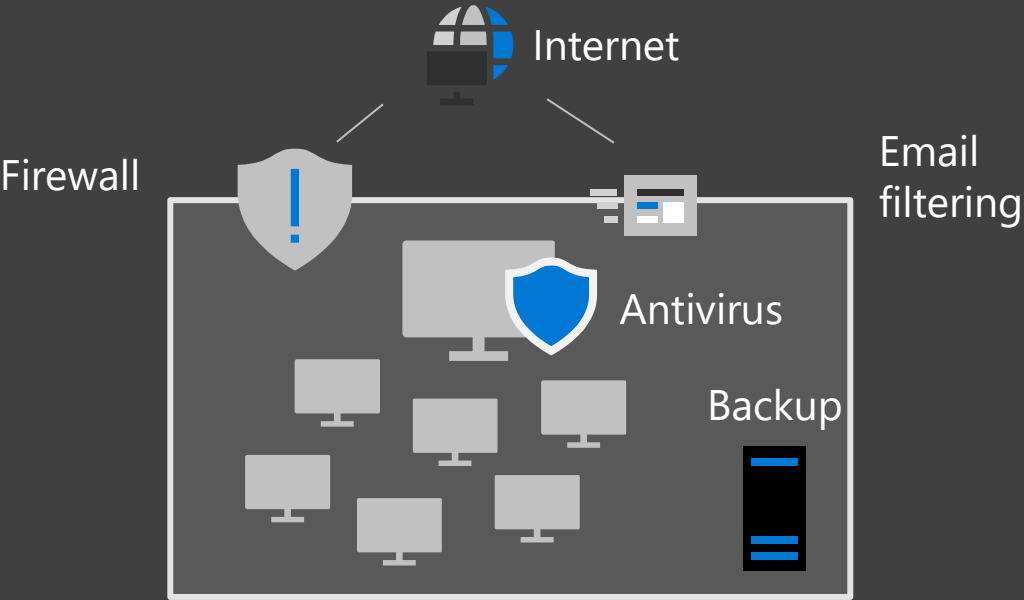





# Today's SMB IT environment is **challenging**

## Old model

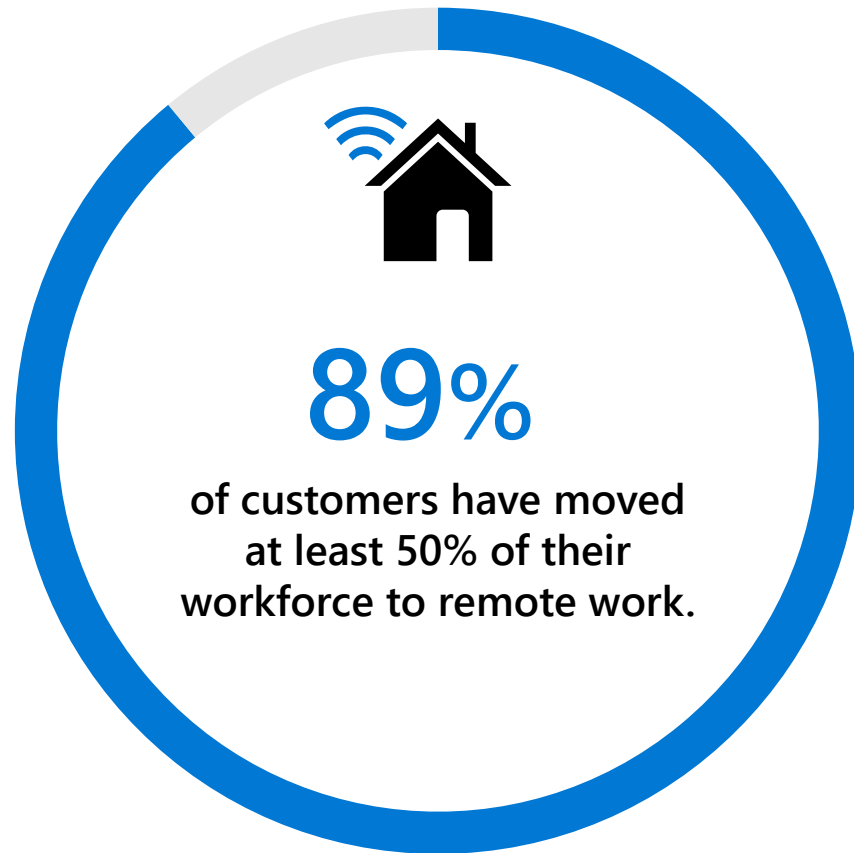


## What's changing

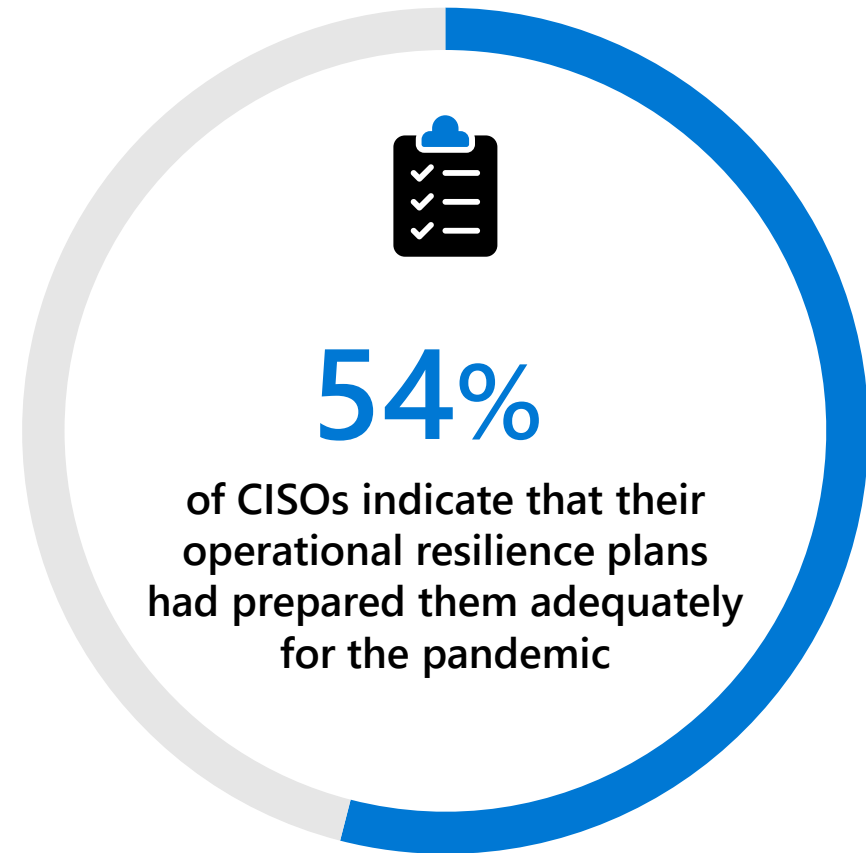
-  More mobile devices
-  Employees working from more places
-  Increased cyber attacks

# Business trends are changing

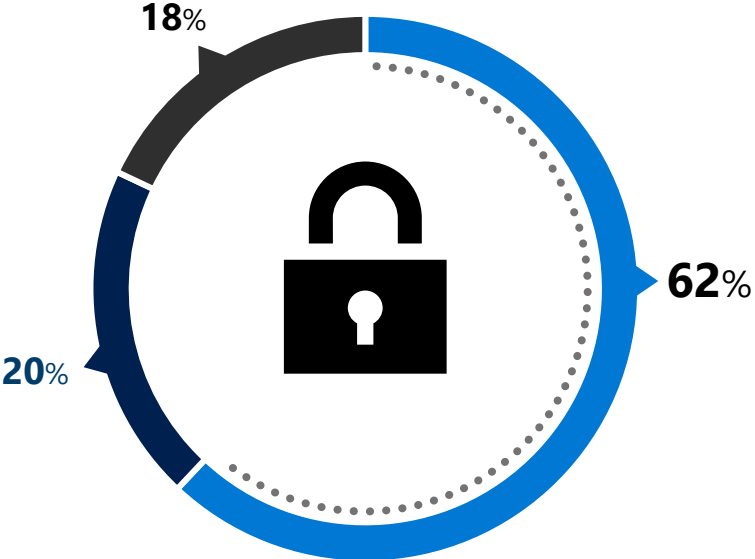
## Remote everything



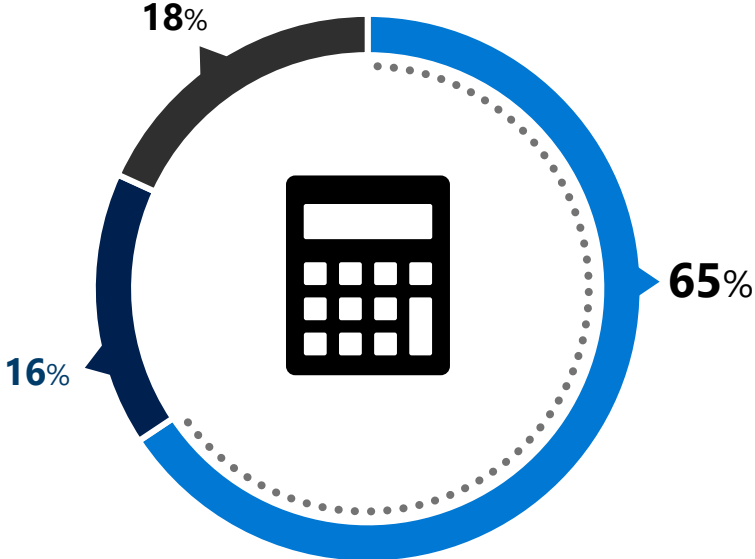
## Operational resiliency



# Budgets increasing to support remote work



Cybersecurity  
Budget Change



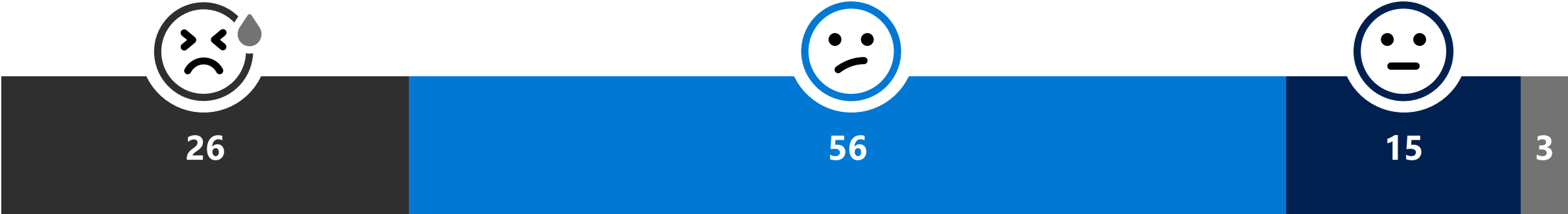
Compliance  
Budget Change

increased    decreased    no change

# There is pressure to lower costs throughout the year

## Pressure to Lower Cybersecurity Costs

n524; Shown as %



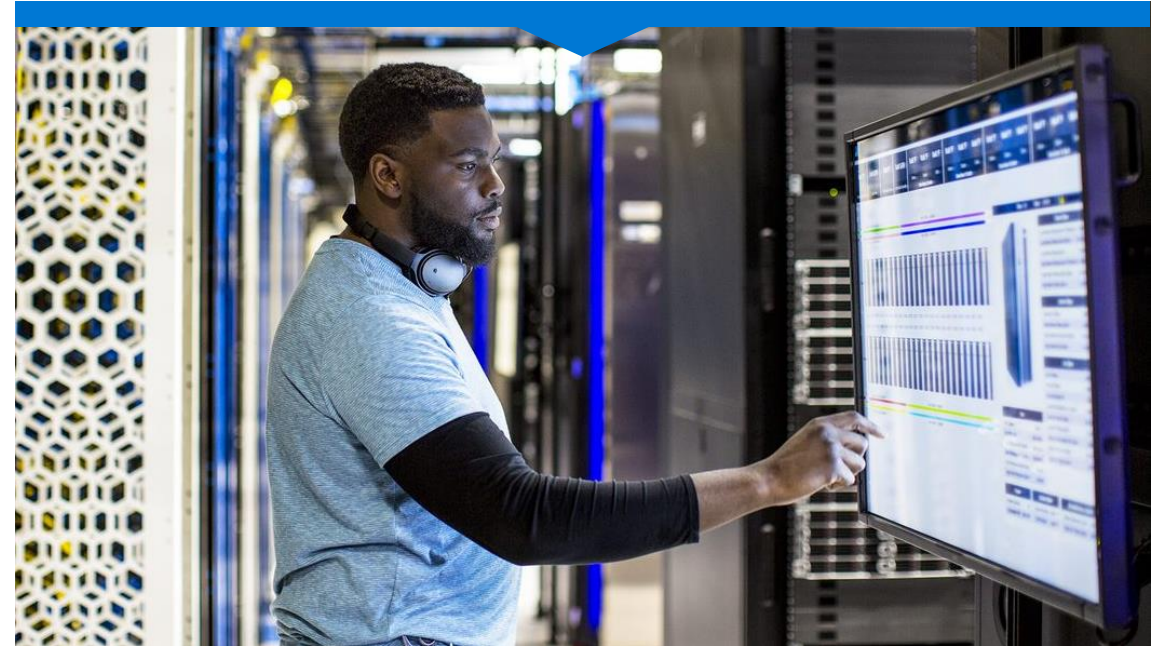
82%

■ Series1 ■ Series2 ■ Series3 ■ Series4

## Where customers will focus in FY21



**Reduce spend**



**Pivot to the cloud**

# Navigating a shifting world

**Budgetary pressures**

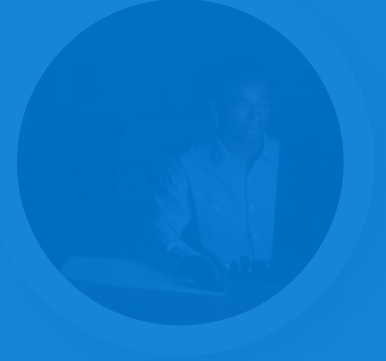
**Economic uncertainties**

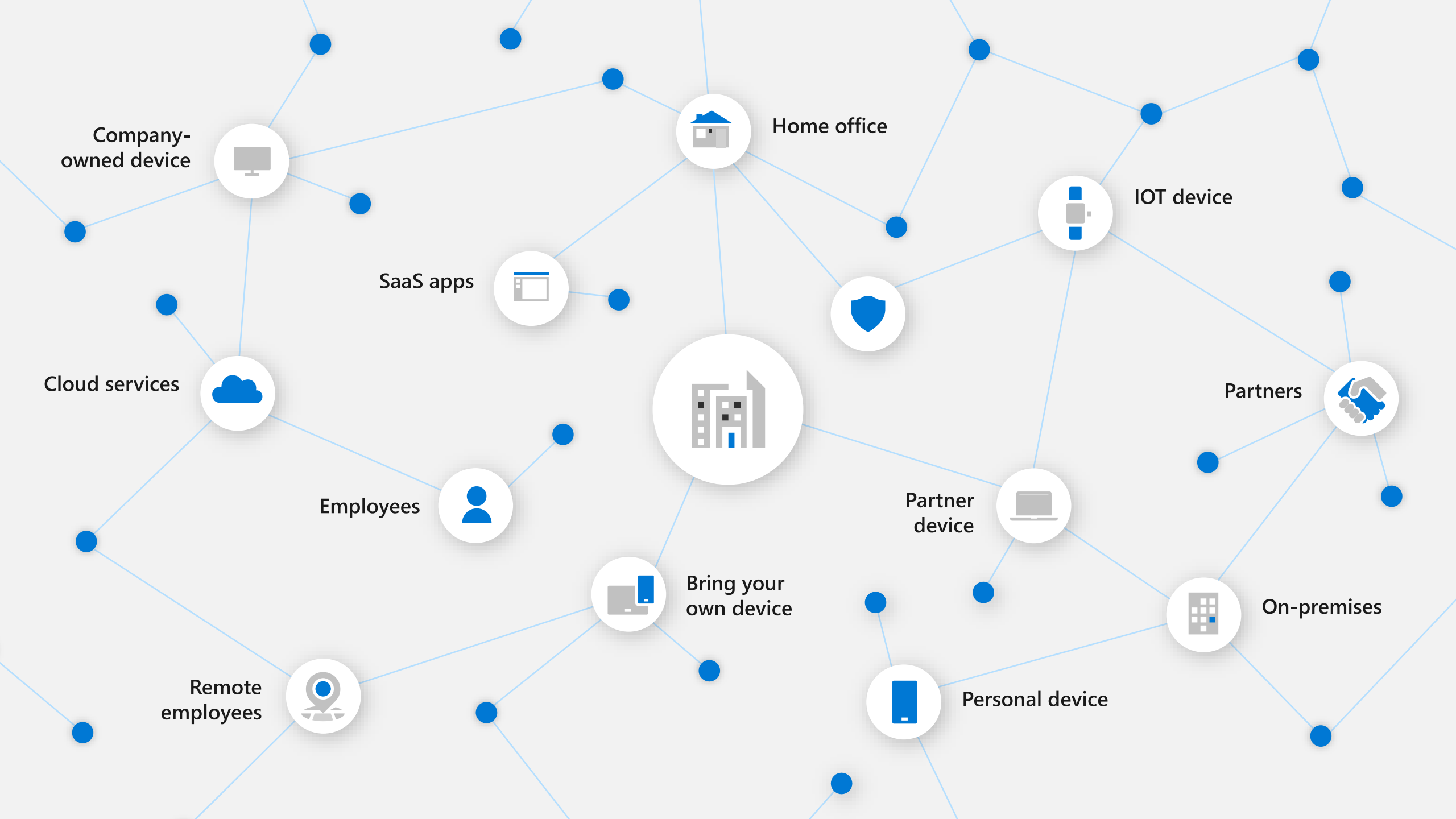
**Resource constraints**

Conventional security tools have not kept pace.

The nature of business and work has changed.

Cost of breaches and regulations are increasing.







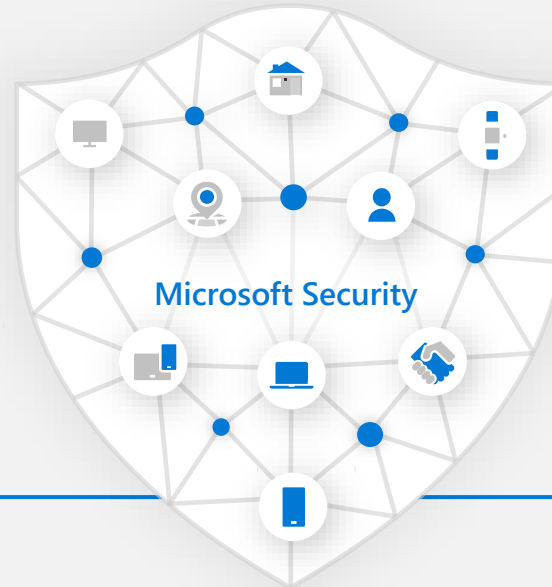
Microsoft Security



Budgetary pressures

Economic uncertainties

Resource constraints



Vendor License Cost Consolidation

IT Admin & Deployment Savings

Savings on Automation and Process Improvements (AI)

Reduced Total Cost of Risk

# How Microsoft can help you



**Consolidate security  
with Microsoft's  
cost-effective solution.**



**Deliver seamless  
end-user experiences  
for greater security.**



**Reduce cyber risk  
with integrated,  
best-in-class protection.**

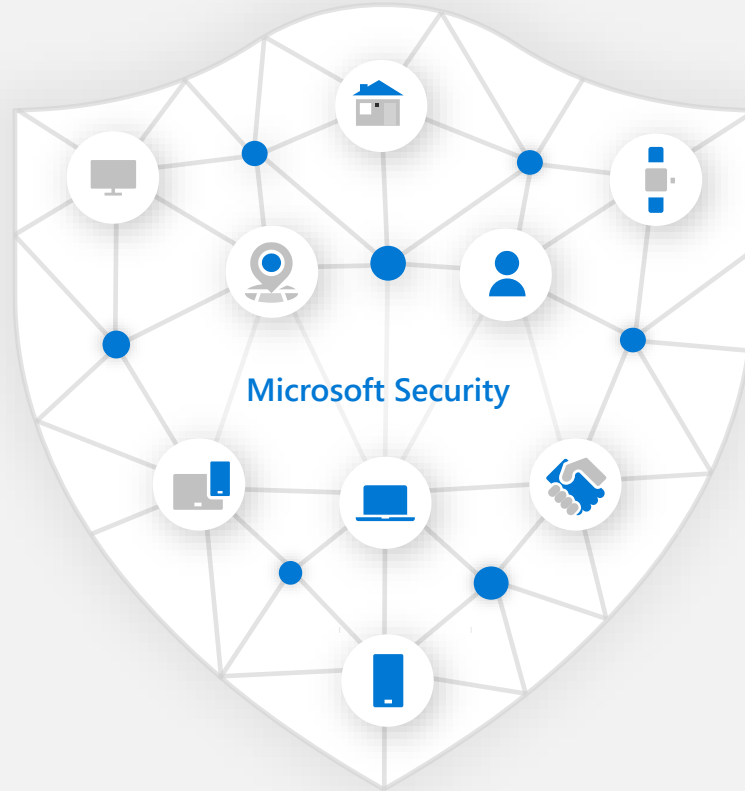
Replace up to

40

products

\$0

built in Cloud Security  
Posture Management with  
Azure Security Center



Up to

60%

savings with  
Microsoft 365 E5 Security

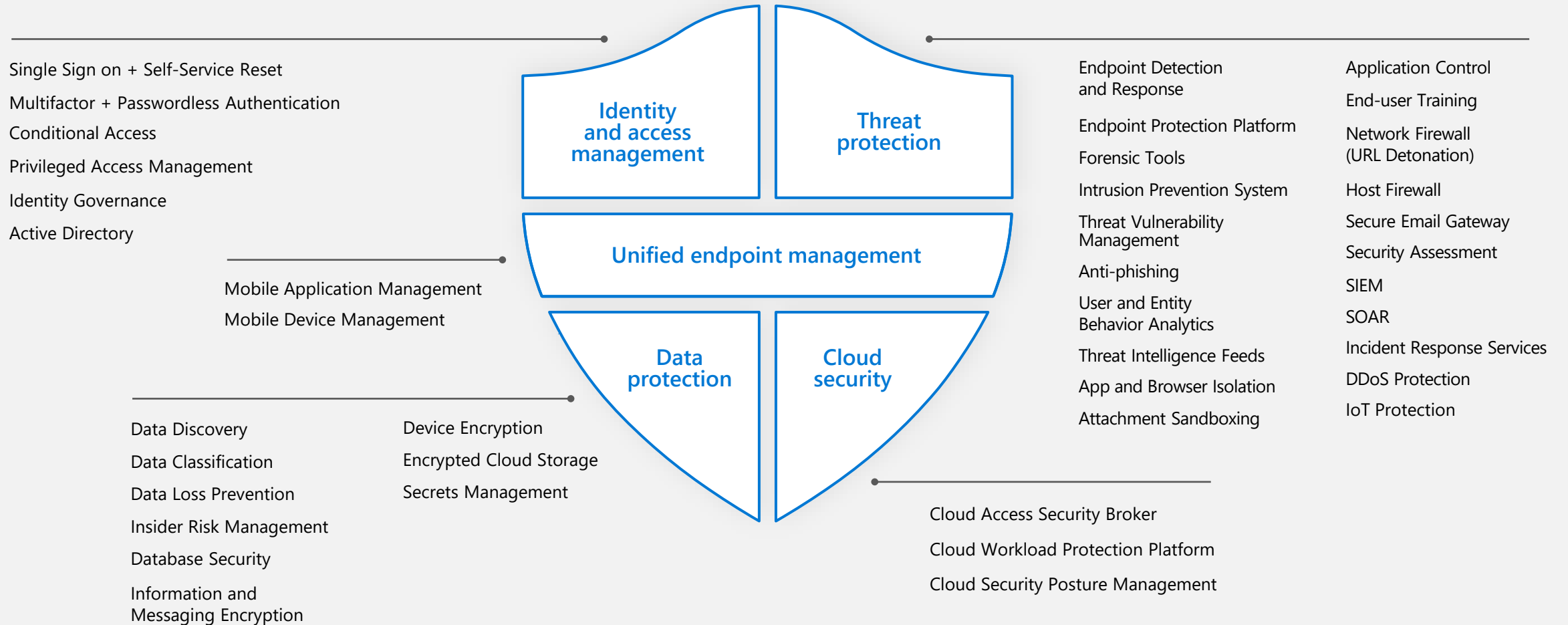
11%

savings with  
Cloud-native SIEM



# Streamline and strengthen

Replace up to 40 disparate products with integrated, end-to-end security.





# Microsoft Security—a leader in five Gartner magic quadrants.



Access Management



Cloud Access Security Brokers



Enterprise Information Archiving



Endpoint Protection Platforms



Unified Endpoint Management Tools

\*Gartner "Magic Quadrant for Access Management," by Michael Kelley, Abhyuday Data, Henrique, Teixeira, August 2019

\*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Steve Riley, Craig Lawson, October 2019

\*Gartner "Magic Quadrant for Enterprise Information Archiving," by Julian Tirsu, Michael Hoech, November 2019

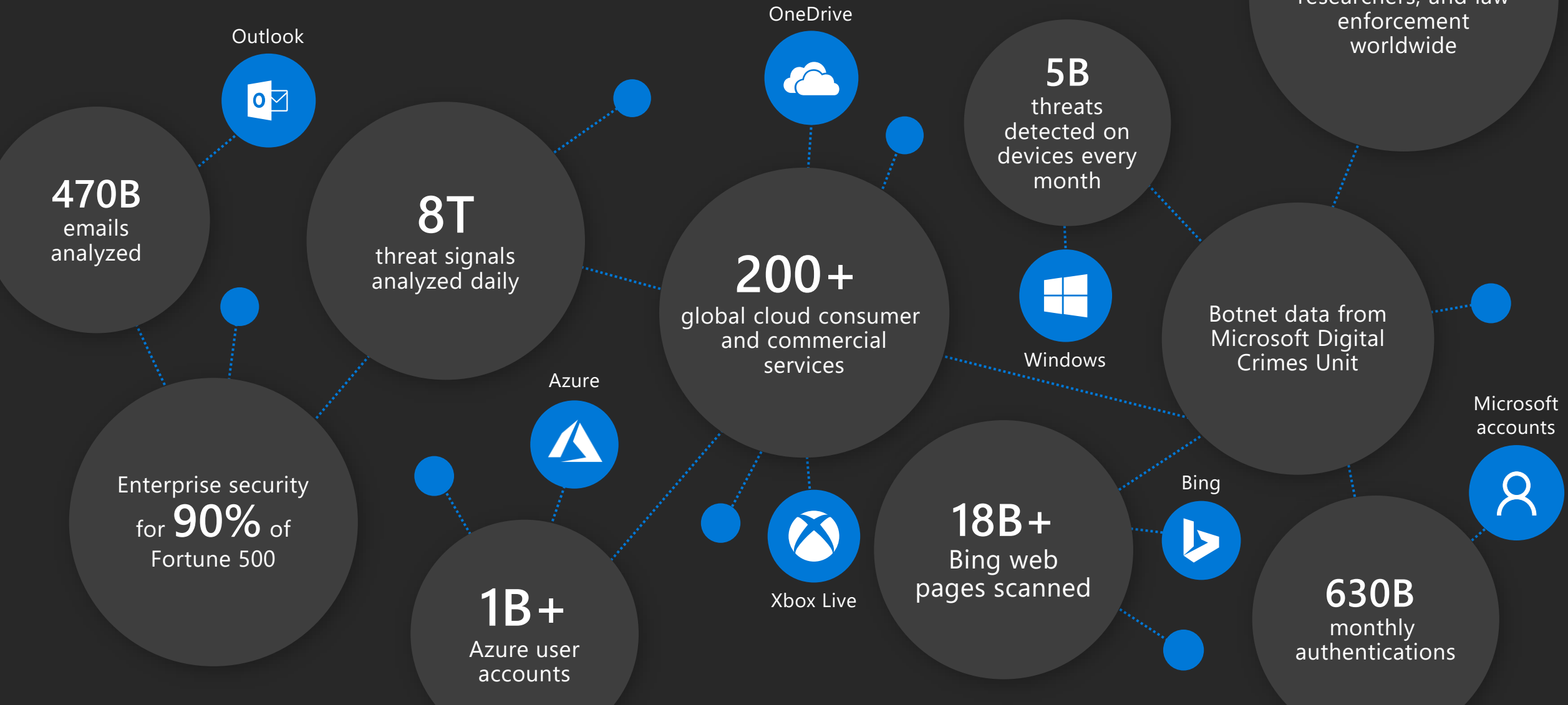
\*Gartner "Magic Quadrant for Endpoint Protection Platforms," by Peter Firstbrook, Dionisio Zumerle, Prateek Bhajanka, Lawrence Pingree, Paul Webber, August 2019

\*Gartner "Magic Quadrant for Unified Endpoint Management Tools," by Chris Silva, Manjunath Bhat, Rich Doheny, Rob Smith, August 2019

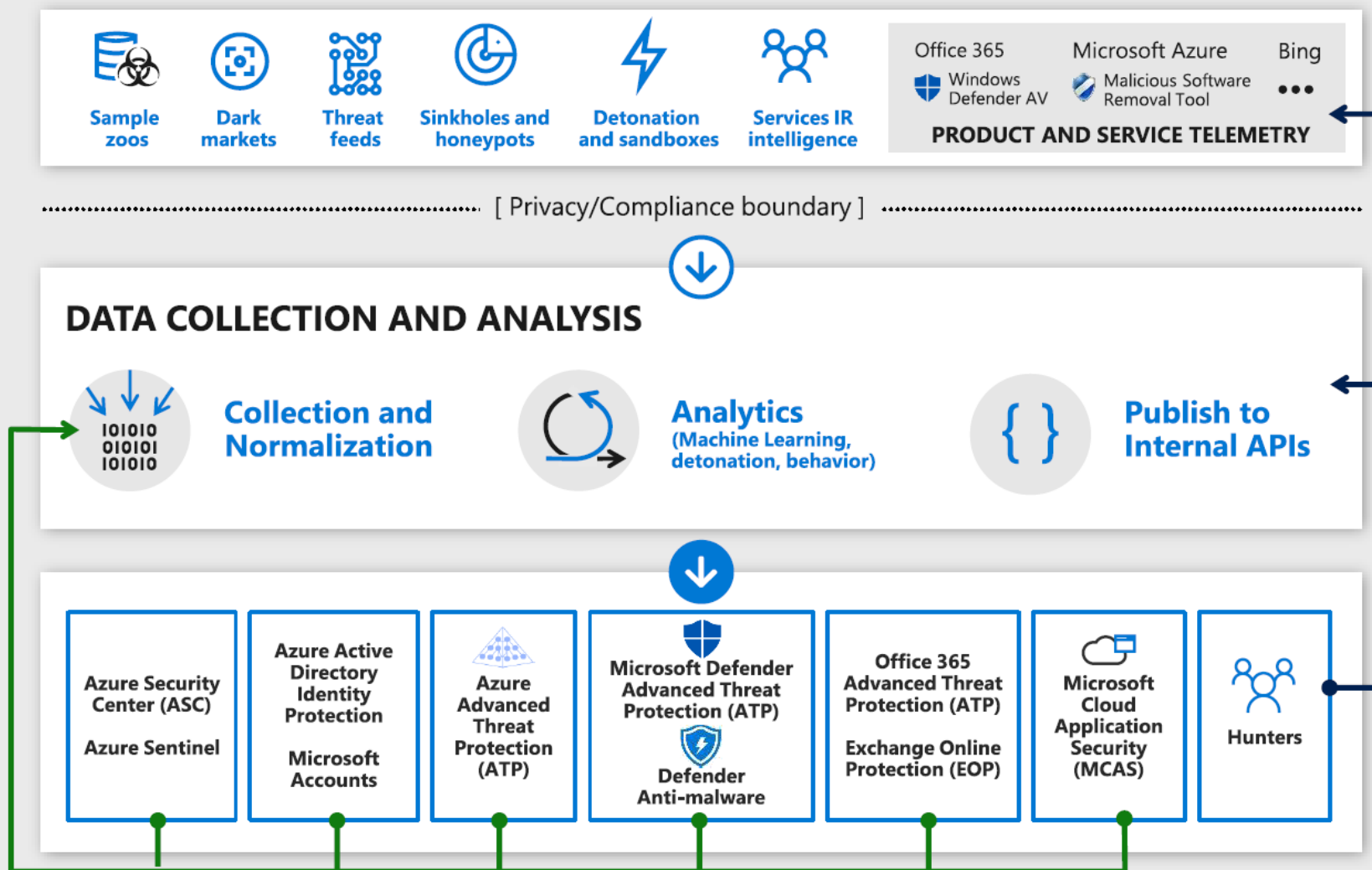
*These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, 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.*



# Microsoft has competitive advantage in AI Security



# 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

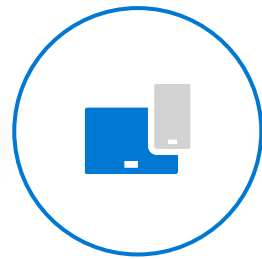
→ Hunters identify attacks, improve analytics, feed back into product design

# Stop attacks

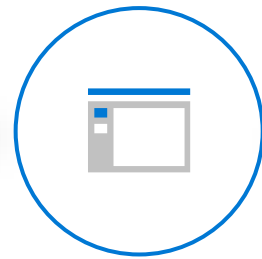
With a comprehensive, best-in-class portfolio



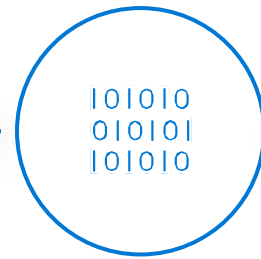
Identities



Endpoints



Apps



Data



Infrastructure

**12B**

Cloud activities inspected, monitored, and controlled in 2019

**11B**

Malicious and suspicious messages blocked in 2019

**300B**

User activities profiled and analyzed in 2019

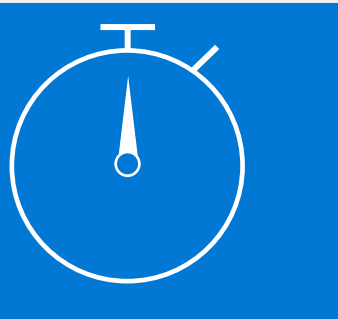
**2.3B**

Endpoint vulnerabilities discovered daily



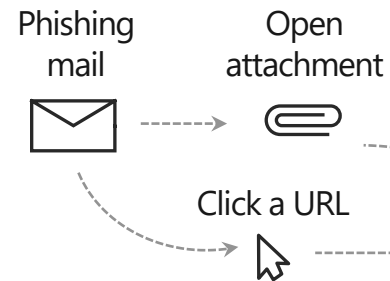
# Stop attacks

With an integrated approach across the attack kill chain



## Office 365 ATP

Malware detection, safe links, and safe attachments



Exploitation & Installation

Command & Control

## Azure AD Identity Protection

Identity protection & conditional access



Brute force account or use stolen account credentials

User account is **compromised**

Attacker attempts lateral movement

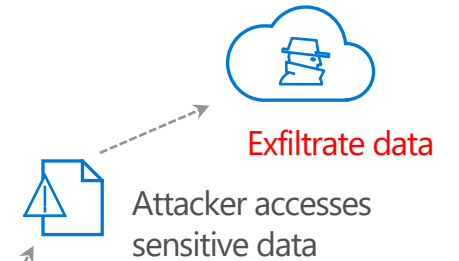
Privileged account **compromised**

Domain **compromised**

Attacker collects **reconnaissance & configuration data**

## Microsoft Cloud App Security

Extends protection & conditional access to other cloud apps



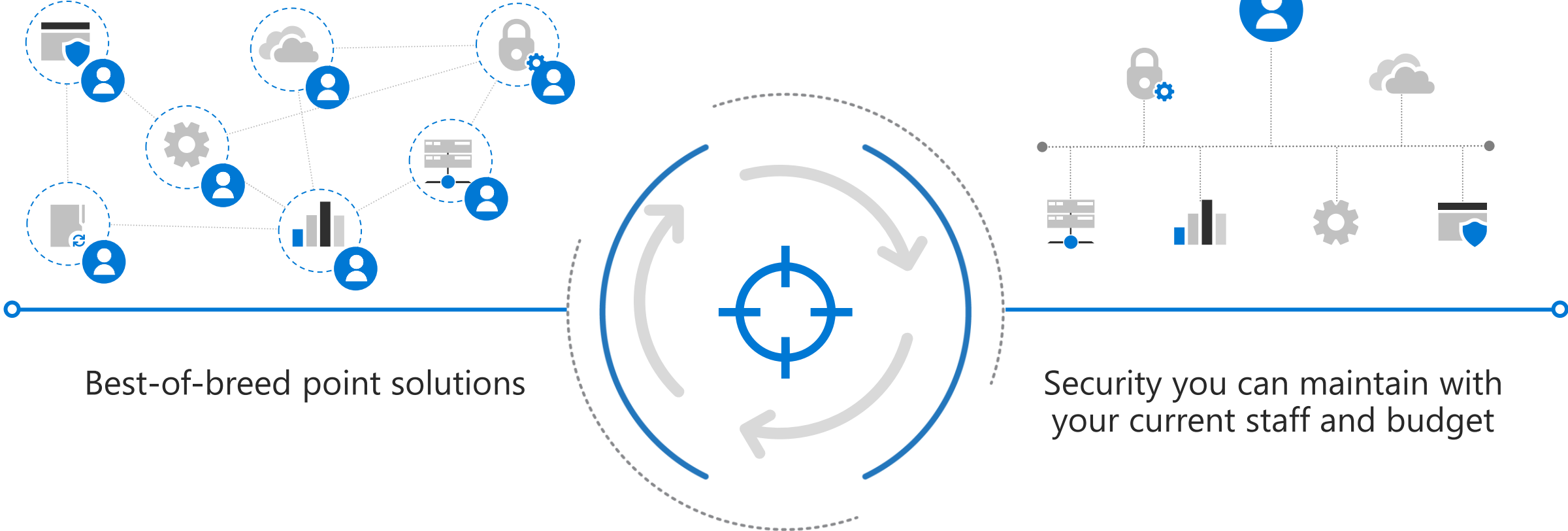
## Microsoft Defender ATP

Endpoint Detection and Response (EDR) & End-point Protection (EPP)

## Azure ATP

Identity protection

# The security paradigm needs to change.



# Microsoft's unique and open security approach

## Cloud-native, open and integrated platform



Reduce dependence on third party solutions

Integrated capabilities premised on identity and zero trust

Frictionless user experience across clouds and devices

## Unmatched threat intelligence



Unmatched magnitude and diversity of threat signals

Populated from Microsoft, third-party feeds, threat hunters

Rapid access to threat and response professionals

## End-to-end threat protection



Prevents lateral movement across cyber kill chain

Forward and backward visibility across your estate

Pervasive integration through intelligent security graph

## Security orchestration/automation



Reduce alert fatigue through use of machine learning

Automated remediation of common incidents

Scalable SIEM/SOAR capability, open to third parties

### Microsoft



### Public cloud



### Endpoints



### Mobile devices



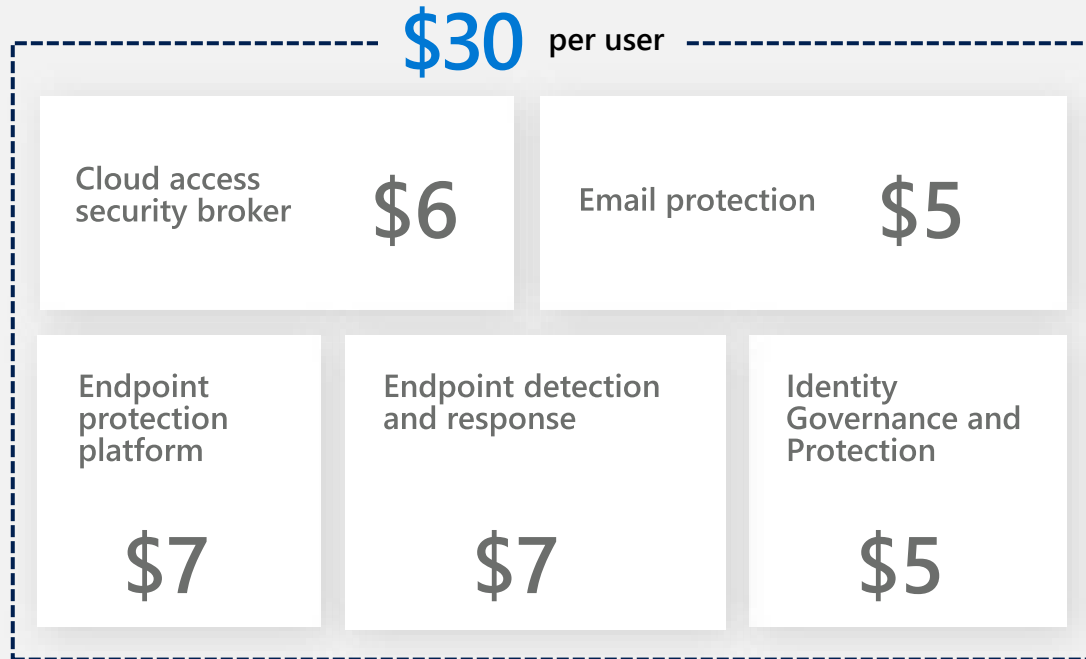
### IoT/Edge



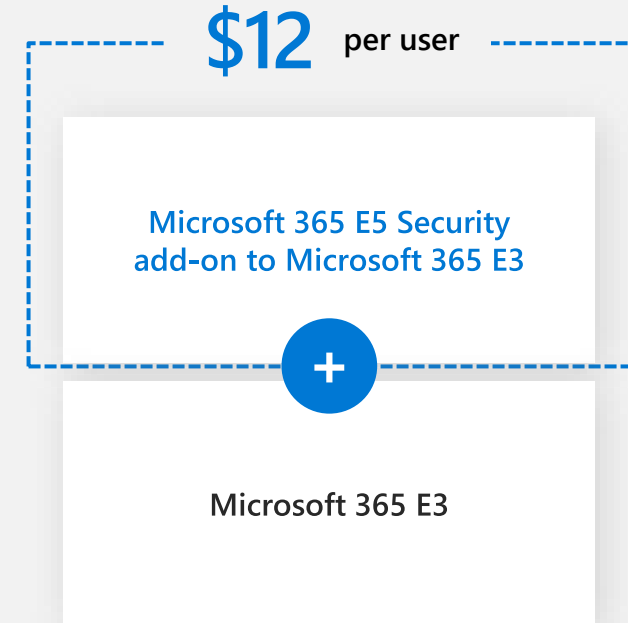
# Streamline and strengthen

60% percent savings with Microsoft 365 E5 Security.

## Average multi-vendor security



## Microsoft



# Annual estimated cost savings

COST SAVINGS CATEGORIES	20,000 seats	1,000 seats	50 seats
Vendor license cost consolidation	\$4,300,000	\$220,000	\$11,000
IT administration and deployment savings	\$6,100,000	\$330,000	\$41,000
Reduce total cost of risk	\$2,200,000	\$390,000	\$290,000
Save on automation and process improvements	\$12,000,000	\$600,000	\$30,000
POTENTIAL COST SAVINGS PER YEAR	Up to <b>\$25M</b>	Up to <b>\$1.5M</b>	Up to <b>\$380K</b>

Rounded estimates based on commissioned Forrester TEI studies and Microsoft Total Cost of Risk calculator and illustrate first year cost estimates. Contact your Microsoft representative for estimates for your organization.



# Cyberthreats– primer

**Phishing** is a form of fraud in which an attacker masquerades as a reputable person or company in email or other electronic communication channels. A common phishing tactic is to send an email with a forged return address, so that the message appears to have originated from a legitimate source, making it more likely that the recipient will open it. Phishing attacks are popular with cybercriminals, because it is easier to trick someone into clicking a malicious link in a seemingly legitimate email than it is to break through a computer's defenses.

**Ransomware** is malicious software that blocks access to a computer system or files unless a sum of money is paid. Ransomware twists the power of encryption against you. Encryption should protect your data and files, but ransomware uses it to take files hostage. This means being locked out of your documents, spreadsheets, photos and videos, and other important files. Plus, an infected PC can spread the ransomware to other computers on your network.

## “Is Microsoft Defender really as good as 3<sup>rd</sup> party antivirus solutions?”

Microsoft Defender delivers comprehensive, ongoing and real-time protection against software threats like viruses, malware and spyware across email, apps, the cloud and the web.

- Leverages human experts + AI + almost 1B cloud-connected Windows devices
- Signals are analyzed by AI & protection is delivered in milliseconds
- Received perfect score in Jan/Feb 2018 test conducted by AV-TEST (independent antivirus testing firm)





# Microsoft recognized as a leading Security provider by Gartner

## Endpoint protection platforms



## Unified endpoint management tools





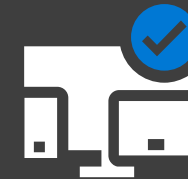
# Microsoft 365 Business is stronger with new product value



Defend against  
cyberthreats



Protect  
business data



Manage  
your devices

Office 365 Advanced Threat Protection

Microsoft Defender

+ Azure Multi Factor Authentication **NEW**

+ Self Service Password Writeback **NEW**

Office 365 Data Loss Prevention

Azure Information Protection P1

Exchange Online Archiving

+ Conditional Access **NEW**

Intune

Windows Virtual Desktop  
Public Preview

+ Office 365  
Shared Computer Activation **NEW**

# Defend against cyberthreats

Protect against phishing, ransomware, and other advanced threats

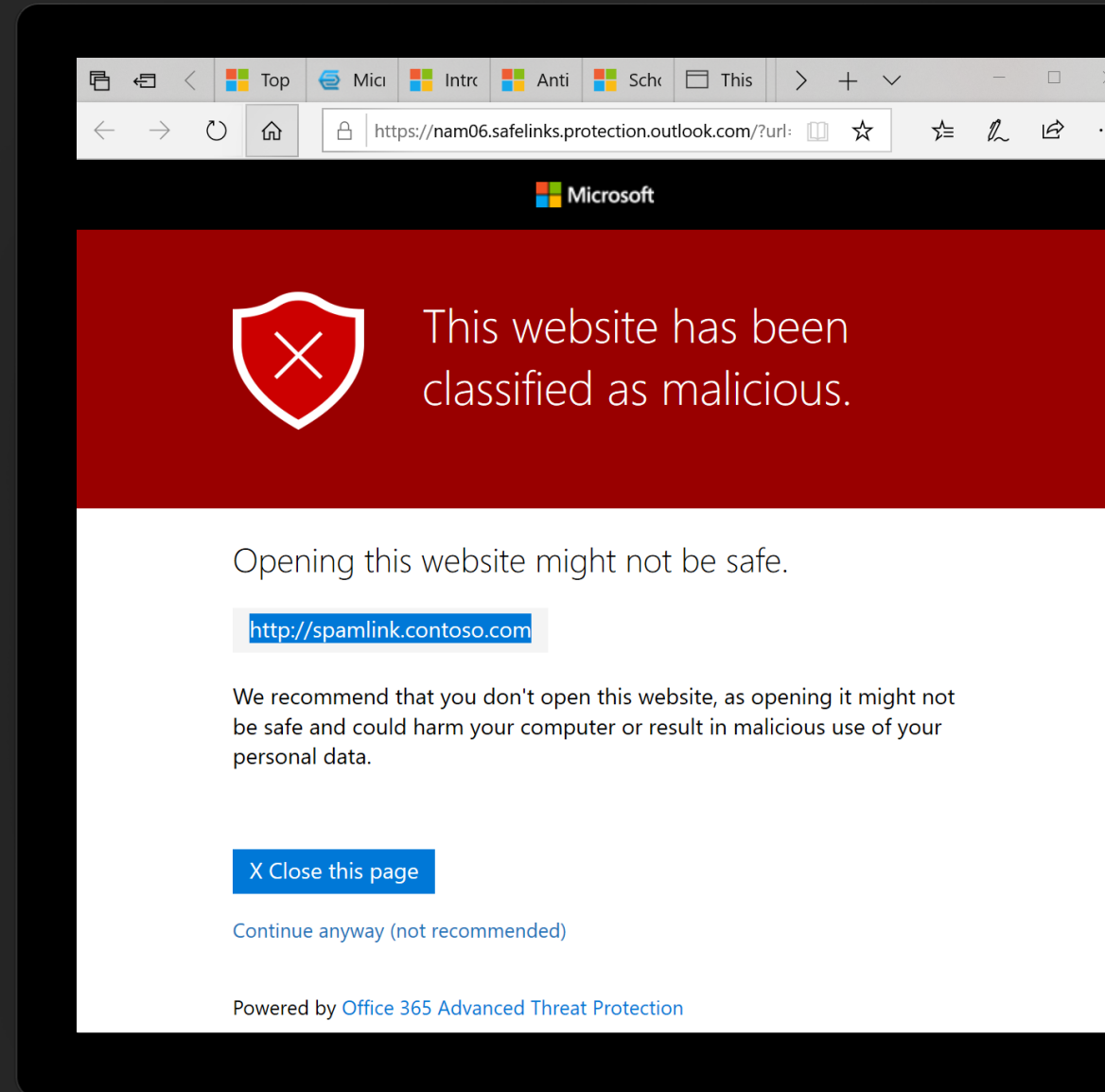
Links are **checked in real time** to warn you if destination is a malicious

AI-powered **attachment scanning** detects malware previously not seen with **ATP safe attachments**

AI-powered **anti-phishing intelligence** helps protect against spoofing with **ATP anti-phishing**

**Advanced multifactor authentication** limits attacker access even if an employee's password

Windows devices get better **protection against suspicious processes** like ransomware



# Protect business data

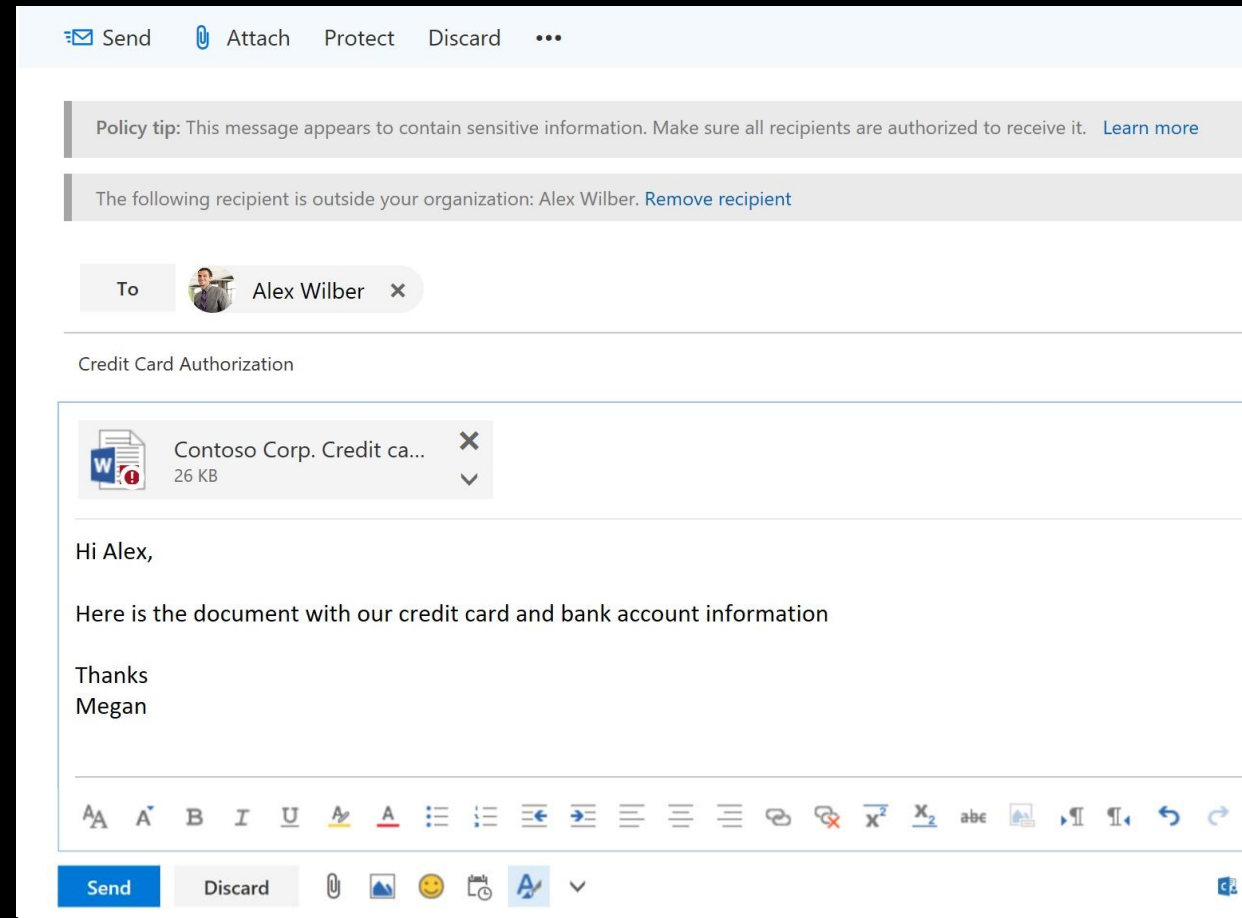
## Control who has access to sensitive information

Use **data loss prevention policies** to help keep sensitive information from falling into the wrong hands

Apply **encryption** and restrictions like **do not forward** to emails and documents

Use **long-term archiving** to meet legal and regulatory requirements

Use **Conditional Access (CA)**, to control which devices reach your Office 365 data. Allow or deny access depending on when the user is logging in, their location, what apps they are using



# Securing the devices

Phones



iOS and Android devices

Tablets

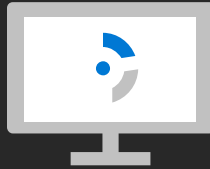


Laptops



Windows PCs

Desktops

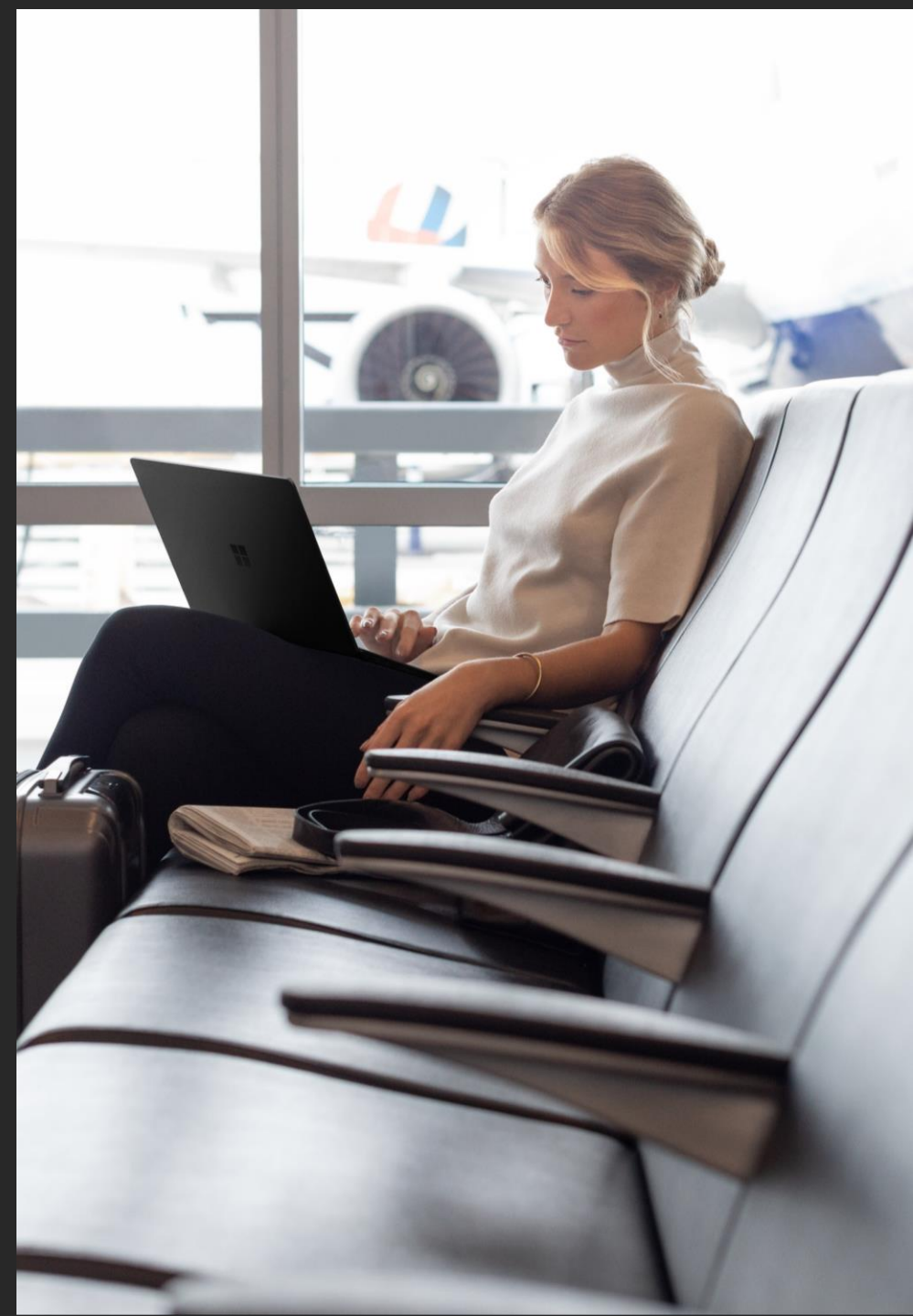


## Comprehensive device management solution

Includes the full capabilities of Microsoft Intune

Ensures devices and apps are compliant with your organization's security requirements

Includes policies that help keep your organization data safe



# Securing devices double click



## Mobile Application Management (MAM)

- Manage how data moves between apps with controls for copy, paste, download etc.
- MAM protects an organization's data within an application using app protection policies(APP).
- **Does not require device enrollment** and therefore great for BYOD scenarios.

### Administration

Managed via setup wizard and simplified UI

## Mobile Device Management (MDM)

- Best option for company-owned devices.
- Ability to configure mobile device policies, such as enforcing complex PINs or passwords, remote wipe/lock, device encryption, etc.
- Since it controls the entire device, **Requires device enrollment.**

### Administration

Managed via Intune admin center

Additional steps to set up (provision certificates, etc)

# Breaking down the MSP market for Security

## Partner Types

### Transactional Reseller

Focused on transaction with some project work. Usually come from PC background

#### Security Products Offered

- A/V with PC sale

### Small MSP

Usually between 1-10 employees. Born in break-fix model. Offer basic managed service

#### Security Products Offered

- Basic Endpoint Protection
- Email Threat Protection
- MFA

### Medium MSP

Usually between 10-150 employees. Moving into the security game quickly. Standardize on small number of vendors and train staff

#### Security Products Offered

- Windows Device Management
- Mobile Device Management
- Identity Protection
- Firewall

### MSSP

Partners that have developed specialist skills in Security and have a number of specialists on staff. Usually over 150 employees

#### Security Products Offered

- SIEM
- Threat Hunting

## Security Managed Services

- Remote monitoring

- Security assessments
- Remote monitoring
- Patching
- Network security

- Security Operations Centre (SOC)
- SIEM
- Policy Modernization
- Compliance as a Service

## Profitability

Low margin  
Many owners looking to sell or retire over the next 5 years

Low- high margin  
Margin pressure from support  
Unable to secure customers fully

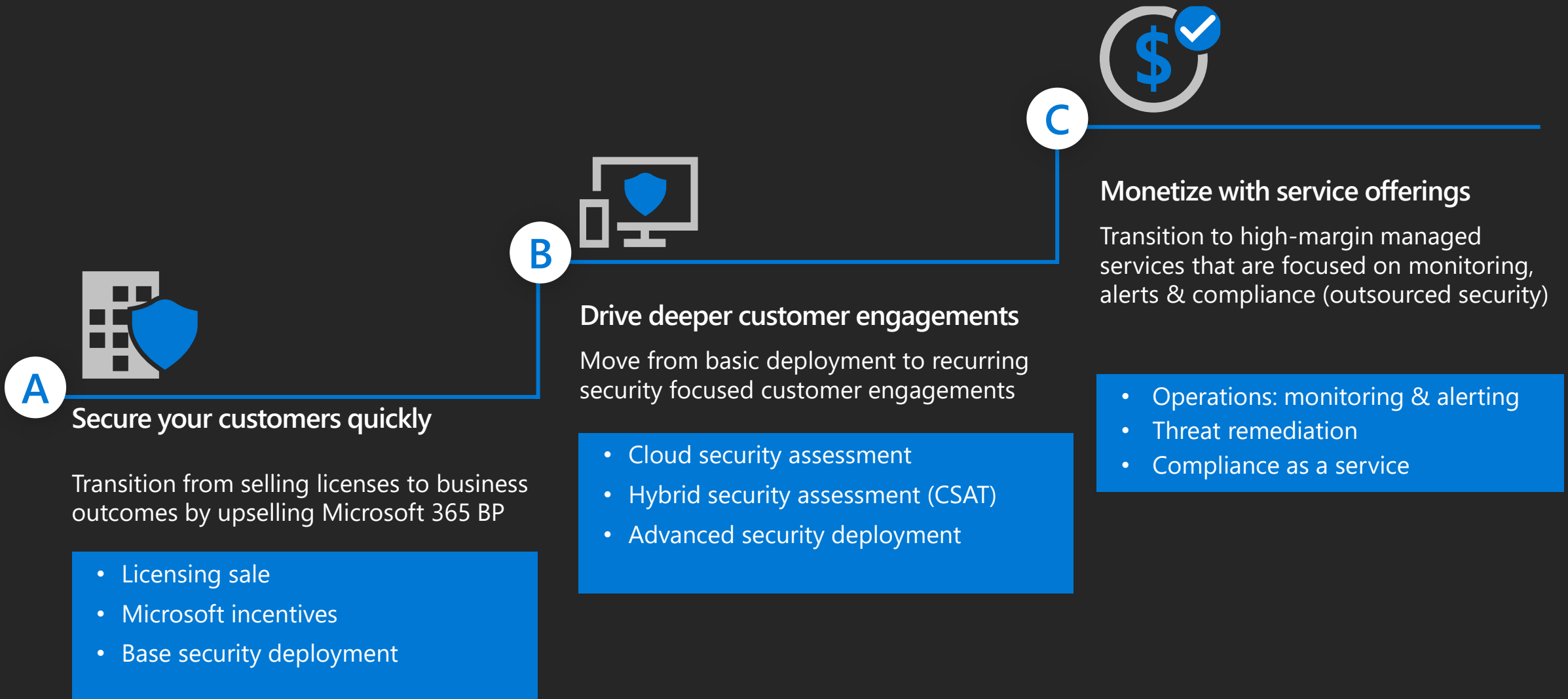
Medium- high margin  
Developing & expanding Security practice

High margin  
High cost to develop business  
Not enough MSSP's in market

Focus for Recruit

Focus for Connecting

# Build a profitable security practice with Microsoft



# Bringing it together

## \$720

### Secure your customers

Sell Microsoft 365 Business

- Licensing sale
- Base security feature deployment
- Supplement on-prem AD with AAD
- Reduce operational cost



## +\$310

### Drive assessment

Add high-value, easy-to-sell services based on deployment of Microsoft 365.

- Cloud security assessment
- Hybrid security assessment (CSAT)
- Implement compliance features
- End-user security readiness



## +\$340

### Monetize with services

Grow the lifetime value of the customer relationship with services that set you apart.

- Monitoring and alerting
- IAM policy management
- Device policy management
- Threat remediation (P2P)
- Compliance as a service (P2P)

Three-year **average revenue** per SMB seat from Microsoft 365 Business Premium



# Use **Secure Score** to drive security conversations

Helped increase cold call related lead quotes by **5X** for one partner

## Resources

[Partner Smart Office](#)

[Using the Secure Score API](#)

[Secure Score Deep Dive](#)

The screenshot displays the Microsoft 365 security dashboard. The left sidebar contains navigation options: Home, Alerts, Monitoring & reports, Secure score (highlighted), Hunting, Classification, Policies, Permissions, More resources, Customize navigation, and Show all. The main content area is titled "Microsoft Secure Score" and includes tabs for Overview, Improvement actions, and History. The "Overview" tab shows a "Total score: 98 / 707" and a description: "Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps, and infrastructure." Below this, five categories are listed with progress bars: Identity (32 / 223), Data (6 / 219), Device (60 / 245), Apps (0 / 20), and Infrastructure (No data to show). The "History" tab shows a score of "0 points in 30 days" and a line chart for tracking performance over time. A legend at the bottom of the chart identifies "Your score" (purple), "Global average" (teal), and "Similar seat count" (pink).

Microsoft 365 security

### Microsoft Secure Score

Overview Improvement actions History

Your secure score

**Total score: 98 / 707**

Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps, and infrastructure.

**Identity** 32 / 223  
Protection state of your Azure AD accounts and roles

**Data** 6 / 219  
Protection state of your Office 365 documents

**Device** 60 / 245  
Protection state of your devices

**Apps** 0 / 20  
Protection state of your email and cloud apps

**Infrastructure** No data to show  
Protection state of your Azure resources

[Learn more about Microsoft Secure Score](#)  
[Get your score using Microsoft Graph API](#)

### History

**0 points** in 30 days Total score

Your secure score over time and how you compare to other organizations.

100  
75  
50  
25  
0  
08 PM

Your score Global average Similar seat count

[View history](#)

Improvement actions

# Drive deeper customer engagements

Become the security advisor through high value services

## Develop services around vulnerability assessments

Use tools to do a comprehensive security assessment for customers on a regular basis:

- Cloud security assessment
- Hybrid security assessment (CSAT)

Ensure you charge for them (they are valuable!). Repeat them quarterly and use them to inform your roadmap with your customers

## Use M365BP to transition into advanced security services deployment projects

M365B Capability	Deploy
Advanced Threat Protection	✓
Microsoft Defender (setup wizard)	✓
BYOD Mobile Policies (setup Wizard)	✓
MFA (baseline policies)	✓
O365 Message Encryption (enabled by default)	✓
Data Loss Prevention	✓
Full Intune Mobile Device Management	✓
Azure Information Protection	✓
Conditional Access	✓
Archiving & Retention Policies	✓

New

# Go deeper with a Security Assessment



Preparation  
15 minutes

Installation  
2.5 hours

Run the scan  
30 minutes

Presentation  
15 minutes



Available @ <https://cybersecurityassessmenttool.com>



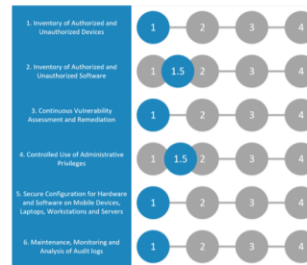
# Fast & Light Deliverables

## Maturity status

After reviewing the findings for each of the Security Control Domains described in detail in the Report, the overall assessment of <Customer>'s cybersecurity program has a Maturity Rating of: **Basic (1)**.



What is more important than the single, all-up Cybersecurity Maturity Rating, are the specific maturity ratings associated with each control domain. The 6 Basic CIS controls are considered essential and represent a "Cyber Hygiene" starting level.



**[Recommendation]**  
No clear governance and policies are available, think about Cyber security Policies, data governance policies, data retention policies and make sure they align with GDPR and ISO 27001 standards.

**[Recommendation]**  
IT security is a top-level strategic issue requiring executive leadership participation as stakeholders in the process.

## Highest risk findings

The findings below require <Customer> to take immediate action.

Finding	Action	Software products
Contractors that are no longer working for <Company> still have access to classified documents	<ul style="list-style-type: none"> <li>Deploy MFA</li> <li>Deploy AIP</li> </ul>	<ul style="list-style-type: none"> <li>In EMS E3 bundle, licenses already available</li> </ul>
30 users with very high Administrative rights	<ul style="list-style-type: none"> <li>Deploy PIM</li> </ul>	<ul style="list-style-type: none"> <li>Upgrade to EMS E5</li> </ul>
12 Windows XP machines were detected	<ul style="list-style-type: none"> <li>Upgrade the OS</li> </ul>	<ul style="list-style-type: none"> <li>Windows 10</li> </ul>

**[Immediate action required]**  
Not taking action will keep <Customer> exposed to serious security incidents. Not addressing these findings could lead to negative consequence in case of inquiries after a breach.

New

# Security partner competency

## Silver partners

- **Industry Certification Requirements**  
1 Individual in M500: M365 Security Admin
- **Demonstrated Customer Performance**  
1000 Active Users in security workload
- **Pay program fee**

### BENEFITS

Internal use rights for M365  
Co-marketing MPN benefits

## Gold partners

- **Industry Certification Requirements**  
4 individuals: Pass Microsoft Professional Program in Cybersecurity AND either pass MS500 (M365 Security Admin) or AZ-500 (Azure Security Engineer)
- **Demonstrated Customer Performance**  
4000 Active Users in security workload
- **Pay program fee**

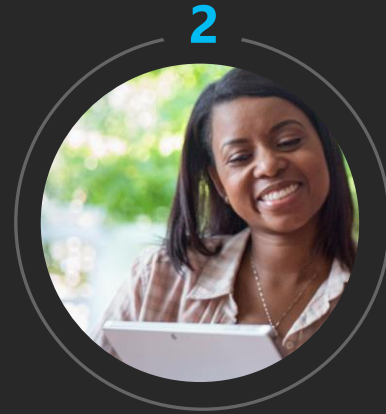
### BENEFITS

Internal use rights for M365  
Usage incentive eligibility  
ECIF & Customer matching prioritization  
Co-marketing MPN benefits

# Going to market with a security practice: path to success



Targeting



Demand gen



Pre-sales



Post-sales

Basic

Utilize Cloud Ascent to derive customer propensity

Hook into Microsoft Graph and utilize SecureScore as a conversation starter with customers

Conduct security assessments utilizing CSAT to build a roadmap

Utilize security deployment kit in Launchpad to drive utilization

Advanced

Drive pre-engagement workshop and threat check to provide threat mitigation recommendations

Execute against strategy workshops post threat check to build roadmap

Leverage FastTrack and milestone-based usage incentives (15 & 40%)

# Your next steps!



Lead the sale with Microsoft 365 Business Premium today to drive security



Develop your security practice strategy, starting with assessment



Learn more about security through the assets at [aka.ms/m365bpartners](https://aka.ms/m365bpartners)



# Resources

- Understand our Sales programs along the customer journey: [\\_aka.ms/SecurityPartnerPractice](https://aka.ms/SecurityPartnerPractice)
- Access resources & nominate your customers for a Security Workshop: <https://aka.ms/SecurityWorkshop>
- Learn more about Security in our “October Cyber Security Awareness Month” <https://aka.ms/CyberAwarenessMonth>
- Join our community to stay connected [aka.ms/SecurityPartnerYammer](https://aka.ms/SecurityPartnerYammer)





End of Building a Security Practice.

For more information, contact [msftcsp@synnex.com](mailto:msftcsp@synnex.com)