



PARTNER OPPORTUNITY PLAYBOOK

SMB Security and Compliance



TABLE OF CONTENTS

Opportunity and introduction to SYNEX	3
Cyberthreats in 3 key zones	6
Security as a Service	11
Secure the front door	14
Secure content	20
Secure devices	24
Great employee experiences	30
Microsoft 365	32
Next steps	36



Times have changed, and so have your customers' security needs

Security and compliance are top of mind for your SMB customers, and it's no wonder: with **43% of breaches occurring at SMBs**¹ at an average cost of **\$120K per breach**,² the threats they face are real.

But managing these threats isn't as easy as it once was. Gone are the days when SMBs could protect themselves with a simple network of antivirus software, spam folders, and a firewall. Now, between the cloud, increasingly sophisticated cybercrime, and a high risk of internal security errors, it's become much harder for customers to defend their businesses.

Making matters more complicated, **62% of SMBs lack the skills in-house**³ to deal with security issues on their own. But SMBs are savvy—they know they need a trusted partner to help them face security threats. In fact, 89% of businesses see cybersecurity as a top priority, and 84% of those without a managed service provider (MSP) would consider using one.⁴

As a reseller, you have a major opportunity to step up for your customers and simplify their security equation with Microsoft 365. They'll get a comprehensive solution that helps them easily prevent and respond to issues in-house—while you grow a thriving security practice.

¹ Verizon. Data Breach Investigations Report. 2019.

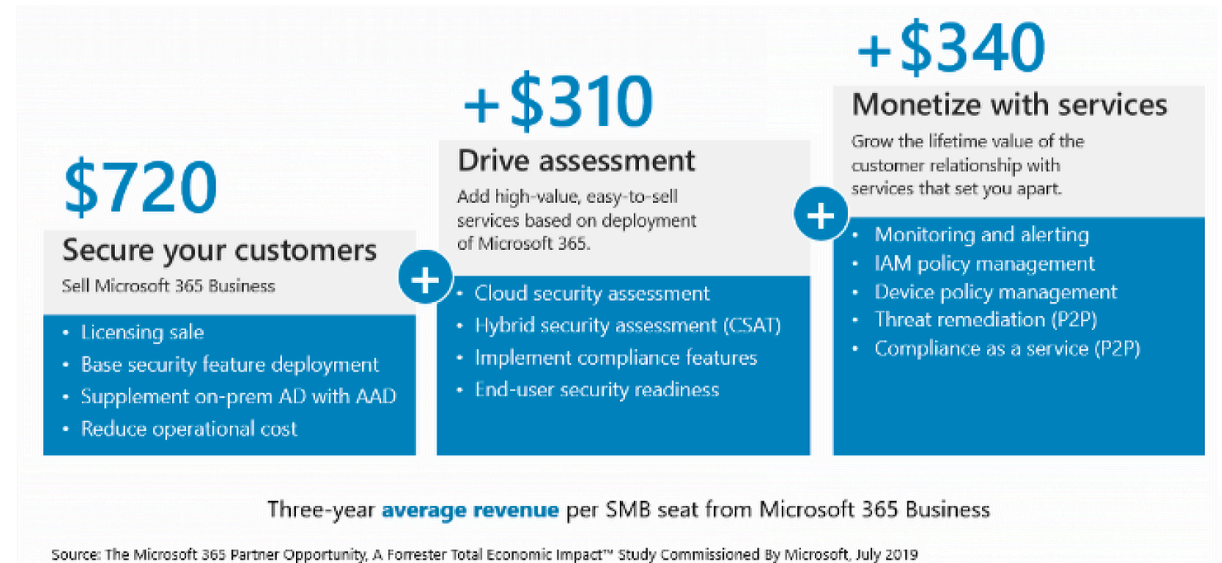
² Kaspersky Lab Study. 2018.

^{3,4} Vanson Bourne, commissioned by Continuum. Underserved and Unprepared: The State of SMB Cyber Security in 2019.

Security is key to your customers' success—and your growth

The partner opportunity for security is big—now is the perfect time to become your customers' trusted security partner *and* boost profits. In fact, **92% of SMB respondents¹** in a recent survey indicated that their organizations would consider moving to a new MSP if they offered the right security solution—and of those, **25% would be willing to pay more²** on average, too.

And it's not just customers who win big. Microsoft 365 helps security partners boost profitability by \$15.75 per user, per month. And it can be even more gainful as you grow your security practice to add assessments, and eventually fully manage your customers' outsourced security.



^{1,2} Vanson Bourne, commissioned by Continuum. Underserved and Unprepared: The State of SMB Cyber Security in 2019.

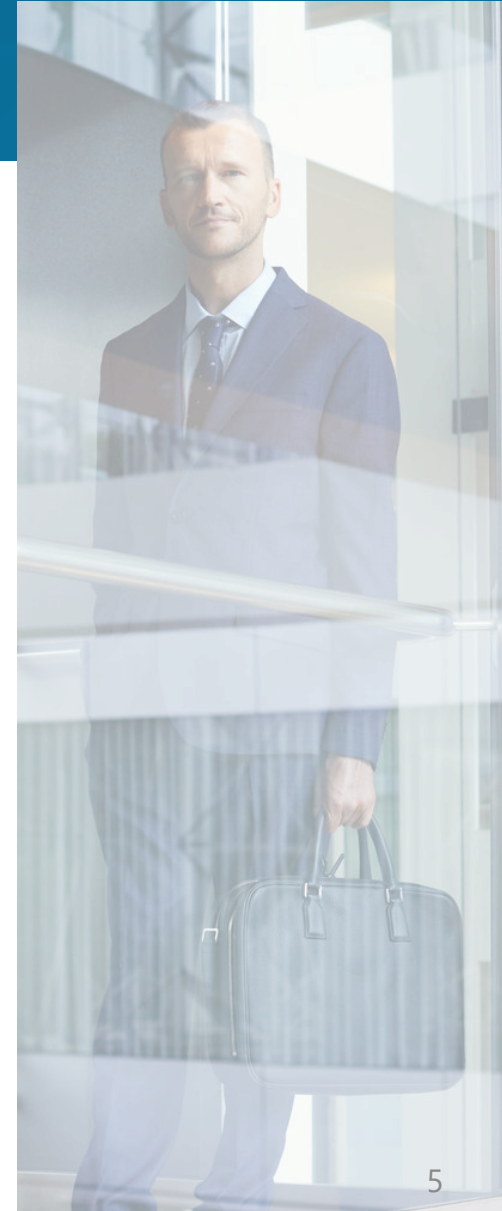
SYNNEX has everything you need to grow your security practice

Building a security practice may feel overwhelming, but you don't have to go it alone—SYNNEX is here to support you every step of the way.

We'll help you grow the security practice that's right for you. Count on us to help with security assessments, licensing, and selling, as you take full advantage of our ecosystem of hardware, software, and endpoint solutions to create unique offerings. We know the ins and outs of today's most common security tools, and we're ready to put that knowledge to work so you can create the security practice your customers need—while you drive more recurring revenue.

When you offer Microsoft 365 with SYNNEX, your customers will benefit from a single, holistic solution that unites Office 365 best-in-class productivity tools with advanced security and device management capabilities. We'll make sure you have everything you need to capture this profitable partner opportunity. As a plus, Microsoft 365 is ideal to pitch for partners because it's so affordable for customers: while the monthly cost of third-party solutions for security and productivity total more than \$50 per user, **Microsoft 365 offers holistic security starting at \$20 per user.**

Read on to find out how you can bring more value to your customers with Microsoft 365 and SYNNEX.



Cyberthreats in 3 key zones

EMAIL

Within 4 minutes

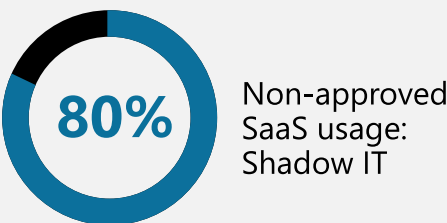
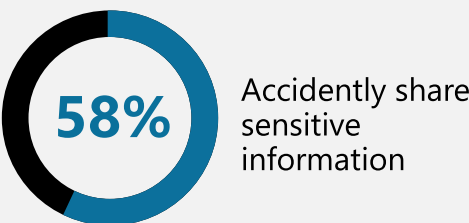
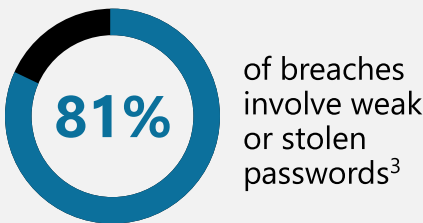


It takes
206 days
to detect intrusion¹

And another
73 days
to contain damage²

BRIEF:
It takes hackers 4 minutes to get into networks through email attacks and 206 days for detection, followed by an additional 73 days for damage control.

USER



DEVICE



53 seconds
A laptop is stolen nearly every minute⁴

55,000
Average devices compromised by ransomware every month in 2016, a 5X increase from 2015 and 4X increase in Android base

200,000
PCs attacked by WannaCrypt across 150 countries

\$1 billion
Average earning of a hacker from ransomware (FBI estimate)

^{1,2} Ponemon Institute, commissioned by IBM. Cost of a Data Breach. 2019.

³ Verizon. 2017 Data Breach Investigations Report. 2017.

⁴ Gartner, commissioned by Kensington.



As much as SMB and Enterprise customers differ, they do share common ground. Increasingly, SMBs are approaching their technology investments in much the same way as Enterprise customers. The gap between how SMBs and Enterprises see their businesses, their customers, and their technology initiatives is narrowing. In recent research, Forrester reported that SMBs are becoming more active in both new technology adoption and acceleration of their refresh cycles.¹ Just as similar priorities guide SMBs' and Enterprises' investments and focus, SMBs' technology investment patterns map closely to those of Enterprises.

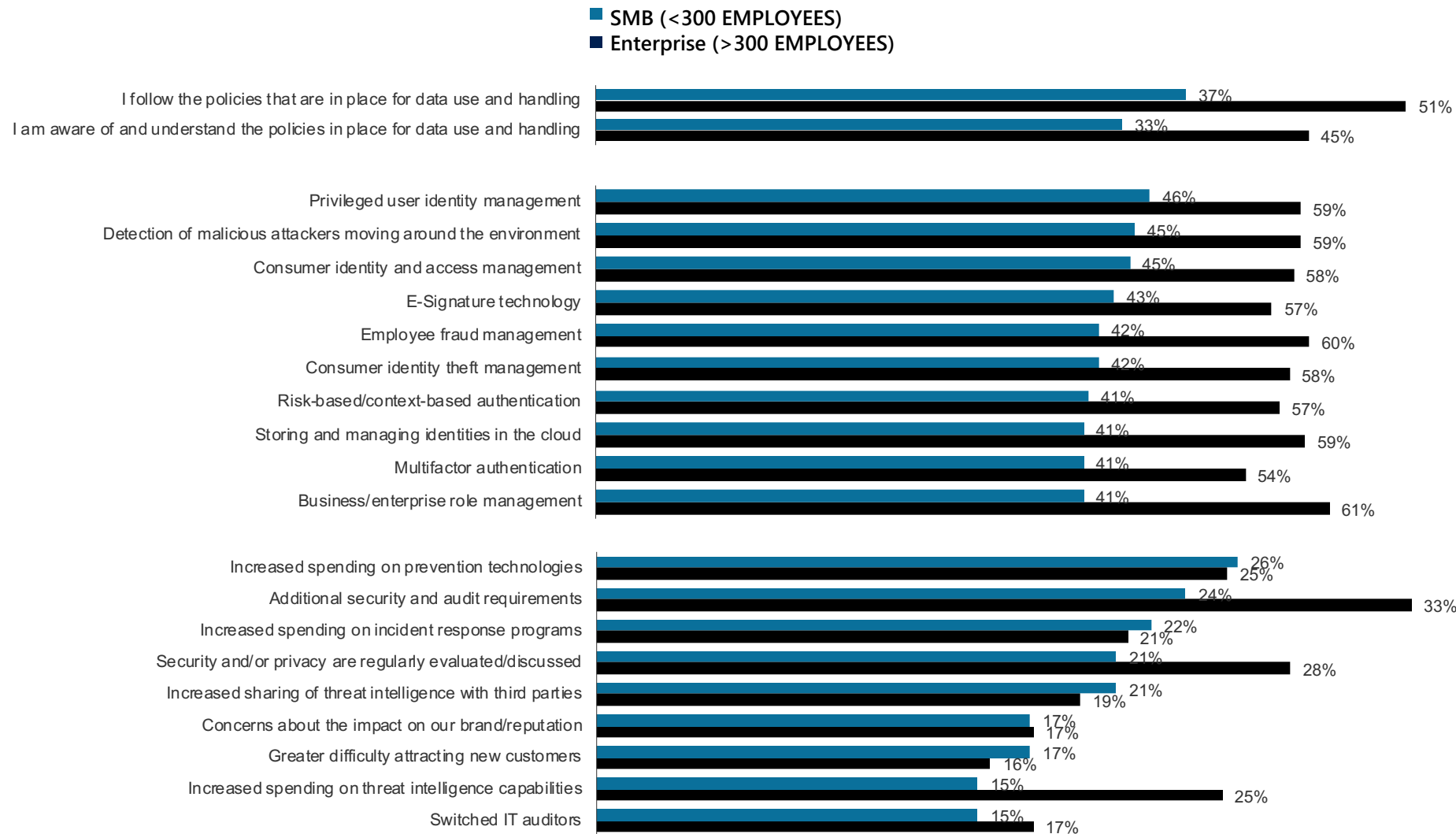
That's good news if your organization targets SMB-size customers. IDC forecasts worldwide IT spending by SMBs will approach **\$630 billion in 2019** in a new update of the Worldwide Semiannual Small and Medium Business Spending Guide.²

The report makes the case that while SMBs, especially smaller ones, have immediate tactical needs to sharpen performance, they are also looking to coordinate resources in a meaningful way. For many, this will be an important step forward in their digital transformation.

¹ Forrester, SMBs Now View Their Tech Investments Through an Enterprise-Like Lens, May 8, 2017.

² IDC. Worldwide Semiannual Small and Medium Business Spending Guide. 2019.

Technology planning – SMB vs. Enterprise



- **Most companies have employees who are not following or not aware of policies.¹**
- **Larger companies are more likely to adopt a wider array of identity and access management technologies.²**
(What are your firm's plans to adopt the following identity and access management technologies?)
- **Larger companies are also more likely to increase their threat intelligence spending and security requirements post-breach although many of the responses were similar.³**
(What has changed at your firm as a result of the breaches occurring in the past 12 months?)

¹ Base: N=2,454 (SMB(<300 employees)), N=4,948 (Enterprise (>300 employees)); Global information workers. Source: Forrester's Global Business Technographics Security Survey, 2016.

² Base: N=233 (SMB(<300 employees)), N=840 (Enterprise (>300 employees)); Global network security decision-makers (20+ employees) Source: Forrester's Global Business Technographics Security Survey, 2016.

³ Base: N=144 (SMB(<300 employees)), N=475 (Enterprise (>300 employees)); Global network security decision-makers whose firms have had a security breach in the past 12 months

Source: Forrester's Global Business Technographics Security Survey, 2016.

SMB decision-making based on organization size

Internal research done by Microsoft in March 2017 provides an even deeper breakdown into the differences between different SMB customers based on their size. The research looked individually at core small business (CSB) with 6–49 information workers (IW), lower midmarket (LMM) with 50–99 IW, and core midmarket (CMM) with 100–249 IW.

The findings show that each segment is in a distinctly different place in several key areas of customer concern:

Hacking is top of mind but employees may be the threat

- Viruses/external threats come to mind first when asked about security, but what really keeps BDMs up at night is the inability to manage internal threats from employees, ranging from accidental device loss to falling victim to phishing attacks and theft of IP.
- The perceived inability to manage these internal threats has often lead to “lock down mode” in CMMs, while many LMMs have realized the need but have not yet taken action.

Mobility and security are at odds with each other

- Mobility is not always seen as important for productivity, which is causing devices to be a key target of lock down mode to mitigate internal threats. This was especially the case for CMMs and smaller organizations in legal, architecture, and publishing.
- Although there is demand from employees for greater mobile access, there is no understanding that mobile security controls exist that allow an organization to be both more productive and less susceptible to internal threats.

Security investments are an inconsistent priority

- Neither the level of concern nor increased mobile use is prompting action, with new solutions being put in place only as the result of an incident that has a significant impact, due to an intangible ROI.
- The basics are covered by point solutions and seen as enough, largely due to a combination of two beliefs: 1) If Target can be hacked, so can anyone, and 2) I am too small for them to go after.
- There was a low awareness of GDPR, but a few BDMs from larger organizations mentioned IT work happening for new compliance needs.

Product differentiation is not well understood




- Office 365 is often trusted to have enough security without knowledge or use of many features, resulting in a general lack of awareness regarding capabilities in other Microsoft solutions.
- The lack of BDM awareness within larger companies is likely in part a function of having an IT department that owns security and related purchasing decisions.

- CSB: core small business with 6–49 information workers (IW)
- LMM: lower midmarket with 50–99 IW
- CMM: core midmarket with 100–249 IW

Recommendations from this research:

1. Unlock interest by tuning key messages and refining targeting based on size
2. Lean into features that resonate and differentiate across groups:
Internal controls:
 - Remove corporate data and apps (●●●)
 - Collaborate more securely (●●)
 - Protect data at all times (●●)Advanced security:
 - Threat detection for on-premises (●●)
 - Intelligent security (●●)
3. CMMs are inclined to prioritize security solutions. Focus efforts on them, with these key points as a smarter alternative to locking down:
 - A single solution provides consistency and efficiency (costs savings)
 - Enable mobile productivity without sacrificing security (productivity gains)
 - AI-driven proactive feature sets (a higher end insurance policy)

Protect customers with proactive security

AREA OF VULNERABILITY	REMEDY	LEVEL OF DIFFICULTY	PRIORITY	CORE TECH
 Identity	Turn on multi-factor authentication	Medium	1	Azure Active Directory
	Turn on single sign-on across 2,600+ SaaS applications	Medium	1	Azure Active Directory
	Leverage Intelligent Security Graph for real-time risk assessment and identity-based access	Low	1	Azure Active Directory
 Desktop	Deploy down-level Windows updates regularly	Low	1	Windows Professional & Enterprise
	Host intrusion protection against vectors originating from social media scripts, emails	High	2	Windows Enterprise
 Applications	Discover SaaS apps, bring under single sign-on	Low	1	Azure Active Directory
	Protect users from vulnerable links and attachments in emails	Low	1	Office 365 Advanced Threat Protection
	Use Microsoft 365 security services	Medium	2	Microsoft 365 Enterprise
	Information protection via Microsoft Cloud App Security	Medium	3	Cloud App Security, Azure Info Protection



SMB customers need Security as a Service

Today's mobile and entrepreneurial workforce extends the business beyond the office and customary work hours. Security as a Service, powered by **Microsoft 365**, helps businesses stay agile and competitive, while keeping their data, tools, and resources accessible, yet more secure, anywhere, anytime.

Microsoft 365 provides a modular solution that addresses the IT and Bring-Your-Own-Device (BYOD) challenges of your SMB customers, while providing a secure end-to-end managed cloud environment that encompasses identity, apps, content, and devices.

Conversation starters: Can your customer answer yes to **these 5 questions**?

1.

Do you **know** who is accessing your data?

2.

Can you **grant access** to your data based on risk in real time?

3.

Can you quickly **find and react** to a breach?

4.

Can you **protect** your data on devices, in the cloud, and in transit?

5.

Do your users **love** their work experience?

If not, then they might need **Security as a Service!**

Security as a Service – 4 key areas



SECURE THE FRONT DOOR

Protection from identity-driven breaches, email attacks, and attacks targeting OS



SECURE CONTENT

Protect content: at the time of creation, in transit, and during consumption



SECURE DEVICES

Workplace issued or BYOD devices



GREAT EMPLOYEE EXPERIENCES

Productivity without compromise



**Secure the
front door**

Secure the front door



With **Microsoft 365**, you can equip SMB customers to better manage their identity and access controls, secure links and attachments in emails, and stop breaches before they escalate in severity.

Determine if your customer needs help securing the front door:

- Do they know who is accessing their data?
- Can they grant access based on risk in real time?
- Can they quickly identify and react to a breach?



¹ Vanson Bourne, commissioned by Continuum. Underserved and Unprepared: The State of SMB Cyber Security in 2019.

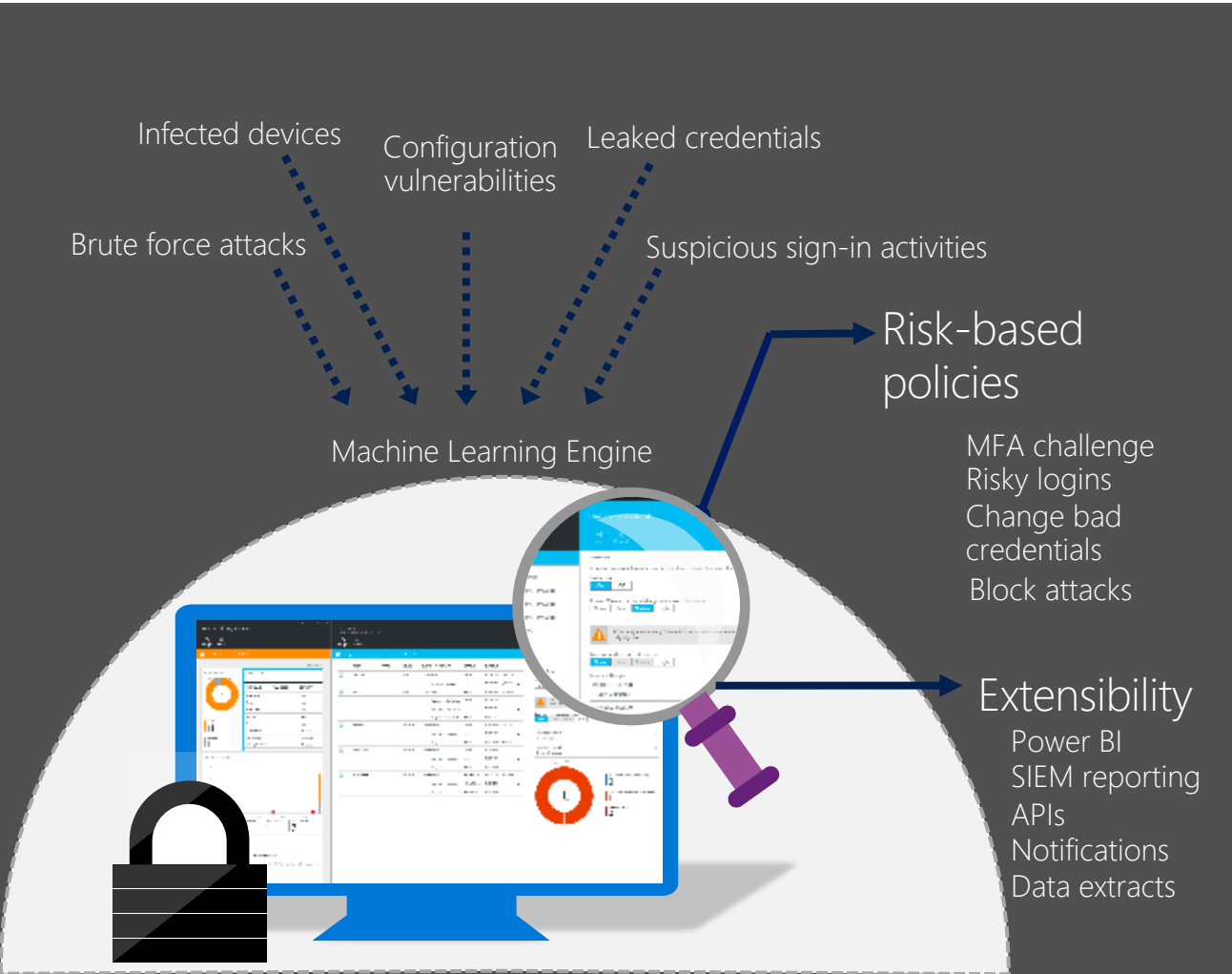
² Microsoft. Security Intelligence Report, vol. 24. 2018.

³ Verizon 2017 Data Breach Investigations Report.

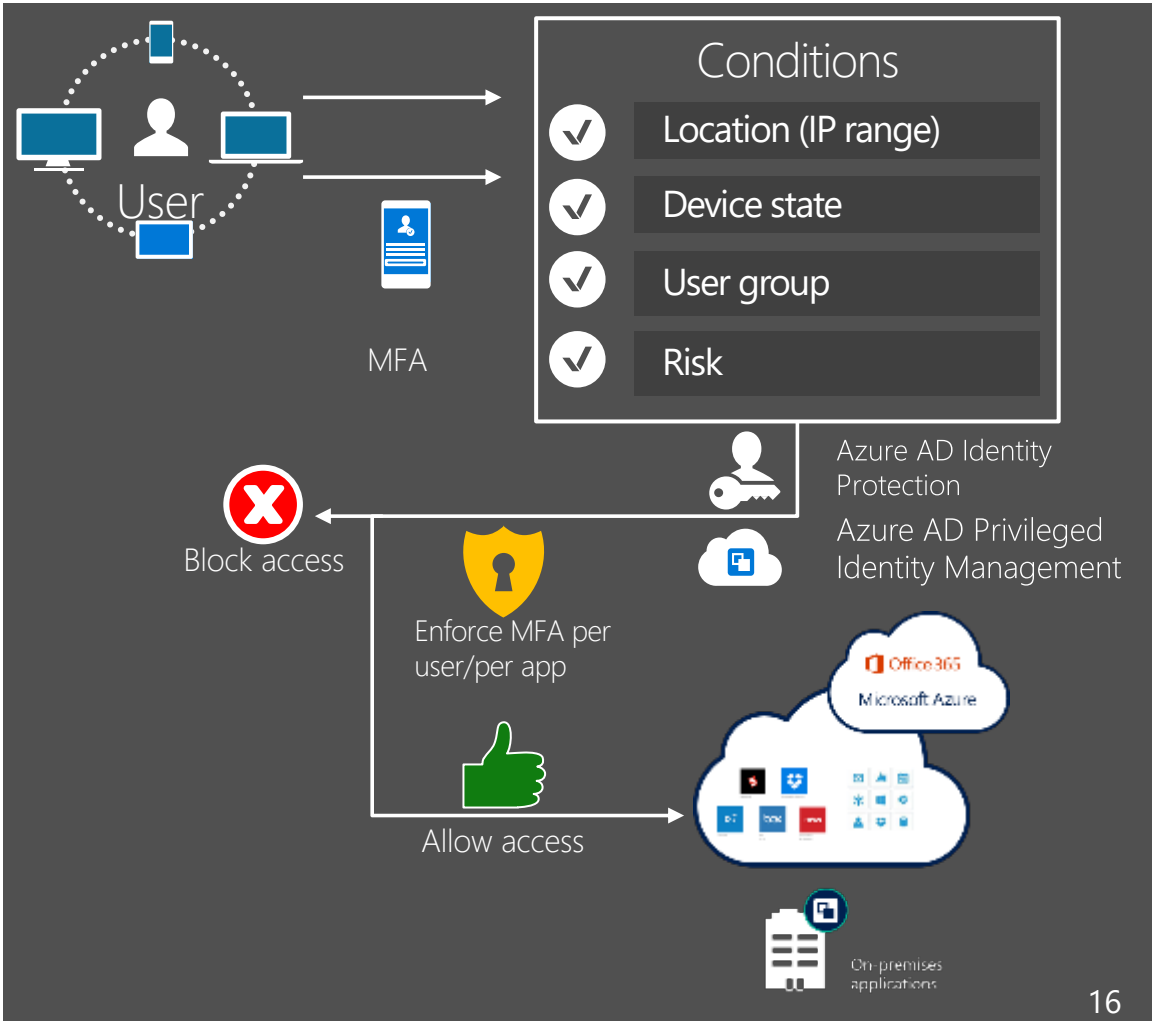
⁴ Security Week Survey.

Secure the front door: Real-time risk assessment

Machine learning and risk profiling



Open the front door based on risk

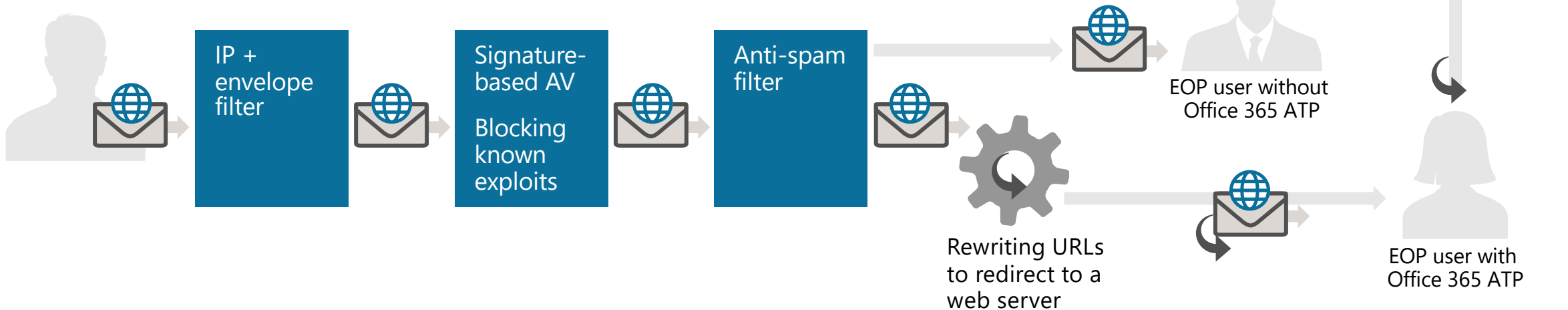


Safe links

Helps protect against **phishing** and sites with malicious content.

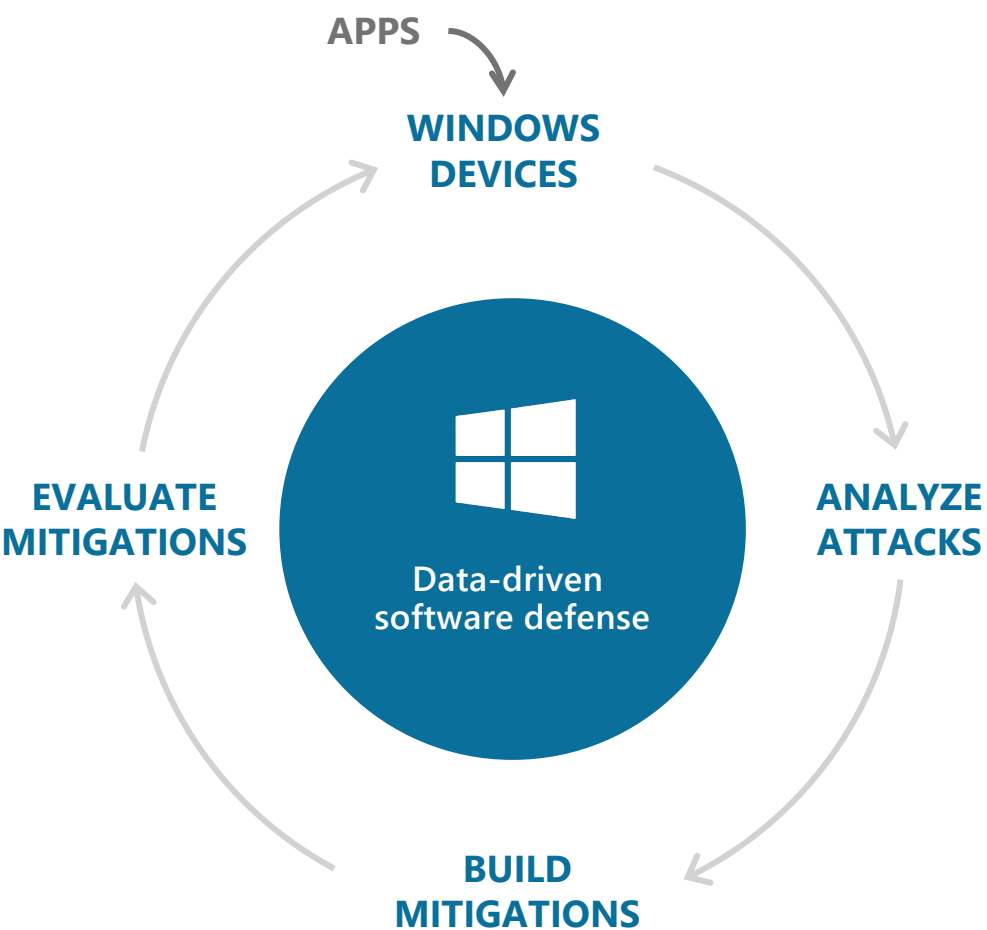
Provides **visibility** into compromised users for administrators.

Rewrites **all URLs** to proxy through an EOP server.



Securing apps with Windows Defender Exploit Guard

Reduce the attack surface of applications while balancing security with productivity.



MINIMIZE THE ATTACK SURFACE

Signature-less, control entry vectors, based on cloud intelligence. Attack surface reduction (ASR) controls, such as behavior of Office Macros.



BREAK EXPLOITATION TECHNIQUES

Modern exploit mitigations for your apps. Protect legacy applications, without recompilation.



CONTAIN DAMAGE & PREVENT PERSISTENCE

Protect sensitive folders, processes, and data assets from undetected malware and unknown threats.



LIMIT THE WINDOW OF EXPOSURE TO THREATS

Respond to emerging exploits or threats. Reactively turn on anti-exploit mitigations and set ASR controls.

Secure the front door



Microsoft 365 products and services can help you develop solutions for identity-driven security.



Azure Active Directory Premium – Manage and control access to resources

In a mobile-first, cloud-first world, IT professionals need to protect corporate assets while empowering user productivity at any location at any time.



Cloud App Security – Security for your cloud apps

Bring security capabilities to SaaS cloud applications to gain better visibility and enhanced protection against cloud security issues.



Microsoft Advanced Threat Analytics – Detect suspicious activity right away

Given the rapidly changing threat landscape, enterprises need tools that provide a succinct, real-time view of attacks, and identify suspicious user or device behavior.



Windows Hello – Authenticate identities without passwords

Password authentication is not sufficient to keep users safe. Users reuse and forget passwords. Passwords are vulnerable and difficult for users to employ.



Exchange Advanced Threat Protection – Safeguard against attacks

As hackers launch increasingly sophisticated attacks, organizations seek tools that provide stronger protection against specific types of advanced threats.



Advanced Security Management – Enhanced visibility and control

Gain insight into suspicious activity in Office 365 so you can investigate potential problems and take action to address security issues.



**Secure
content**

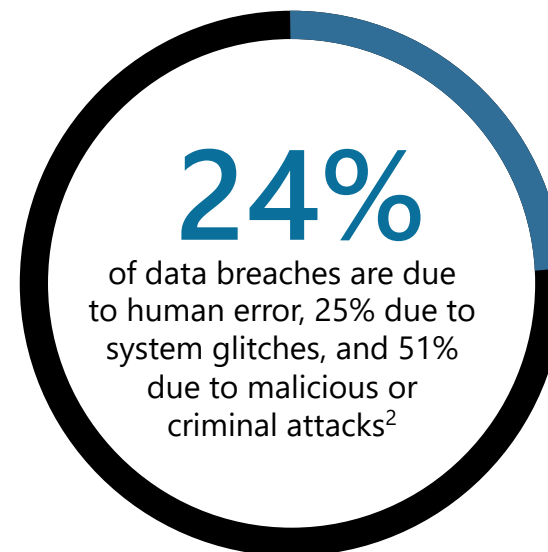
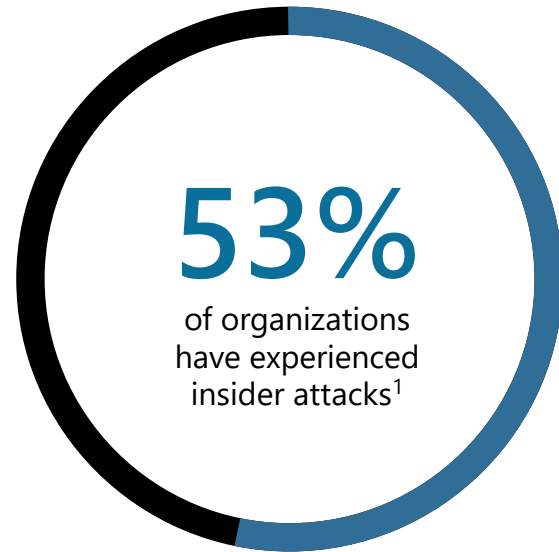
Secure content



With **Microsoft 365**, you can help your SMB customers employ tools that will better protect business data, guard against accidental sharing of sensitive information, protect data in cloud applications, and improve compliance.

Determine if your customer needs help securing their information:

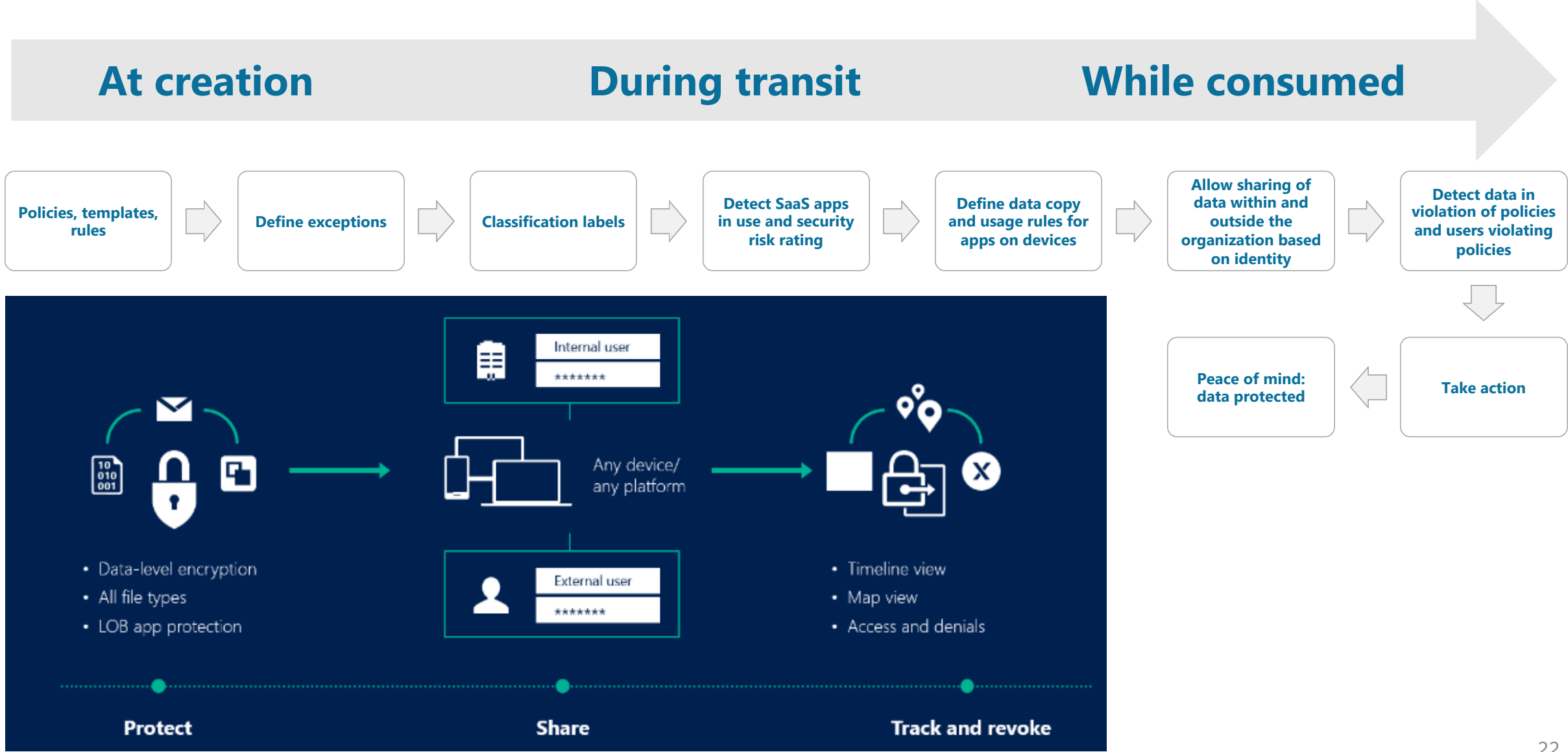
- Is their data secured regardless of where it's stored or shared?
- Does a data compliance policy control access to sensitive information?
- Can users meet all compliance obligations without interrupting their workflow?
- Do they have the ability to classify and encrypt sensitive data?



¹ Microsoft. Security Intelligence Report, vol 24. 2018.

^{2, 3} Ponemon Institute, commissioned by IBM. Cost of a Data Breach. 2019.

Secure content



Secure content



Microsoft 365 products and services can help you develop solutions for a security practice focused on protecting content (creation, transit, and consumption).



Azure Active Directory Premium – Manage and control access to resources

In a mobile-first, cloud-first world, IT professionals need to protect corporate assets while empowering user productivity at any location at any time.



Cloud App Security – Security for your cloud apps

Bring security capabilities to SaaS cloud applications to gain better visibility and enhanced protection against cloud security issues.



Azure Information Protection – Better secure sensitive information anytime, anywhere

SMB customers need control over the access to information, no matter where it's stored or who it's shared with.



Microsoft Intune – Meet your data protection needs while delivering the best user experience

Flexible mobile device and app management controls let employees work with the devices and apps they choose while protecting company information.



Data Loss Prevention – Create policies to identify, monitor, and protect sensitive data

To comply with business standards and industry regulations, organizations need to protect and prevent the disclosure of sensitive information such as financial data, credit card numbers, social security numbers, or health records.



Advanced eDiscovery – Better understand your Office 365 data and reduce your eDiscovery costs

Analyze unstructured data within Office 365, perform more efficient document review, and make decisions to reduce data for eDiscovery.



Secure devices

Secure devices



With **Microsoft 365**, you can build a practice that helps your customers proactively guard against threats, use advanced analytics to identify breaches and threats, and automate responses to threats companywide.

Determine if your customer needs help with threat protection:

- Do they have tools that allow them to automatically detect high-risk usage?
- Are they leveraging machine learning to uncover suspicious activities?
- Are they able to easily access reporting to find patterns that reveal threats?
- Can they automatically guard users against phishing attacks and dangerous links?
- How quickly can they react after a breach has been detected?

\$170.4B

Cumulative global
spending prediction
for cybersecurity
by 2022¹

4,000

ransomware
attacks per day²

53s

A laptop is stolen
every 53 seconds³

\$1B

losses from
ransomware⁴

¹ Gartner. Forecast Analysis: Information Security Worldwide. 2018.

² FBI. Ransomware Prevention and Response for CISOS, 2016.

³ Gartner, commissioned by Kensington.

⁴ Vircom. 10 Craziest Cybersecurity Statistics of 2016.

Secure mobile devices and content on apps



MANAGE DEVICES

Access management

- Conditional access
- Device settings and compliance enforcement
- Multi-identity support

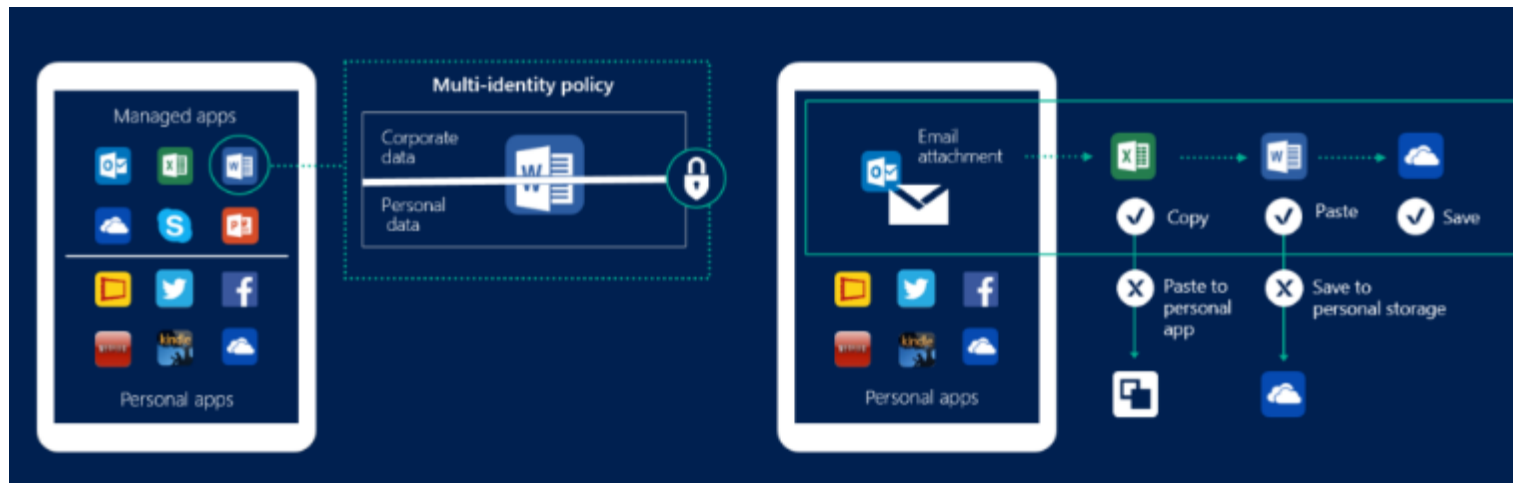
Built-in security

- Mobile app management
- File-level classification, labeling, encryption
- Supporting rights management services

Gold standards

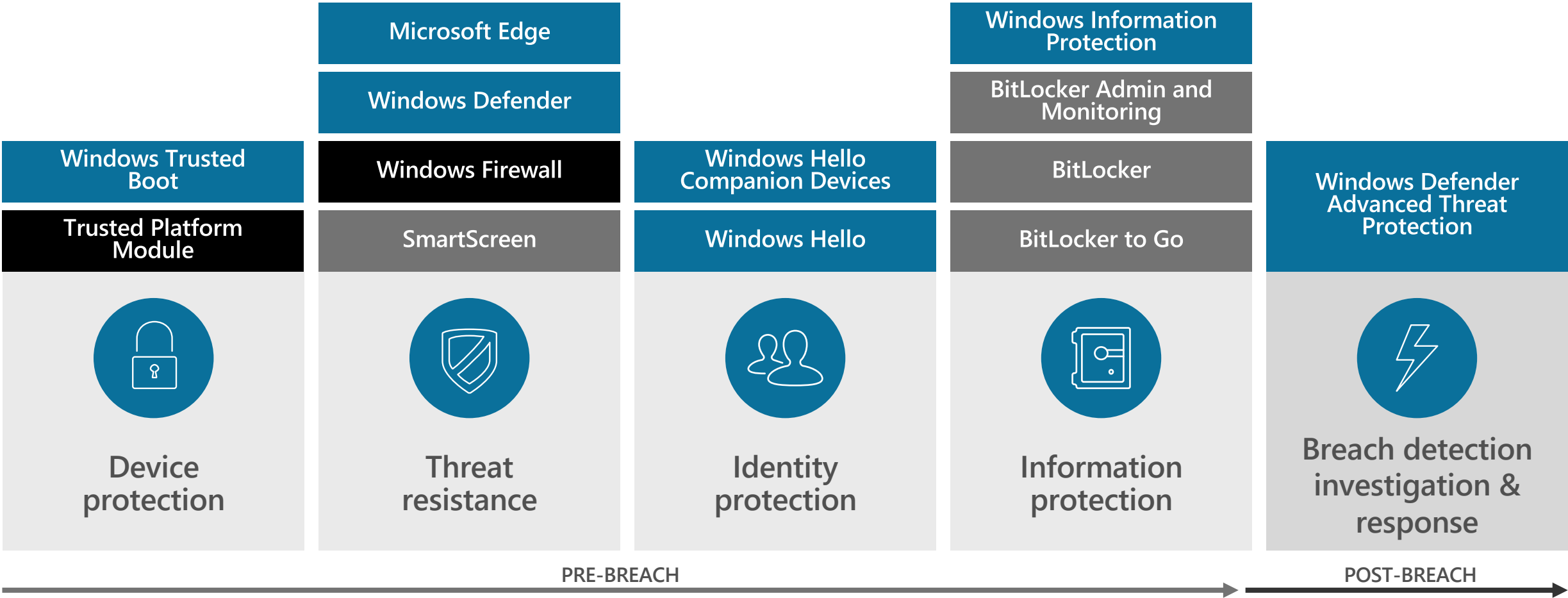
- Office mobile apps

Manage apps and experience

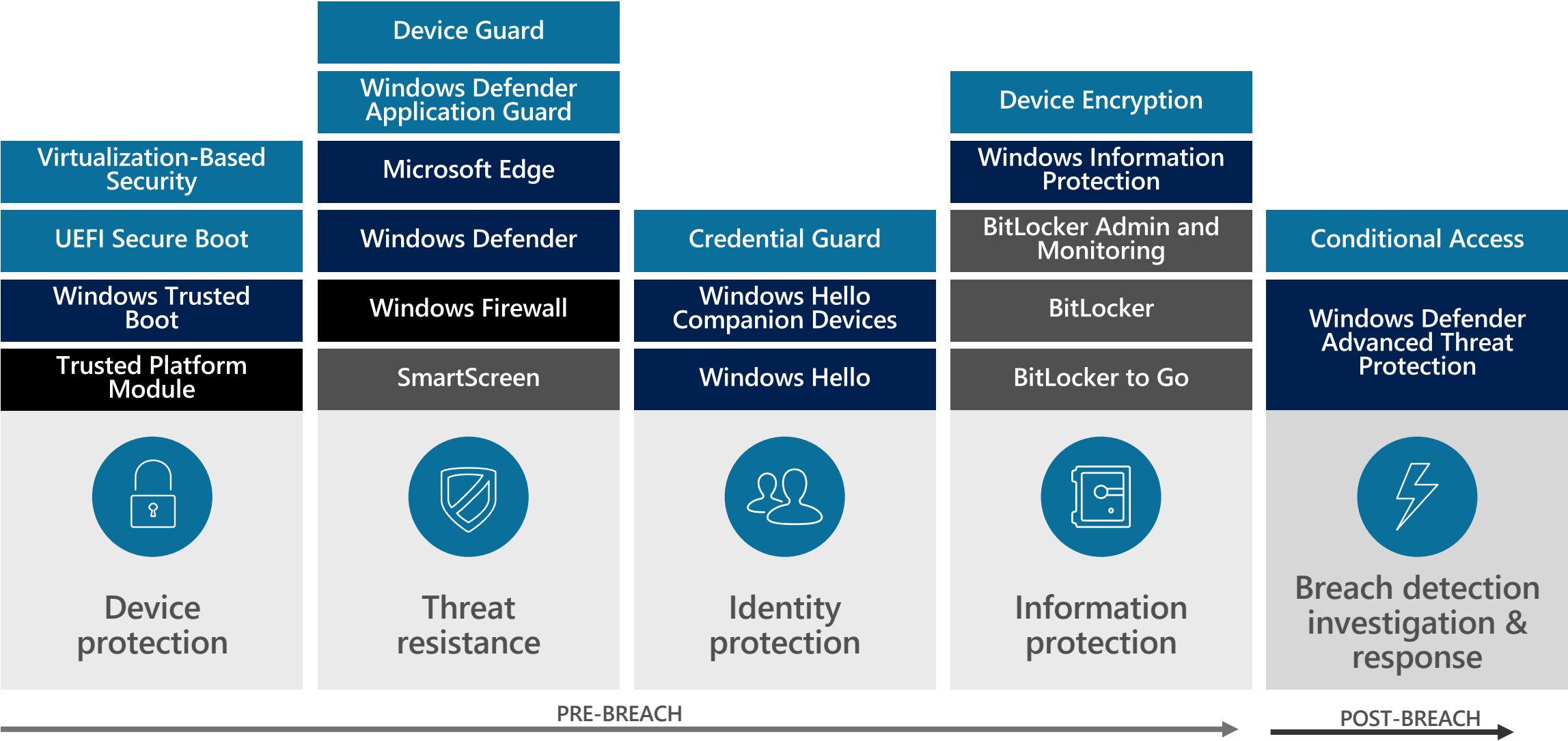


- Define app-work data relationships
- Maintain visibility and control without intrusion

Windows 10 security on Windows 7 hardware



Windows 10 security on Windows 10 hardware



Secure devices



Microsoft 365 products and services can help you secure workplace-issued or BYOD devices.



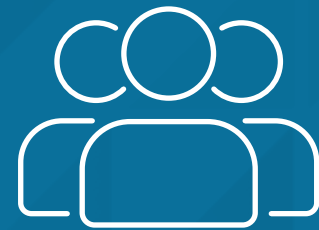
Azure Active Directory Premium – Manage and control access to resources

In a mobile-first, cloud-first world, IT professionals need to protect corporate assets while empowering user productivity at any location at any time.



Microsoft Intune MDM and MAM – Meet your data protection needs while delivering the best user experience

Flexible mobile device and app management controls let employees work with the devices and apps they choose while protecting company information.

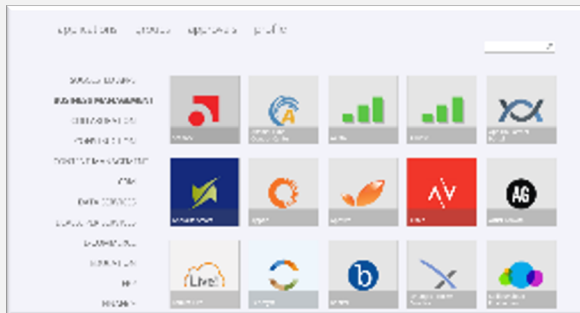


**Great
employee
experiences**

Opportunities for great employee experiences

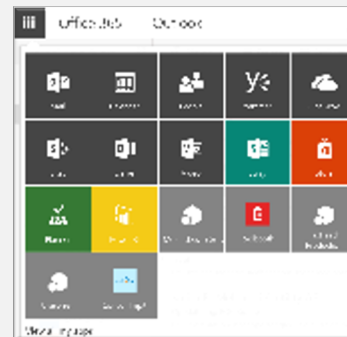
Single sign-on

- Single sign-on to on-premises, on-Microsoft cloud apps
- Single sign-on to 2,700+ non-Microsoft SaaS apps (Dropbox, Salesforce, etc.)



Self-service

- Reset/change passwords without bothering IT
- Multi-factor authentication
- Work from anywhere
- Pick and choose work apps; create, join groups



Work from anywhere

- Work from any device
- Choose between calls/SMS/app for multi-factor authentication
- Non-intrusive security





Introducing **Microsoft 365**

We are living in a time of inflection. Digital transformation is the biggest change any of us has seen in our lifetime. Companies invest in technology to optimize operations, transform products, engage customers, and empower employees. The challenge is finding the way to empower people to do their best work. This starts with fostering a culture of work that is inspiring for everyone, and embraces the trends in the workplace that make work inspiring.

To deliver on the tremendous opportunity for business growth and innovation, we are simplifying the customer experience by bringing together Office 365, Windows 10, and Enterprise Mobility + Security with the introduction of Microsoft 365.

It's a complete, intelligent solution that empowers everyone to be creative and work together, securely.

Four core principles of Microsoft 365



**Unlocks
creativity**



**Built for
teamwork**

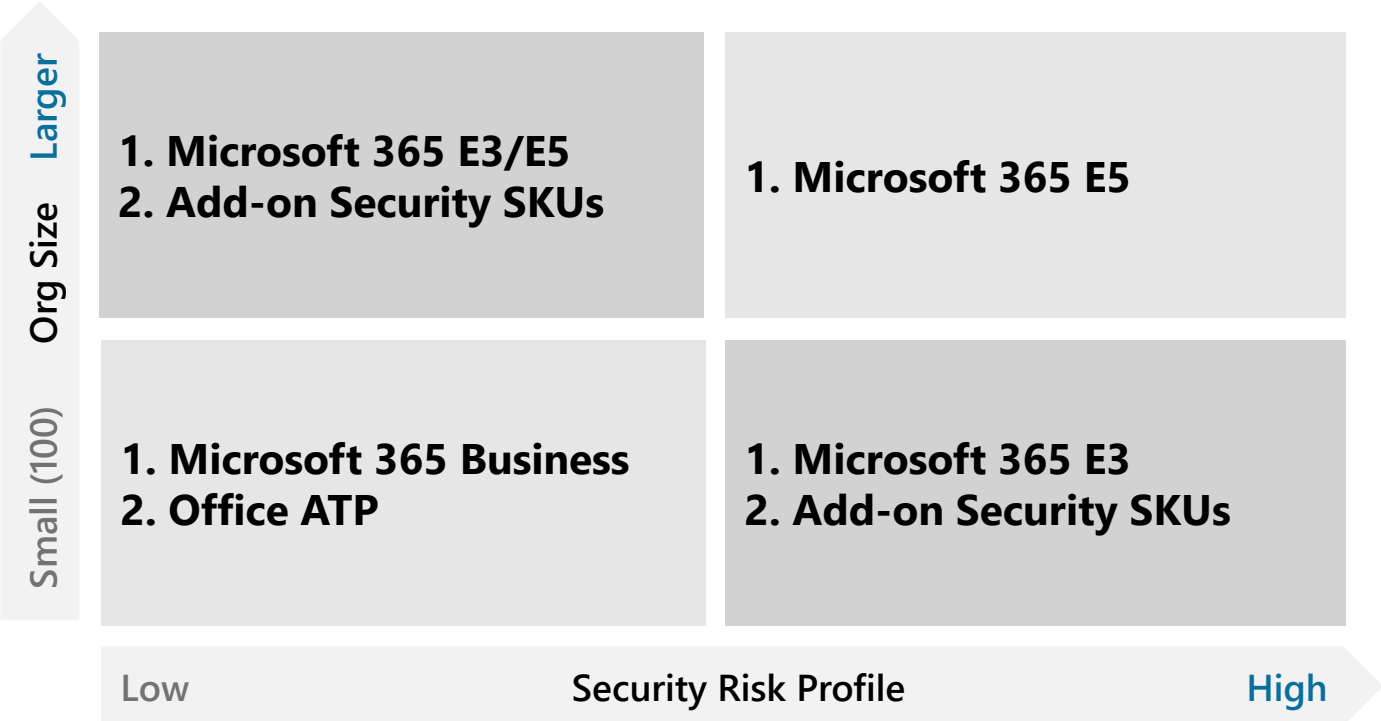


**Integrated
for simplicity**



**Intelligent
security**

Fitting the right Microsoft 365 plan to your SMB customer



Selecting a **Microsoft 365** plan for your SMB customers requires more than matching their size—the right fit depends primarily on their risk profile, determined by the sensitivity of the data they must protect, the amount of regulation they face, and how and where their employees access data and apps.

LOWER RISK PROFILE:
Microsoft 365 Business
No financial data
Minimal customer information
Limited IP to protect
No unauthorized cloud app usage
Minimal compliance requirements

HIGHER RISK PROFILE:
Microsoft 365 Enterprise
Highly sensitive financial data
Personal health information
Extensive IP requiring advanced threat protection
Extensive cloud application usage
Extensive compliance requirements (GDPR)

SMB security staircase: New customers

Microsoft 365 Business
\$20

Security & Compliance Controls

- The most secure and up-to-date version of Office and Windows
- Threat Protection (virus, malware) for emails
- Malware and spyware detection and removal
- Virus detection and removal, Boot-time protection
- Data always encrypted on devices
- 2 Factor authentication needed to access data on PC/mobile
- Data safe on mobile devices (copy/paste/save operations)
- Benchmark your controls with Secure Score
- Gain visibility with Security & Compliance Center



ATP
\$2

EMS E3
\$8.75

+

Office 365 E3
\$20

Identity, Information, & Device Protection

- Intelligent Security Graph
- Classification and labeling
- Multi-Factor Authentication
- Single sign-on to 2,600+ SaaS applications
- Mobile Application Management
- Mobile Device Management
- Encryption and Rights Management
- Tracking, reporting, and revoking privileges
- Data Loss Prevention
- Archiving
- Advanced Threat Protection: Safe Links, Safe Attachments
- Full Office client



ATP
\$2

Microsoft 365 Enterprise E3
\$34

Proactive Attack Prevention

- Host intrusion prevention capabilities
- Device Guard: Preventing malicious code from running
- Credentials Guard
- DirectAccess
- Windows Information Protection
- BranchCache
- Microsoft Desktop Optimization Pack



Pricing based on US CSP pricing. Please customize according to licensing program and geography.
Microsoft 365 Business has a limit of 300 seats/tenant

ADD-ON

SUITE

EMS E3 = AADP-P1 + AIP-P1 + Microsoft Intune
M365 E3 = EMS E3 + O365 E3 + Win E3

SMB security staircase: Cross-selling to existing customers

ATP

AADP-P1

Any Office 365 Suite

Identity and Advanced Email Protection

- Intelligent Security Graph
- Multi-Factor Authentication
- Single sign-on to 2,600+ SaaS applications
- Advanced Threat Protection: Safe Links, Safe Attachments



ATP

EMS E3

Office 365 E3

Identity, Information & Device Protection

- Classification and labeling
- Mobile Application Management
- Mobile Device Management
- Encryption and Rights Management
- Tracking, reporting, and revoking privileges
- Data Loss Prevention
- Archiving
- Full Office client



ATP

Microsoft 365 Enterprise E3

Proactive Attack Prevention

- Host intrusion prevention capabilities
- Device Guard: Preventing malicious code from running
- Credentials Guard
- DirectAccess
- Windows Information Protection
- BranchCache
- Microsoft Desktop Optimization Pack



Pricing based on US CSP pricing. Please customize according to licensing program and geography

ADD-ON	SUITE
--------	-------

EMS E3 = AADP-P1 + AIP-P1 + Microsoft Intune
M365 E3 = EMS E3 + O365 E3 + Win E3

Next steps

SYNNEX has everything you need to help protect customers

Want to take a deep dive into security? SYNNEX has all the resources, trainings, and programs you need to build an effective, profitable security practice.

[Modern Workplace Solutions with SYNNEX](#)

Learn how to help your customers build a secure, productive workplace with top-tier security and productivity tools in Microsoft 365.

[Microsoft 365 + SYNNEX Security Resource Hub](#)

Ready to start putting your security practice together? Get everything you need to find new leads and close more deals.

[On-Demand Webinar: SMB Security and Compliance with Microsoft 365 Business](#)

Watch our on-demand webinar, where SYNNEX experts show you how to create new revenue streams and grow your business with Microsoft security and compliance tools.

[Capture the Cloud Partner Program](#)

In this SYNNEX-exclusive program, we'll help you deepen your understanding of Microsoft cloud services, boost your cloud practice, and set you up to succeed in a changing market.

[Microsoft Security Learning Path](#)

Gain a stronger understanding of Microsoft 365 and learn how it helps businesses efficiently manage security, whether it's in the cloud, on-premises, or across a hybrid environment.

Microsoft: the **security and compliance** vendor SMB customers need

While a customer's complete security environment may include a mix of solutions from different vendors, you can feel confident with Microsoft at the heart of your offering. We're on your side, with:

- Solutions built secure from the bottom up
- Over **3,500** people dedicated to security—more than most governments, let alone companies
- Internal spending of **~\$1B/year** on security
- Applied intelligence based on trillions of signals across all Microsoft services

And of course:

Microsoft 365—an integrated, end-to-end security and compliance solution





Let's start boosting your business

To begin selling security and compliance solutions with SYNEX, connect with our team at MSFTCSP@SYNEX.COM.

SYNEX brings the most relevant technology solutions to the IT and consumer electronics market to help our partners sustainably grow their businesses. We distribute over 30,000 technology products from more than 300 of the world's leading and emerging manufacturers, and provide complete solutions to more than 20,000 resellers and retail customers. We also provide a wide range of financial options to ensure that our partners always have the means to close deals.

