



SMALL AND MID-SIZED BUSINESS

Security and Compliance Partner Opportunity Playbook



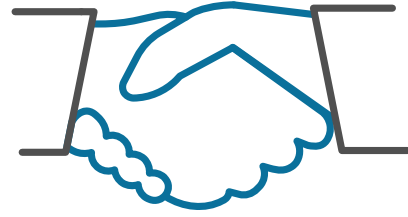
TABLE OF CONTENTS

- Opportunity and introduction to SYNEX3
- Customer insights5
- Security as a Service10
 - Secure the front door13
 - Secure content19
 - Secure devices23
 - Great employee experiences29
- Microsoft 36531
- Next steps36



Business and technology are changing faster than ever, each evolving rapidly to keep pace with the other. But with every new solution comes new security and compliance challenges, which can leave companies vulnerable—specifically small businesses that may lack resources to protect themselves. In fact, *Small Business Trends* estimates that 43 percent of cyberattacks target small businesses, disrupting productivity and costing millions in lost revenue.

Because of the critical impact cyberattacks can have, both small and mid-sized businesses (SMBs) often require more tailored security coverage than companies with large IT staffs. SMBs today work hard to get out in front of cyberthreats. They prioritize investments in not just the right security features, but also the right partnerships. That means your customers will look to you to provide a smart, robust security foundation, without costly infrastructure investments.



You don't have to go at it alone. With SYNnex and Microsoft 365, you're covered. Microsoft 365 unites the top-tier productivity tools of Office 365 with advanced security and device management capabilities to help keep data safe. SYNnex delivers solution experts and an ecosystem of vendors that enable you to provide customers with modern, cloud-based compliance and device management features, as well as data protection tools previously available only to larger organizations.

Between Microsoft 365 and always-on SYNnex support, **you'll be well-positioned to help your customers protect themselves from threats, identify potential breaches, secure devices, and guard information—all while adding to your monthly recurring revenue.** Customers will depend on your guidance to keep their data safe and ensure their practices are compliant and secure. Are you ready for the challenge? This playbook will show you how to bring more value to your customers as you build your business with Microsoft 365 and SYNnex.



Cyberthreats in 3 key zones

EMAIL

Within 4 minutes

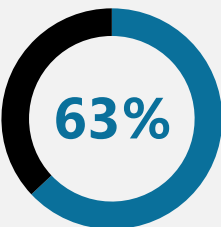


It takes
286 days
to detect intrusion

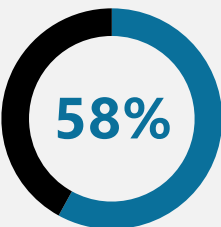
And another
80 days
to contain damage

BRIEF:
It takes hackers 4 minutes to get into networks through email attacks and 286 days for detection, followed by an additional 80 days for damage control.

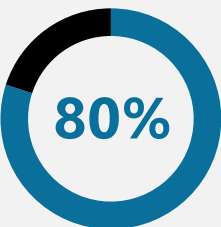
USER



Weak, default, or stolen passwords



Accidentally share sensitive information



Non-approved SaaS usage: Shadow IT

90%
Data leakage caused by user mistakes

DEVICE



53 seconds

A laptop is stolen nearly every minute

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 guesstimate)



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,¹ Forrester reported that SMBs are becoming more active in both new technology adoption and acceleration of their refresh cycles. 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. IDC² forecasts worldwide IT spending by SMBs will approach **\$568 billion in 2017** in a new update of the *Worldwide Semiannual Small and Medium Business Spending Guide*.

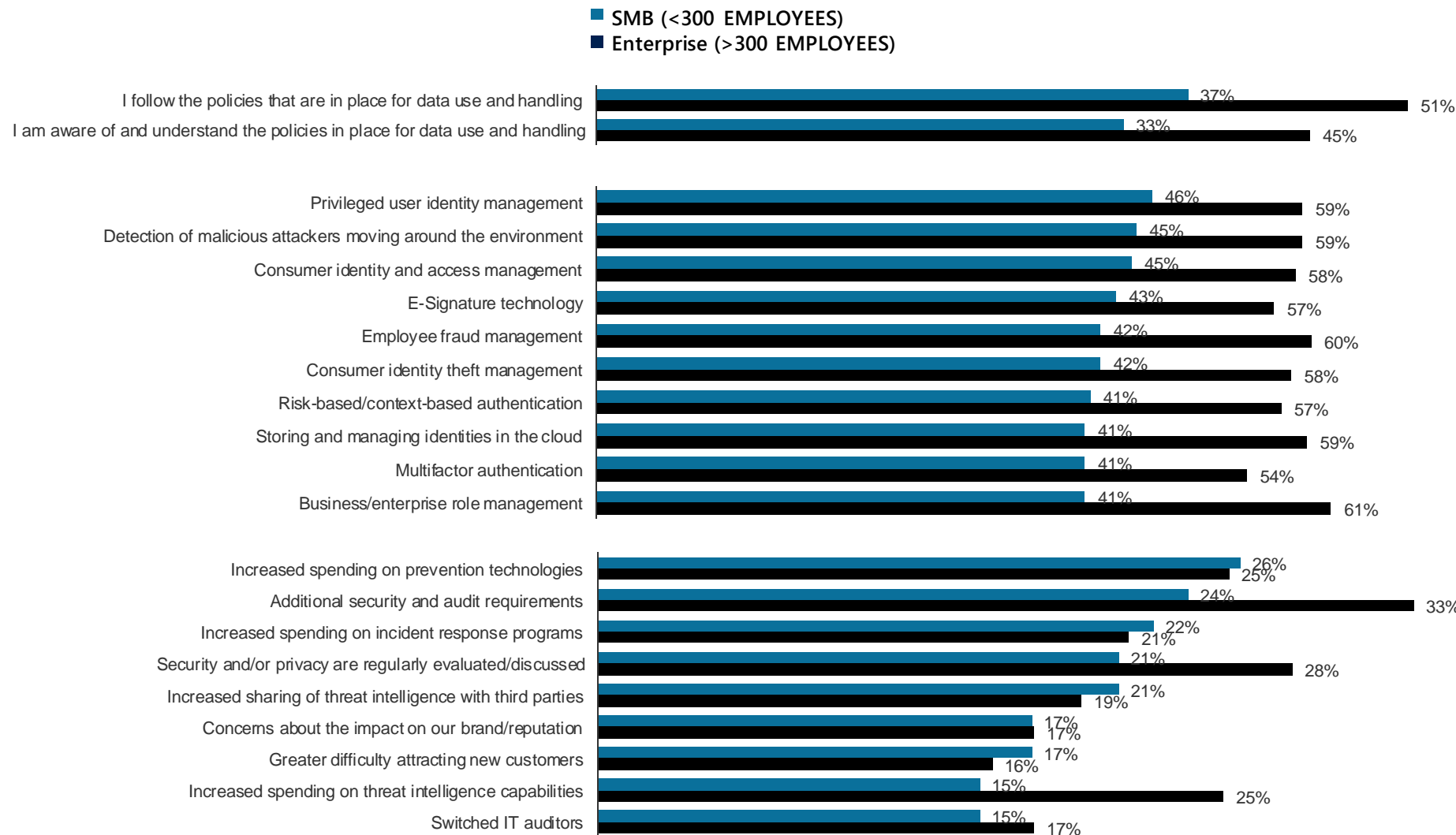
The report makes the case that while SMBs, especially smaller ones, have immediate tactical needs to sharpen performance, they are also looking to coordinate resources in a meaningful way. For many, this will be an important step forward in their digital transformation.

The increase is projected to grow by more than \$100 billion to **exceed \$676 billion in 2021**.

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

²IDC, Worldwide Semiannual Small and Medium Business Spending Guide, July 2017

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?)

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

²Base: 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

³Base: 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**

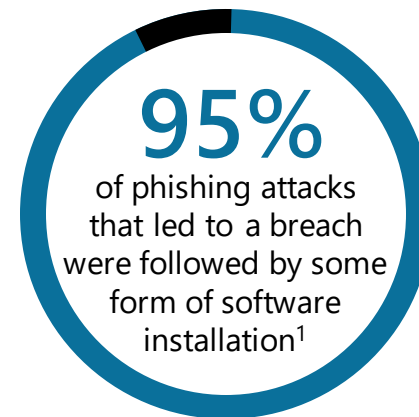
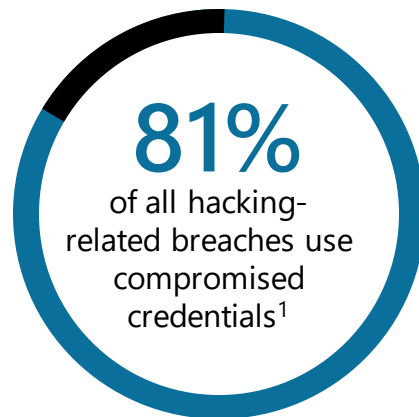
Secure the front door



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?

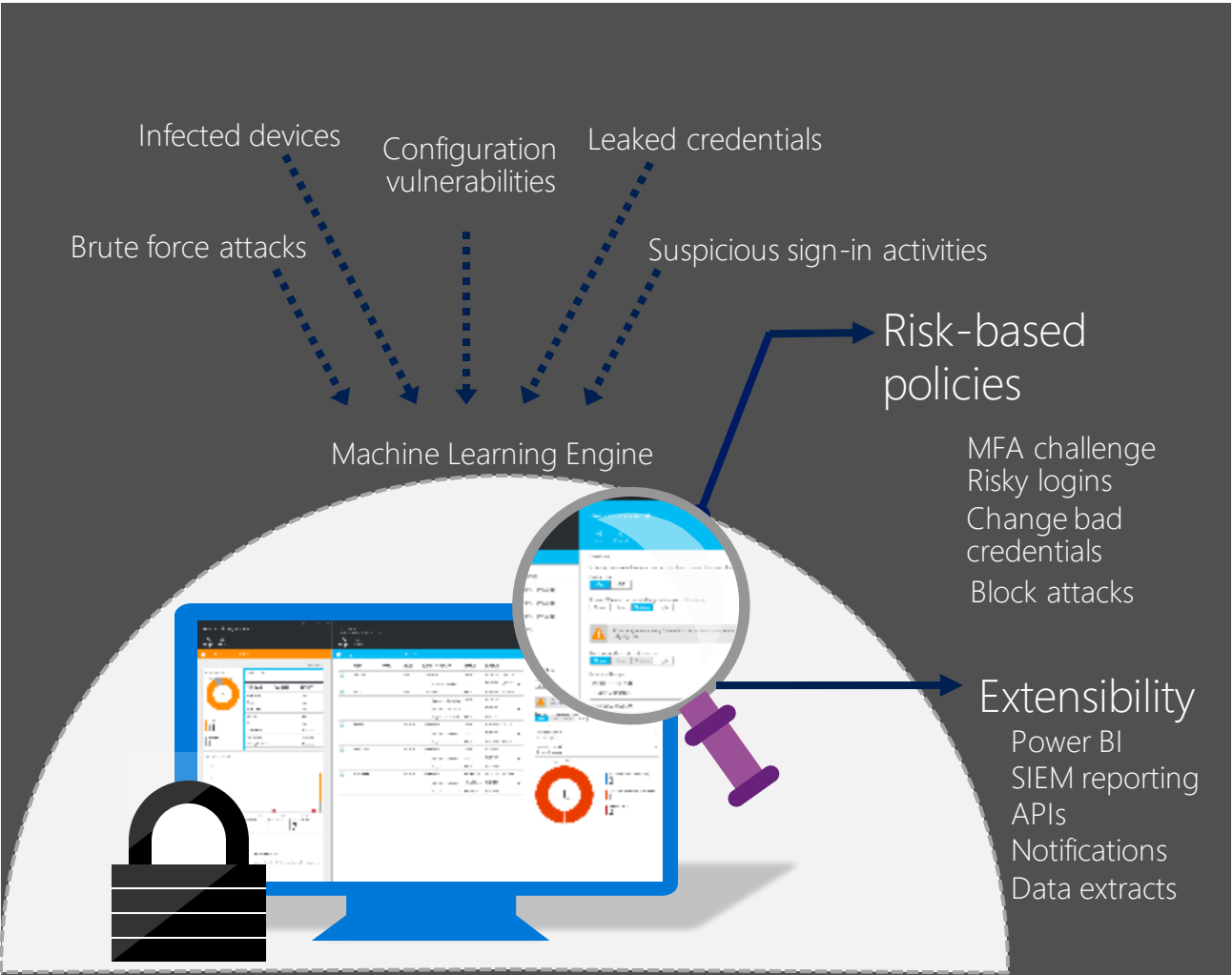


¹ Verizon 2017 Data Breach Investigations Report (ref. P11 of Security Playbook)

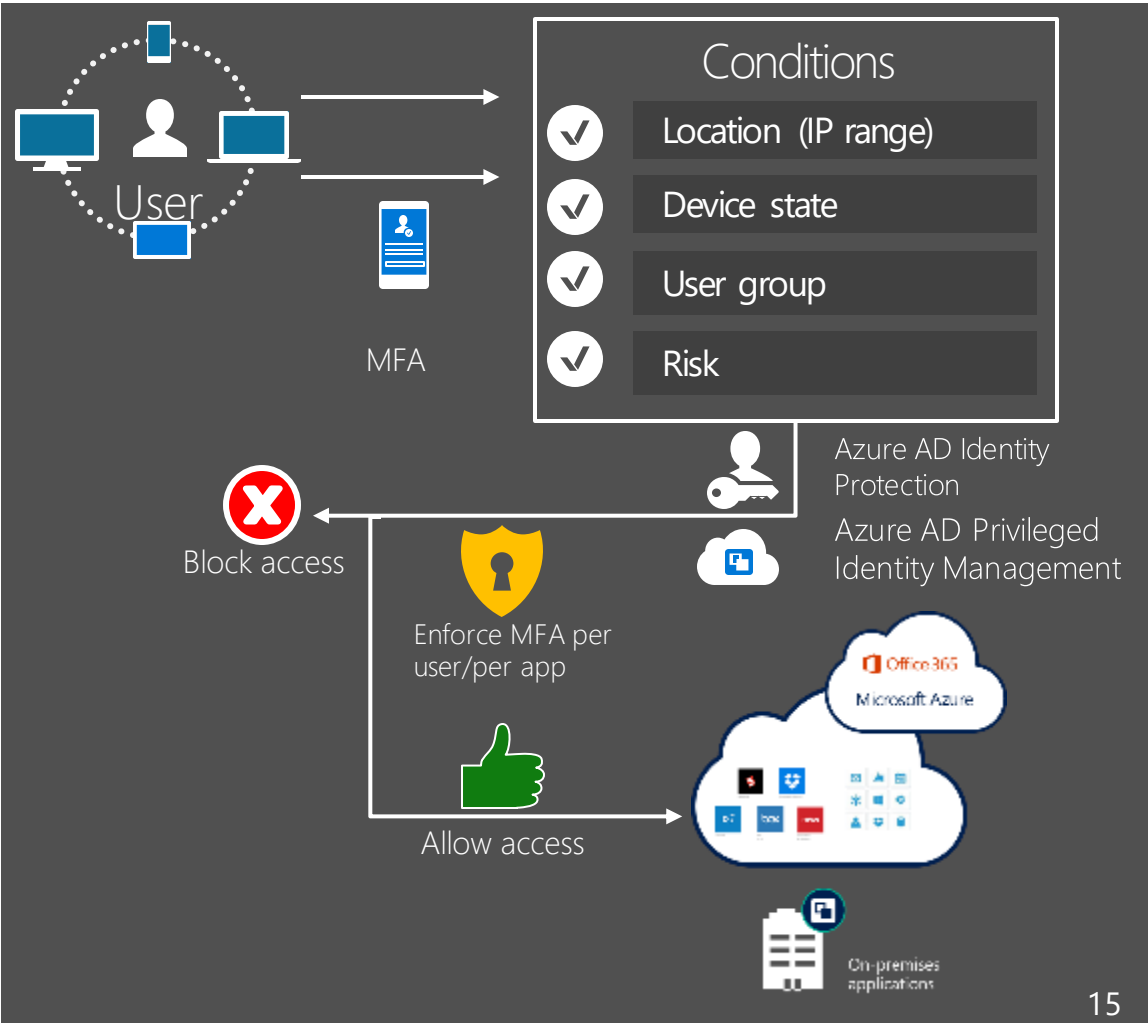
² Security Week Survey (ref. P35 of Security Playbook)

Secure the front door: Real-time risk assessment

Machine learning and risk profiling



Open the front door based on risk

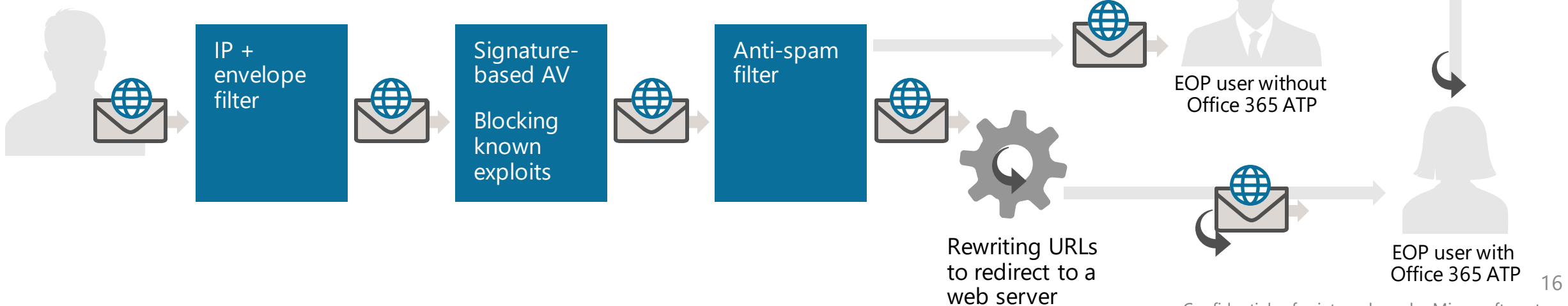


Safe Links

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

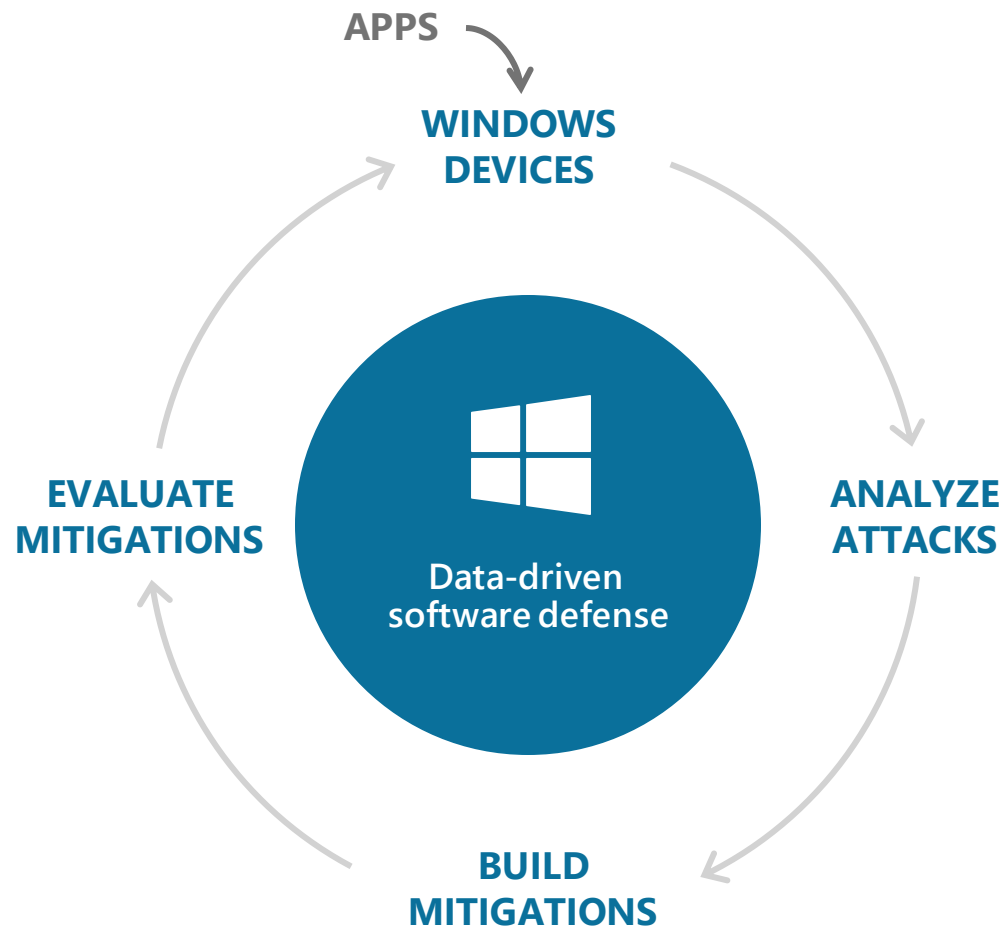
Provides **visibility** into compromised users for administrators.

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**

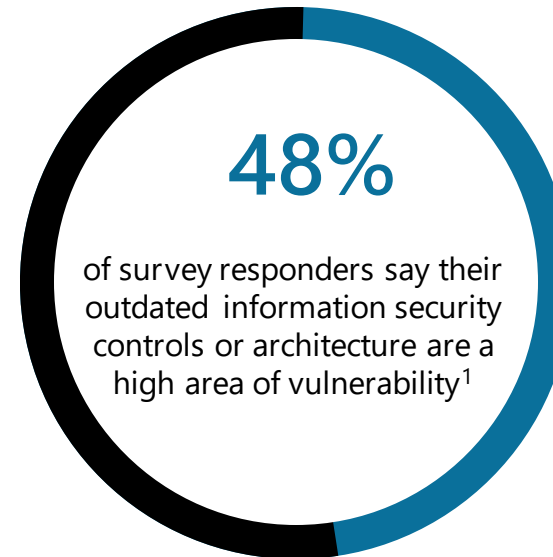
Secure content



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:

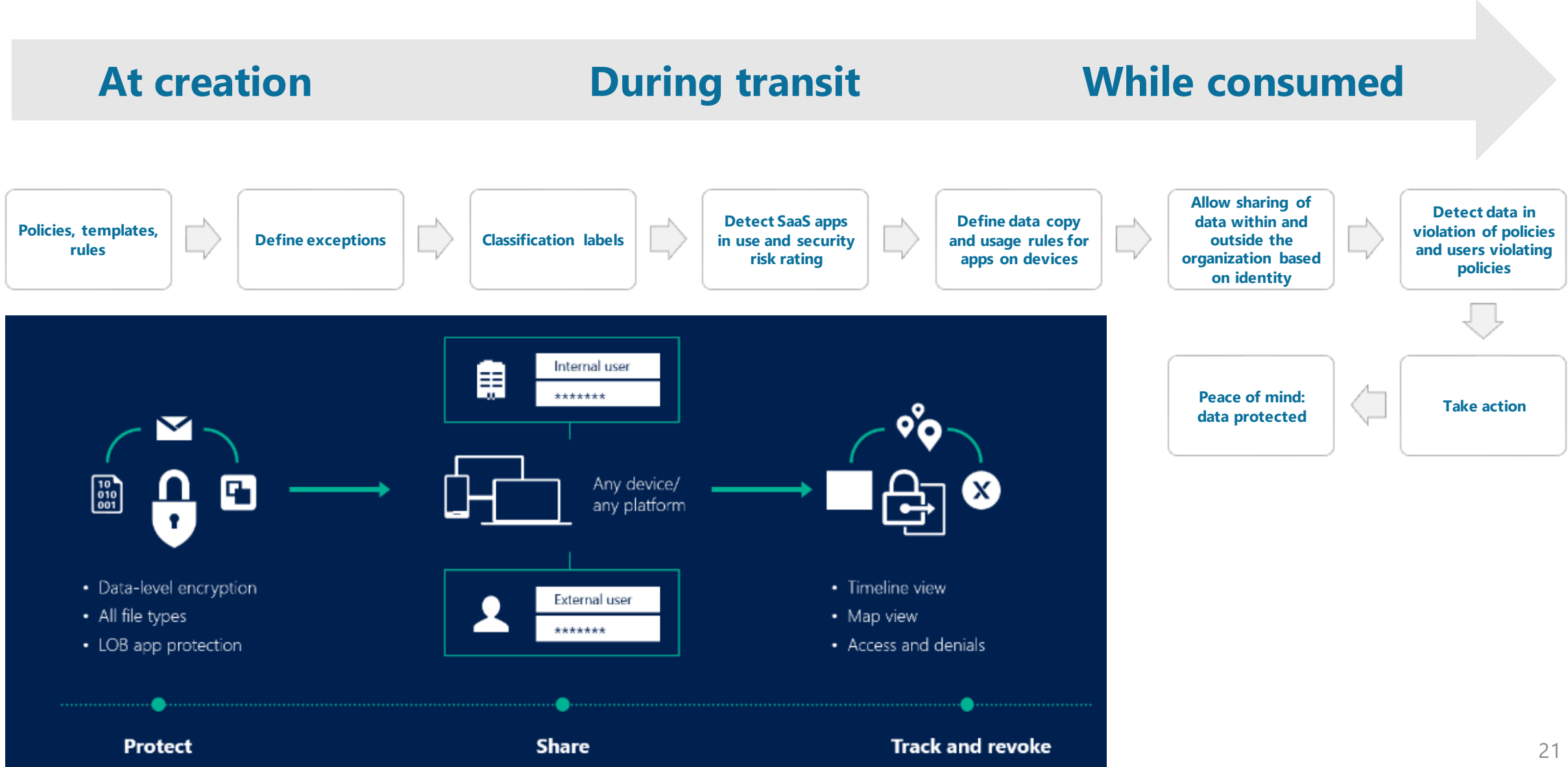
- Is their data secured regardless of where it's stored or shared?
- Does a data compliance policy control access to sensitive information?
- Can users meet all compliance obligations without interrupting their workflow?
- Do they have the ability to classify and encrypt sensitive data?



¹ 2016 EY Global Information Security Survey <http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016>

² 2016 Ponemon Institute Cost of a Data Breach Study <https://securityintelligence.com/media/2016-cost-data-breach-study>

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

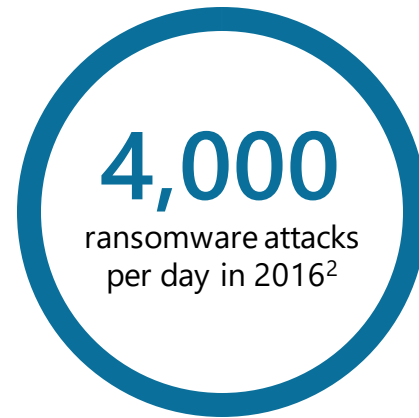
Secure devices



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?



¹ <https://www.vircom.com/blog/the-10-craziest-cybersecurity-statistics-of-2016>
³ <https://phishme.com/2016-enterprise-phishing-susceptibility-report>

² <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>
⁴ <http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-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

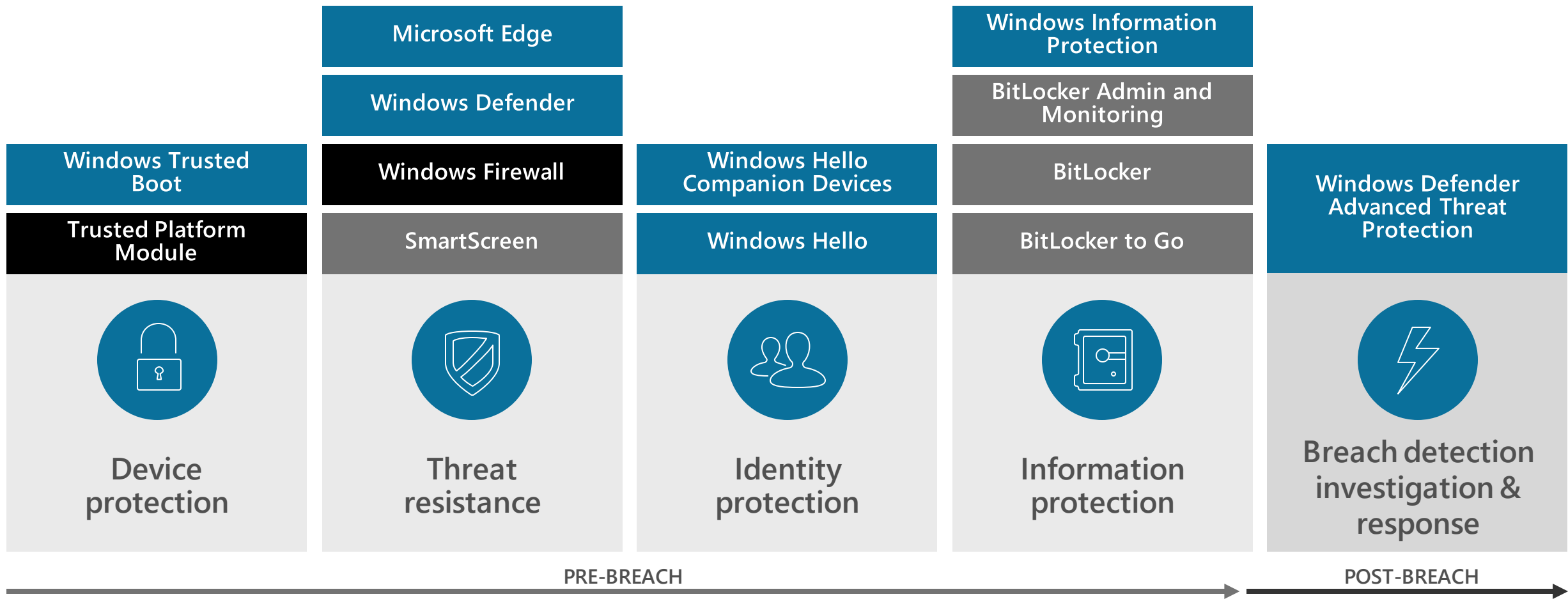
- Office mobile apps

Manage apps and experience

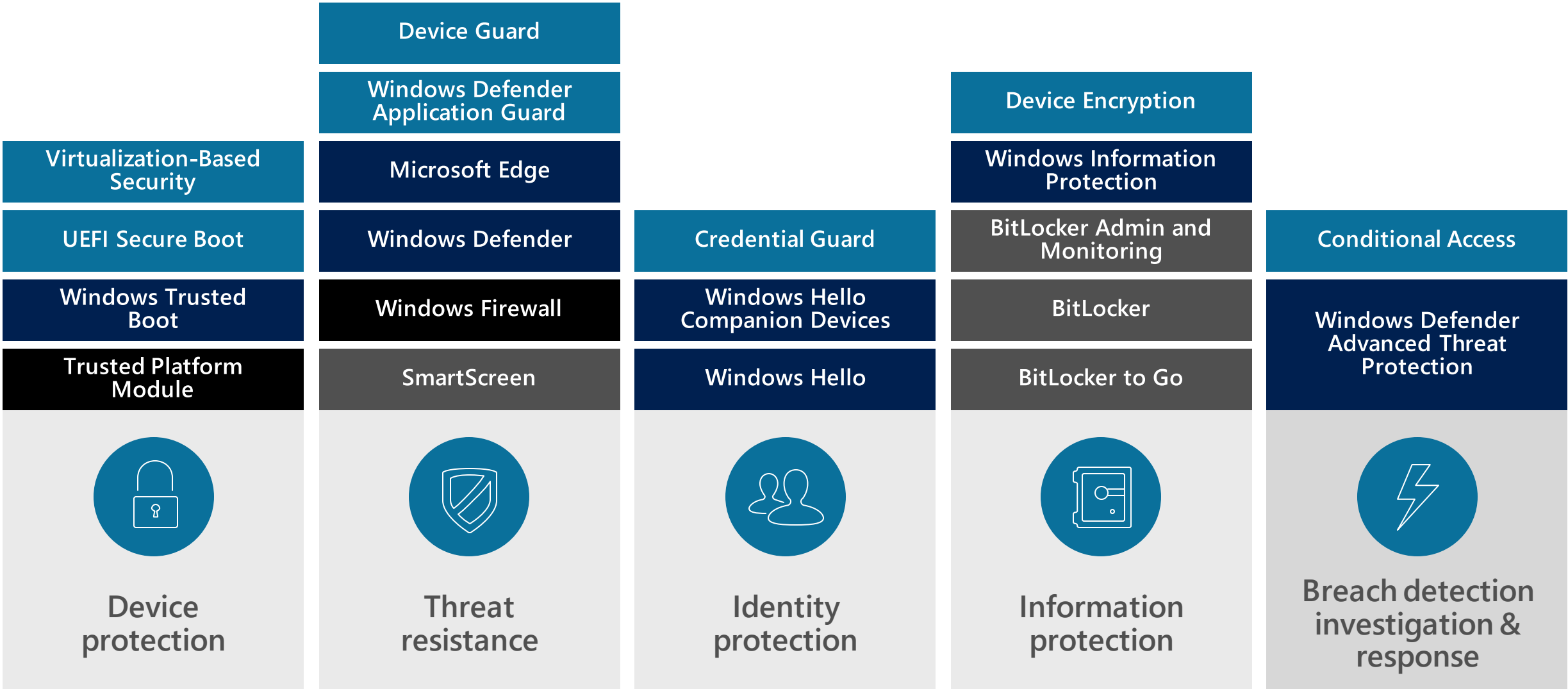


- Define app-work data relationships
- Maintain visibility and control without intrusion

Windows 10 security on Windows 7 hardware



Windows 10 security on Windows 10 hardware



PRE-BREACH

POST-BREACH

Secure devices



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



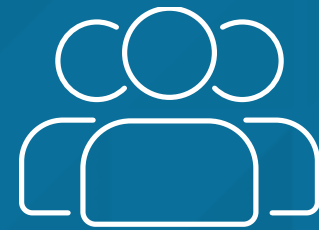
Azure Active Directory Premium – Manage and control access to resources

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

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.

