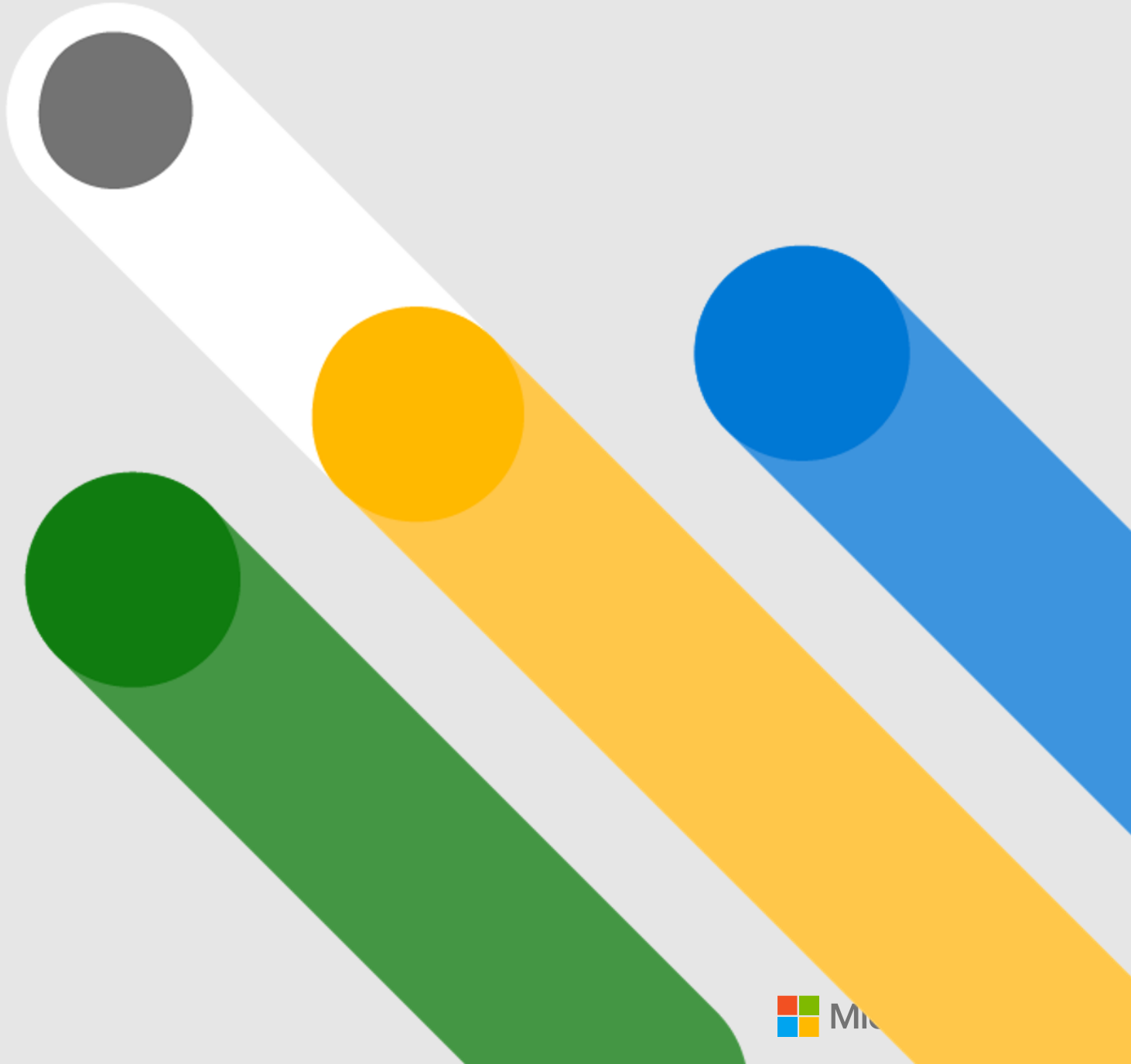
Microsoft Security

Securing the World:
Individuals, Companies, and Countries

C. Kelly Bissell
KellyBissell@microsoft.com



Topics for Today

1. Where I am coming from
2. Current cybersecurity market
3. The Future: how to make it better
4. Kelly's PICARD model
5. How Microsoft is making it better

Where am I coming from?

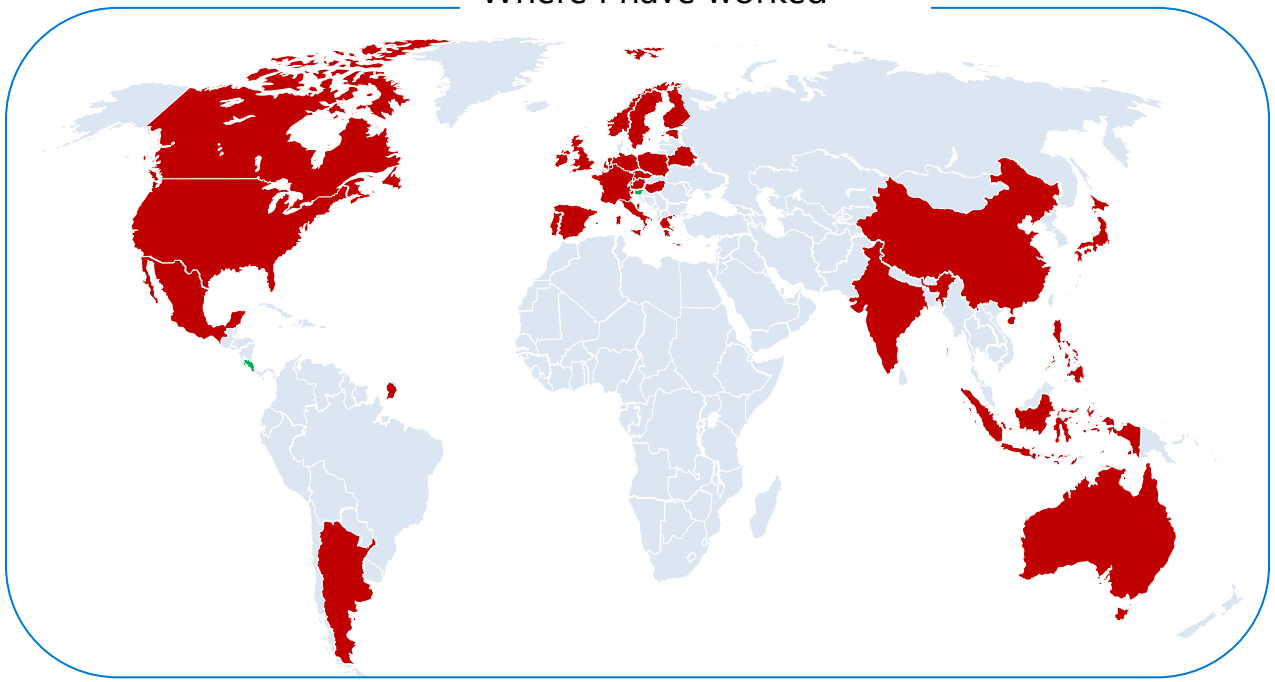
27
Years
Cyber
Experience

500+
Companies served

4
Roles: CISO, CIO,
Consultant, Vendor

18
Patents Issued

Where I have worked



What is Microsoft seeing?

Insights from

785K organizations in 120 countries

Analyzing

34T threat signals every day

Tracking

250+ nation-state actors & 160+ threat groups

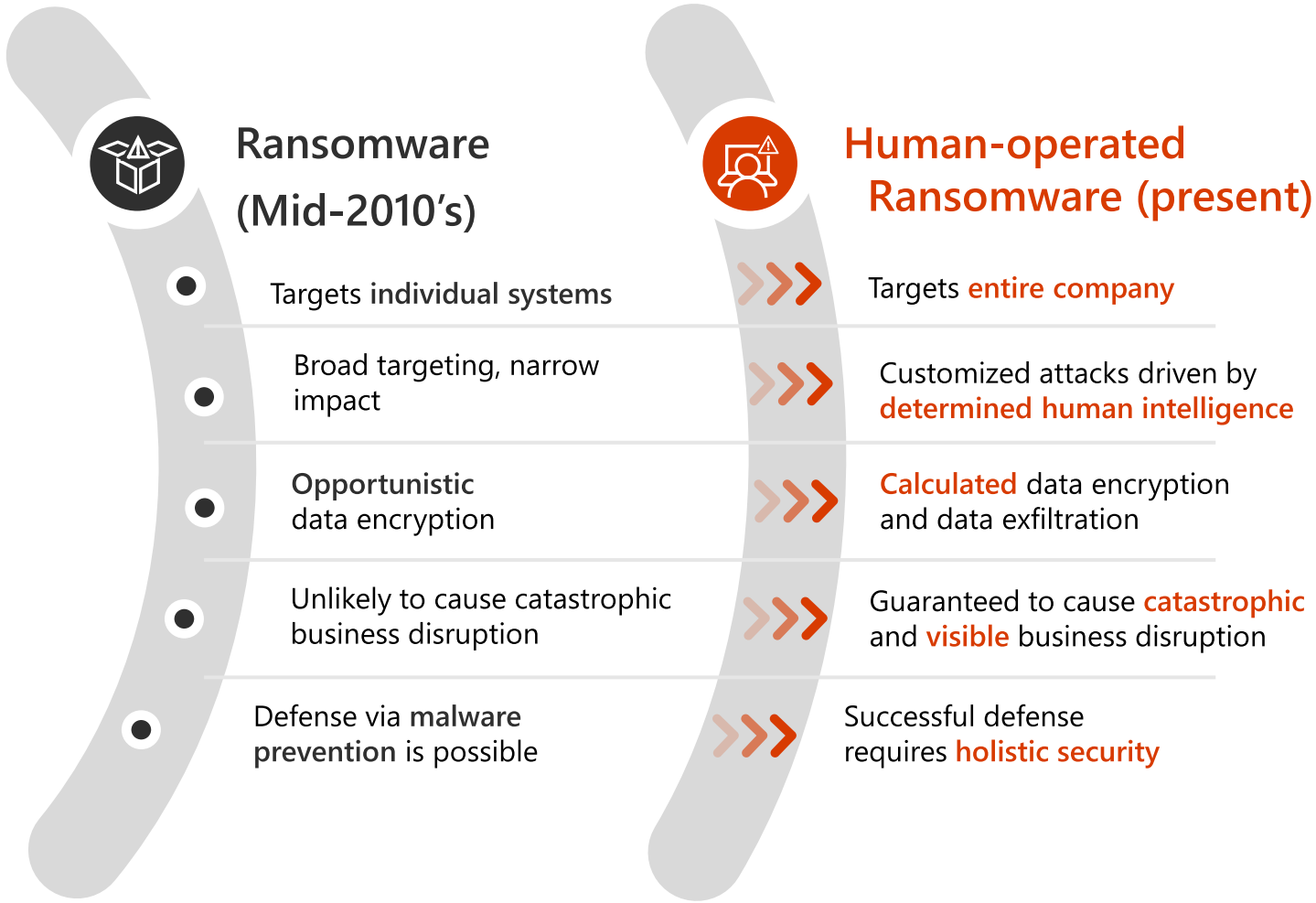
Blocked

32B email threats last year

How are attackers evolving?

A human-driven threat

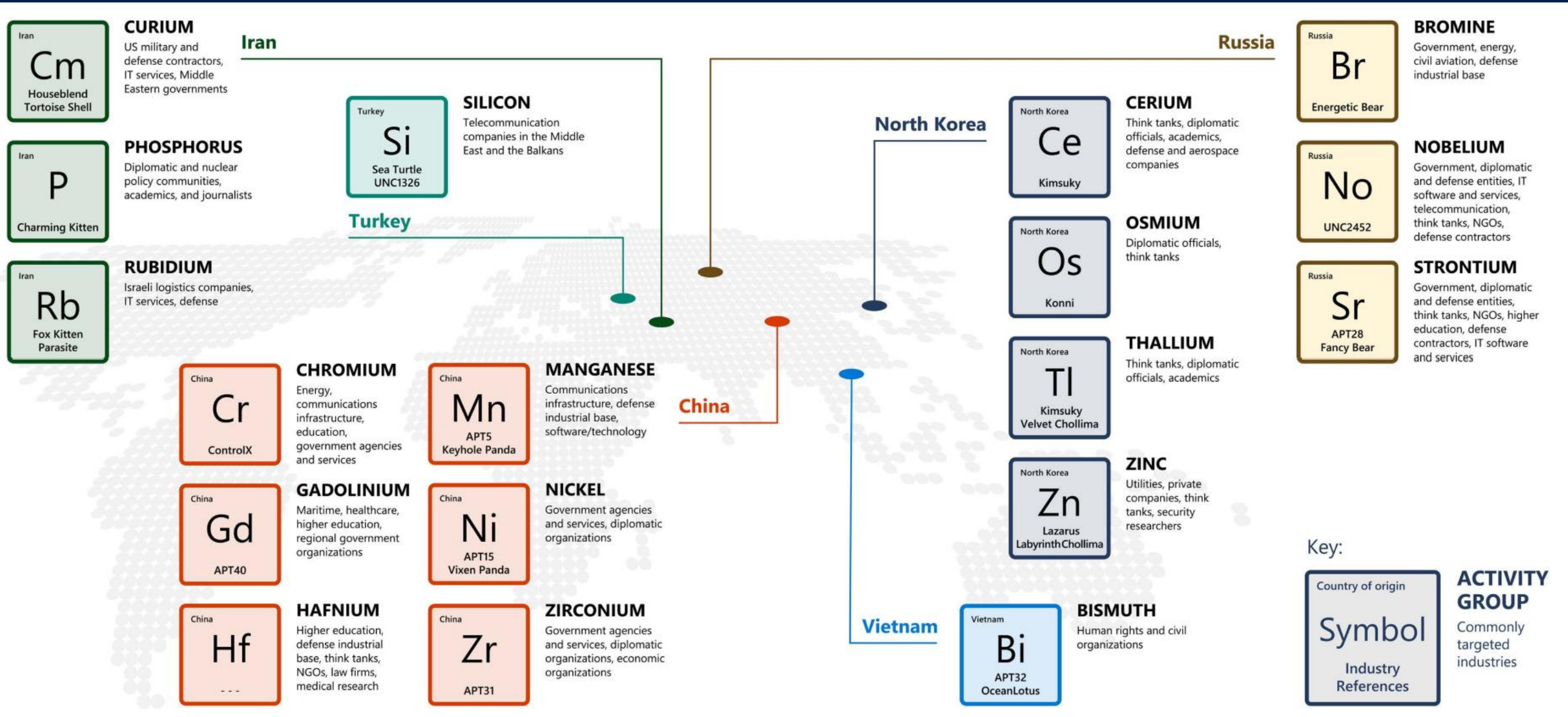
https://aka.ms/ransomware-economy



How do attackers specialize?

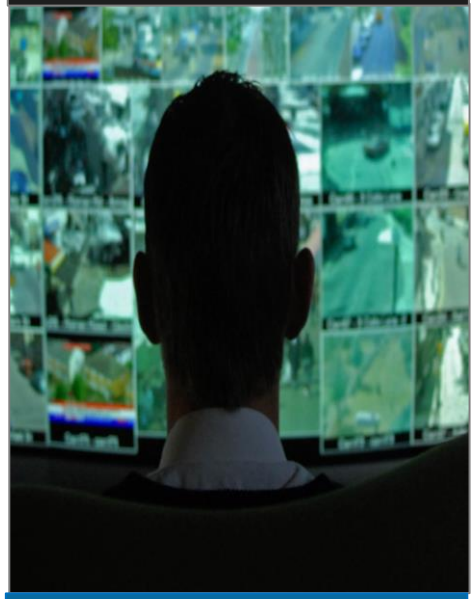
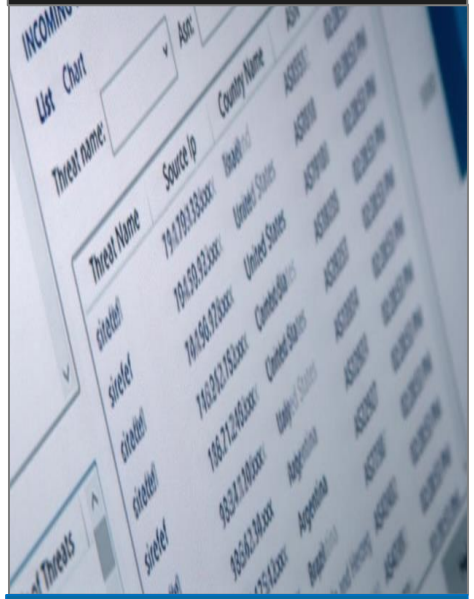
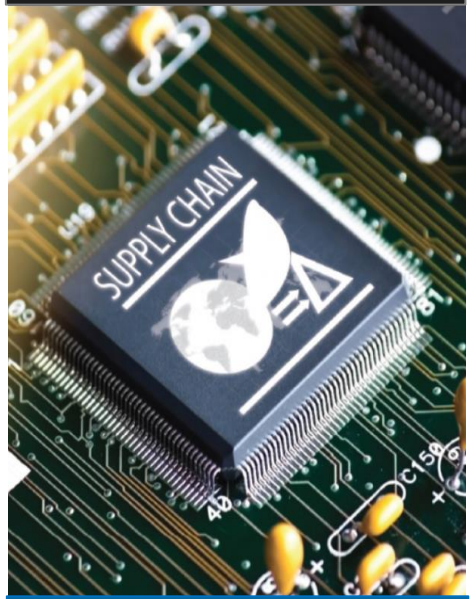
Source: Microsoft Digital Defense Report

https://aka.ms/ransomware-economy



Trends in Threat Landscape

Same tactics. New sophistication (mostly)

Thriving: **Nation State**	Growing: **Ransomware**	Growing: **Supply chain**	**On premises-to-cloud tenant attacks**	Emerging: **Cyber Mercenaries**
				
National, International, Financial motivations	More elusive Higher stakes	Trusted channels Broad attacks	Target on-premises to enable cloud access	Bespoke services Highly-customized

OK…so what?

How do we make it better?

P – from fragmentation to age of **Platform**

I - from noise to **Insights** (Intelligence)

C – safety in the **Cloud**

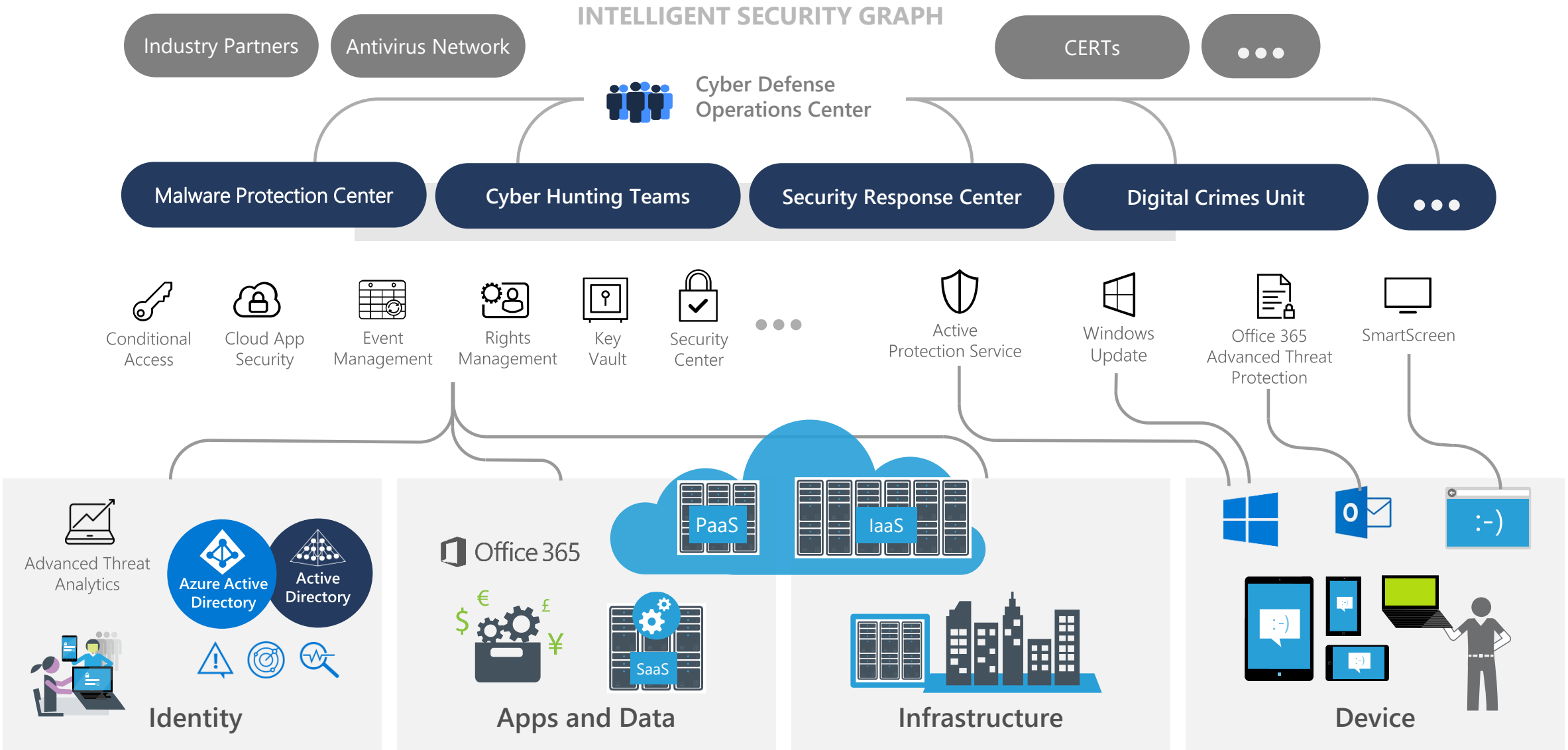
A – **AI** and emerging tech: arms race

R – **Regulations:** apply across the platform

D – **Data** sovereignty: edge, OT, ecosystems

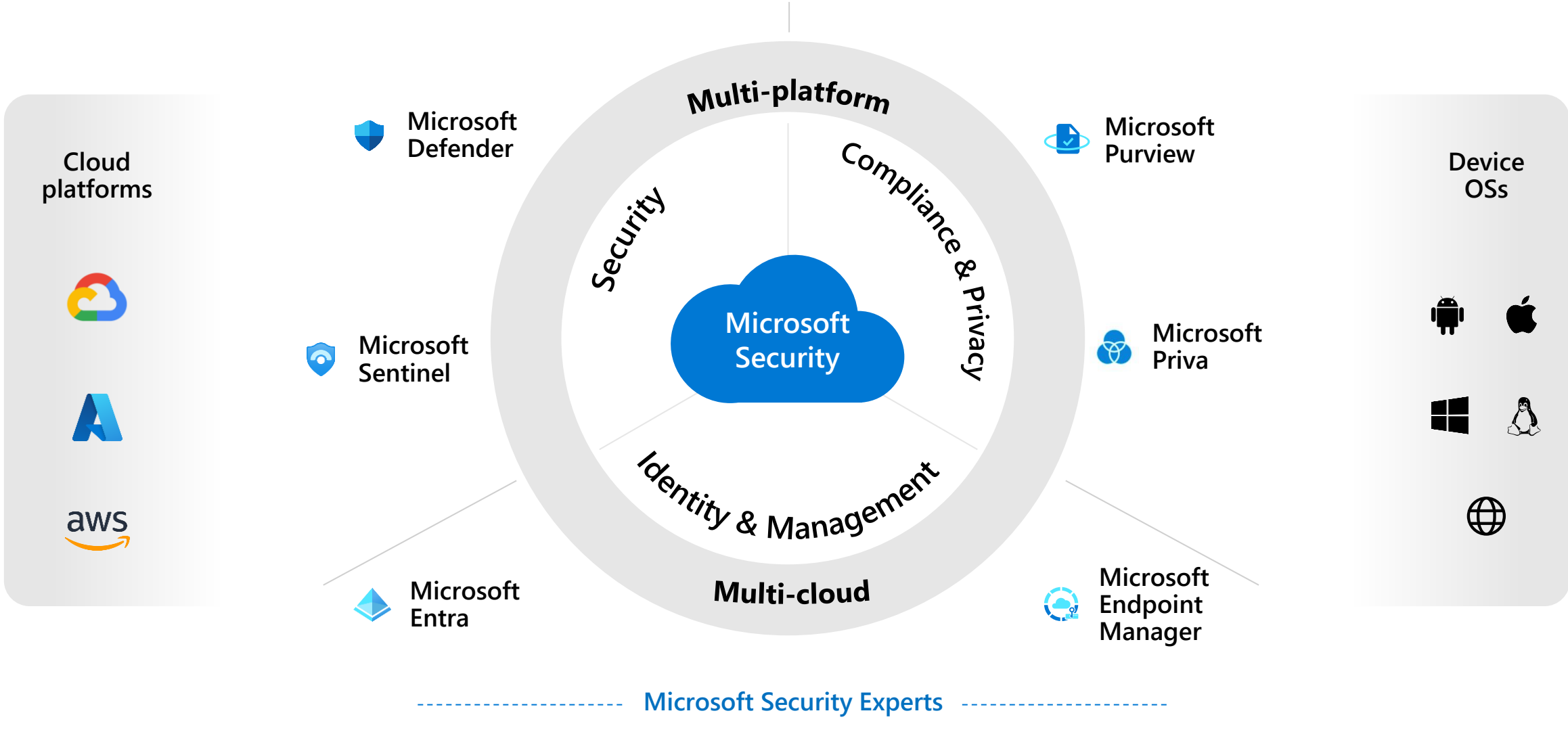
What does this look like

With Microsoft?



Six product families

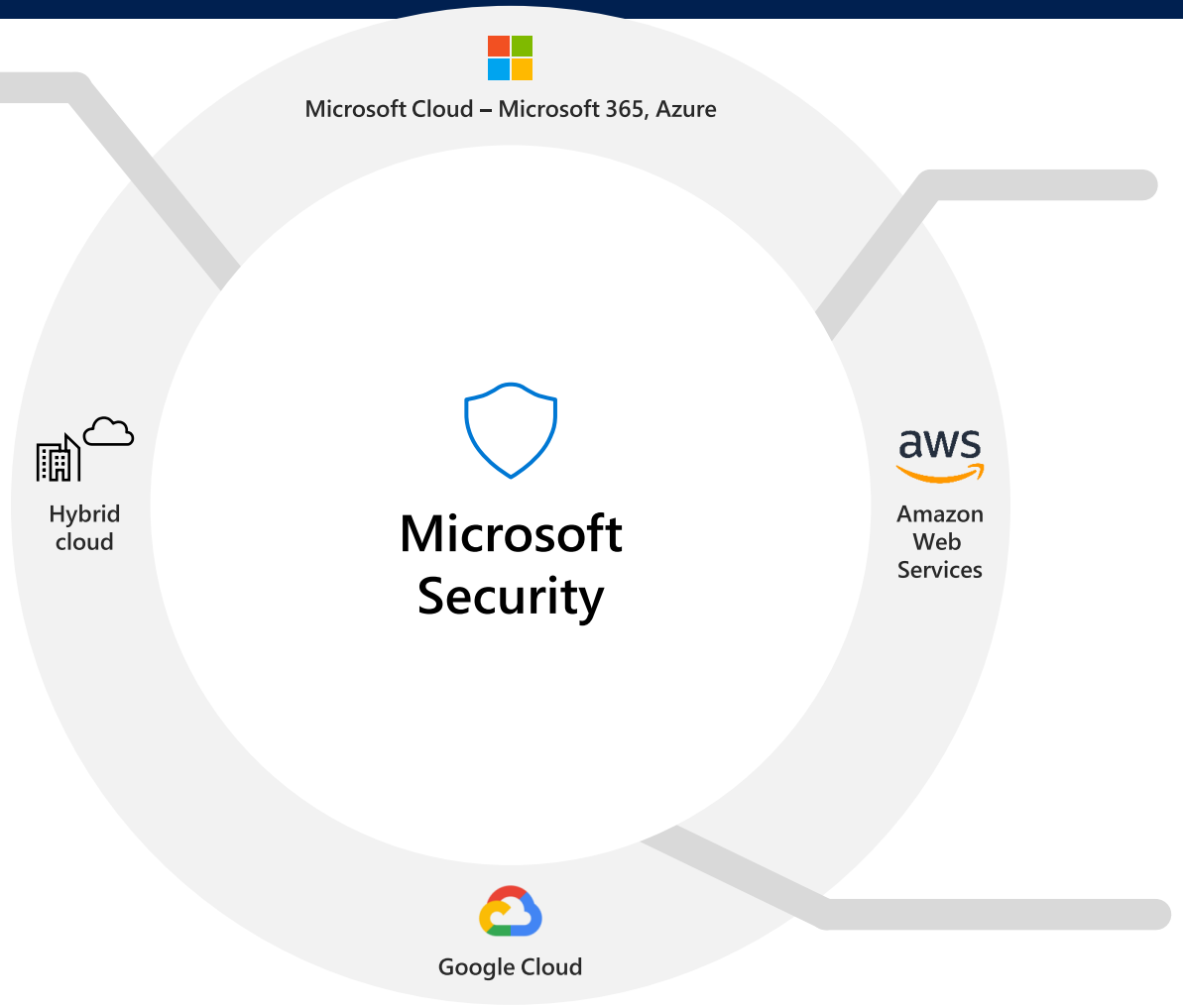
Integrating over 50 product categories



Want to see detail?

Here it is

- 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 assessment
- Privileged access management
- Compliance management
- Information and messaging encryption

- Identity and access management
- Single sign-on
- User provisioning
- Multi-factor authentication
- Passwordless authentication
- Risk-based conditional access
- Identity protection
- Self-service password reset
- Identity governance
- Priviledged identity management
- Endpoint management
- Mobile application management
- Mobile device management

How we are making it better

For customers: Lower cost + easier integration = Better Security

Average multi-vendor security

$30 per user

- Cloud access security broker — $6
- Email protection — $5
- Endpoint protection platform — $7
- Endpoint detection and response — $7
- Identity governance and adaptive access — $5

Microsoft Security

$12 per user

- Cloud access security broker
- Email protection
- Endpoint protection platform
- Endpoint detection and response
- Identity governance and adaptive access
- ...and more

Microsoft 365 E5 Security
(add-on to Microsoft 365 E3)

Up to **60%** savings

Web direct/base price shown for Microsoft offerings. Multi-vendor prices based on publicly available estimated pricing for other vendor solutions and are illustrative.

Thank you

C. Kelly Bissell
KellyBissell@microsoft.com
+1-404-502-5940
ckbissell

Microsoft Security