Microsoft

Microsoft 365 SMB

Security, Deployment & Collaboration

February 27, 2020

SMB Security Overview

John Petersen
Microsoft Design Sales Engineer
johnpe@synnex.com
March 2020

Small businesses are most vulnerable and need help

58%

of breaches took place at small businesses.[1]

$120K

$120K is the average cost of a SMB data breach.[2]

62%

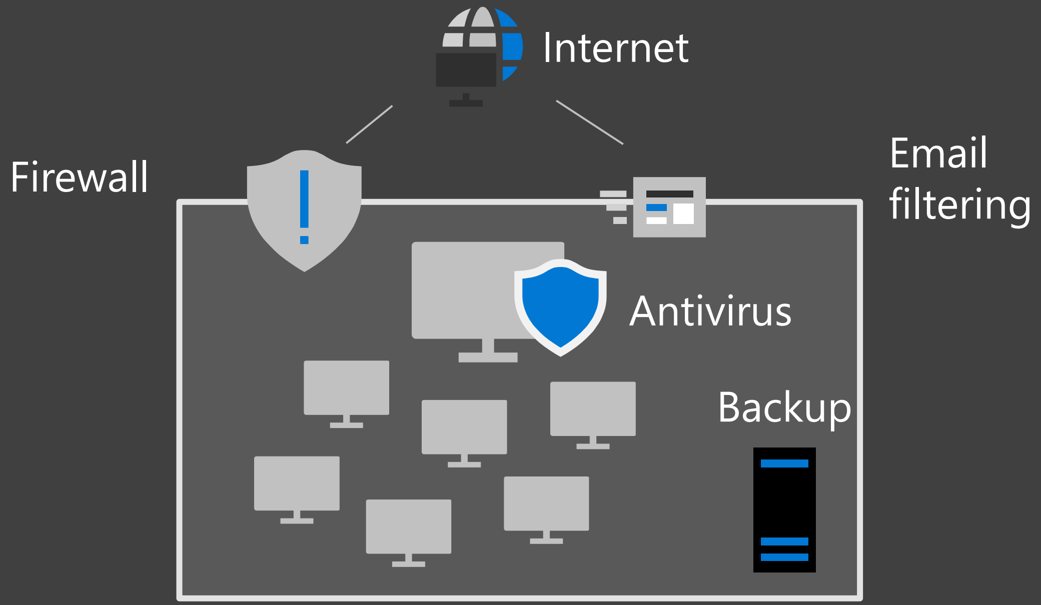
lack the skills in-house to deal with security issues.[3]

[1] Verizon 2018 Data Breach Investigations Report

[2] Kapersky Lab study, 2018

[3] Underserved and Unprepared: The State of SMB Cyber Security in 2019, Vanson Bourne for Continuum

Today's SMB IT environment is challenging

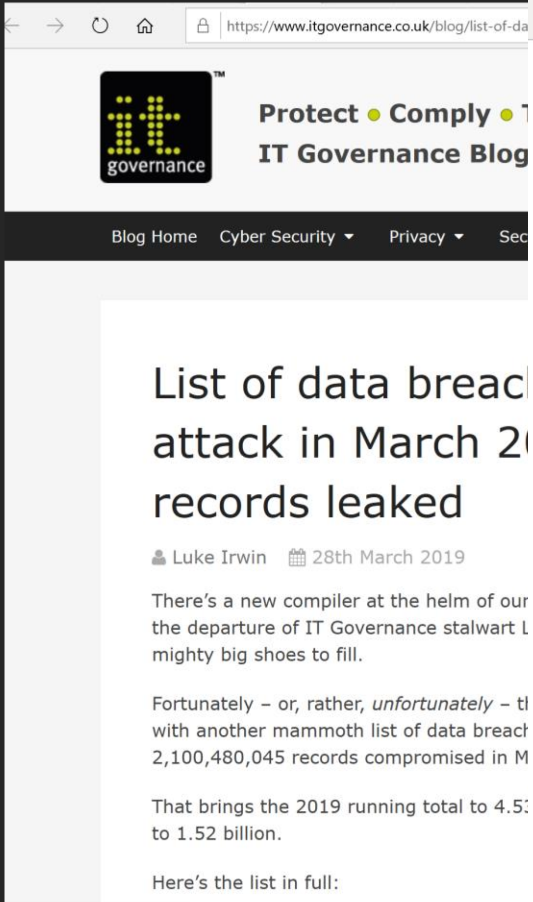


More mobile devices

Employees working from more places

Increased cyber attacks

Recent Data breach attacks


https://www.itgovernance.co.uk/blog/list-of-da

List of data breac attack in March 2(records leaked

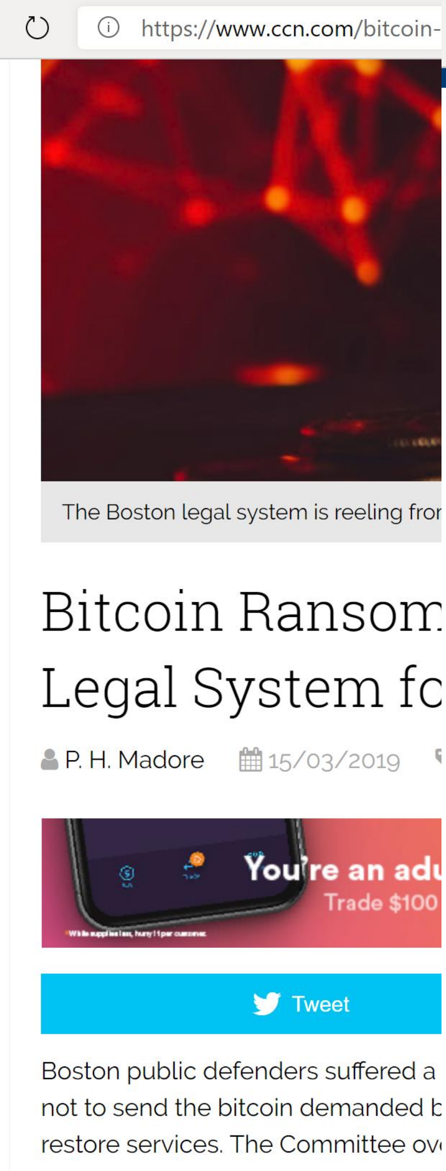
Luke Irwin 28th March 2019

There's a new compiler at the helm of our the departure of IT Governance stalwart L mighty big shoes to fill.

Fortunately – or, rather, *unfortunately* – tl with another mammoth list of data breach 2,100,480,045 records compromised in M

That brings the 2019 running total to 4.53 to 1.52 billion.

Here's the list in full:

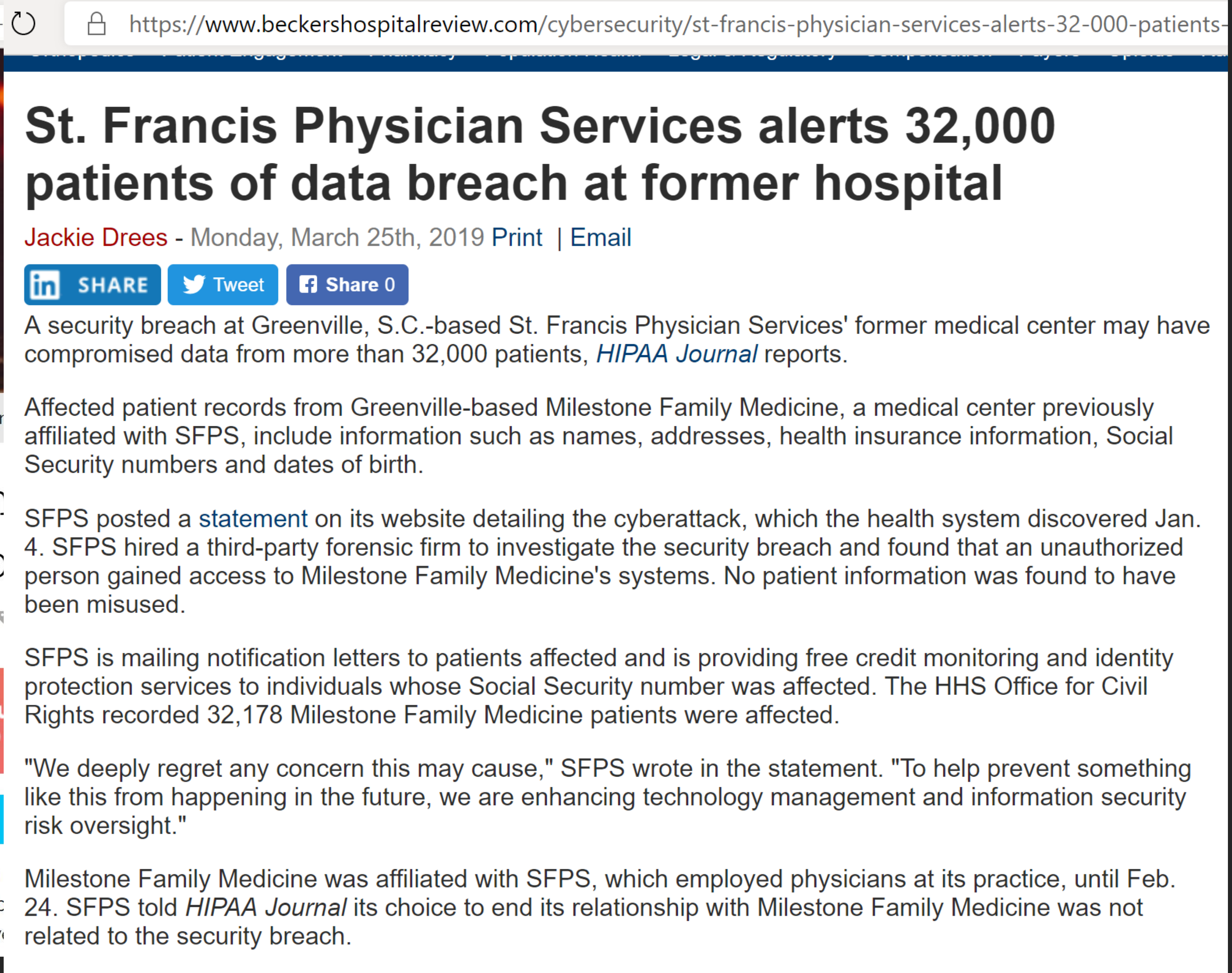

https://www.ccn.com/bitcoin-

The Boston legal system is reeling fror

Bitcoin Ransom Legal System fc

P. H. Madore 15/03/2019

Boston public defenders suffered a not to send the bitcoin demanded b restore services. The Committee ove


https://www.beckershospitalreview.com/cybersecurity/st-francis-physician-services-alerts-32-000-patients-

St. Francis Physician Services alerts 32,000 patients of data breach at former hospital

Jackie Drees - Monday, March 25th, 2019 Print | Email

A security breach at Greenville, S.C.-based St. Francis Physician Services' former medical center may have compromised data from more than 32,000 patients, *HIPAA Journal* reports.

Affected patient records from Greenville-based Milestone Family Medicine, a medical center previously affiliated with SFPS, include information such as names, addresses, health insurance information, Social Security numbers and dates of birth.

SFPS posted a statement on its website detailing the cyberattack, which the health system discovered Jan. 4. SFPS hired a third-party forensic firm to investigate the security breach and found that an unauthorized person gained access to Milestone Family Medicine's systems. No patient information was found to have been misused.

SFPS is mailing notification letters to patients affected and is providing free credit monitoring and identity protection services to individuals whose Social Security number was affected. The HHS Office for Civil Rights recorded 32,178 Milestone Family Medicine patients were affected.

"We deeply regret any concern this may cause," SFPS wrote in the statement. "To help prevent something like this from happening in the future, we are enhancing technology management and information security risk oversight."

Milestone Family Medicine was affiliated with SFPS, which employed physicians at its practice, until Feb. 24. SFPS told *HIPAA Journal* its choice to end its relationship with Milestone Family Medicine was not related to the security breach.

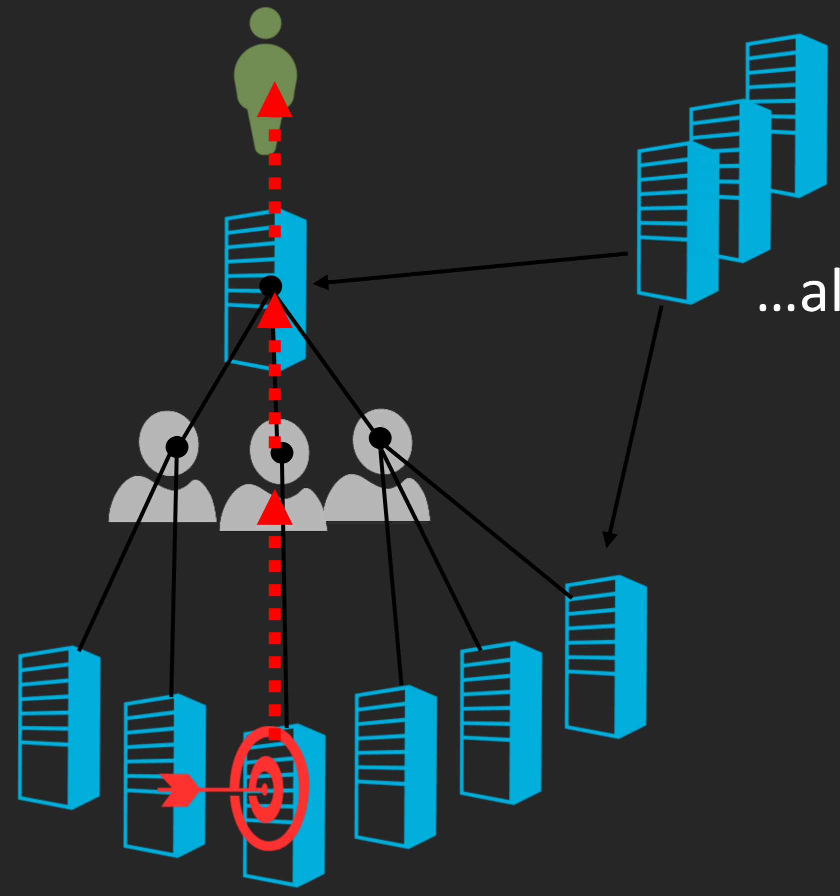
Dependency Analysis

This is an important account

…Which logs in a on a server

…Which has other admins

…Who log on to other servers



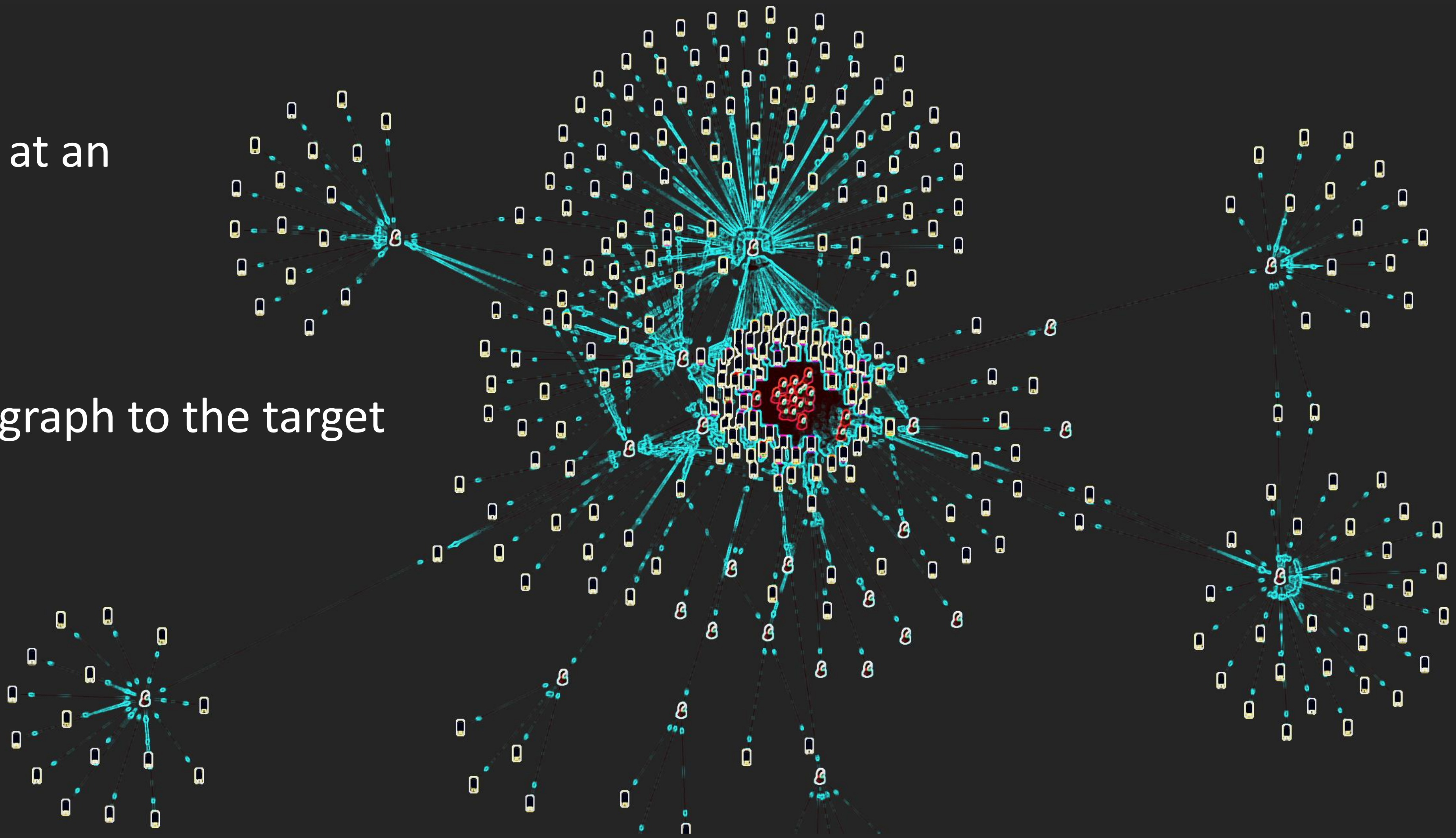
…all managed by these tools

Password	ABC123DE….
NTLM Hash	NTLM
Kerberos TGT	TGT
Management Agent	Agent

…Usually Leads to Discovery of a ^ **Big** Graph

Once adversaries get in at an edge….

…they can traverse the graph to the target



Microsoft 365 Business – our SMB security approach

Defend against cyberthreats

Office 365 Advanced Threat Protection

Microsoft Defender

+ Azure Multi Factor Authentication NEW

+ Self Service Password Writeback NEW

+

Protect business data

Office 365 Data Loss Prevention

Azure Information Protection P1

Exchange Online Archiving

+ Conditional Access NEW

+

Manage your devices

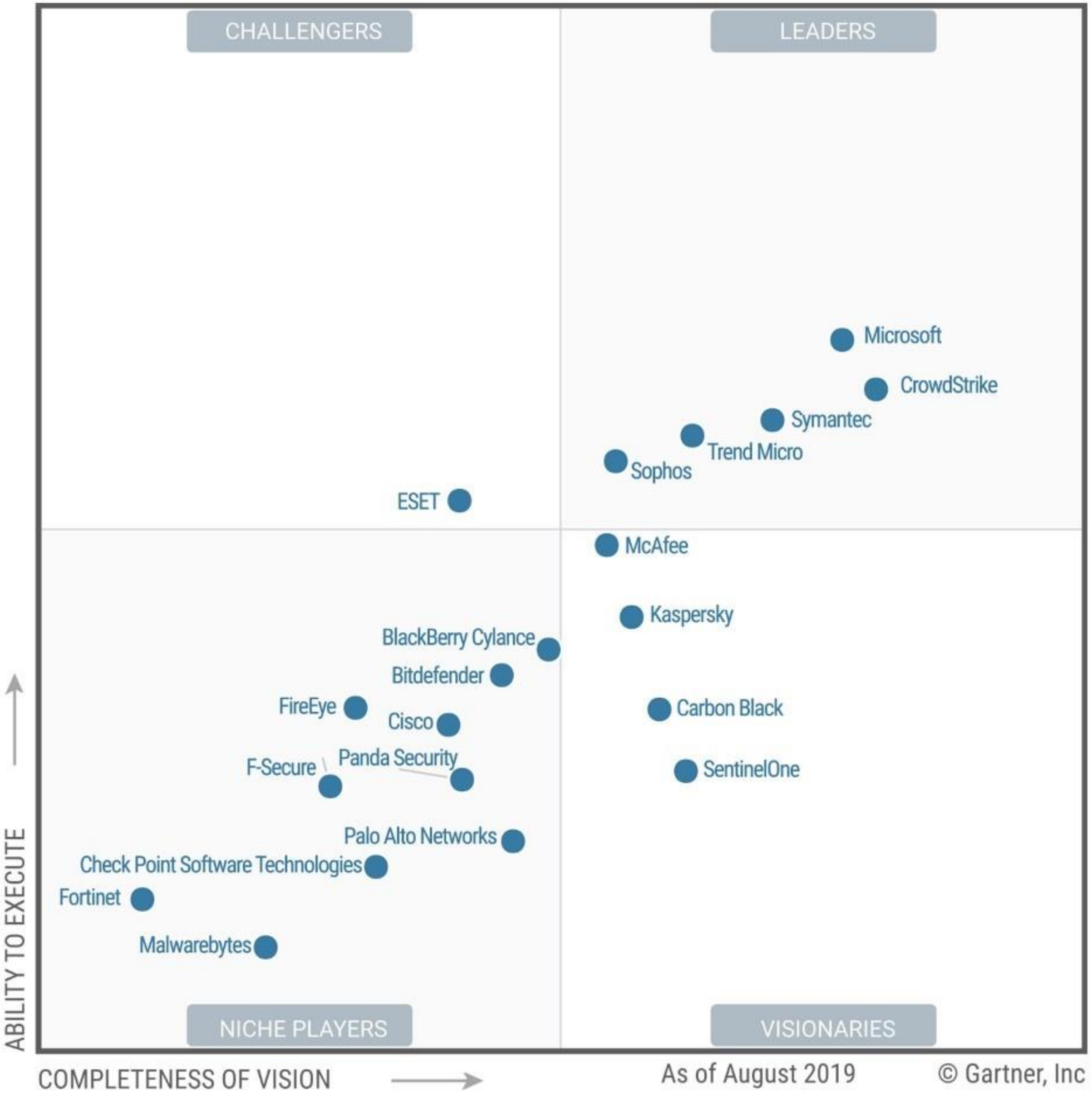
Intune

Windows Virtual Desktop

+ Office 365
Shared Computer Activation NEW

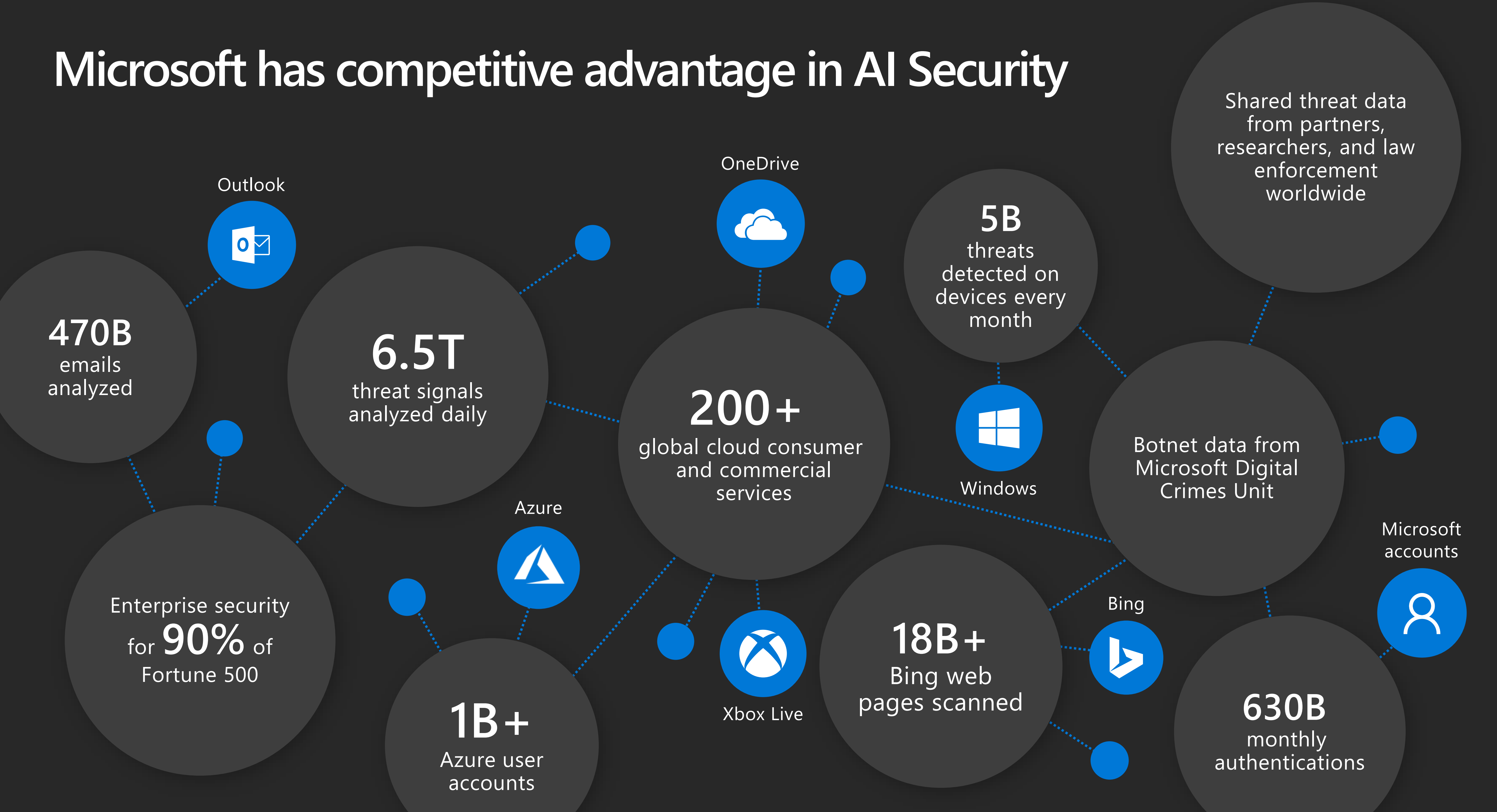
Microsoft recognized as a leading Security provider by Gartner

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (August 2019)

Microsoft has competitive advantage in AI Security



Outlook

470B emails analyzed

6.5T threat signals analyzed daily

OneDrive

200+ global cloud consumer and commercial services

5B threats detected on devices every month

Shared threat data from partners, researchers, and law enforcement worldwide

Windows

Botnet data from Microsoft Digital Crimes Unit

Microsoft accounts

Enterprise security for 90% of Fortune 500

Azure

1B+ Azure user accounts

Xbox Live

18B+ Bing web pages scanned

Bing

630B monthly authentications

Microsoft 365 Business | Simplifying SMB technology investment

Archiving	~$6.50
Device Management	~$6.50
Cloud identity management	~$3
Chat-based teamwork	$8
Email Filtering	$30
Device Anti Virus	~$12.50
Online Meetings	~$29
File Storage	~$12.50
Productivity Software	$10

3rd party solutions >$100

- Office 365 Business Premium
- Windows 10 Business
- Intune
- Office 365 Advanced Threat Protection
- Azure Information Protection P1
- Data Loss Prevention
- Exchange Online Archiving
- AAD Features

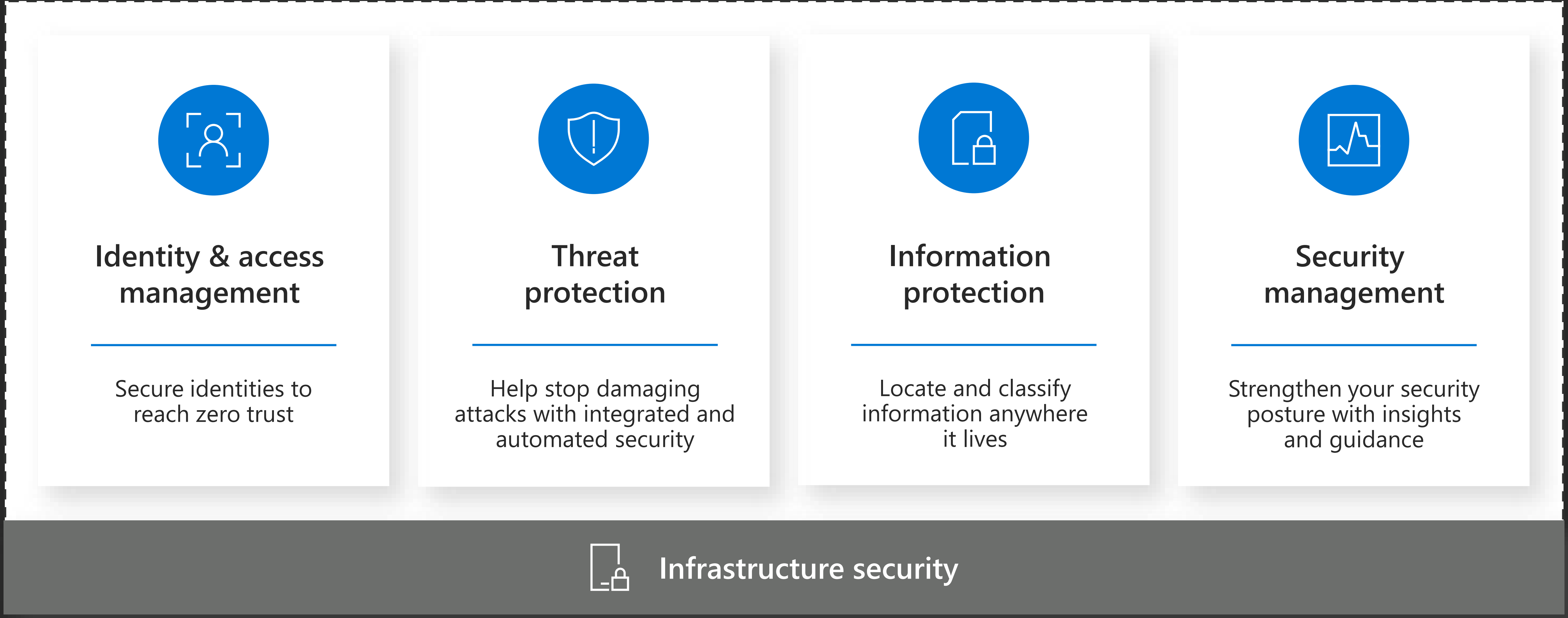
Microsoft Offerings

Microsoft 365 Business

A single, integrated solution with support for hybrid identity

$20

Enterprise-class technology



Identity & access management

Secure identities to reach zero trust

Threat protection

Help stop damaging attacks with integrated and automated security

Information protection

Locate and classify information anywhere it lives

Security management

Strengthen your security posture with insights and guidance

Infrastructure security

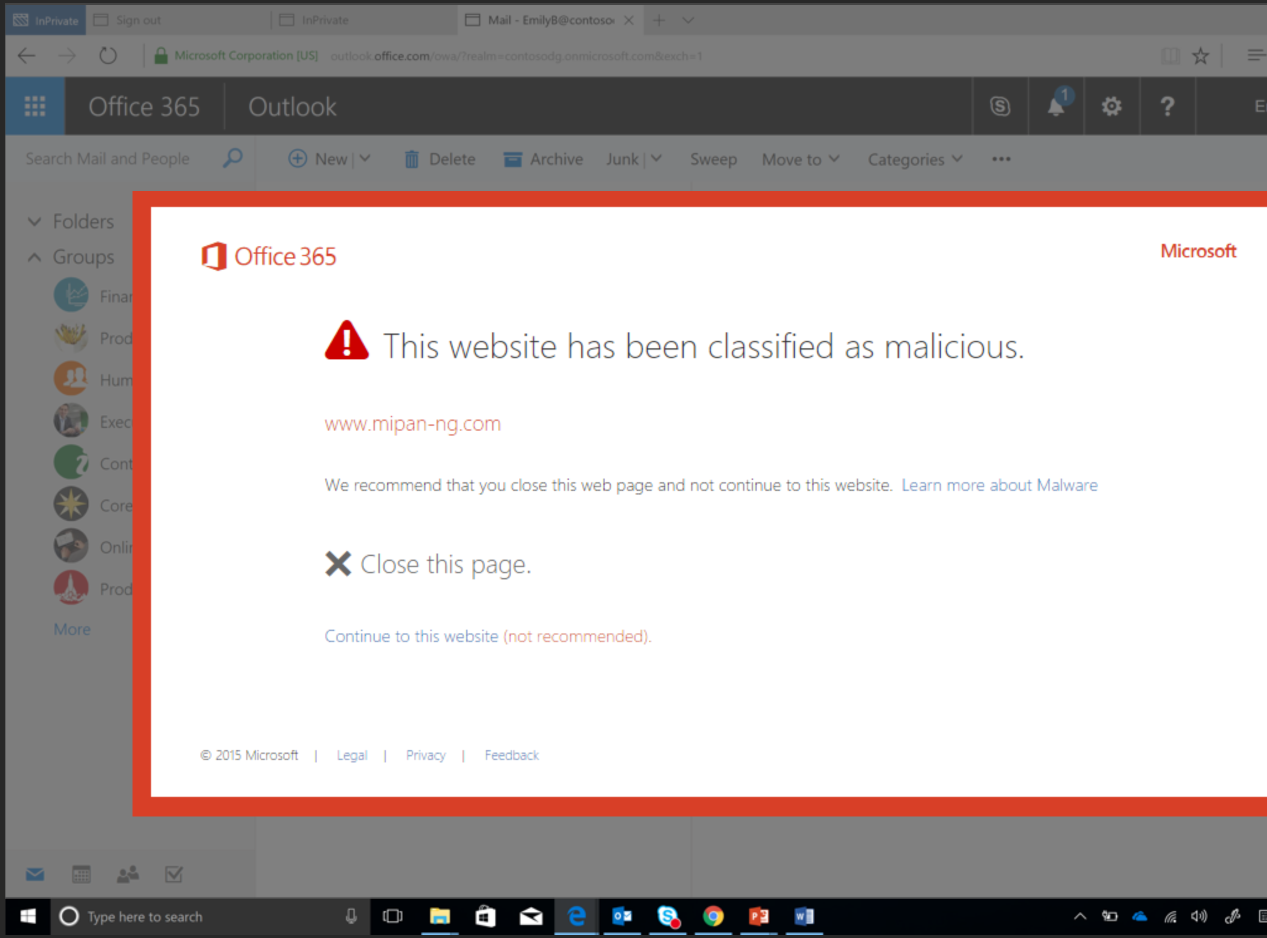
Key Feature #1: O365 Advanced Threat Protection

What is it?

Office 365 Advanced Threat Protection (ATP) helps to protect organizations from malicious attacks and malware

What you need to know

- Scanning email attachments with ATP Safe Attachments
- Scanning web addresses (URLs) in email messages and Office documents with ATP Safe Links
- Identifying and blocking malicious files in online libraries with ATP for SharePoint, OneDrive, and Microsoft Teams
- Checking email messages for unauthorized spoofing with spoof intelligence
- Detecting when someone attempts to impersonate users and an organization's custom domains with ATP anti-phishing capabilities in Office 365



Office 365

Microsoft

This website has been classified as malicious.

www.mipan-ng.com

We recommend that you close this web page and not continue to this website. Learn more about Malware

✕ Close this page.

Continue to this website (not recommended).

© 2015 Microsoft | Legal | Privacy | Feedback

Key Feature #2: Conditional Access

What is it?

Simple & powerful automated access control based on conditions such as:

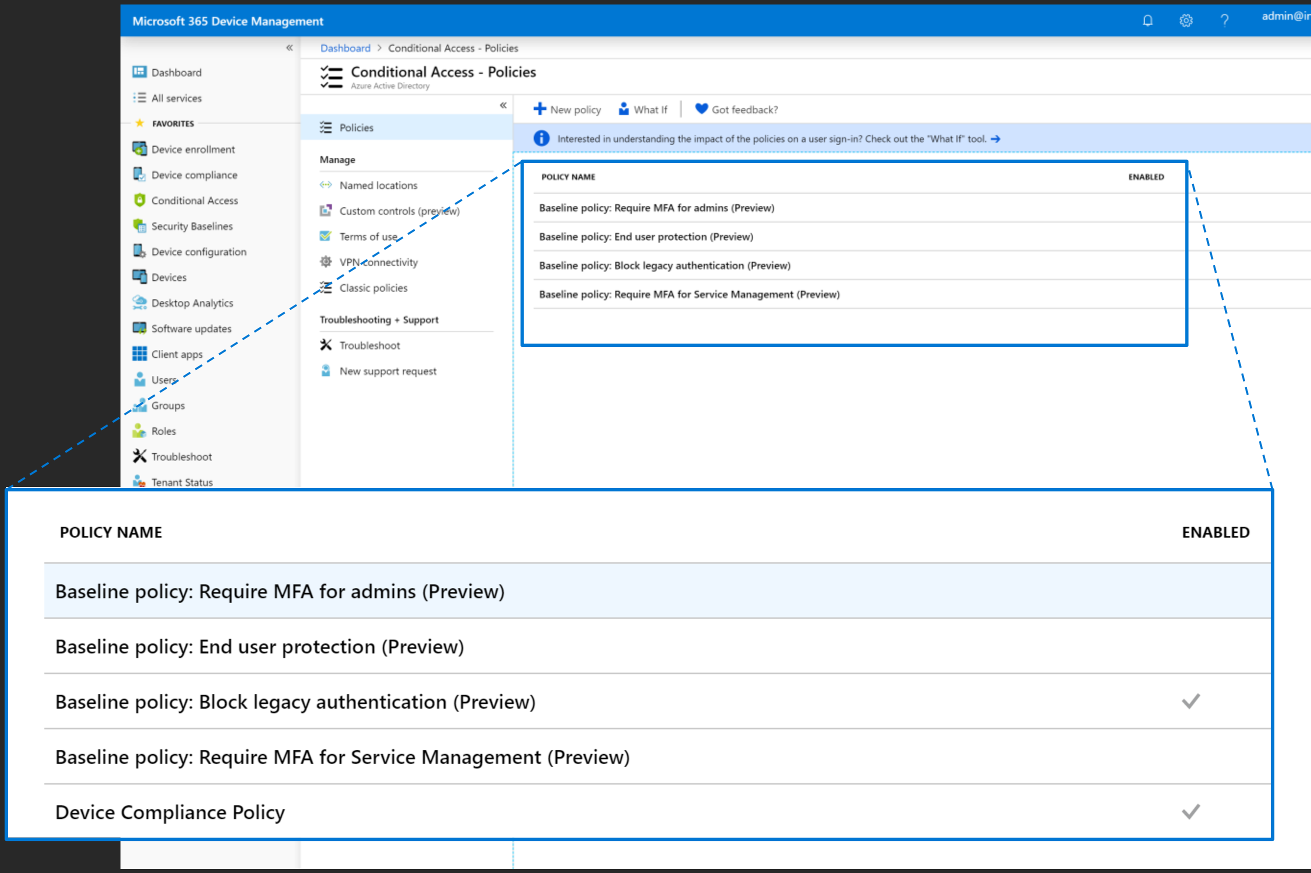
- Device Compliance
- Trusted Locations

What you need to know

Baseline policies enable strong security via simple on/off toggle: Example are:

- Require MFA For admins
- Block legacy authentication

Additional policies are fully customizable. Can be used to block unauthorized logons even when the password is stolen.



Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED
Baseline policy: Require MFA for admins (Preview)	
Baseline policy: End user protection (Preview)	
Baseline policy: Block legacy authentication (Preview)	✓
Baseline policy: Require MFA for Service Management (Preview)	
Device Compliance Policy	✓

Key Feature #3: Microsoft Intune

What is it?

Manages mobile devices and apps from the cloud

Enables device security and ensures it’s on and configured

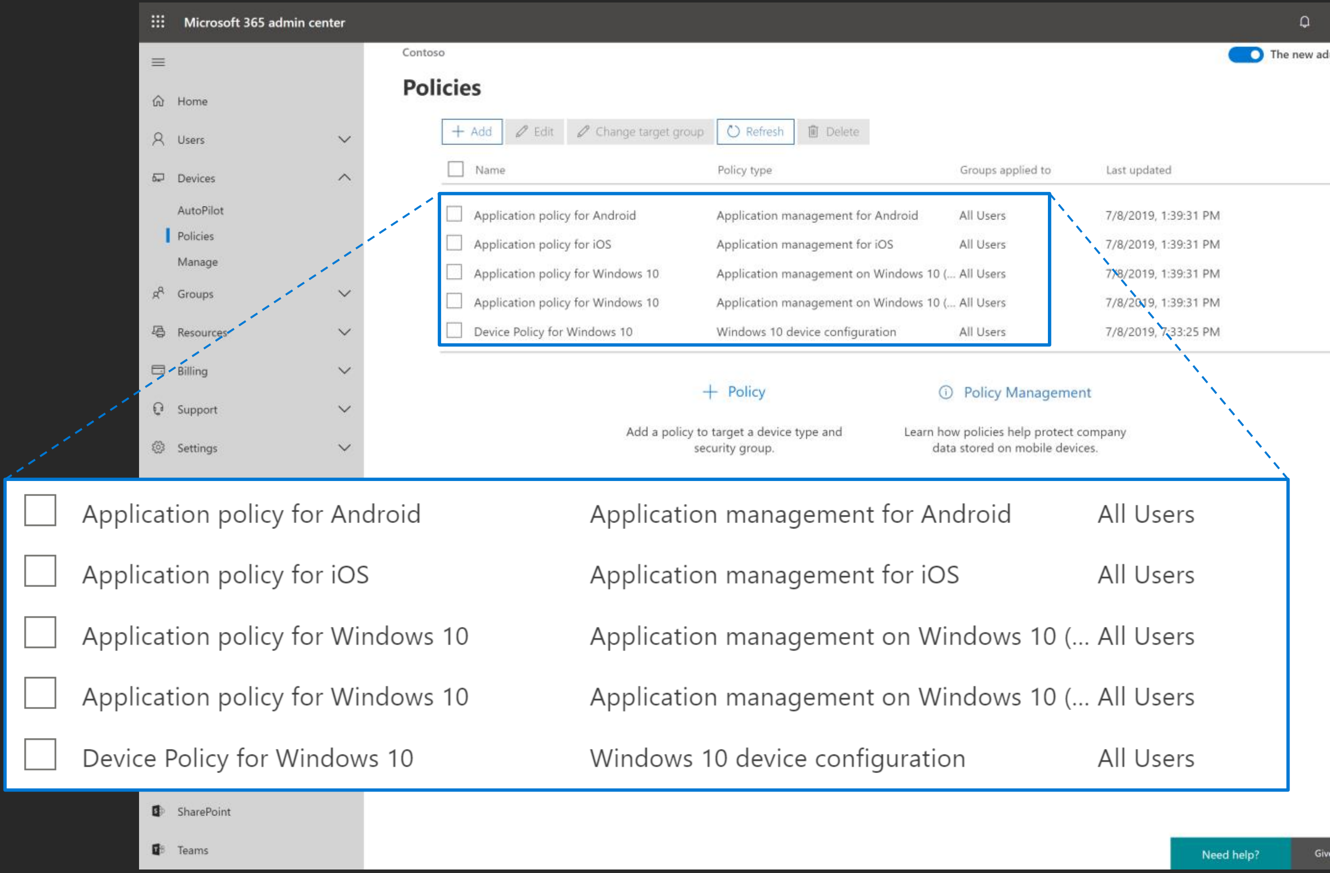
Protects company data on employee devices

What you need to know

Initial policies created by Microsoft 365 Business configuration wizard

Simple policy workflows in the generalist workspace - Microsoft Admin Center (MAC)

Advanced customization in the specialist workspace - Device Management Admin Center (DMAC)



Policies

□ Name	Policy type	Groups applied to	Last updated
□ Application policy for Android	Application management for Android	All Users	7/8/2019, 1:39:31 PM
□ Application policy for iOS	Application management for iOS	All Users	7/8/2019, 1:39:31 PM
□ Application policy for Windows 10	Application management on Windows 10 (...	All Users	7/8/2019, 1:39:31 PM
□ Application policy for Windows 10	Application management on Windows 10 (...	All Users	7/8/2019, 1:39:31 PM
□ Device Policy for Windows 10	Windows 10 device configuration	All Users	7/8/2019, 7:33:25 PM

+ Policy

Add a policy to target a device type and security group.

Policy Management

Learn how policies help protect company data stored on mobile devices.

□ Application policy for Android Application management for Android All Users
□ Application policy for iOS Application management for iOS All Users
□ Application policy for Windows 10 Application management on Windows 10 (... All Users
□ Application policy for Windows 10 Application management on Windows 10 (... All Users
□ Device Policy for Windows 10 Windows 10 device configuration All Users

Securing the devices that connect to your data

Phones Tablets Laptops Desktops

iOS and Android devices

Windows PCs

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

Phones

Tablets

Managing mobile devices – two approaches

Mobile Application Management (MAM)

Commonly used for total management of **company-owned devices**

Company manages the security of the entire device

Key capabilities

- Secure corporate data within apps
- Report app inventory & usage
- Remove corporate data

Administration

Managed via setup wizard and simplified UI

Mobile Device Management (MDM)

Commonly used for **personal devices** (Bring Your Own Device scenario)

Company manages the security of only those applications that are enrolled

Key capabilities

- Provision settings, certs, profiles
- Advanced policy controls
- Report & measure device compliance

Administration

Managed via Intune admin center

Additional steps to set up (provision certificates, etc)

https://docs.microsoft.com/en-us/intune/ios-enroll
https://docs.microsoft.com/en-us/intune/android-enroll

Require key security features on mobile devices

The problem:

Mobile devices provide productivity benefits, but they can be difficult to secure company data on.

The solution:

Easily enforce use of key security features with Intune Mobile Application Management:

- Deny access to jailbroken or rooted devices
- Prevent users from saving documents or pasting data to unsecured apps

Remove company data when employee leaves company

The problem:

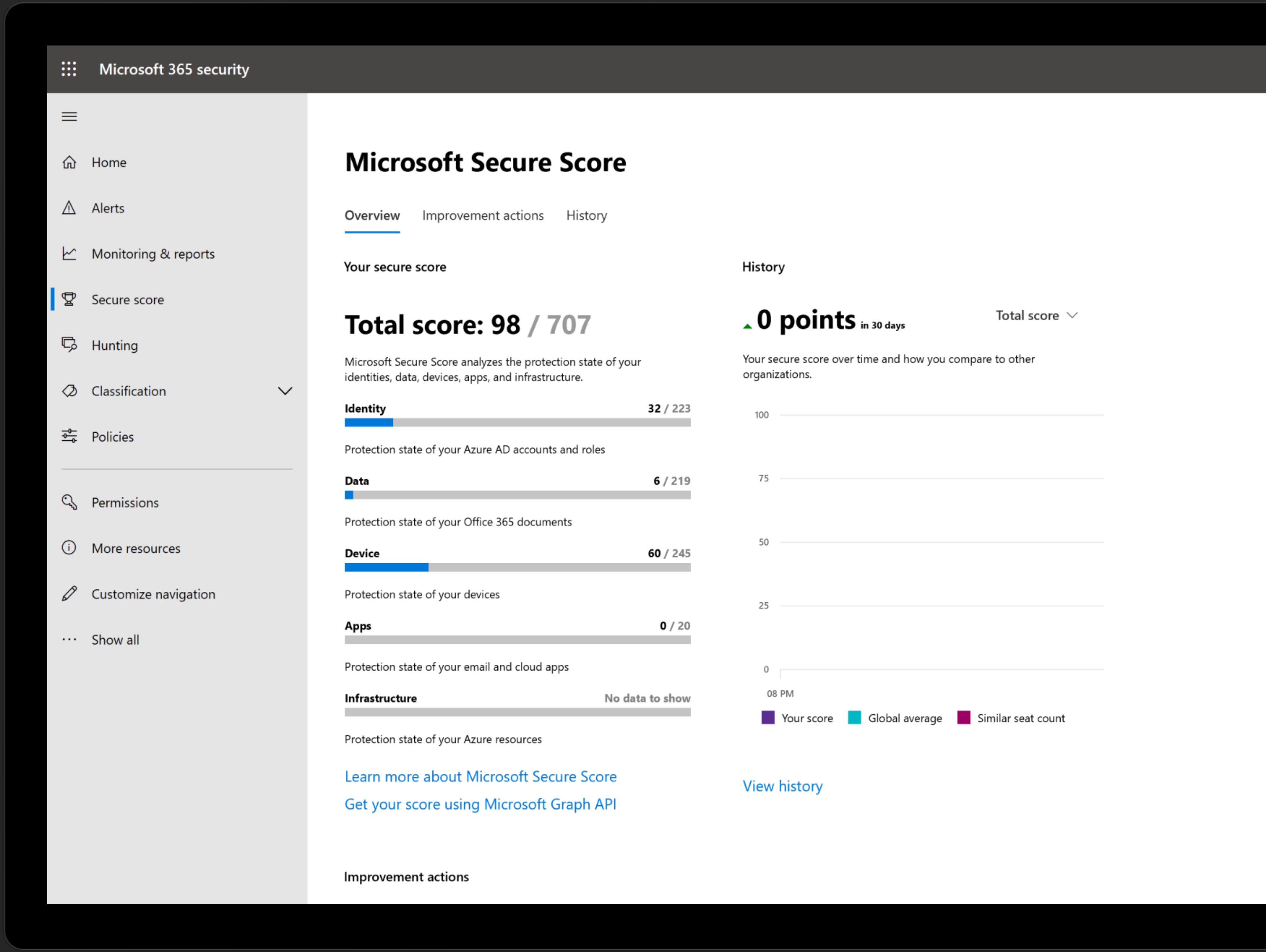
When an employee loses a device, or leaves the company, your data is still on their device.

Completely wiping the device will delete the employee's personal files such as photos and text messages

The solution:

Remotely delete company data from a device without impacting personal files personal information intact.

Secure Score



Microsoft 365 security

- Home
- Alerts
- Monitoring & reports
- Secure score
- Hunting
- Classification
- Policies
- Permissions
- More resources
- Customize navigation
- ··· Show all

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.

View history

Improvement actions

Resources

[Partner Smart Office]

[Using the Secure Score API]

[Secure Score Deep Dive]

Deployment/Autopilot

Mark Layton
Microsoft Design Sales Engineer
March 2020

What is Windows Autopilot?

A modern desktop management deployment tool for Windows 10 enabled by Intune

Key Benefits:

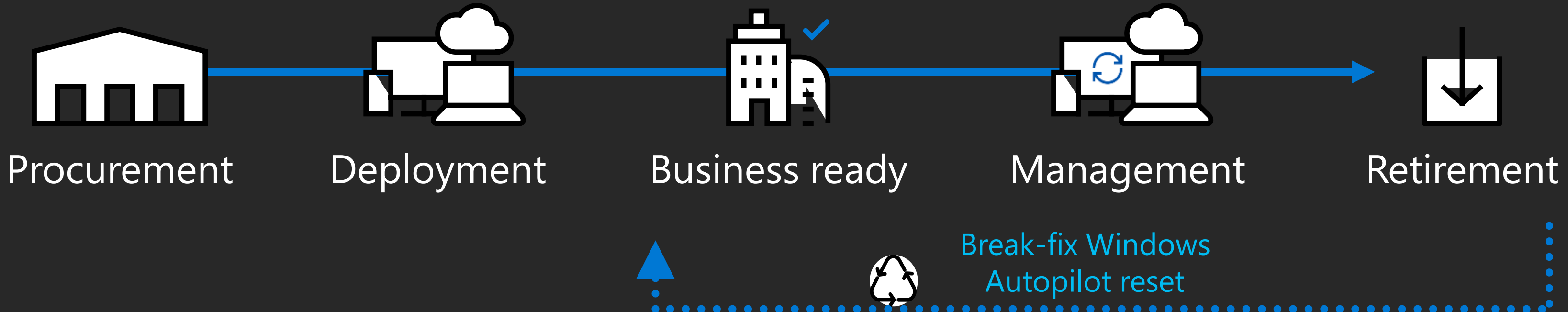
No more maintenance of images and drivers

No need for IT to touch the devices

Simple process for users and IT

Integration in the device supply chain

Reset device back to a business ready state



Windows Autopilot deployment

Cloud driven

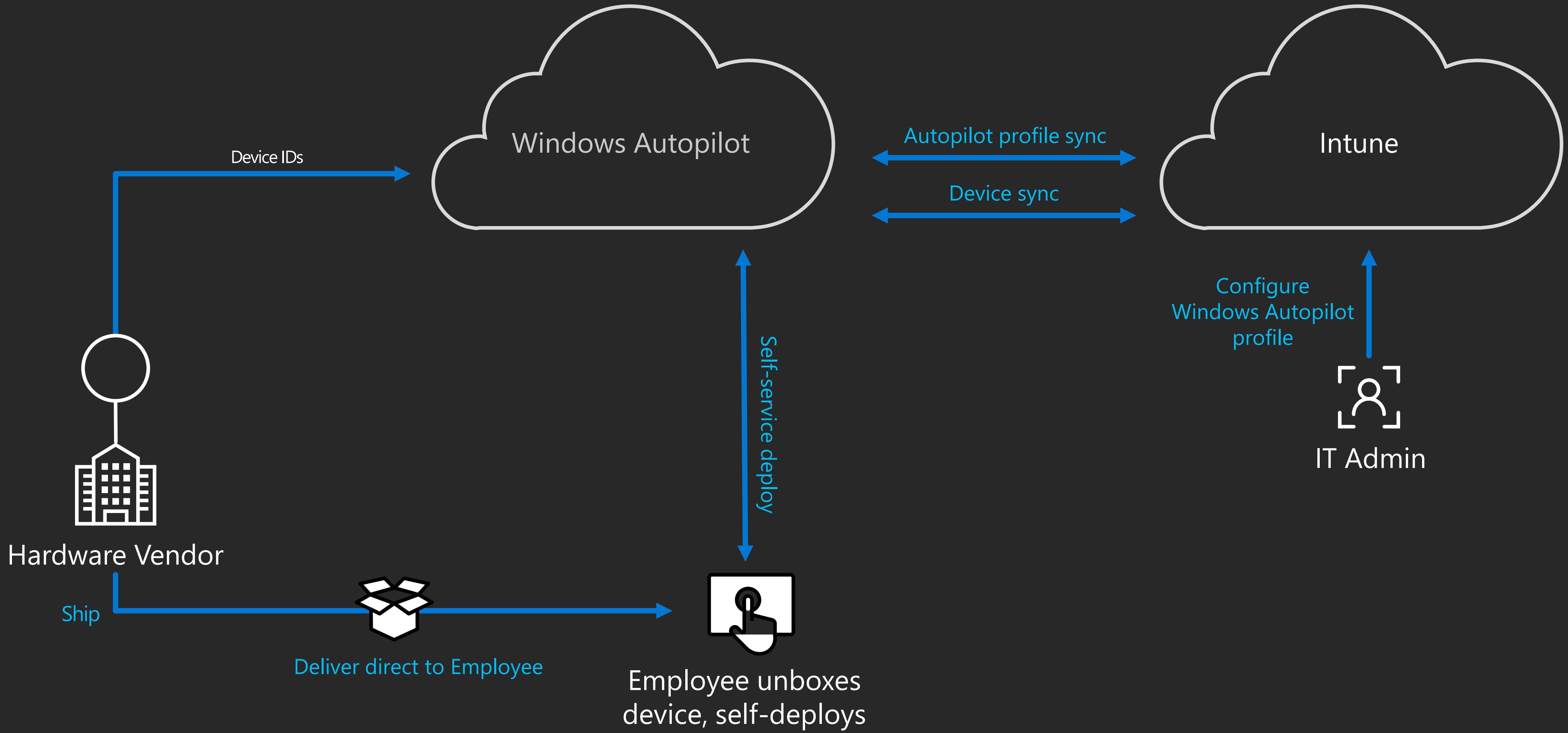
Three simple steps

Register devices

Create an Autopilot profile and assign to a group

Ship the device to the user

Windows Autopilot overview



Windows Autopilot

Intune

Device IDs

Autopilot profile sync

Device sync

Self-service deploy

Configure
Windows Autopilot
profile

IT Admin

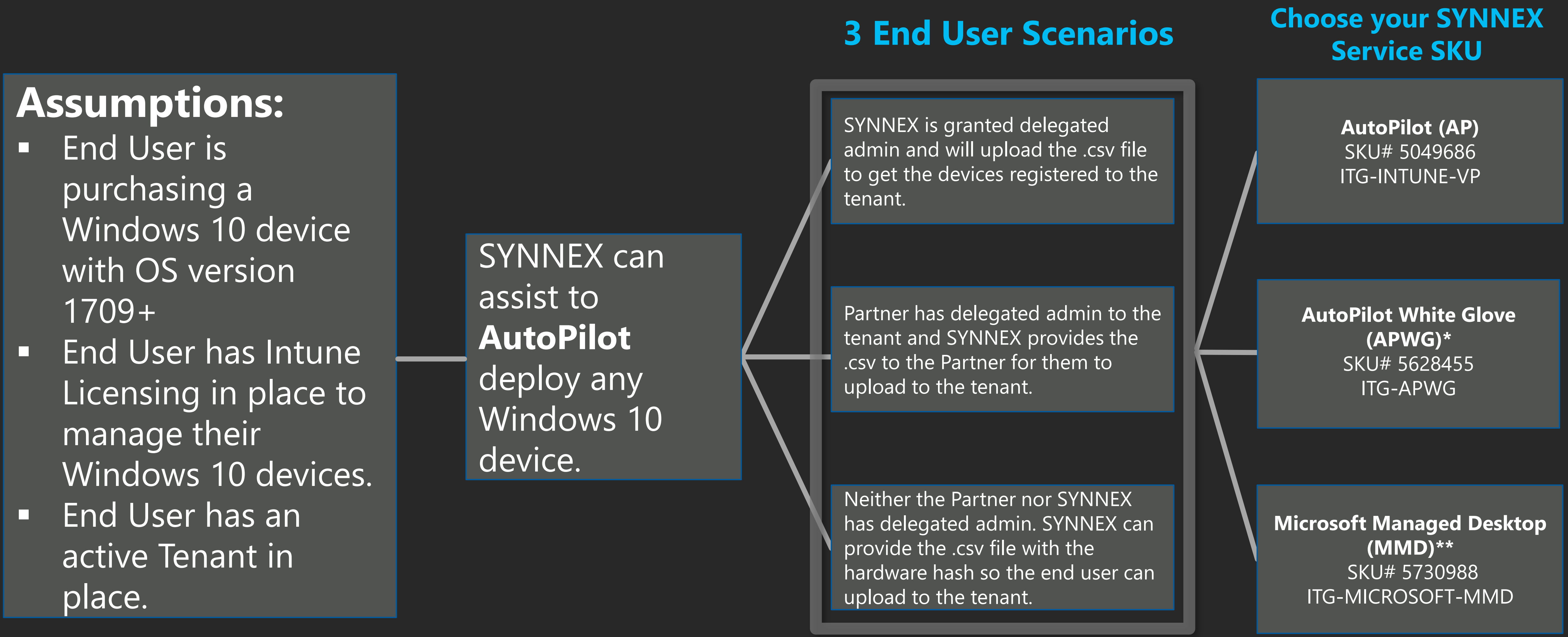
Hardware Vendor

Ship

Deliver direct to Employee

Employee unboxes
device, self-deploys

SYNNEX Microsoft Integration Services: AutoPilot (AP)
AutoPilot White Glove (APWG) & Microsoft Managed Desktop (MMD)



Assumptions:

- End User is purchasing a Windows 10 device with OS version 1709+
- End User has Intune Licensing in place to manage their Windows 10 devices.
- End User has an active Tenant in place.

SYNNEX can assist to **AutoPilot** deploy any Windows 10 device.

3 End User Scenarios

SYNNEX is granted delegated admin and will upload the .csv file to get the devices registered to the tenant.

Partner has delegated admin to the tenant and SYNNEX provides the .csv to the Partner for them to upload to the tenant.

Neither the Partner nor SYNNEX has delegated admin. SYNNEX can provide the .csv file with the hardware hash so the end user can upload to the tenant.

Choose your SYNNEX Service SKU

AutoPilot (AP)
SKU# 5049686
ITG-INTUNE-VP

AutoPilot White Glove (APWG)*
SKU# 5628455
ITG-APWG

Microsoft Managed Desktop (MMD)**
SKU# 5730988
ITG-MICROSOFT-MMD

***AutoPilot White Glove requires the Windows 10 device to be OS version 1903+**
****MMD only available for select devices**

AutoPilot Offerings

AutoPilot, AutoPilot White Glove & Microsoft Managed Desktop

AutoPilot (AP)

Good

- SYNNEX can help AutoPilot deploy any Windows 10 device.
- Devices registered to the End User Tenant so they can be managed via MDM (Example: Intune Portal).
- Value to the customer: Devices shipped directly to the End User, avoids delays and additional shipping costs.

AutoPilot White Glove (APWG)

Better

- Power device, Check for DOA's, & Pre-charge the device.
- Pre-provision so 1st time deployment cycle is reduced by 75% to 5-10 mins per device.
- Verifies profile has been pushed to the device before it ships to the End User.
- Value to customer: shorter deployment cycle, helpful for large deployments (Example: Schools).

Microsoft Managed Desktop (MMD)

Best

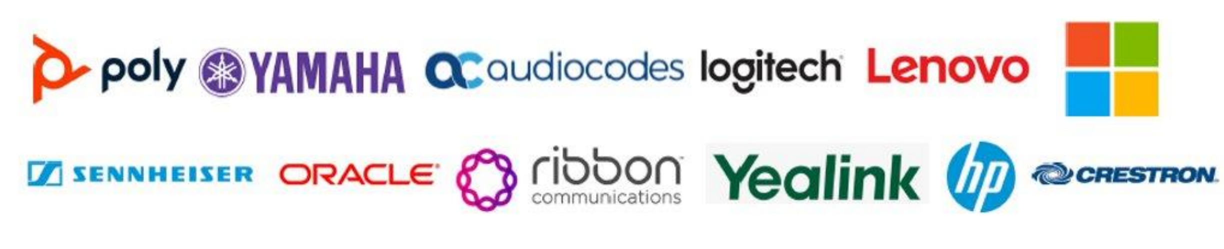
- Device arrives to End User with most recent Windows 10 OS version & Security updates.
- AutoPilot is included.
- Pre-req's:
- Must on the approved devices list (Surface, Dell and HP).
  - Must have MMD Tenant.
  - U.S. only for now looking to expand to Canada.
- Value to customer: devices always arrive with latest Windows updates, out of the box.

Microsoft & UC Collaboration

Seth Green
Microsoft Sales Manager

Are you interested in Microsoft Teams integrations?

"Who"

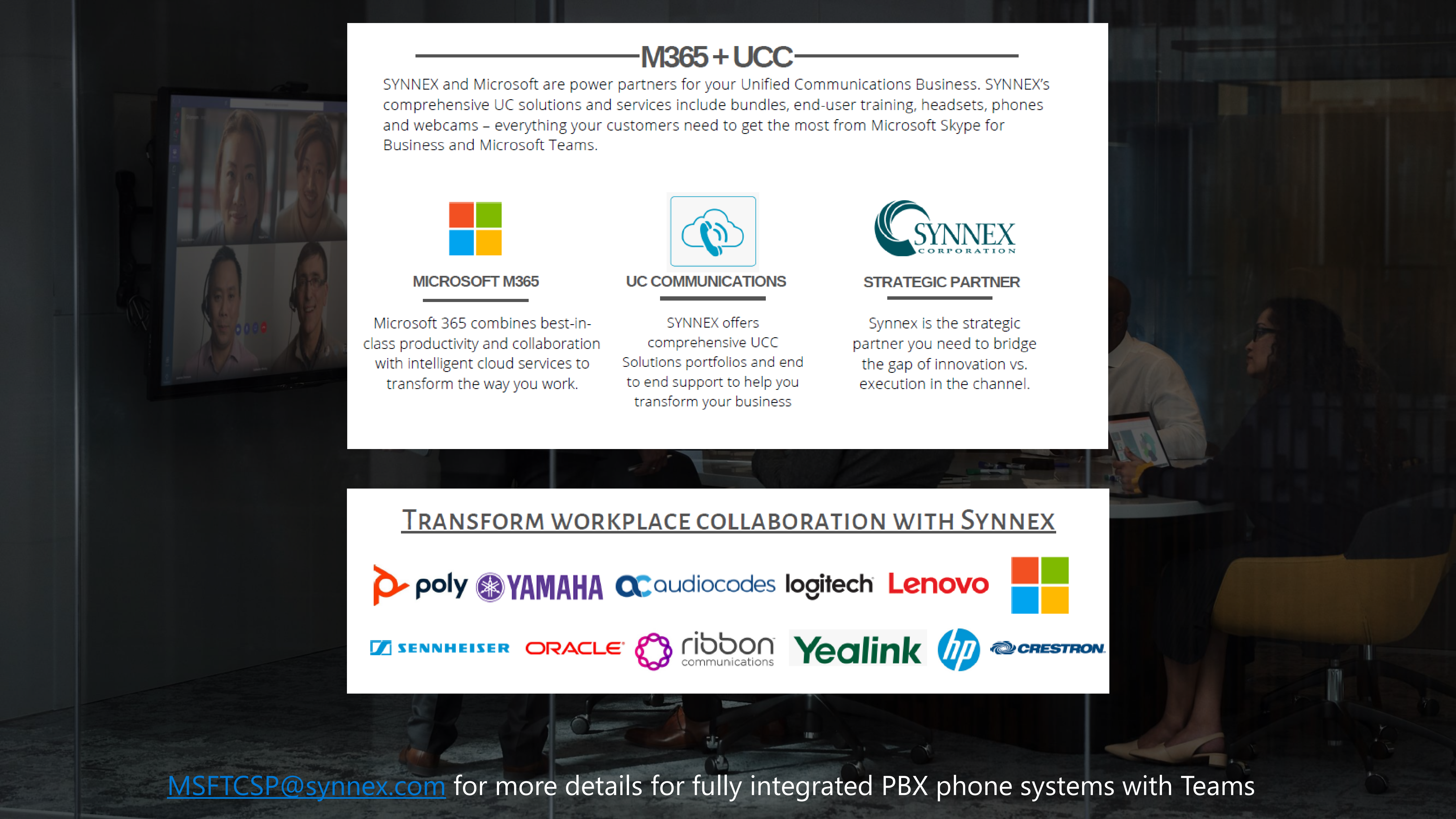


"What"

- Fully Integrate your PBX or Cloud PBX phone number directly into Teams
- Place & receive calls directly from Teams
- Take your office with you while on the go

"How"

- Use SYNNEX's ISV community who specialize in this integration
- Less than 8 minutes per phone number
- Automated tools for services offering



M365 + UCC

SYNNEX and Microsoft are power partners for your Unified Communications Business. SYNNEX's comprehensive UC solutions and services include bundles, end-user training, headsets, phones and webcams – everything your customers need to get the most from Microsoft Skype for Business and Microsoft Teams.

MICROSOFT M365

Microsoft 365 combines best-in-class productivity and collaboration with intelligent cloud services to transform the way you work.

UC COMMUNICATIONS

SYNNEX offers comprehensive UCC Solutions portfolios and end to end support to help you transform your business

SYNNEX CORPORATION

STRATEGIC PARTNER

Synnex is the strategic partner you need to bridge the gap of innovation vs. execution in the channel.

Transform workplace collaboration with Synnex

poly YAMAHA audiocodes logitech Lenovo

SENNHEISER ORACLE ribbon communications Yealink hp CRESTRON

MSFTCSP@synnex.com for more details for fully integrated PBX phone systems with Teams

Q&A

Thank you!

Comparison of Business Premium, Microsoft 365 Business and Office 365 E3

	Features	Office 365 BP	Microsoft 365 Business	Office 365 E3
	Estimated retail price per user per month $USD (with annual commitment)	$12.50	$20	$20
	Maximum number of users	300	300	unlimited
Office Apps	Install Office on up to 5 PCs/Macs + 5 tablets + 5 smartphones per user (Word, Excel, PowerPoint, OneNote, Access), Office Online	Business	Business	ProPlus
Email & Calendar	Outlook, Exchange Online	50GB	50GB	100GB
Hub for Teamwork	Chat-based workspace, online meetings, and more in Microsoft Teams	●	●	●
File Storage	OneDrive for Business	1 TB/user	1 TB/user	Unlimited
Social, Video, Sites	Stream, Yammer, Planner, SharePoint Online[1], Power Apps[1], Flow[1]	●	●	●
Business Apps	Scheduling Apps – Bookings[2], StaffHub	●	●	●
	Business Apps – Outlook Customer Manager, MileIQ[2]	●	●	
Threat Protection	Office 365 Advanced Threat Protection		●	
	Windows Exploit Guard Enforcement		●	
Identity Management	Self-service password reset for hybrid Azure Active Directory accounts		●	
	Azure Multi-Factor Authentication, Conditional Access Policies		●	
Device & App Management	Microsoft Intune, Windows AutoPilot, Windows Pro Management		●	
	Shared Computer Activation		●	●
	Upgrade rights to Windows 10 Pro for Win 7/8.1 Pro licenses		●	
Information Protection	Office 365 Data Loss Prevention		●	●
	Azure Information Protection Plan 1, BitLocker Enforcement		●	
On-Prem CAL Rights	ECAL Suite (Exchange, SharePoint, Skype)			●
Compliance	Unlimited email archiving[3]		●	●

[1] Indicates Office 365 Business Premium has Plan 1 of the functionality and Office 365 E3 has Plan 2

[2] Available in US, UK, Canada

[3] Unlimited archiving when auto-expansion is turned on

Premium add-ons and their eligibility by plan

Add-ons are SKUs that can be added to an existing suite or service

		Business Essentials or Business Premium	Microsoft 365 Business	Office 365 Enterprise E3	Microsoft 365 Enterprise E3	Office 365 Enterprise E5	Microsoft 365 Enterprise E5	Price (USD)
Security	Office Advanced Threat Protection P1	Add-on	Included	Add-on	Add-on	Included	Included	$2
	Advanced Compliance	Add-on	Add-on	Add-on	Add-on	Included	Included	$8
	Threat Intelligence	Add-on	Add-on	Add-on	Add-on	Included	Included	$8
Analytics	Workplace Analytics	N/A	N/A	Add-on	Add-on	Included	Included	$6/$2[1]
	MyAnalytics	Add-on	Add-on	Add-on	Add-on	Included	Included	$4
	Power BI Pro	Add-on	Add-on	Add-on	Add-on	Included	Included	$10
Voice	Audio Conferencing	Add-on	Add-on	Add-on	Add-on	Included	Included	$4
	Phone System	N/A	N/A	Add-on	Add-on	Included	Included	$8
	Calling Plan (Select countries)	N/A	N/A	Add-on Phone System Required	Add-on Phone System Required	Add-on	Add-on	$12/$24[2]

[1] 5,000 Seat Minimum. $6pupm for E1/E3, $2pupm for E5

[2] Dial-out conferencing capabilities may incur additional per minute Communications Credits charges. Customers can disable these features to avoid additional billing. $24 includes both International and Domestic calling plans. Domestic only calling plans are available for $12. Tax is included in price in the US. Service usage limits exist to manage fraud, abuse, excessive use, and maintain service performance. Further details about these services can be found in our recently published Skype for Business Online Service Use Terms.