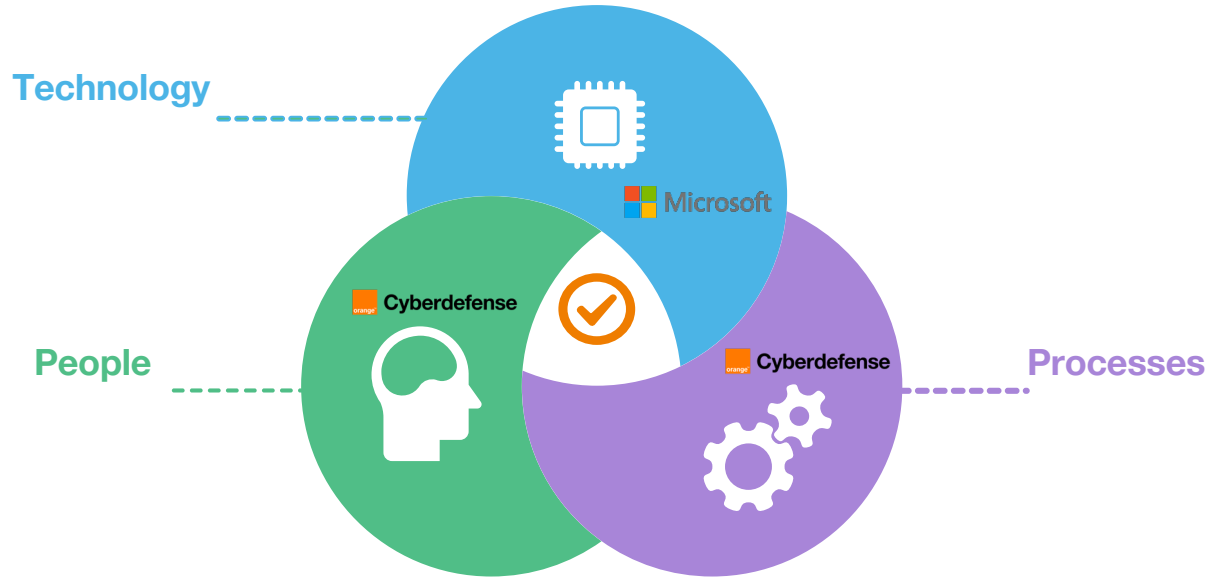


Microsoft's end-to-end security

Integrate up to 40 categories



Two leaders



The Orange Cyberdefense end-to-end Microsoft security framework



Assess



Advise



Build



Run

Assess your security solutions

1. Threat Protection
2. Security Operations
3. Hybrid Cloud Security
4. Securing Identities
5. Securing Assets
6. Securing Data
7. Manage and Investigate Privacy & Compliance Risks
8. Automation Opportunities
9. Ethical Hacking

Provide best practice and embed security strategy

1. Best practice utilization
2. Best practice configuration
3. Security Maturity Assessment
4. Cloud Security Maturity Assessment
5. Risk Management
6. Cyber Resilience and Crisis Management

Configure and onboard services

1. Best practice configuration and preparation for managed services
2. Operational handbook to prepare and establish operating model between client and MSSP



- **Managed Workspace Protection** and **Managed Threat Detection [xdr]** for Microsoft Defender 365
- **Managed Threat Detection [log]** for Sentinel
- **Managed Industrial System** for Defender IOT
- **Managed Vulnerability Intelligence** for Defender Vulnerability
- **Managed Cloud Security** for Microsoft Defender for Cloud and Microsoft Entra
- **Incident Response** Retainer ensuring you are prepared to handle major breaches across your Microsoft environment

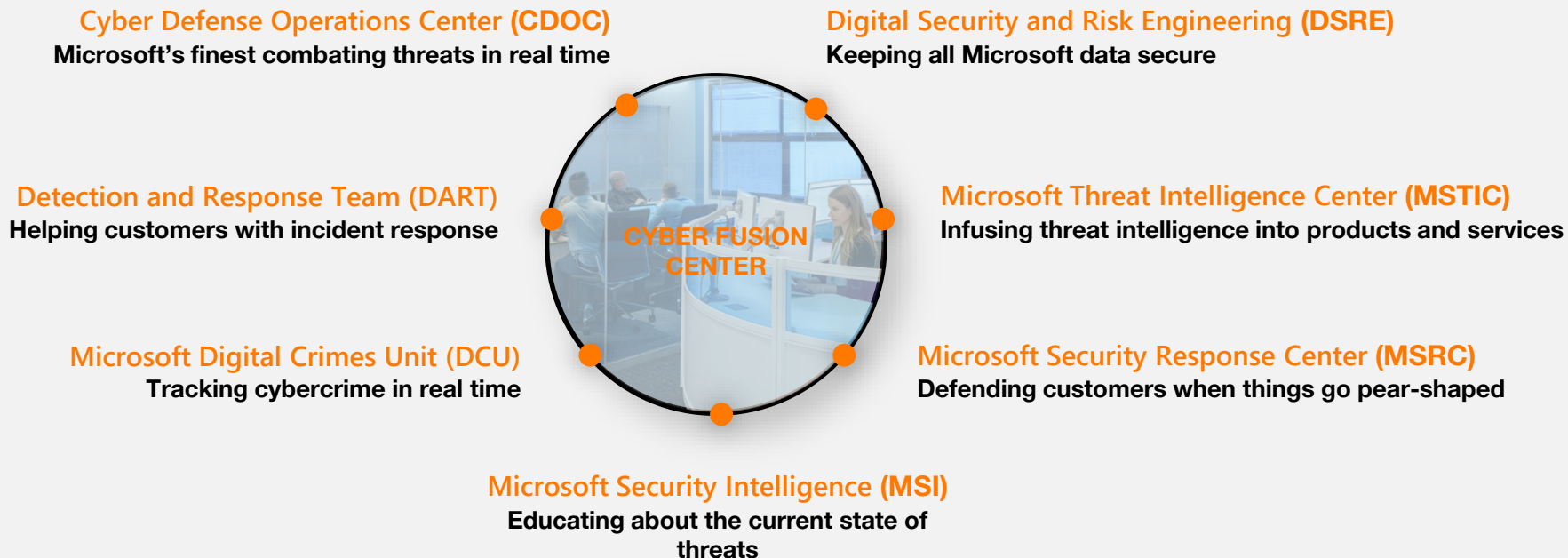
Professional Services

Managed Services

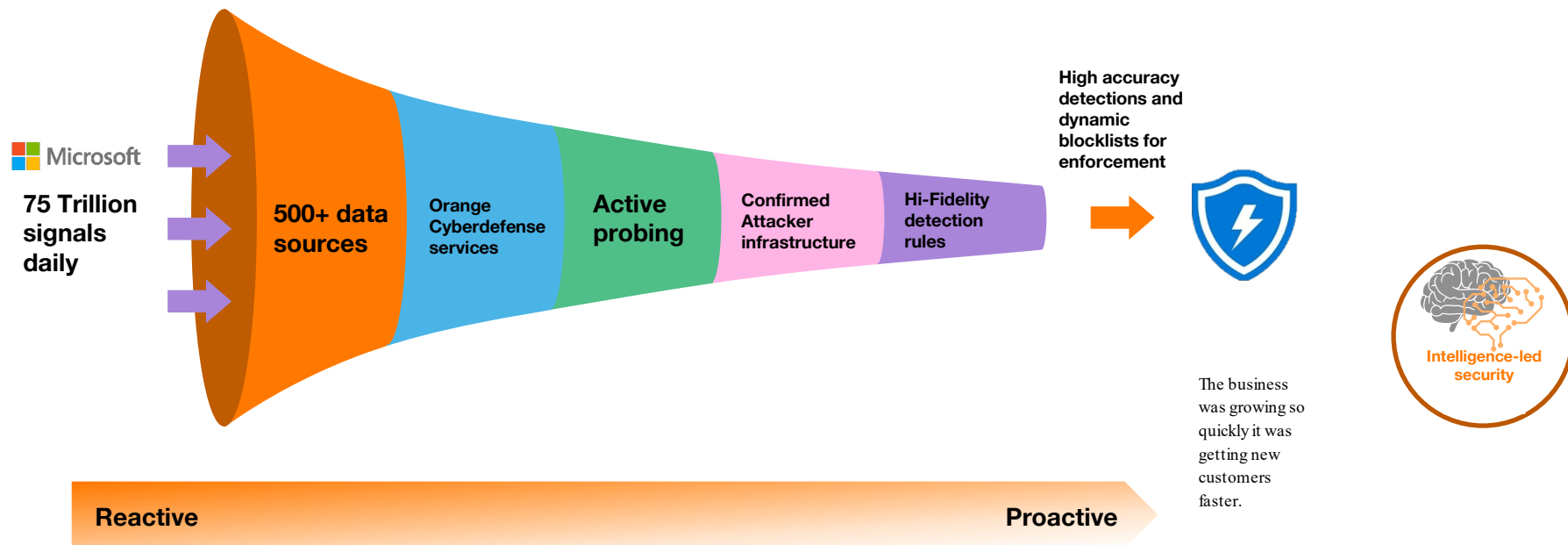
Working together: Coordinated response

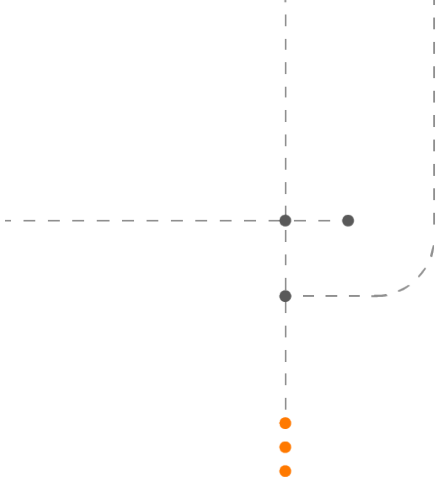


Using intelligence gained, Microsoft security teams work together to secure our platform



Orange Cyberdefense advanced intelligence





**Our security approach is driven by our knowledge of the threat,
and allows you to make the right decisions.**

So you can...

...ensure that you are gaining maximum value from your Microsoft investments.

...get an honest view of where Microsoft can consolidate security toolsets, and where it cannot.

...build Microsoft into a broader security strategy, supported by a cybersecurity leader in Orange Cyberdefense.

...utilize security operations provider that can deliver significant outcomes to drive improved cyber resilience.

Why Orange Cyberdefense?

Detection coverage

Broadest range of detection service options: log, endpoint, network, dark/deep web.

Proven methodology

Determine, visualize and improve your detection ability with our Threat Detection Framework and extensive Threat Intelligence Datalake.

Response coverage

Broadest range of response service options. Complement your own abilities in an optimal way.

Experience and expertise

Strong global footprint and more than 200 analysts, delivering MDR services for over 12 years.

Security and partnership

Our local teams work closely with our customers to continuously improve detection and response abilities.



Thanks



Cyberdefense