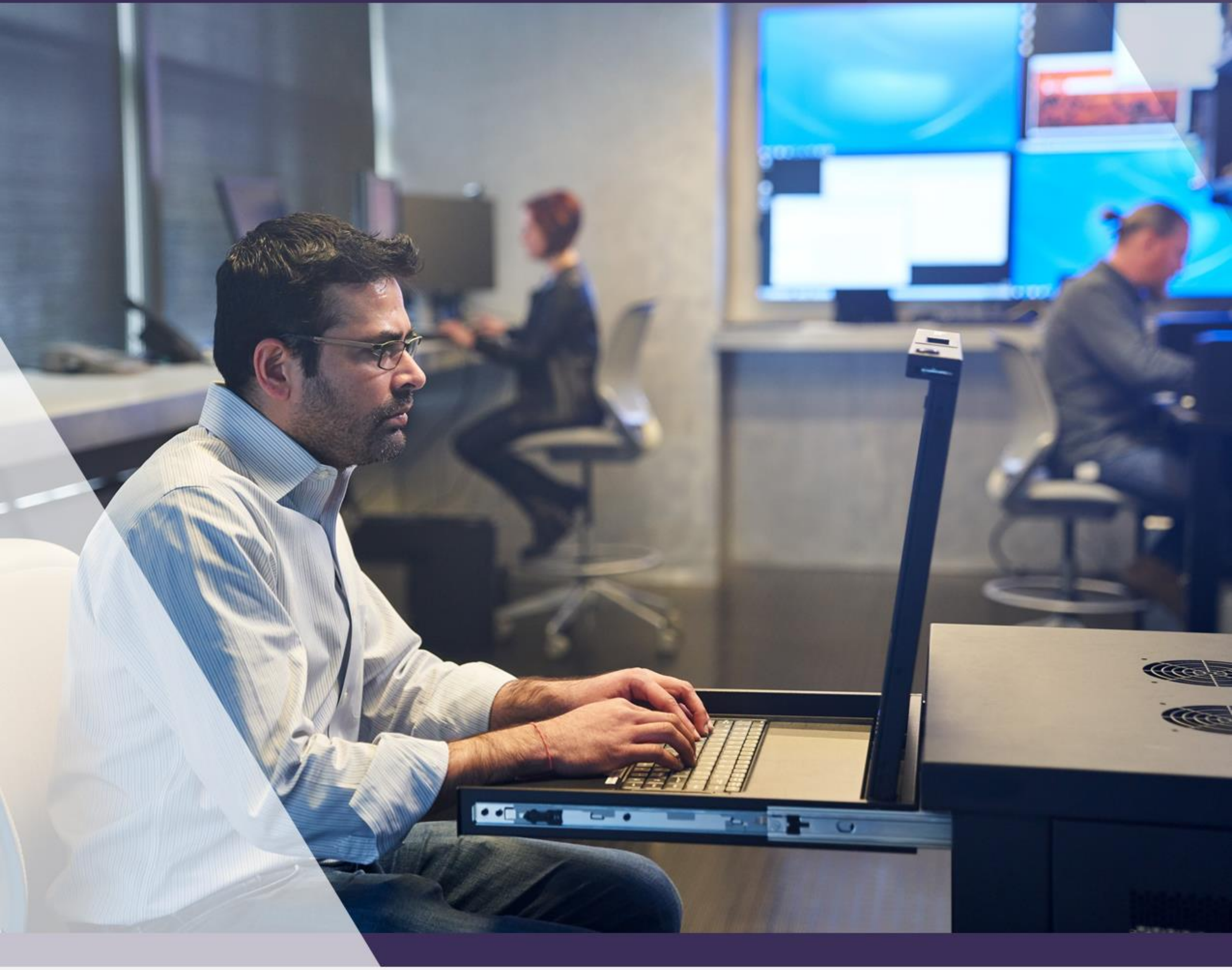
Microsoft

Security, Compliance, and Identity

Microsoft Practice Development Playbook

Published: November 2021



aka.ms/practiceplaybooks

About the playbook

Developed by partners, for partners, as a guide to building or optimizing a security, compliance, and identity focused practice.

This playbook provides high-level guidance and valuable resources for driving new revenue opportunities, developing strategies for marketing and lead capture, selling, and building deeper and longer-term engagements with customers through potential new offerings such as managed services.

It offers guidance on the technical skills needed, the Microsoft resources available to accelerate learning, and the key opportunities for technical delivery. The intent is to help partners understand the practice opportunity and best practices, not to re-write the existing body of detailed guidance on how to perform any given recommendation. Instead, it points to the relevant resources at any given stage of building an security, compliance, and identity focused practice.

Many of the resources and programs referenced in this playbook require membership in the Microsoft Partner Network (MPN) to access. There is no cost to join. Information about the program and how to register can be found on the MPN website.

Partner Practice Development Framework

The playbook is structured into five stages that take a practice from concept to growth.

Define strategy	Hire and train	Operationalize	Go-to-market and close deals	Optimize and grow
Define the offer, benchmark the practice, and identify required resources	Hire talent, train resources, and complete certifications	Prepare for launch with systems, tools, and process in place	Execute sales and marketing strategy to find customers and close deals with winning proposals	Collect feedback, identify expansion opportunities, optimize the practice, grow partnerships, and refine the offer

How this playbook was made

This playbook is part of a series of guidance written by Microsoft Partner, Solliance, in conjunction with the Microsoft Global Partner Solutions group and 14 other successful partners that have volunteered time to provide input and best practices to share with the rest of the partner community.

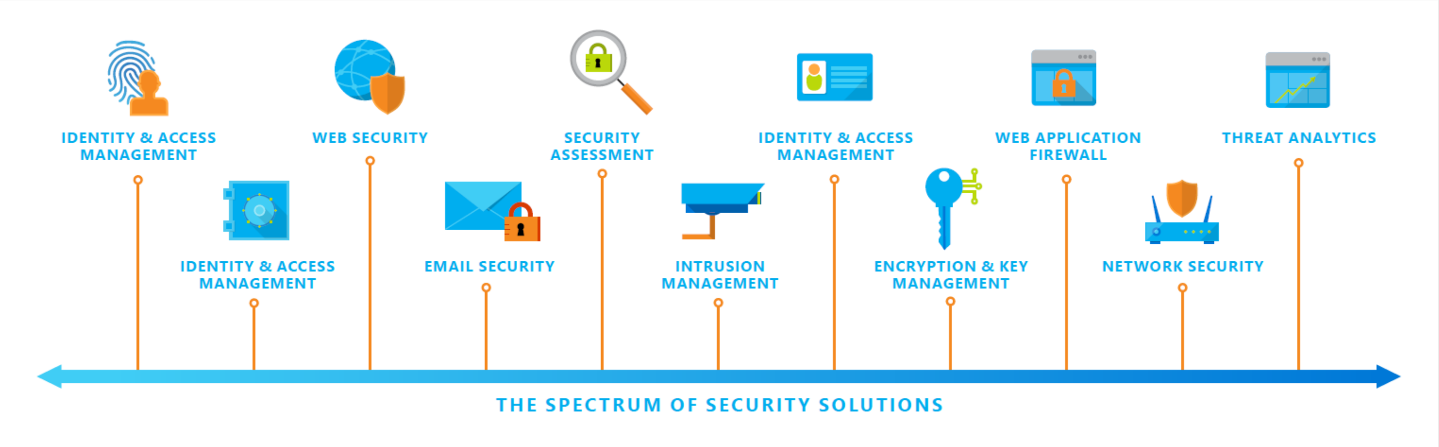
To validate the guidance, Microsoft worked with MDC Research to survey 484 global partners. The results of this survey are provided in-line with the guidance found within this playbook.

CONTRIBUTING PARTNERS	
Accenture	KPMG
Atea	Performanta
BT	ResourceIT
Dimension Data	Slalom
Extra Mile Marketing	SoftwareOne
Ernst & Young	VBC
Hanu Software	Wortell

Contents

The security, compliance, and identity landscape

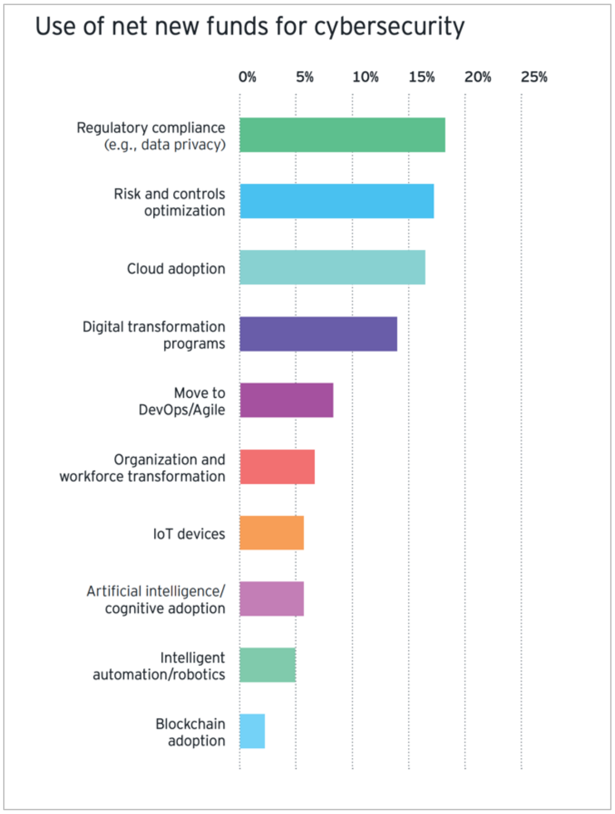
The current digital security landscape for businesses can accurately be described in one word: complicated. More numerous and advanced threats, more nebulous and complex compliance requirements, more difficult and intricate infrastructure to secure. Simply put, keeping data, workloads, and users secure is more than a full-time job—and organizations are having trouble keeping up. The graphic below illustrates the myriad offerings and postures taken by security companies, highlighting the fragmented nature of the market. However, this harsh environment represents a significant opportunity for partners looking to offer security as a managed service.


IDENTITY & ACCESS MANAGEMENT
IDENTITY & ACCESS MANAGEMENT
WEB SECURITY
EMAIL SECURITY
SECURITY ASSESSMENT
INTRUSION MANAGEMENT
IDENTITY & ACCESS MANAGEMENT
ENCRYPTION & KEY MANAGEMENT
WEB APPLICATION FIREWALL
NETWORK SECURITY
THREAT ANALYTICS
THE SPECTRUM OF SECURITY SOLUTIONS

For even the most adept IT and incident response teams, effectively handling patching, malware threats, and intrusion detection can be too difficult to manage without help. Managed Service Providers can offer services to ensure enterprise clients are secured. But in this age where new security breaches surface in the news almost daily, how can partners help customers stay ahead of the game, and avoid becoming a statistic?

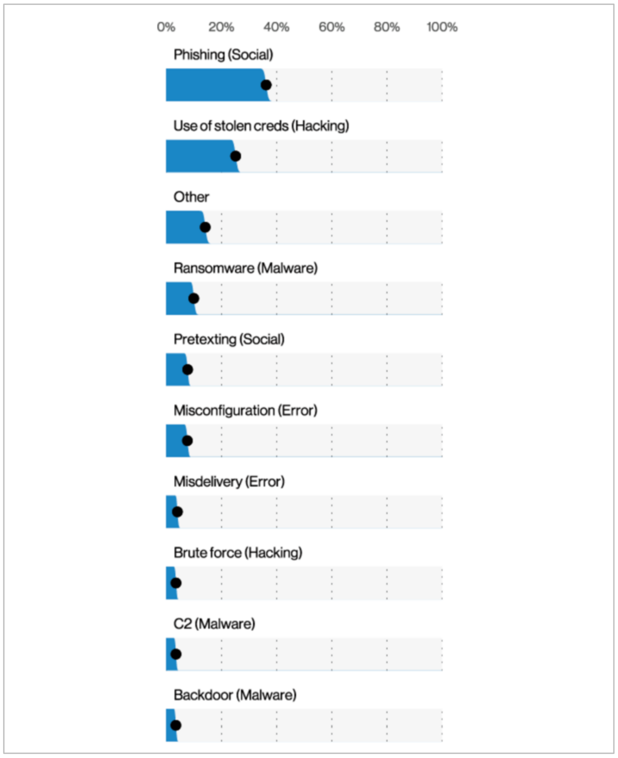
According to the Microsoft Digital Defense Report 2020, attacks have become more sophisticated and ransomware was the most common reason for incident responses from October 2019 to July 2020. Microsoft blocked more than 13 billion suspicious emails, and more than a billion of those used URLs set up to launch phishing credential attacks. And the first half of 2020 saw a 35% increase in IoT attacks compared to the second half of 2019.

According to the 2020 IBM Cost of a Data Breach Report, the cost incurred for each lost or stolen record of sensitive data is now at $150, with the total consolidated cost of a data breach at $3.86 million. Meanwhile, according to the PWC Global State of Information Security Survey, the sources of security incidents perpetrated by current employees remains high, and that from business partners continues to rise. Additionally, many CISOs feel the most challenging thing is to secure the budget they need to provide the levels of cybersecurity they desire, according to the EY Global Information Security Survey. All of this combines to create the demand for partners to improve their customers defense with information protection.



Source: 2020 EY Global Information Security Survey

According to the Verizon 2021 Data Breach Investigations Report, organizations surveyed saw phishing as the top threat. Additionally, these organizations identified zero-day attacks and targeted cyber-attacks to steal financial information, disrupt or deface the organization, or steal intellectual property or data. Yet, according to the EY Global Information Security Survey, only 26% of breaches from these threats in the last 12 months were detected by the SOC.



Source: Verizon 2021 Data Breach Investigations Report

PROTECTING AGAINST EVOLVING CYBERSECURITY THREATS

In today's world, it's clear that increasing trust and managing security, compliance and identity is a struggle for many organizations. But as Microsoft's Digital Defense Report points out, actors have continued to evolve their attack techniques making the importance of improving security comprehensively has become even more evident:

36%	280 Days	$120 Billion
Of breaches had phishing present in them.[1]	Average time to identify and contain a breach.[2]	Forecasted global spending on security solutions in 2021.[3]

COMPLIANCE REGULATIONS

Privacy regulations such as the General Data Protection Regulation (GDPR) and California Consumer Protection Act (CCPA) continue to impact organizations that collect and process information for citizens of the EU and California. In addition to CCPA, many other US states are considering adopting privacy legislation, but the United States still lacks an "omnibus" approach to privacy protection. Both GDPR and CCPA have progressed from readiness requirements to actual prosecution of punitive damages for companies that fail to comply or suffer privacy breaches as a result of non-compliance.

A recent study by Microsoft research shows that 93% of Chief Information Security Officers (CISOs) and Data Protection Officers are concerned with insider risk. In addition, 66% stated they were "very concerned". Insider threats are reportedly the primary cause for over 60% of data breaches and percentage is increasing. Last year we saw a former employee at Amazon charged with insider trading by having access to sensitive financial data and sharing with family members, there was an unsuccessful attempt to bribe to a Tesla employee with $1 million in exchange for installing malware in the system, and an incident with "two rogue" employees resulted in Shopify's stock price to drop 1.2%.

SOURCES:

- [1]Verizon 2021 Data Breach Investigations Report
- [2]2020 Cost of Data Breach Report
- [3]IDC Worldwide Semiannual Security Spending Guide

Partner opportunities

The identity and access management opportunity

The opportunity to help customers here should be plain—equip them to better manage identity, access controls, and stop breaches before they escalate in severity.

Consider using the following Microsoft products and services to develop solutions for a security practice focused on identity and access management:

SAFEGUARD AND MANAGE IDENTITY	Azure Key Vault Azure Active Directory (AAD)
DETECT AND RESPOND TO IDENTITY-BASED THREATS	Azure Active Directory (AAD) Microsoft Cloud App Security Microsoft Defender for Identity
PROTECT AGAINST PASSWORD ATTACKS	Windows Hello for Business Windows Defender Credential Guard Multi-Factor Authentication

The threat protection opportunity

The threat protection opportunity is about enabling customers to remain constantly aware of the current threat landscape and identifying attackers—and the attacks they are using—before they cause damage.

Consider using the following Microsoft products and services to develop solutions for a security practice focused on threat protection:

PROTECT AGAINST MALWARE ATTACKS	Windows Defender Windows Defender Device Guard UEFI Secure Boot and the Trusted Boot Process
MANAGE MOBILE DEVICES AND APPLICATIONS	Microsoft Enterprise Mobility + Security (EMS) Microsoft Endpoint Manager

The security management opportunity

Consider using the following Microsoft products and services to develop solutions for a security practice focused on security management:

DETECT AND RESPOND TO THREATS	Azure Sentinel Azure Security Center Azure Advisor Microsoft Defender for Endpoint
PROTECT AGAINST THREATS	Microsoft Azure Windows Server Azure Defender Microsoft Defender for Endpoint
GAIN VISIBILITY INTO SECURITY HEALTH	Azure Sentinel Azure Security Center Azure Network Watcher Azure Monitor Microsoft Secure Score Microsoft 365 Defender Microsoft Cloud App Security

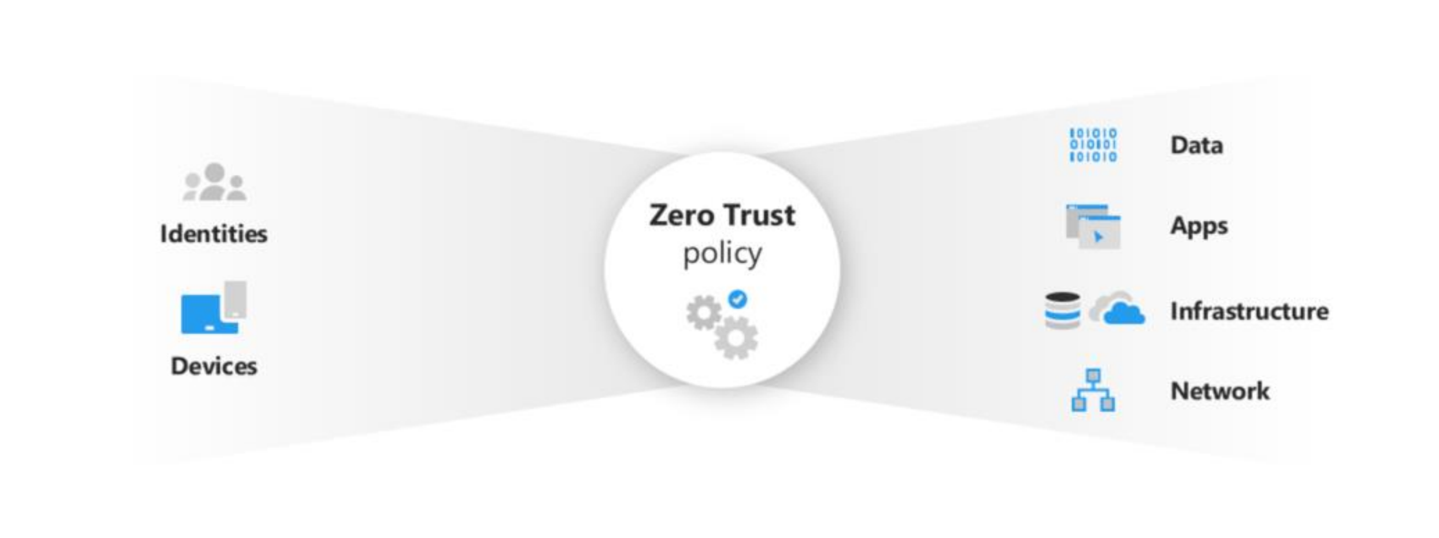
Microsoft security solutions

Partners can help customers protect against breaches, detect breaches, and respond to breaches with a comprehensive security solution. The overarching security environment of the enterprise includes a mix of solutions provided by many different vendors. This playbook focuses coverage on Microsoft products and services that play a critical role in securing this environment.

Microsoft's intelligent cloud offers smart, adaptive security solutions that does not hamper productivity, starting with a user authentication experience accessible from any device and threat detection tools that communicate with each other across the entire digital footprint and automate detection, investigation, and remediation.

ZERO TRUST

Cloud applications and the mobile workforce have redefined the security perimeter, and Microsoft has shared its guiding principles with its Zero Trust security model, designed to more effectively adapt to the complexity of the modern workplace, by protecting people, devices, apps, and data wherever they're located. In a Zero Trust model, every access request is strongly authenticated, authorized within policy constraints and inspected for anomalies before granting access by using the model of "never trust, always verify". Partners are encouraged to use this model as well as to take advantage of the Zero Trust Deployment Center, to build Zero Trust into their customers' organizations.



The table below provides a summary of select, important security-related services (with features of a service explicitly called out when that is more relevant) grouped into these major security categories: storage, networking, compute, database, identity and access management, and security management and monitoring. Within each category is a selection of services or resources related to the security objective and the Azure services or features that can be leveraged to meet that security objective. This list is constantly evolving and is more comprehensive than what can be covered in this playbook. For the most up-to-date and comprehensive treatment, visit the Zero Trust Guidance Center at https://docs.microsoft.com/security/zero-trust/.

STORAGE

IF YOU ARE USING...	AND YOU WANT TO...	THEN CONSIDER...
Azure Storage	Encrypt data at rest	- Service Encryption - Client-Side Encryption
	Protect data in transit	- File Shares with SMB 3.0 Encryption - TLS protocol
	Control data access	- Account Keys - Shared Access Signatures (SAS) - Stored Access Policy - Cross Origin Resource Sharing (CORS)
	Audit usage	- Storage Analytics
Azure Data Lake Store	Encrypt data at rest	- Block encryption
	Protect data in transit	- TLS protocol
	Control data access	- Access control lists - Firewall
	Audit usage	- Audit logs - Diagnostic logs

NETWORKING

IF YOU ARE USING...	AND YOU WANT TO...	THEN CONSIDER...
Virtual Networks	Secure the virtual network perimeter	- Network Security Groups - Azure Application Gateway
	Secure hybrid connectivity	- Azure VPN Gateway - Azure ExpressRoute - Azure Application Proxy
	Audit usage	- Azure Network Watcher - Log analytics for Network Security Groups

COMPUTE

IF YOU ARE USING...	AND YOU WANT TO...	THEN CONSIDER...
Virtual Machines	Secure Virtual machines	• Azure Disk Encryption • Microsoft Antimalware • Diagnostic logs
Azure Cloud Services (extended support)	Secure cloud services	• Microsoft Antimalware • Diagnostic logs
App Services	Secure app services	• Enforce HTTPS • TLS mutual authentication • Diagnostic logs

DATABASE

IF YOU ARE USING...	AND YOU WANT TO...	THEN CONSIDER...
Azure SQL	Encrypt data at rest	• Transparent data encryption • Column level encryption • Always encrypted
	Protect data in transit	• TDS over TLS protocol
	Control data access	• SQL Authentication • Azure Active Directory Authentication • Dynamic Data Masking • Row Level Security • Role Membership & Object Level Permissions • Firewall • Virtual network service endpoints
	Audit usage	• SQL Database Usage
	Detect threats	• SQL Database Threat Detection

IDENTITY & ACCESS MANAGEMENT

IF YOU ARE USING...	AND YOU WANT TO...	THEN CONSIDER...
Azure Services	Control management plane access to Azure Services	• Azure Resource Manager • Role Based Access Control
	Manage identity	• Azure Active Directory • Azure Active Directory B2C • Azure Active Directory Domain Services
	Store secrets & encryption keys	• Azure Key Vault
	Audit usage	• SQL Database Usage
	Protect identities	• Azure Multi-Factor Authentication

SECURITY MANAGEMENT & MONITORING

IF YOU ARE USING...	AND YOU WANT TO...	THEN CONSIDER...
Azure Services	Manage and monitor security of Azure resources	• Azure Security Center • Azure Monitor • Azure Sentinel
	Manage and audit logs	• Log Analytics • Azure Log Integration

Microsoft 365

Microsoft 365 is a complete, intelligent solution to empower employees to be creative and work together, securely.

Microsoft 365 Enterprise	Microsoft 365 Business
Microsoft 365 E3 and Microsoft 365 E5 offerings with additional security and compliance specific add-ons	Designed for small and midsize businesses with up to 300 users

EMS is included with Microsoft 365 Enterprise or is provided as an add-on package to Office 365 Enterprise. It provides an identity-driven security solution that offers a holistic approach to the security challenges in this mobile-first, cloud-first era. It bundles five products to deliver a device-management and virtual identity management suite. The suite is offered in two tiers, EMS E3 and EMS E5 that offer the suite of services for a single per user price. Customers with EMS E3 can also purchase the Identity & Threat Protection offering and Information Protection & Compliance offering simplifying the path to Microsoft 365 E5, delivering cost savings over purchasing standalones.

AZURE ACTIVE DIRECTORY PREMIUM

Azure Active Directory Premium provides the single sign-on capability for the entire enterprise targeting resources both in the cloud and on-premises. At the E3 level, Enterprise Mobility + Security includes AAD Premium P1 which provides the secure single sign-on to cloud and on-premises apps, along with multi-factor authentication support (requiring further authentication via phone call, text message or mobile app verification), conditional access (based on group membership, geographic location, and device state), and advanced security reporting. With the Identity & Threat Protection offering and at the EMS E5 level, AAD Premium P2 is included that builds on AAD Premium P1 by adding more advanced protection for users (such as conditional access based on sign-in or user risk) and support for privileged identities (which enables on-demand, "just in time" privilege escalation for administrative access).

MICROSOFT ENDPOINT MANAGEMENT

Microsoft Intune is included for both EMS E3 and E5 to provide mobile device and app management capabilities to protect corporate apps and data on any device—even when users bring their own personal devices.

AZURE INFORMATION PROTECTION

Azure Information Protection (AIP) enables control over the access to files and emails across cloud and on-premises and is provided at two levels in EMS. Within EMS E3, Azure Information Protection Premium P1 is provided and includes support for file and email encryption and cloud-based tracking of files. The Identity & Threat Protection Offering and EMS E5 provides Azure Information Protection Premium P2, which layers on automated, intelligent classification and encryption for files and emails.

MICROSOFT CLOUD APP SECURITY

Microsoft Cloud App Security brings the security capabilities traditionally available to on-premises systems to SaaS cloud applications like Dropbox, Office 365, G Suite, and Salesforce, and enables deeper visibility, comprehensive controls, and enhanced protection against cloud security issues. Cloud App Security is included in the Identity & Threat Protection offering and with EMS E5.

AZURE DEFENDER FOR IDENTITY

Azure Defender for Identity is an on-premises platform that leverages on-premises Active Directory signals to help protect the enterprise from advanced targeted attacks by automatically analyzing, learning, and identifying normal and abnormal entity (user, devices, and resources) behavior. It is available in EMS E5.

MICROSOFT 365 AND THE INTELLIGENT CLOUD HELP CUSTOMERS

- Protect, detect, and respond to today's modern security landscape, which presents new risks and opportunities
- Drive digital transformation that includes everyone, from the executive office to the frontline worker

As a fully integrated, end-to-end solution, Microsoft 365 provides unique customer value, which in turn creates amazing new partner opportunities.

ENGAGE CUSTOMERS IN STRATEGIC CONVERSATIONS

Microsoft 365 will enable partners to engage customers in strategic conversations around:

- Advanced Security
- Compliance & GDPR
- Collaboration & Cloud Voice
- Microsoft 365 powered device
- Frontline Workers

Leverage Microsoft 365 to spark dialogue with customers about the growing threat of cyber-attacks, the need for the advanced security in Microsoft 365, and the importance of protecting privacy, especially in context of compliance regulations. Discuss collaboration and what the teams of today need to get work done together, what modern desktop and devices have to offer businesses, and how Microsoft 365 helps to empower first line workers.

GROW BUSINESS WITH MICROSOFT 365

- **Grow with Managed Services**. Modernize the customer's environment leading with security.
- **Differentiate offerings**. Offer advanced enterprise services based on intelligence capabilities of Microsoft 365.
- **Increase deal size**. Elevate the customer conversation by leveraging the broad value of Microsoft 365.

Microsoft

Define the Strategy

Security, Compliance, and Identity

aka.ms/practiceplaybooks

Microsoft
Partner
Network

Introduction

This section will begin by providing an overview of the areas of expertise within the security, compliance and identity practice: identity and access management, threat protection, information protection & governance, and cloud security. The nature of the business opportunity and the key Microsoft products and services leveraged in delivering solutions that capitalize on the opportunity will be discussed.

The next step is to define an offer and its value proposition. This section will include a review of the four cloud business models (reselling, project services, managed services, and intellectual property), their respective profitability, and how partners can assess the profitability of their own practice. It will include guidance on what other successful partners are selling, and recommendations on what to include in each type of service offering.

For more on how to determine the value of a solution and package that value into a differentiated offer, refer to the Define the Strategy Guide. The guide covers how to price an offer and build a solid business plan that addresses team, marketing, pre-sales, sales, and financial aspects.

The guide dives deeper into sales to help define a pre-sales and post-sales engagement process, and how to compensate sales executives. It highlights the Microsoft Partner Network programs for growing a practice, and how to maximize the benefits from the program, and concludes by helping partners understand support—how to support customers, Microsoft's support offerings, and the support-related benefits available in the Microsoft Partner Network.

Define the practice focus

Through a security, compliance and identity practice, partners can help keep customers productive and secure—and company data protected—on their favorite apps and devices with Microsoft solutions. Partners help turn the potentially dizzying array of services, licensing options, and overlapping feature sets into a cohesive, comprehensive, and understandable security solution that enables customers to manage security, protect assets, and respond to security incidents.

IDENTITY AND ACCESS MANAGEMENT

Help customers protect their identities and data. Use behavioral analysis to provide actionable insights and ensure that customers have a sound approach to manage users and groups, as well as secure access to on-premises and cloud apps.

THREAT PROTECTION

Build a practice that helps customers proactively guard against threats, identify breaches and threats using advanced analytics, and automate the response to threats enterprise wide.

INFORMATION PROTECTION

Manage and protect corporate apps and data. Provide customers with mobile device management, mobile app management, and PC management capabilities. Enable employees with access from virtually anywhere on almost any device, while helping to keep corporate information secure and compliant.

SECURITY MANAGEMENT

Help customers increase their resilience with protecting against threats due to misconfigurations, authentication misuse, loss of sensitive data, and other weaknesses. Provide a secure cloud environment with integrated reporting and security improvements with Cloud Security Posture Manage and Cloud Workload Protection Platform solutions in the Microsoft cloud.

Define and design the solution offer

Project services typically drive a range of approximately 35% gross margin, but this has been under pressure for some time. This is a result of little differentiation in the channel, which has caused billable price points to hold steady over the past five or more years, while increasing salary and benefit costs of consultants and inflation have eroded profitability.

As a result, aggressive and entrepreneurial members of the channel have adapted and gone after the higher margin opportunities of managed services, which generate on average 45% gross margin and packaged IP, which often exceeds 70%.

This section details the types of project services, managed services, and intellectual property partners can consider in a security, compliance, and identity practice.

Understanding project services

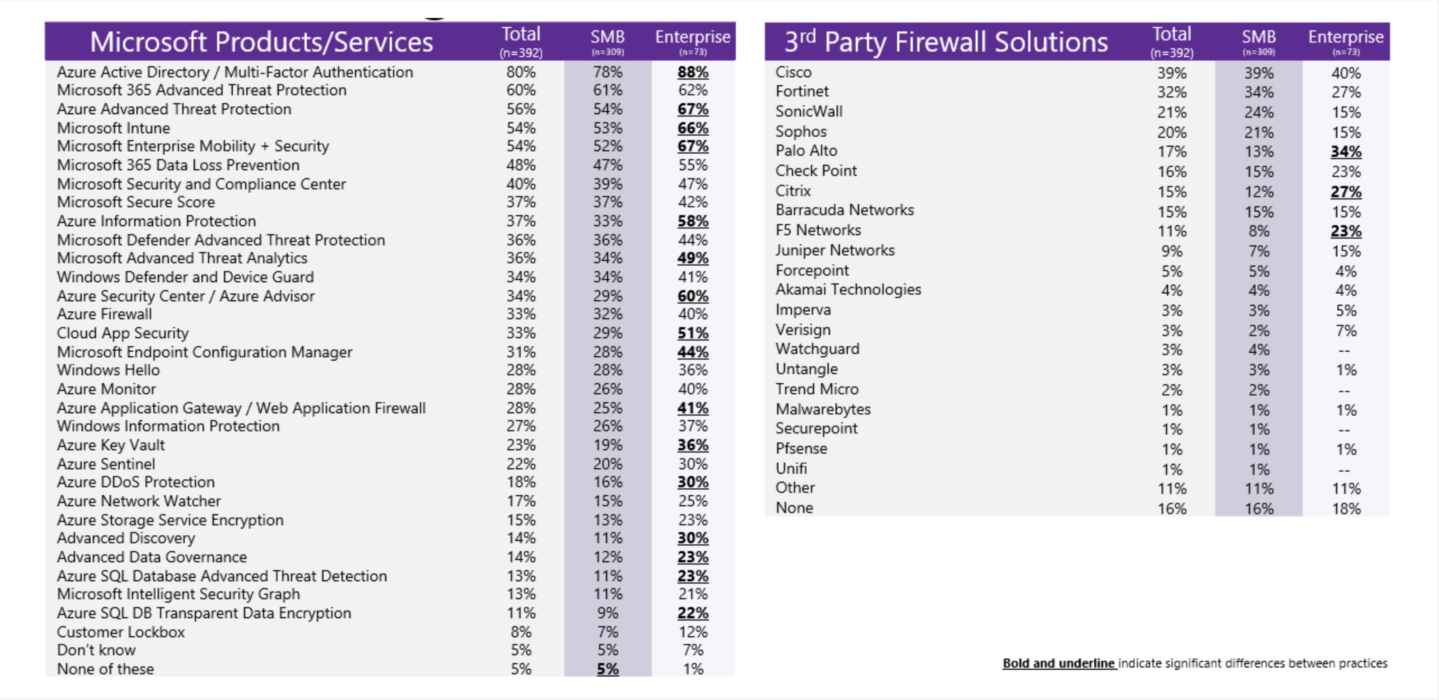
Building a new practice is not that different from starting a business from scratch. It is important to start with a vision of what the business will do, what problems it will solve, and how it will make money.

In the Microsoft Cloud Security Practice Development Study, partners were asked what project services they offer within their security practice. The wide range of offerings illustrates the importance and prevalence of security considerations across all partner practices.

PROJECT SERVICES (n=373)	
Cloud Migration Planning	73%
Multi-factor Authentication Enablement	73%
Advanced Threat Protection	67%
Configuration	64%
Cloud Readiness Assessment	58%
Deployment Services	57%
Help-Desk Support	56%
Patch Management	55%
Mobile Device Management	55%
Systems Integration	54%
Identity & Access Control Enablement	54%
Office Client Deployment	51%
Auditing, Security & Compliance Assessments	51%
Cloud Solution Costing & Spend Optimization	50%
Data Migration Management	49%
Activity and Log Audit Management	47%
Health Checks	46%
Proof of Concept	45%
Solution Support & Training	45%
Data Leakage/Loss Prevention	44%
Security/Compliance Assessment & Enablement	44%
Information Protection Configuration	43%
Solution Configuration/Customization	42%
Strategic Planning Services	41%
Cyber Security Risk Assessment	41%
Threat Detection & Mitigation Enablement	40%

PROJECT SERVICES (n=373)	
Solution Analysis, Scope, & Design	39%
Password Complexity Management	38%
Policy Recommendation and Improvement	35%
User Monitoring and Enablement	35%
Training on Azure or Microsoft Security Products or Services	33%
Device Procurement and Deployment	33%
Data Classification and Data Governance	32%
Incidence Response Management	32%
User Training and Customer Self-Serve Portal	31%
Security Operations Center Management	30%
Penetration Testing	25%
Productivity Cloud App Usage Management	23%
Security Penetration Testing	23%
CISO or Security Analyst as a Service	21%
Custom Application Development	21%
We do not offer any of these project services	2%

When partners deliver a cloud security solution, these are the top Microsoft Services and third-party firewall solutions leveraged across practices:



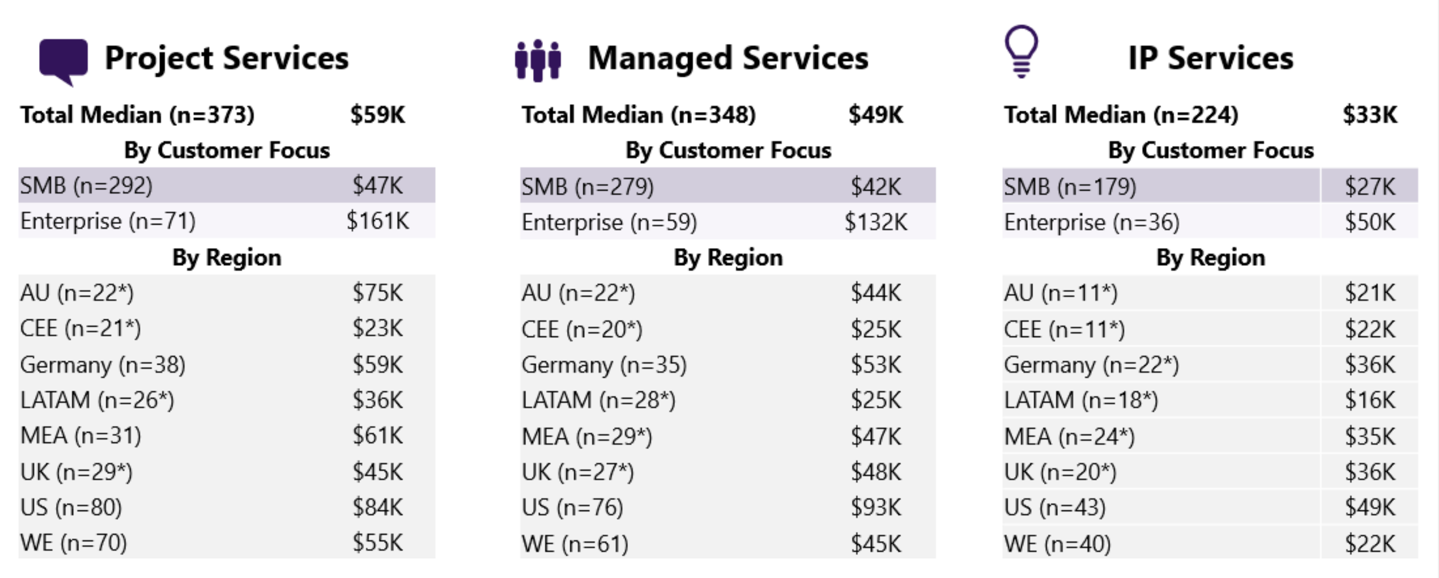
Microsoft Products/Services	Total (n=392)	SMB (n=309)	Enterprise (n=73)
Azure Active Directory / Multi-Factor Authentication	80%	78%	**88%**
Microsoft 365 Advanced Threat Protection	60%	61%	62%
Azure Advanced Threat Protection	56%	54%	**67%**
Microsoft Intune	54%	53%	**66%**
Microsoft Enterprise Mobility + Security	54%	52%	**67%**
Microsoft 365 Data Loss Prevention	48%	47%	55%
Microsoft Security and Compliance Center	40%	39%	47%
Microsoft Secure Score	37%	37%	42%
Azure Information Protection	37%	33%	**58%**
Microsoft Defender Advanced Threat Protection	36%	36%	44%
Microsoft Advanced Threat Analytics	36%	34%	**49%**
Windows Defender and Device Guard	34%	34%	41%
Azure Security Center / Azure Advisor	34%	29%	**60%**
Azure Firewall	33%	32%	40%
Cloud App Security	33%	29%	**51%**
Microsoft Endpoint Configuration Manager	31%	28%	**44%**
Windows Hello	28%	28%	36%
Azure Monitor	28%	26%	40%
Azure Application Gateway / Web Application Firewall	28%	25%	**41%**
Windows Information Protection	27%	26%	37%
Azure Key Vault	23%	19%	**36%**
Azure Sentinel	22%	20%	30%
Azure DDoS Protection	18%	16%	**30%**
Azure Network Watcher	17%	15%	25%
Azure Storage Service Encryption	15%	13%	23%
Advanced Discovery	14%	11%	**30%**
Advanced Data Governance	14%	12%	**23%**
Azure SQL Database Advanced Threat Detection	13%	11%	**23%**
Microsoft Intelligent Security Graph	13%	11%	21%
Azure SQL DB Transparent Data Encryption	11%	9%	**22%**
Customer Lockbox	8%	7%	12%
Don't know	5%	5%	7%
None of these	5%	**5%**	1%

3rd Party Firewall Solutions	Total (n=392)	SMB (n=309)	Enterprise (n=73)
Cisco	39%	39%	40%
Fortinet	32%	34%	27%
SonicWall	21%	24%	15%
Sophos	20%	21%	15%
Palo Alto	17%	13%	**34%**
Check Point	16%	15%	23%
Citrix	15%	12%	**27%**
Barracuda Networks	15%	15%	15%
F5 Networks	11%	8%	**23%**
Juniper Networks	9%	7%	15%
Forcepoint	5%	5%	4%
Akamai Technologies	4%	4%	4%
Imperva	3%	3%	5%
Verisign	3%	2%	7%
Watchguard	3%	4%	--
Untangle	3%	3%	1%
Trend Micro	2%	2%	--
Malwarebytes	1%	1%	1%
Securepoint	1%	1%	--
Pfsense	1%	1%	1%
Unifi	1%	1%	--
Other	11%	11%	11%
None	16%	16%	18%

Bold and underline indicate significant differences between practices

Source: Microsoft Cloud Security Practice Development Study, MDC Research, July 2020

Project services generate the most revenue, particularly for enterprise customers.



Project Services

Total Median (n=373)	$59K
By Customer Focus	
SMB (n=292)	$47K
Enterprise (n=71)	$161K
By Region	
AU (n=22*)	$75K
CEE (n=21*)	$23K
Germany (n=38)	$59K
LATAM (n=26*)	$36K
MEA (n=31)	$61K
UK (n=29*)	$45K
US (n=80)	$84K
WE (n=70)	$55K

Managed Services

Total Median (n=348)	$49K
By Customer Focus	
SMB (n=279)	$42K
Enterprise (n=59)	$132K
By Region	
AU (n=22*)	$44K
CEE (n=20*)	$25K
Germany (n=35)	$53K
LATAM (n=28*)	$25K
MEA (n=29*)	$47K
UK (n=27*)	$48K
US (n=76)	$93K
WE (n=61)	$45K

IP Services

Total Median (n=224)	$33K
By Customer Focus	
SMB (n=179)	$27K
Enterprise (n=36)	$50K
By Region	
AU (n=11*)	$21K
CEE (n=11*)	$22K
Germany (n=22*)	$36K
LATAM (n=18*)	$16K
MEA (n=24*)	$35K
UK (n=20*)	$36K
US (n=43)	$49K
WE (n=40)	$22K

Source: Microsoft Cloud Security Practice Development Study, MDC Research, July 2020.

PROJECT SERVICES BY REGION

	Total (n=373)	AU (n=22*)	CEE (n=21*)	Germany (n=38)	LATAM (n=26*)	MEA (n=31)	UK (n=29*)	US (n=80)	WE (n=70)
Cloud Migration Planning	73%	68%	76%	79%	73%	81%	76%	76%	70%
Multi-factor Authentication Enablement	73%	82%	76%	76%	38%	65%	72%	85%	76%
Advanced Threat Protection	67%	73%	62%	58%	50%	81%	62%	70%	67%
Configuration	64%	73%	71%	68%	54%	77%	66%	71%	56%
Cloud Readiness Assessment	58%	59%	43%	66%	62%	61%	62%	61%	56%
Deployment Services	57%	50%	57%	45%	42%	71%	83%	69%	40%
Help-Desk Support	56%	73%	48%	55%	31%	74%	69%	63%	53%
Patch Management	55%	73%	33%	68%	38%	52%	69%	70%	46%
Mobile Device Management	55%	59%	52%	61%	23%	52%	66%	69%	51%
Systems Integration	54%	45%	71%	74%	38%	45%	48%	66%	47%
Identity & Access Control Enablement	54%	50%	33%	63%	31%	52%	66%	64%	56%
Office Client Deployment	51%	55%	43%	63%	42%	58%	62%	54%	49%
Auditing, Security & Compliance Assessments	51%	50%	33%	55%	35%	55%	55%	64%	49%
Cloud Solution Costing & Spend Optimization	50%	41%	48%	68%	46%	58%	52%	51%	41%
Data Migration Management	49%	50%	48%	58%	38%	58%	55%	54%	36%
Activity and Log Audit Management	47%	55%	52%	55%	23%	39%	41%	51%	46%
Health Checks	46%	68%	48%	45%	19%	58%	66%	48%	36%
Proof of Concept	45%	41%	43%	42%	31%	71%	38%	55%	36%
Solution Support & Training	45%	27%	57%	42%	38%	48%	52%	50%	43%
Data Leakage/Loss Prevention	44%	45%	24%	66%	31%	42%	45%	50%	44%
Security/Compliance Assessment & Enablement	44%	45%	29%	53%	27%	42%	59%	56%	40%
Information Protection Configuration	43%	32%	33%	55%	35%	55%	48%	56%	34%
Solution Configuration/Customization	42%	32%	38%	42%	23%	42%	55%	46%	44%
Strategic Planning Services	41%	45%	24%	39%	35%	32%	48%	65%	33%
Cyber Security Risk Assessment	41%	59%	24%	45%	31%	52%	52%	48%	30%
Threat Detection & Mitigation Enablement	40%	32%	19%	50%	27%	35%	48%	50%	39%
Solution Analysis, Scope, & Design	39%	32%	38%	39%	27%	42%	41%	53%	31%
Password Complexity Management	38%	50%	24%	39%	31%	39%	55%	51%	30%
Policy Recommendation and Improvement	35%	45%	14%	37%	15%	29%	41%	50%	30%
User Monitoring and Enablement	35%	50%	38%	29%	19%	35%	45%	49%	20%

	Total (n=373)	AU (n=22*)	CEE (n=21*)	Germany (n=38)	LATAM (n=26*)	MEA (n=31)	UK (n=29*)	US (n=80)	WE (n=70)
Training on Azure or Microsoft Security Products or Services	33%	32%	24%	32%	15%	45%	14%	46%	34%
Device Procurement and Deployment	33%	32%	19%	47%	15%	29%	52%	39%	30%
Data Classification and Data Governance	32%	36%	10%	29%	35%	32%	45%	46%	26%
Incidence Response Management	32%	36%	14%	34%	8%	39%	45%	44%	21%
User Training and Customer Self-Serve Portal	31%	55%	19%	34%	12%	29%	28%	40%	29%
Security Operations Center Management	30%	36%	24%	37%	15%	45%	38%	36%	23%
Penetration Testing	25%	23%	10%	24%	23%	26%	24%	39%	20%
Productivity Cloud App Usage Management	23%	27%	19%	21%	23%	26%	28%	31%	16%
Security Penetration Testing	23%	23%	14%	13%	15%	32%	24%	34%	17%
CISO or Security Analyst as a Service	21%	23%	10%	16%	15%	19%	21%	36%	17%
Custom Application Development	21%	14%	14%	34%	23%	19%	10%	30%	13%
We do not offer any of these project services	2%	--	5%	3%	8%	--	7%	3%	--

Source: Microsoft Cloud Practice Development Study, MDC Research, June 2020

> “
>
> Our biggest success basically is that we introduce, or we analyze our customers’ security level by implementing or by taking them through a secure score analysis, and based on that, doing all different sorts of recommendations.
>
> **DANNY BURLAGE,**
>
> Founder & CTO Wortell

Enable and support deployment

Offer a set of project services and capabilities that enable customer use of identity products and cloud services and offer deployment support.

Ten key capabilities for identity and access management practices:

1. Improve user experience by enabling hybrid identity

Today, businesses, and corporations are becoming more and more a mixture of on-premises and cloud applications. Users require access to those applications both on-premises and in the cloud. Managing users both on-premises and in the cloud poses challenging scenarios. Microsoft's identity solutions span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorization to all resources, regardless of location. We call this hybrid identity.

Resources:

- Azure AD Connect: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect
- What is hybrid identity: What is hybrid identity with Azure Active Directory? | Microsoft Docs
- Password hash synchronization: What is password hash synchronization with Azure AD? | Microsoft Docs
- Pass-through Authentication: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta
- Federation with Azure AD: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

2. Improve security and user experience using passwordless authentication

Azure AD provides ways to natively authenticate users, using passwordless methods that simplify the sign-in experience and reduce risk of attack. Safeguard customers with a seamless identity solution and bring them into the future with passwordless authentication. New standards like Web Authentication API (WebAuthN) and Fast Identity Online (FIDO2) are enabling passwordless authentication across platform

Resources:

- Why Passwordless: Use passwordless authentication to improve security – Microsoft Security
- 10 Reasons to Love Passwordless: 10 Reasons to Love Passwordless #10: Never use a password – Microsoft Tech Community
- Choose the right passwordless technology: Multi-Factor Authentication (MFA) – Microsoft Security
- Whitepaper: RE2KEup (microsoft.com)
- Deployment Guidance: MyIgnite – Ask the Experts: Deploying secure passwordless solutions (microsoft.com)
- Documentation: Azure Active Directory passwordless sign-in | Microsoft Docs

3. Deploy resilient identity Infrastructures with AzureAD

Identity and access management (IAM) is a framework of processes, policies, and technologies that facilitate the management of identities and what they access. It includes the many components supporting the authentication and authorization of user and other accounts in the system. IAM resilience is the ability to endure disruption to system components and recover with minimal impact to the business, users, customers, and operations. Reducing dependencies, complexity, and single-points-of-failure, while ensuring comprehensive error handling will increase resilience.

Resources:

- Building resilience: Building resilient identity and access management with Azure Active Directory | Microsoft Docs
- Infrastructure Resilience: Build resilience in your IAM infrastructure with Azure Active Directory | Microsoft Docs
- Application Resilience: Increase resilience of authentication and authorization applications you develop – Microsoft identity platform | Microsoft Docs
- Customer Identity and Access Management (CIAM) Resilience: Building resilient identity and access management with Azure Active Directory | Microsoft Docs
- Build resilience by using Continuous Access Evaluation: Build resilience by using Continuous Access Evaluation in Azure Active Directory | Microsoft Docs

4. Secure access to all applications using AzureAD

Azure AD must be configured to integrate with an application. In other words, it needs to know what apps are using it for identities. Making Azure AD aware of these apps, and how it should handle them, is known as application management. The growth in app usage with Azure AD shows that organizations are connecting more apps to single sign-on. While this provides seamless and secure access to more apps, the best experience will come from connecting all apps to Azure AD so people can complete all work-related tasks from home and stay safer during the pandemic. Connecting all apps to Azure AD also simplifies the identity lifecycle, tightens controls, and minimizes the use of weak passwords.

Resources:

- Application Management: What is application management in Azure Active Directory | Microsoft Docs
- The state of apps by Microsoft identity: The state of apps by Microsoft identity: Azure AD app gallery apps that made the most impact in 2020 – Microsoft Security
- AzureAD App Gallery: All products – Microsoft Azure Marketplace
- Migrating applications to Azure Active Directory: Resources for migrating apps to Azure Active Directory | Microsoft Docs
- Azure AD Application Proxy: Remote access to on-premises apps – Azure AD Application Proxy | Microsoft Docs
- Secure hybrid access – Secure legacy apps with Azure Active Directory: Azure AD secure hybrid access | Microsoft Docs
- AD FS migration To Azure AD: Use the activity report to move AD FS apps to Azure Active Directory | Microsoft Docs

5. Choose and build secure-by-design applications

Because attacks on applications are growing, it's important to go a step beyond integrating apps with Azure AD to deploying apps that are secure by design. Build secure authentication into authored apps using the Microsoft Authentication Library (MSAL makes it easy for developers to add identity capabilities to their applications).

Resources:

- Microsoft Authentication Library: Microsoft identity platform overview – Azure – Microsoft identity platform | Microsoft Docs
- Documentation: Learn about MSAL – Microsoft identity platform | Microsoft Docs
- Microsoft Graph: Overview of Microsoft Graph – Microsoft Graph | Microsoft Docs
- Getting Started with Microsoft Graph: Getting Started with Microsoft Graph

6. Reduce risk by implementing Zero Trust environments

The Zero Trust model assumes breach and verifies each request as though it originates from an open network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to "never trust, always verify." Every access request is fully authenticated, authorized, and encrypted before granting access. Micro segmentation and least privileged access principles are applied to minimize lateral movement. Rich intelligence and analytics are utilized to detect and respond to anomalies in real time.

Resources:

- Guidelines: Zero Trust Security (microsoft.com)
- Zero Trust Business Plan: RE4JasW (microsoft.com)
- Azure AD App Proxy: Azure AD Application Proxy now natively supports apps that use header-based authentication – Microsoft Tech Community
- Identity Protection: Enhanced AI for account compromise prevention – Microsoft Tech Community
- Continuous Access Evaluation: Continuous Access Evaluation in Azure AD is now in public preview! – Microsoft Tech Community
- Zero Trust Assessment: Take the Zero Trust Assessment (microsoft.com)
- Deployment Guide: Zero Trust Deployment Center | Microsoft Docs

7. Streamline access management by integrating external identities

Provide seamless and highly secure digital experiences for partners, customers, citizens, patients, or any other user outside the organization with the required level of customization and control. Bring user directories together into one portal to manage access across organizational boundaries.

Resources:

- Consumer Identities with Azure AD B2C: https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview
- Azure AD B2B: What is B2B collaboration in Azure Active Directory? | Microsoft Docs
- Documentation: External Identities documentation | Microsoft Docs
- Access Reviews: https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview
- Access Reviews for guests in all Teams and Microsoft 365 Groups: Access Reviews for guests in all Teams and Microsoft 365 Groups is now in public preview – Microsoft Tech Community
- Frontline workers with simplified and secure access: Azure Active Directory empowers frontline workers with simplified and secure access – Microsoft Security
- External Customer and Partner Identity Management: Azure AD Customer and Partner Identity Management (microsoft.com)

8. Establish Trusted Identities with Verifiable Credentials

Verifiable credentials are the digital equivalent of documents like driver's licenses, passports, and diplomas. In this paradigm, individuals can verify a credential with an ID verification partner once, then add it to Microsoft Authenticator (and other compatible wallets) and use it everywhere in a trustworthy manner

Resources:

- Decentralized Identity: Decentralized identity explained
- Start Here: Announcing Azure AD Verifiable Credentials – Microsoft Tech Community
- Documentation: Introduction to Azure Active Directory Verifiable Credentials (preview) | Microsoft Docs

9. Improve compliance using identity governance capabilities

Securing remote work requires strong authentication and controlling access to resources based on real-time risk assessments. Secure users, govern access with intelligent policies, continuously monitor threats, and take appropriate action. Use real-time machine learning and heuristic signals to automatically protect against compromised identity before granting access to corporate resources.

Resources:

- Govern the identity lifecycle: https://docs.microsoft.com/en-us/azure/active-directory/governance/
- Manage privileged users efficiently and securely: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/
- Secure access to resources through MFA: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks
- Set Conditional Access policies: Azure AD Conditional Access documentation | Microsoft Docs
- Apply Real time Machine Learning: Azure AD Identity Protection documentation | Microsoft Docs

10. Build and verify technical expertise

The following identity certifications are industry-aligned to meet specific job roles and market needs. They don't just assess what individual know, but also their ability to apply what they know to solve real business challenges.

Resources:

1. SC 900: Exam SC-900: Microsoft Security, Compliance, and Identity Fundamentals – Learn | Microsoft Docs
2. SC 300: Exam SC-300: Microsoft Identity and Access Administrator – Learn | Microsoft Docs

> “
>
> Nothing produces more 'aha!' moments than when a customer first sees advanced threat protection block malicious emails that normally would have gone into their inbox.
>
> **BRUCE WARD,**
>
> Vice President of Business Strategy,
>
> Peters & Associates

Managed services offerings

With managed services, partners can help their customers on a regular basis by offering white-glove services. Managed service offerings can span planning and enablement to day-to-day operations and support.

PLANNING	ENABLEMENT	SUPPORT OPERATIONS
• Assess the customer's IT environment and determine risks and policies that are viable security opportunities • Deliver ongoing Security Assessments utilizing Secure Score • Offer customers a roadmap based on their Secure Score mitigation or recommendations • Provide TCO and ROI analysis for moving their security to the cloud	• Migrate workloads to Azure and Microsoft 365 • Remediate security gaps found in the Security Assessment Workshop • Address security needs across enterprise, including on-premises • Optimize security workloads for apps running across on-premises and in Azure and Microsoft 365 cloud environments • Optimize advanced security workloads	• Offer further support while delivering on SLAs and uptime guarantees • Operate and monitor the customer's Azure, Microsoft 365, and hybrid cloud environments • Provide customers with governance over their cloud strategy by managing their policies

The project services discussed earlier are all potential managed services offerings. Beyond those, a managed service provider (MSP) can offer a much broader set of long-term support and consulting offerings.

In the Microsoft Cloud Practice Development Study, partners were asked which managed services they offered within their practices. These longer-term services tend to center around the monitoring, management, and support of customer solutions.

MANAGED SERVICES (n=348)	
Multi-Factor Authentication Enablement	62%
Help-Desk Support	61%
Configuration	60%
Advanced Threat Protection	59%
Desktop & Device Management & Support	59%
Domain Management	59%
Patch Management	57%
Troubleshooting	54%
Active Directory Federation & Management	54%
User Rights & Account Management	51%
Mobile Device Management	51%
New Accounts Added & Removed	48%
Data Migration Management	47%

MANAGED SERVICES (n=348)	
Identity & Access Control Management	45%
Hybrid Environment Support (Basic Infrastructure)	44%
Reactive Help Desk Support	43%
Activity and Log Audit Management	43%
Single Sign-On Management	42%
Password Complexity Management	42%
User Monitoring	41%
Threat Detection, Monitoring & Mitigation (On-Going)	41%
Security Management & Identity Protection	39%
Performance Monitoring and Reporting	39%
Managed Access to Email Groups	39%
Reporting and Analytics	38%
Auditing, Security & Compliance Assessments & Enablement	36%
Cyber Security Risk Assessment	35%
Information Protection Management	34%
Reports and Dashboard Maintenance	33%
Policy Recommendation and Improvement	33%
Data Leakage/Loss Prevention	32%
Incidence Response Management	31%
Security Operations Center Management	28%
Penetration testing	25%
Application Lifecycle Management & Support	24%
Data Classification and Data Governance	24%
Productivity Cloud App Usage Management	23%
CISO or Security Analyst as a Service	22%
Identity as a Service	22%
We do not offer any of these managed services	4%

Source: Microsoft Cloud Security Practice Development Study, MDC Research, July 2020

MANAGED SERVICES BY REGION

	Total (n=348)	AU (n=22*)	CEE (n=20*)	Germany (n=35)	LATAM (n=28*)	MEA (n=29*)	UK (n=27*)	US (n=76)	WE (n=61)
Multi-Factor Authentication Enablement	62%	73%	60%	71%	29%	66%	74%	70%	69%
Help-Desk Support	61%	68%	45%	54%	50%	52%	89%	68%	64%
Configuration	60%	59%	80%	57%	50%	66%	67%	64%	57%
Advanced Threat Protection	59%	55%	50%	51%	43%	79%	67%	64%	57%
Desktop & Device Management & Support	59%	73%	40%	57%	36%	52%	85%	70%	67%
Domain Management	59%	64%	55%	60%	39%	59%	74%	59%	64%
Patch Management	57%	68%	45%	63%	29%	69%	70%	67%	52%
Troubleshooting	54%	59%	40%	49%	39%	62%	63%	68%	52%
Active Directory Federation & Management	54%	50%	45%	57%	39%	41%	63%	58%	59%
User Rights & Account Management	51%	59%	60%	57%	21%	41%	67%	62%	52%
Mobile Device Management	51%	50%	45%	51%	29%	55%	70%	58%	61%
New Accounts Added & Removed	48%	73%	30%	49%	18%	41%	70%	55%	54%
Data Migration Management	47%	41%	50%	46%	39%	45%	52%	53%	41%
Identity & Access Control Management	45%	45%	40%	46%	25%	38%	59%	54%	46%
Hybrid Environment Support (Basic Infrastructure)	44%	50%	30%	51%	32%	45%	59%	45%	44%
Reactive Help Desk Support	43%	68%	30%	43%	25%	41%	67%	49%	41%
Activity and Log Audit Management	43%	41%	50%	31%	25%	41%	56%	42%	43%
Single Sign-On Management	42%	41%	30%	40%	11%	38%	59%	50%	48%
Password Complexity Management	42%	64%	20%	40%	18%	48%	67%	63%	28%
User Monitoring	41%	55%	55%	40%	29%	28%	56%	50%	36%
Threat Detection, Monitoring & Mitigation (On-Going)	41%	55%	20%	37%	18%	45%	52%	62%	30%
Security Management & Identity Protection	39%	36%	25%	37%	25%	41%	52%	51%	38%
Performance Monitoring and Reporting	39%	45%	25%	31%	14%	55%	48%	53%	30%
Managed Access to Email Groups	39%	55%	10%	49%	11%	34%	67%	41%	43%
Reporting and Analytics	38%	32%	30%	31%	25%	41%	44%	54%	34%
Auditing, Security & Compliance Assessments & Enablement	36%	32%	25%	31%	25%	34%	41%	47%	39%
Cyber Security Risk Assessment	35%	41%	15%	37%	32%	38%	48%	45%	25%
Information Protection Management	34%	27%	20%	40%	21%	48%	48%	39%	25%
Reports and Dashboard Maintenance	33%	41%	25%	37%	14%	34%	48%	45%	23%

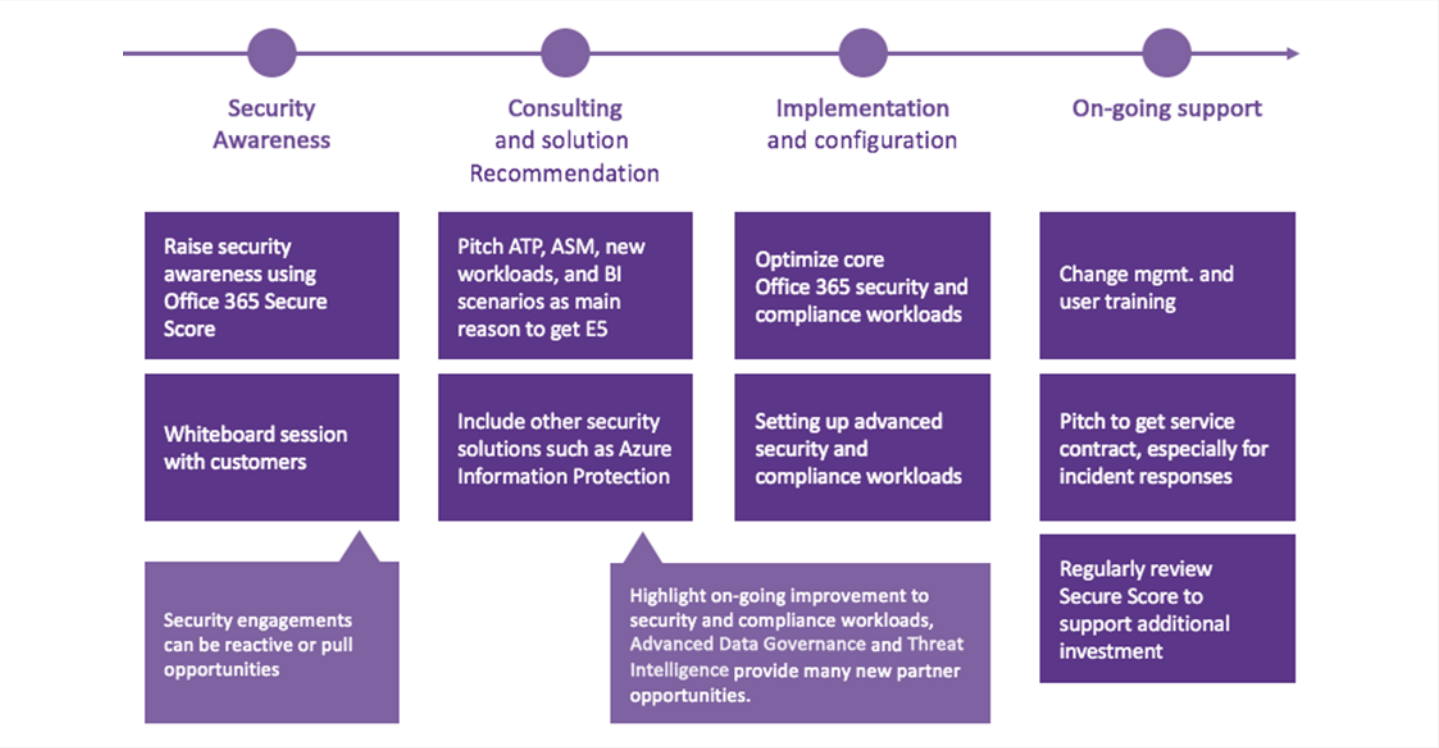
	Total (n=348)	AU (n=22*)	CEE (n=20*)	Germany (n=35)	LATAM (n=28*)	MEA (n=29*)	UK (n=27*)	US (n=76)	WE (n=61)
Policy Recommendation and Improvement	33%	41%	30%	31%	21%	34%	37%	47%	25%
Data Leakage/Loss Prevention	32%	27%	15%	40%	32%	31%	37%	37%	34%
Incidence Response Management	31%	36%	5%	26%	11%	34%	41%	49%	30%
Security Operations Center Management	28%	32%	10%	23%	18%	38%	37%	37%	25%
Penetration testing	25%	27%	15%	17%	25%	45%	30%	30%	20%
Application Lifecycle Management & Support	24%	18%	15%	26%	11%	28%	26%	36%	13%
Data Classification and Data Governance	24%	27%	--	23%	21%	21%	33%	37%	18%
Productivity Cloud App Usage Management	23%	14%	20%	20%	21%	24%	41%	32%	18%
CISO or Security Analyst as a Service	22%	18%	15%	14%	18%	17%	30%	38%	15%
Identity as a Service	22%	14%	25%	23%	11%	21%	19%	29%	21%
We do not offer any of these managed services	4%	--	--	9%	14%	--	4%	4%	2%

Source: Microsoft Cloud Security Practice Development Study, MDC Research, July 2020

When creating managed services, research with partners emphasized the importance of targeting the enterprise customer to attain significantly higher managed revenues.

Going from project services to managed services

Build a practice from providing project services such as assessments and deployments to ongoing managed security services and operational support. This will help create annuity income streams with higher professional services margins.



Security Awareness

Consulting and solution Recommendation

Implementation and configuration

On-going support

Raise security awareness using Office 365 Secure Score

Pitch ATP, ASM, new workloads, and BI scenarios as main reason to get E5

Optimize core Office 365 security and compliance workloads

Change mgmt. and user training

Whiteboard session with customers

Include other security solutions such as Azure Information Protection

Setting up advanced security and compliance workloads

Pitch to get service contract, especially for incident responses

Security engagements can be reactive or pull opportunities

Highlight on-going improvement to security and compliance workloads, Advanced Data Governance and Threat Intelligence provide many new partner opportunities.

Regularly review Secure Score to support additional investment

SEPARATE SECURITY MANAGED SERVICES TEAMS FROM TRADITIONAL IT MANAGED SERVICES TEAMS TO LAND NEW CLIENTS

Separate security services teams can help build a new solution message for an organization. Most partners have a single or integrated team offering managed services and security services.

A few partners are beginning to recognize opportunities to land clients that traditionally would not engage them for traditional managed IT services using security service offerings. Spinning off a separate security services team has allowed these partners to generate a differentiated offering that positions them as experts in the security service space.

Few have separated managed services and security services teams; challenges integrating security into managed services teams center around education.

Because most partners are using the same staff to market and sell security services business as a traditional IT and managed services business, the greatest challenge is ensuring its staff has the right marketing/sales resources and solution knowledge to support a security services conversation.

Compared to many IT offerings today, security services require more intensive education of clients about the risks and solutions available.

Keep in mind that customer conversations and education about security and security services are increasing with C-level or non-technical business decision makers (BDMs), so a different level of information is required to support that interaction.

Security as a managed service

For even the most adept IT and incident response teams, effectively handling patching, malware threats, and intrusion detection can be too difficult to manage without help. Managed service providers can offer services to ensure enterprise customers are secured. But in an age where security breaches are a daily occurrence, how can partners help customers stay ahead of the game, and avoid becoming a statistic?

KEY CUSTOMER CHALLENGES AND QUESTIONS

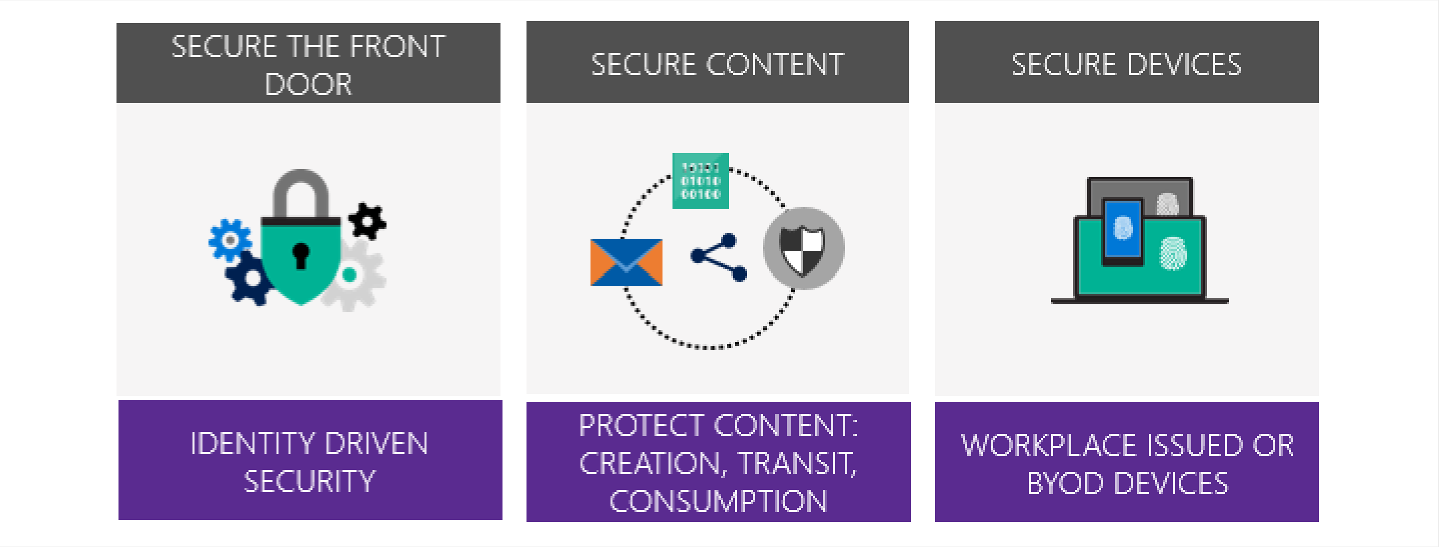
1. Lack of tools and expertise to effectively get ahead of security threats and compliance risks
2. Inability to identify, assess, and mitigate security risks
3. Can detect threats, but are unable to correctly respond in a timely fashion
4. Unfamiliar with security best practices and the overall threat landscape
5. Confusion about myriad offerings available

EXAMPLE OF A SECURITY MANAGED SERVICES OFFERING

BASIC	PRO	PREMIUM
$ per user per month with Microsoft 365	$$ per user per month with Microsoft 365 and EMS	$$$ per user per month with Microsoft 365 Advanced Security & Compliance and EMS
• Plan and deploy Microsoft 365 capabilities • Provide end-user training • Email and data migration to cloud • Deliver end user support and incident management	• Plan and deploy Enterprise Mobility Suite • Increase incident and user support roles • Create monthly services health reports and manage critical IT services dashboards • Enable Advanced Threat Analytics, device management and Identity Management services • + Basic benefits	• Monitor the following services: – SaaS app usage – Top targeted users – Unusual sign-ins – Potential threats – Sensitive information sharing to external users • Manage customer security policies including secure score reports • Support data classification policies • + Pro and Basic benefits

IDENTITY IS FUNDAMENTAL

When considering managed services offerings for a security practice, notice how it helps build a deeper customer relationship. Partners start, metaphorically, by securing the customer's front door by providing identity-driven security. With identity in place, the offer can evolve to securing content (protecting content, managing content creation, transit, and consumption) and securing devices (both workplace-issued devices and staff personal devices).



SECURE THE FRONT DOOR

SECURE CONTENT

SECURE DEVICES

IDENTITY DRIVEN SECURITY

PROTECT CONTENT: CREATION, TRANSIT, CONSUMPTION

WORKPLACE ISSUED OR BYOD DEVICES

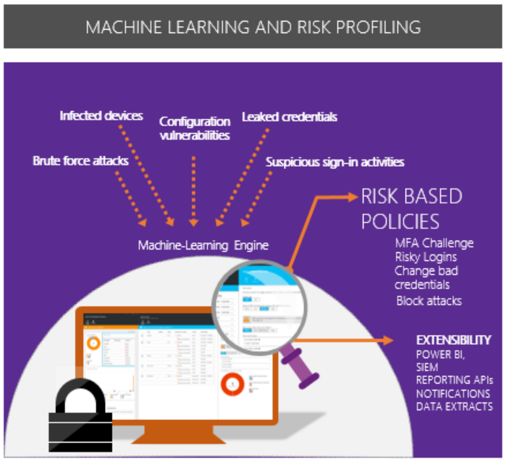
SECURE THE FRONT DOOR

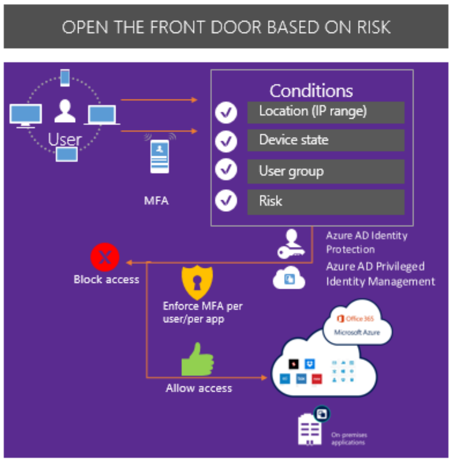
Just like for a house, the front door is where it is decided who to let in. Now, apply that to a customers' data and digital assets. Customers want to be able to answer yes to the following:

- Who is accessing their data?
- Can access to data be granted based on risk in real time?
- Can breaches be discovered and dealt with quickly?

To get to yes, a solution is needed that adapts in a changing environment and learns what is normal credential use from what looks questionable. This occurs when risk-based policies are implemented that are driven by machine learning. The addition of machine learning adds intelligence that lets the system monitor and identify brute force attacks, infected devices, configuration vulnerabilities, leaked credentials, suspicious sign-in activities, sign-ins from atypical locations, or multiple sign-ins from geographically distant locations in less time than the travel would take.

The system detects those types of risk events and assigns a risk level that indicates how strongly an event indicates a compromised identity. With risk level assigned to the risk event detected, risk-based policies can be executed for the detected threat in question. A Multi-Factor Authentication (MFA) challenge could be issued that blocks risky logins or changes credentials known to have been compromised.


MACHINE LEARNING AND RISK PROFILING


OPEN THE FRONT DOOR BASED ON RISK

If this sounds like science fiction, consider this example, which uses machine learning to assign a risk score to a user (e.g., based on intelligence like XYZ), which in turn, is evaluated by a condition that when the risk is determined to be high, the system will mitigate the risk by issuing an MFA challenge. Within Azure Active Directory, the Identity Protection feature can detect the potential vulnerability affecting an organization identity by assigning it a risk level. Automated responses can be configured to detected suspicious actions by their level of risk of compromise using Conditional Access. For example, block access, or allow access but require Multi-Factor Authentication or a password change. A report of the users flagged for risk, the number of risk events triggered, and the status of any remediation actions taken can be reviewed later. Action can be taken to close any listed risk events manually, which can help the machine learning algorithm to improve the classification of similar events in the future.

As an added layer of security, utilize Privileged Identity Management to ensure privileged users (e.g., those with administrator level credentials) must first escalate their user role to admin (referred to as activating the role). Role activation may require approval by other users in the organization and the admin role only applies for a limited window of time.

EXAMPLE COMPONENTS OF AN IDENTITY OFFER

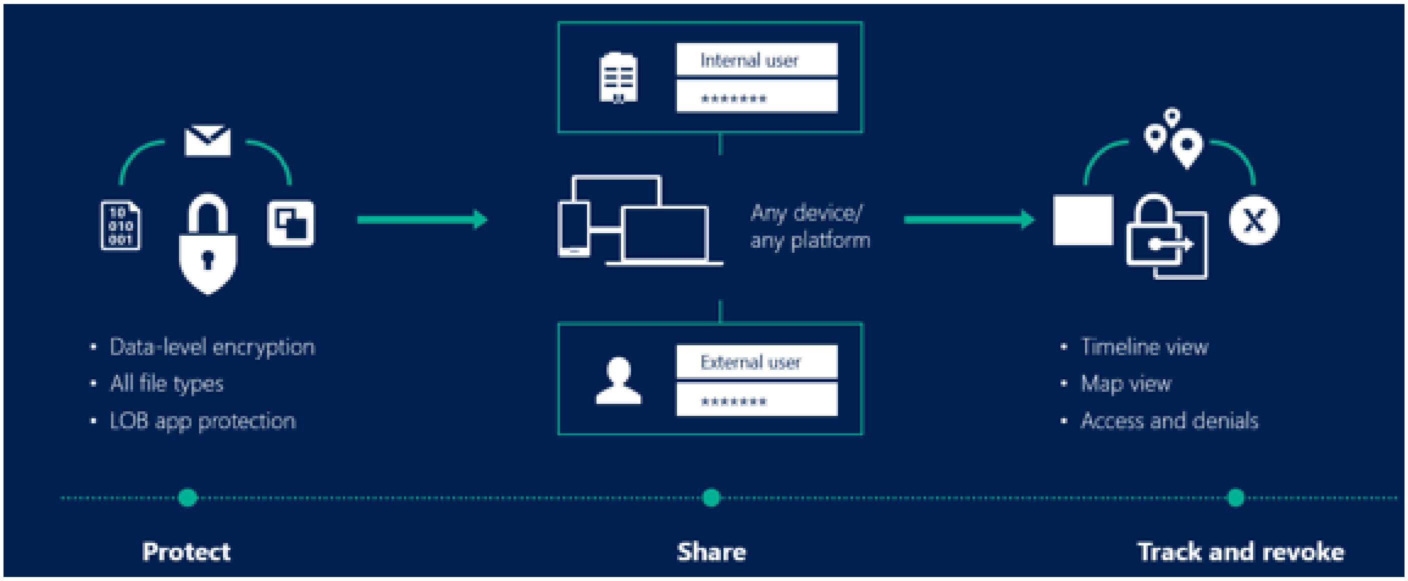
Consider the following table, which provides a sample approach to selling identity-driven security.

Secure the Front Door	Capabilities	Enabling Technologies	Up-sell/Cross-sell
Identity Driven Security	• Risk-based Conditional Access and Multi-Factor Authentication • Advanced security reporting • Identify threats on-premises • Identify high-risk usage of clou apps user behavior, detect abnormal downloads, prevent threat	• Azure Active Directory Premium P2 • Azure Active Directory Premium P1 (included in P2) • Cloud App Security	• No prerequisites. Every organization needs to secure their front door. • Best positioned with: – Business Premium – Microsoft 365 E3 – Microsoft 365 E5 – Azure Deals

SECURE CONTENT

Now that the front door is secured, it is time to focus on securing the contents of the house. Securing content means being able to take a series of steps against the content:

- Define policies, templates and rules for content
- Define exceptions
- Define content classification labels
- Detect the SaaS apps that are in use and assigning them a security risk rating
- Define data copy and usage rules for apps on devices
- Control sharing of data based on identity
- Detect data and users violating content policies
- Take action to maintain the security of content



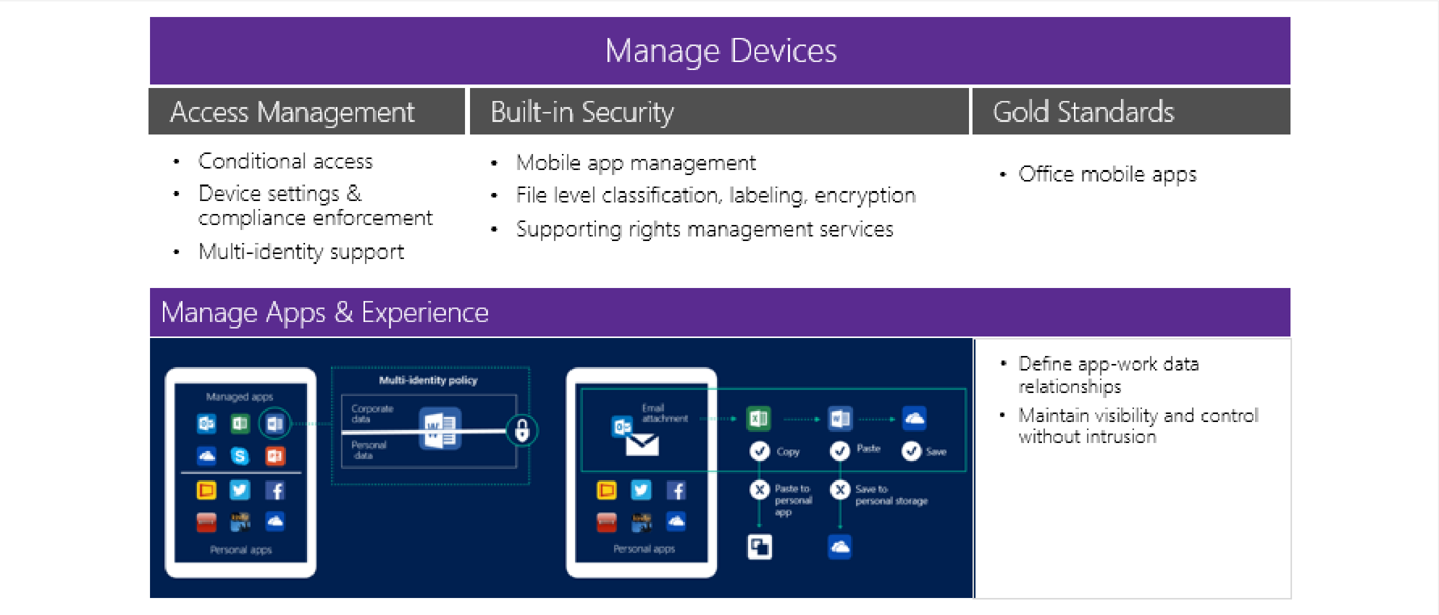
EXAMPLE COMPONENTS WITHIN A CONTENT PROTECTION OFFER

The following table provides a sample approach to selling content protection.

Secure Content	Capabilities	Enabling Technologies	Up-sell/Cross-sell
Protect Content Creation, Transit, and Consumption	• Shadow IT Detection: discovering apps and risk scoring • Intelligent classification and tagging of content • Document encryption, tracking, and revocation • Monitoring shared files and responding to potential leaks • Data segregation at a device/app level	• Azure Active Directory Premium P1 • Cloud App Security • Azure Information Protection P2 • Microsoft Intune	• Prerequisites: access to Office Mobile Apps • Best positioned with: – Business Premium – Microsoft 365 E3 – Microsoft 365 E5

SECURE DEVICES

Devices represent other doors into data and digital assets and need to be secured accordingly. Like the example used in “Secure the Front Door,” the process for securing devices also includes intelligent access management. Conditional Access can be used to restrict access based on the device platform (e.g., iOS, Android) whether, or not, it is enrolled into the mobile device management solution provided by Microsoft Intune. Constraints also can be applied on a per-mobile app basis using the mobile application management capabilities of Microsoft Intune.



Manage Devices

Access Management
- Conditional access
- Device settings & 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 & Experience
- Define app-work data relationships
- Maintain visibility and control without intrusion

EXAMPLE COMPONENTS WITH A DEVICE PROTECTION OFFER

The following table provides a sample approach to selling device protection.

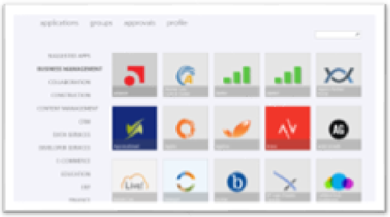
Secure Devices	Capabilities	Enabling Technologies	Up-sell/Cross-sell
Workplace Issued or BYOD Devices	• Conditional access • Device and app access level controls; PIN • Device and app encryption at rest • Save-as, copy, paste restrictions • Device and app level data wipe	• Azure Active Directory Premium P1 • Microsoft Intune	• No prerequisites • Best positioned with: – Business Premium – Microsoft 365 E3 – Microsoft 365 E5

DELIVER A GREAT EMPLOYEE EXPERIENCE

It is no secret that ease-of-use and security are often at odds. In helping secure customers, it is important to also deliver a great experience for the users who will be affected by the security solution deployed. Turn security into an improved experience for a customer's users by enabling capabilities like single sign-on, self-service password reset, and the ability to securely use their own personal devices without IT intrusion.

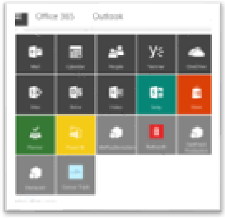
Single Sign-on

- Single sign-on to on-premises, on-Microsoft cloud apps
- Single sign-on to 2700+ non-Microsoft SaaS apps (Dropbox, Salesforce, etc.)



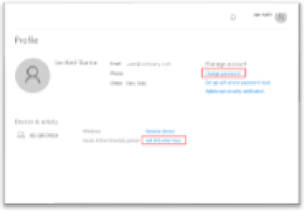
Self-service

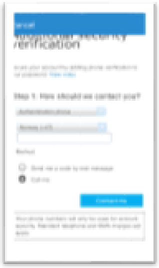
- Reset/change passwords without bothering IT
- Multi-factor authentication
- Work from anywhere
- Pick and choose work apps create, join groups



Work from Anywhere

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





EXAMPLE COMPONENTS OF A GREAT EMPLOYEE EXPERIENCE OFFER

The following table provides a sample approach to a great experience while delivering tight security.

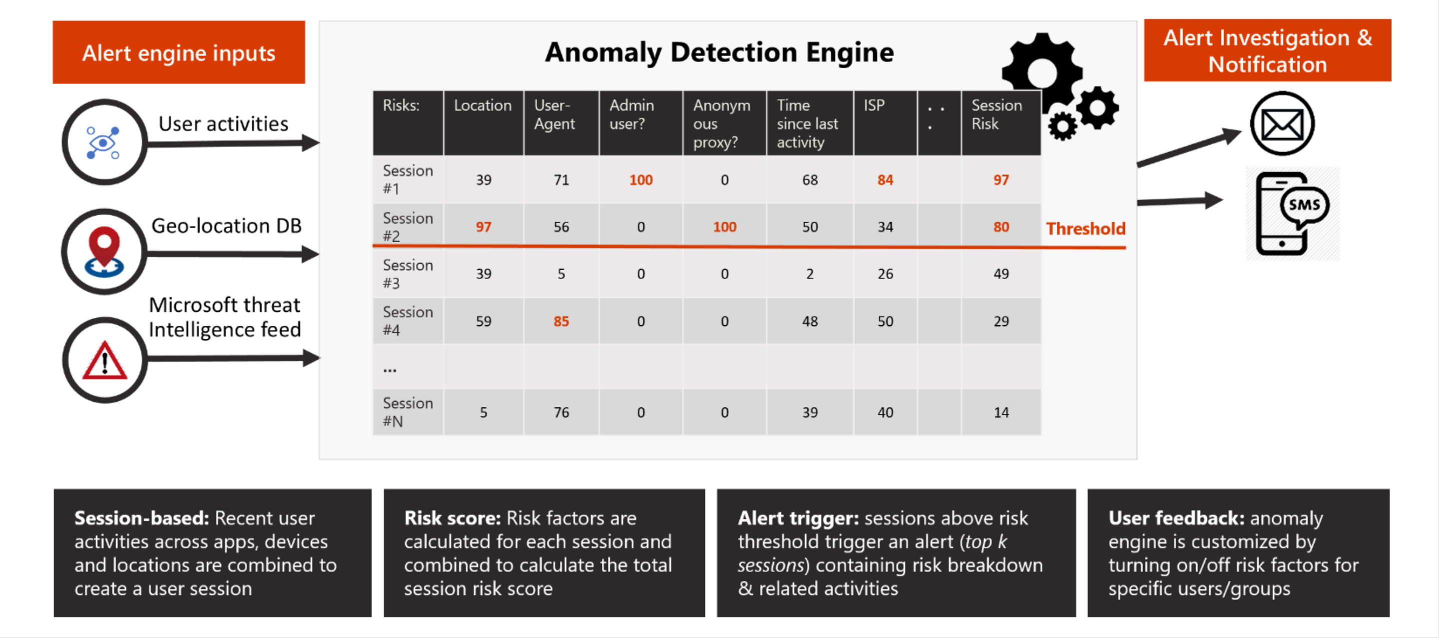
Secure Devices	Capabilities	Enabling Technologies	Up-sell/Cross-sell
Workplace Issued or BYOD Devices	• Conditional access • Device and app access level controls; PIN • Device and app encryption at rest • Save-as, copy, paste restrictions • Device and app level data wipe	• Azure Active Directory Premium P1 • Microsoft Intune	• No prerequisites • Best positioned with: – Business Premium – Microsoft 365 E3 – Microsoft 365 E5

Secure and monitor a customer's Microsoft 365 environment with Microsoft cloud app security advanced security management

Microsoft Cloud App Security advanced security management capabilities provide enhanced visibility and control over Microsoft 365. It increases the security of Microsoft 365 environments by providing:

THREAT DETECTION

Microsoft Cloud App Security enables identification of high-risk user activities and abnormal usage (e.g., impossible travel, logon from unknown or risk IP address, mass downloads by a single user), security incidents, and threats. It provides insights into potential breaches by identifying anomalies in a Microsoft 365 environment, applies behavioral analytics to help assess risk, and leverages Microsoft's Threat Intelligence to identify known attack pattern activities originating from risky sources.



Risks:	Location	User-Agent	Admin user?	Anonymous proxy?	Time since last activity	ISP	. . .	Session Risk
Session #1	39	71	100	0	68	84		97
Session #2	97	56	0	100	50	34		80
Session #3	39	5	0	0	2	26		49
Session #4	59	85	0	0	48	50		29
...								
Session #N	5	76	0	0	39	40		14

Session-based: Recent user activities across apps, devices and locations are combined to create a user session

Risk score: Risk factors are calculated for each session and combined to calculate the total session risk score

Alert trigger: sessions above risk threshold trigger an alert (*top k sessions*) containing risk breakdown & related activities

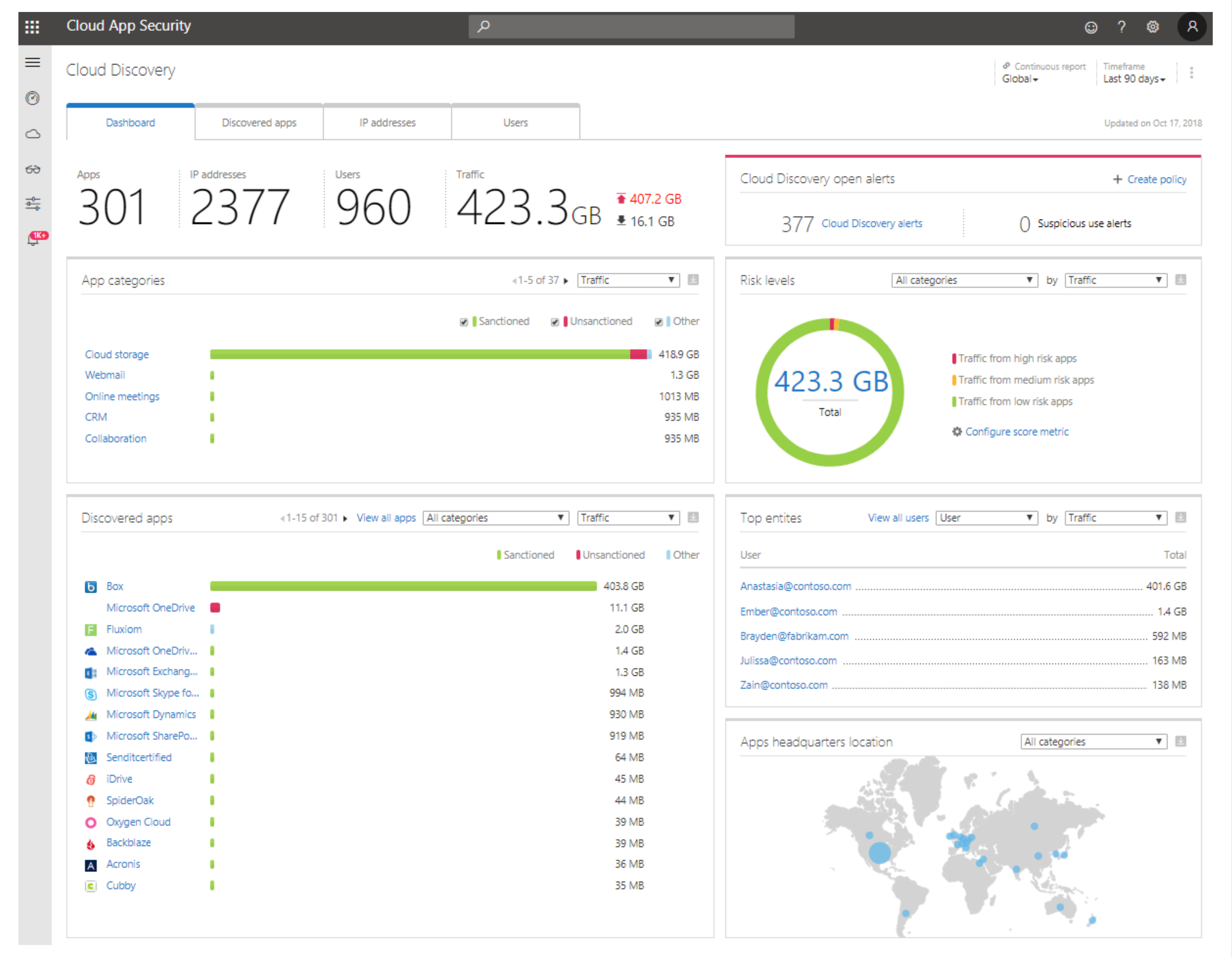
User feedback: anomaly engine is customized by turning on/off risk factors for specific users/groups

ENHANCED CONTROLS

Microsoft Cloud App Security provides both out of the box and customizable policies and provides visibility into violations of those policies as well as supports a response that includes the ability trigger email or SMS text message alerts and automatic remediation (such as by user suspension). Additionally, admins can assess the risk from SaaS apps that have permissions into Microsoft 365 data and remove their rights from a central location.

DISCOVERY AND INSIGHT

Microsoft Cloud App Security enables a view into Microsoft 365 usage via an easy-to-understand dashboard that helps keep tabs on shadow IT by enabling the discovery of more than 1,000 SaaS applications in use on a network.



Cloud App Security

Cloud Discovery

Continuous report: Global | Timeframe: Last 90 days

Dashboard | Discovered apps | IP addresses | Users

Updated on Oct 17, 2018

Apps	IP addresses	Users	Traffic
301	2377	960	423.3GB (↑ 407.2 GB, ↓ 16.1 GB)

Cloud Discovery open alerts — + Create policy

377 Cloud Discovery alerts | 0 Suspicious use alerts

App categories — 1-5 of 37 — Traffic

☑ Sanctioned ☑ Unsanctioned ☑ Other

Category	Traffic
Cloud storage	418.9 GB
Webmail	1.3 GB
Online meetings	1013 MB
CRM	935 MB
Collaboration	935 MB

Risk levels — All categories by Traffic

423.3 GB Total

- Traffic from high risk apps
- Traffic from medium risk apps
- Traffic from low risk apps

Configure score metric

Discovered apps — 1-15 of 301 — View all apps — All categories — Traffic

Sanctioned | Unsanctioned | Other

App	Traffic
Box	403.8 GB
Microsoft OneDrive	11.1 GB
Fluxiom	2.0 GB
Microsoft OneDriv...	1.4 GB
Microsoft Exchang...	1.3 GB
Microsoft Skype fo...	994 MB
Microsoft Dynamics	930 MB
Microsoft SharePo...	919 MB
Senditcertified	64 MB
iDrive	45 MB
SpiderOak	44 MB
Oxygen Cloud	39 MB
Backblaze	39 MB
Acronis	36 MB
Cubby	35 MB

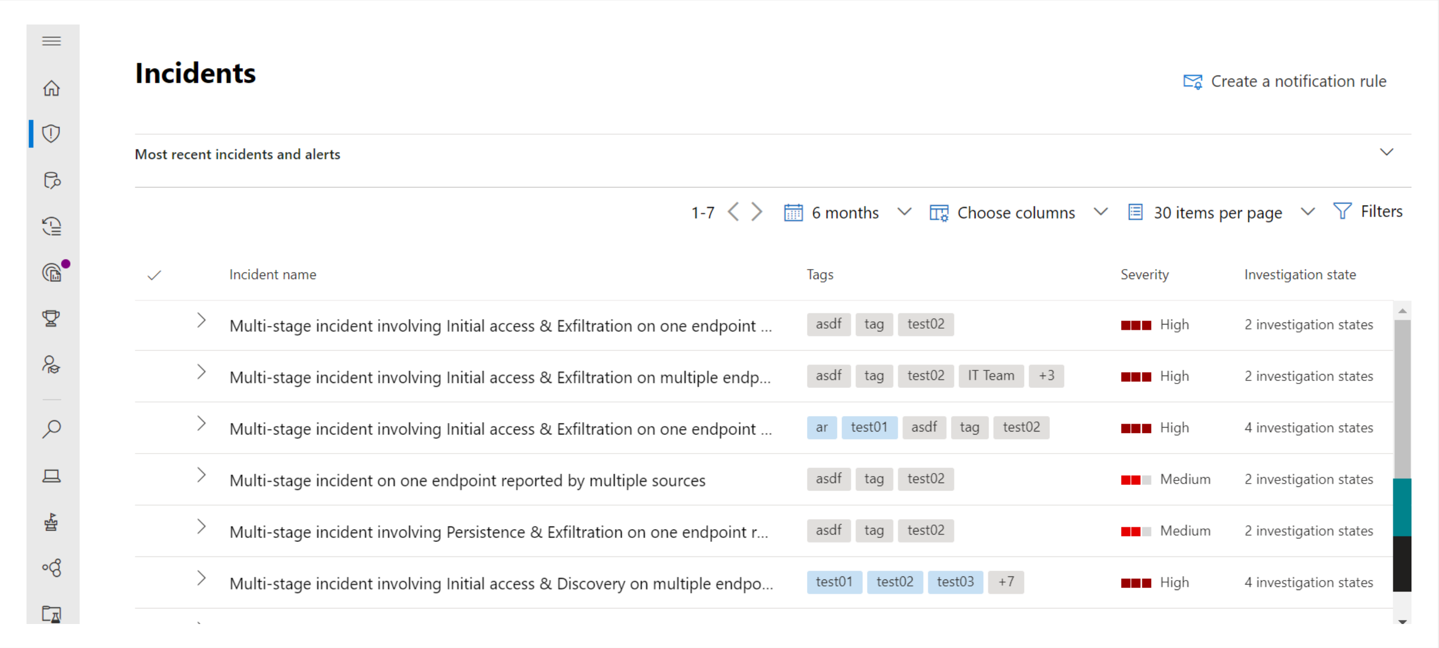
Top entites — View all users — User by Traffic

User	Total
Anastasia@contoso.com	401.6 GB
Ember@contoso.com	1.4 GB
Brayden@fabrikam.com	592 MB
Julissa@contoso.com	163 MB
Zain@contoso.com	138 MB

Apps headquarters location — All categories

ENABLE THREAT ALERTING AND REMEDIATION WITH MICROSOFT 365 DEFENDER

Threat investigation and response capabilities in Microsoft 365 Defender allows partners to take increased control over a Microsoft 365 deployment by enabling full visibility into what threats are in the environment, which users are compromised and what data is at risk. Additionally, Threat analytics provides remediation capabilities for suspicious content.

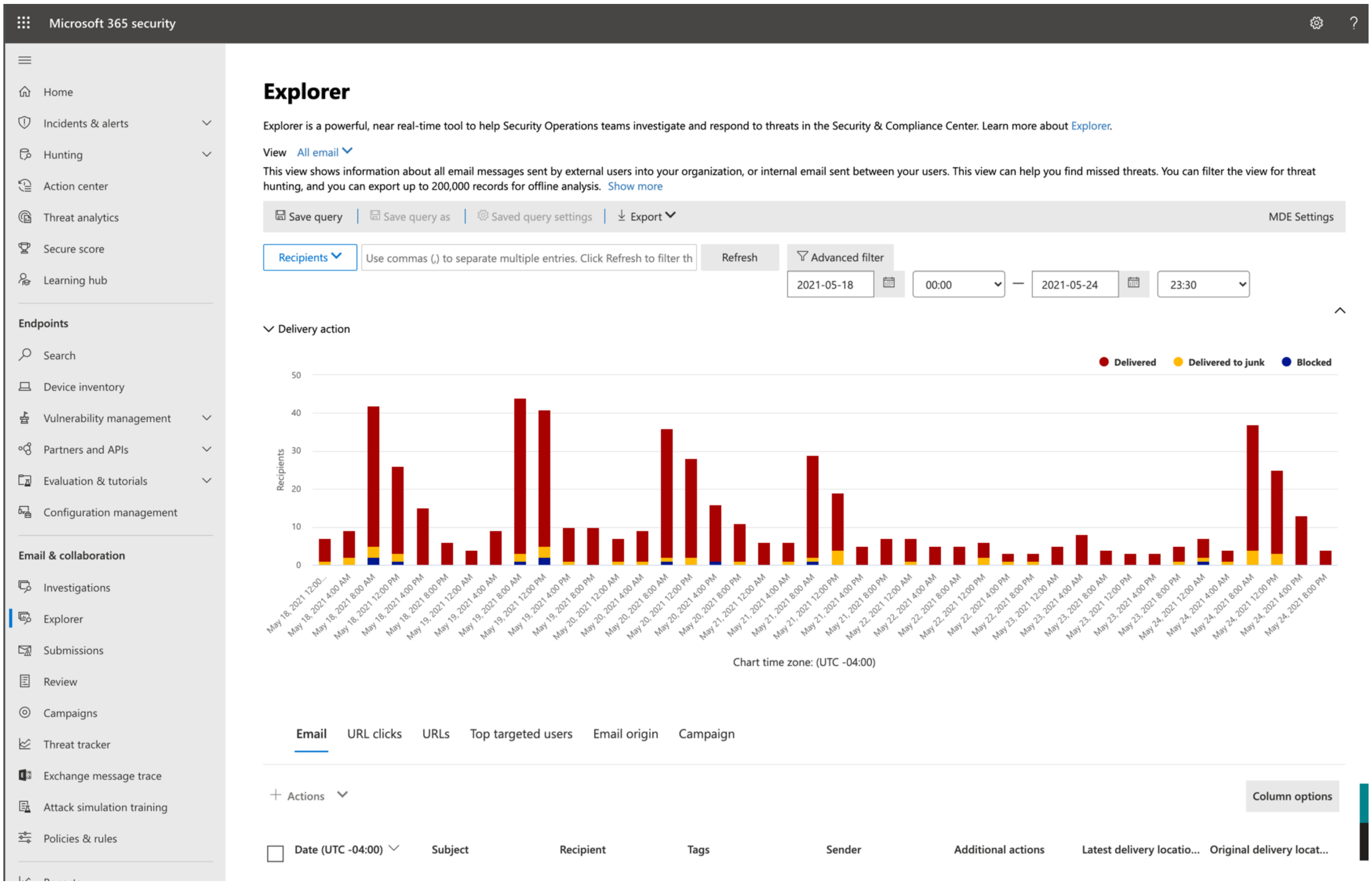


Incidents

✓	Incident name	Tags	Severity	Investigation state
>	Multi-stage incident involving Initial access & Exfiltration on one endpoint ...	asdf tag test02	■■■ High	2 investigation states
>	Multi-stage incident involving Initial access & Exfiltration on multiple endp...	asdf tag test02 IT Team +3	■■■ High	2 investigation states
>	Multi-stage incident involving Initial access & Exfiltration on one endpoint ...	ar test01 asdf tag test02	■■■ High	4 investigation states
>	Multi-stage incident on one endpoint reported by multiple sources	asdf tag test02	■■□ Medium	2 investigation states
>	Multi-stage incident involving Persistence & Exfiltration on one endpoint r...	asdf tag test02	■■□ Medium	2 investigation states
>	Multi-stage incident involving Initial access & Discovery on multiple endpo...	test01 test02 test03 +7	■■■ High	4 investigation states

By collecting rich threat signals from SharePoint, Exchange, OneDrive for Business, Skype for Business and Azure Active Directory, Threat analytics keeps organizations abreast of phishing, malware, and suspicious activity. This threat data is enriched by correlation with security signals from across Microsoft, global targeting data, and actor profiles which give detailed background on threats present in the environment and those actively circulating globally.

Threat analytics provide information into mitigated and potential attacks, as well as investigation tools that allow organizations to explore attack campaigns, people, and data. Threat analytics provides the tools to organize incident response with task-oriented workflows, attack alerts, detailed forensics, and remediation workflows.



Explorer

Explorer is a powerful, near real-time tool to help Security Operations teams investigate and respond to threats in the Security & Compliance Center. Learn more about Explorer.

View All email

This view shows information about all email messages sent by external users into your organization, or internal email sent between your users. This view can help you find missed threats. You can filter the view for threat hunting, and you can export up to 200,000 records for offline analysis. Show more

Save query | Save query as | Saved query settings | Export MDE Settings

Recipients | Use commas (,) to separate multiple entries. Click Refresh to filter th | Refresh | Advanced filter

2021-05-18 00:00 — 2021-05-24 23:30

Delivery action

Chart time zone: (UTC -04:00)

Explorer lets organizations to interactively navigate a timeline view of threats and get more details on detected threats.

For a given threat, administrators can drill into the threat to get documentation on the threat, the users affected by that threat and the technical details of the threat (such as threats often associated with the selected threat).

Additionally, Microsoft 365 Defender integrates with Microsoft Defender for Endpoint—when threats are detected on individual devices these signals are shared with Microsoft 365 Defender so it can take appropriate action to protect other users and devices from the detected threat. For example, if a suspicious activity was detected by Microsoft Defender for Endpoint that resulted from opening an email with Outlook, this signal is shared with Microsoft 365 which automatically blocks all emails having a similar attachment.

ENABLE POST BREACH DEFENSES AS A SERVICE WITH MICROSOFT DEFENDER ADVANCED THREAT PROTECTION

Traditional threat detection focuses on the datacenter and firewall, but device endpoints are often the weak link in the system. Microsoft 365 Defender layers on to Windows 10 devices a monitoring service that helps detect advanced attacks and remediate them.

BUILT INTO WINDOWS

Microsoft Defender for Endpoint is agentless, meaning that there is no additional deployment or infrastructure besides Windows 10. It stays continuously up to date.

STATE OF THE ART BEHAVIORAL DETECTION

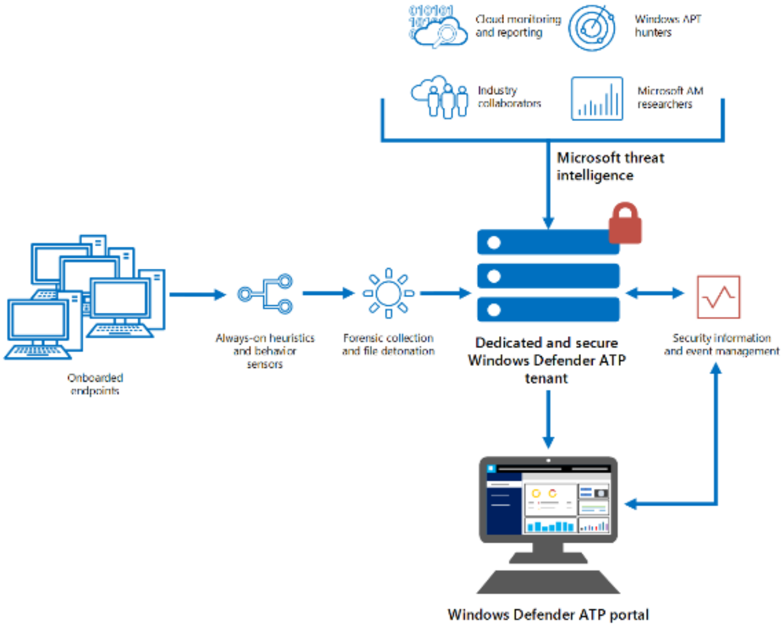
Provides signature-less, intelligent, behavioral, machine learning and past attack detections based on Microsoft's unparalleled optics and security experts.

SOPHISTICATED ANALYTICAL ENGINE

The analytical engine makes it easy to understand the scope of a breach, surfacing data across endpoints with six months of stored log history, presented in a way that shows the evolution of a breach, making it easier to analyze the result.

UNIQUE THREAT INTELLIGENCE KNOWLEDGEBASE

The cloud-based knowledgebase provides threat optics across the world's largest device database, enhanced by 24x7 threat intelligence from both Microsoft and the community of security researchers, as well as third party threat intelligence data to provide detailed actor profiles.


Cloud monitoring and reporting
Windows APT hunters
Industry collaborators
Microsoft AM researchers
Microsoft threat intelligence
Onboarded endpoints
Always-on heuristics and behavior sensors
Forensic collection and file detonation
Dedicated and secure Windows Defender ATP tenant
Security information and event management
Windows Defender ATP portal

THE PARTNER OPPORTUNITY

Microsoft Defender for Endpoint is available with the Identity & Threat Protection offering for customers with Windows 10 E5/A5, Microsoft 365 E5/A5, Microsoft 365 Security E5/A5, and Microsoft Defender for Endpoint licenses. For partners in the Cloud Solution Provider program, this creates multiple opportunities:

- Increase revenue: Drive customers to upgrade from the Windows 10 Enterprise E5 plan to Microsoft 365 E5 license subscription and increase revenue, and the profits that are associated with it.
- Managed service: Provide expert monitoring and remediation using Microsoft Defender for Endpoint as a value-add, managed service to customers. By combining the subscription price of one of the additional plans or E5 plan with the price for the monitoring service, partners can deliver a packaged offer that provides both for one monthly fee to customers.

> “
>
> Customers are asking for more intelligence and insights into threats – it’s something they need and have been asking for constantly. Threat intelligence dashboard is going to be very valuable and will really enhance the solutions we offer.
>
> **ETHAN MCCONNELL**,
>
> Vice President of Olive & Goose

Compliance as a managed service

The adherence to regulatory standards, government regulations, and other industry requirements represents a challenge most customers do not want to face alone—and presents an opportunity for a long-term relationship with partners.

Partners can provide services that help customers to prepare and pre-check for audit, provide compliance auditing services, and help a customer define or implement their compliance strategy.

Partners also can help customers meet general compliance requirements by:

- Driving awareness of how Customer Lockbox can help meet compliance obligations for controlling data access by Microsoft support engineers.
- Enabling full audit tracking to monitor and investigate events related to data.
- Reducing cost and risk with in-place intelligent advanced eDiscovery.
- Equipping customers with the ability to efficiently perform risk assessment with Office 365 Service Assurance.
- Preventing, detecting, and containing internal risks with the insider risk management feature in Microsoft 365
- Managing data retention with Microsoft Information Governance.

In any combination, these make up core components of any compliance-related managed services offer. However, there is an even more critical opportunity on the horizon that motivates building a compliance managed services offering—one that is predicted to create a $3.5 billion market opportunity for security and storage vendors according to IDC.

PRIVACY REGULATIONS

In May 2018, a European privacy law, the General Data Protection Regulation (GDPR) took effect imposing new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents. The GDPR applies no matter where an organization is located.

The California Consumer Privacy Act (CCPA) was enacted in the state of California (CA) in 2018, and is intended to protect the privacy rights for consumers who are residents of CA. In some respects, the CCPA is narrower than GDPR insomuch that it applies to consumers, while the GDPR has a broader context that applies to other end user relationships (such as employees, business associates, and the like). Nevertheless, the CCPA carries similar requirements as GDPR with respect to the general principals of protecting personal information. In general, organizations are subject to CCPA regardless of where they are domiciled if the following conditions are met:

- The organization collects, processes, or stores personally identifiable information (PII) as it is defined under the CCPA regulation; and
- The organization does business in the state of California; and
- The organization has gross annual revenues more than $25M; or
- The organization buys, receives, or sells the personal information of 50,000 or more consumers or households; or
- The organization earns more than half of its annual revenue from selling such information

Customers will need consultants to support the journey to compliance with existing and emerging privacy law. Invariably, the best place to start is performing risk assessments from both a business perspective as well as a technology perspective. Such assistance requires a blended approach to coordinate legal expertise (often from outside specialists), business expertise (typically from the client's internal staff), and technology expertise (the opportunity for partners). Risk assessments must be informed by an understanding of the customer's technology landscape, including on-premises systems, cloud-hosted systems, and – notably – third party service providers.

A technology focused privacy risk assessment should help the customer identify:

- Privacy definitions germane to the jurisdictions in which the customer conducts business
- The nature of personal data that is collected, processed, or stored
- Where such information is stored (both logically and physically)
- How it is protected in-transit, in-use, and at-rest
- How it is shared within the company (e.g., between business units)
- How it is shared with entities outside of the company (e.g., by third party service providers)

Partners can conduct gap assessments that identify privacy "hot spots" and make recommendations on technology, people, and processes that customers will need to address to achieve regulatory compliance with applicable privacy laws.

Both the GDPR and CCPA are intended to provide respective constituents with more control over "personal data" (which is precisely defined by the in the respective regulations). Both regulations also seek to ensure personal data is protected no matter where it is sent, processed, or stored. And both regulations are intended to explicitly protect the rights of the constituents, such as:

- The right to know what personal data is being collected about them
- The right to know whether personal data is sold or disclosed, and (importantly) to whom
- The right to say "no" to the sale of personal data
- The right to access any personal data that has been previously collected
- The right to request that personal information be deleted (also referred to as "the right to be forgotten")
- The right to be free from discrimination for exercising privacy rights

Both regulations contain many requirements about the collection, storage and use personal information. This means not only how to identify and secure the personal data in organizational systems, but also how to accommodate new transparency requirements, detect and report personal data breaches, and train privacy personnel and employees. The table below shows the considerations and provisions that must be made to remain compliant with either or both regulation(s):

PERSONAL PRIVACY	CONTROLS & NOTIFICATIONS	TRANSPARENT POLICIES	IT & TRAINING
Individuals have the right to: Access personal data Correct errors in personal data Erase personal data Object to processing of personal data Export personal data	Strict security requirements Breach notification obligation Appropriate consents for data processing Confidentiality Record keeping	Transparent and easily accessible policies regarding: Notice of data collection Notice of processing Processing details Data retention/deletion	Need to invest in: Privacy personnel and employee training Privacy policies Designated privacy office/ officer Legal Counsel Privacy Impact Assessments Third-Party Risk Assessments that cover privacy matters

Failure to comply with either regulation could prove costly, as companies that do not meet the requirements and obligations could face substantial fines and reputational harm. Companies can be fined substantially for failure to meet certain requirements of either regulation. Additional individual remedies could increase their risk if they fail to adhere to privacy requirements.

THE PARTNER OPPORTUNITY

GDPR applies to companies that trade products or services with European customers or in European market, creating the potential for a global impact. CCPA applies to companies that conduct business in the state of California, but several other states have already passed similar legislation, or have taken up bills in their legislatures which will only increase the complexity and burden of privacy compliance. As a result, there will be a serious resource shortfall of Privacy Professionals—a perfect opportunity for partners to pick up the slack.

Privacy protection requires privacy-by-design and by-default and brings with it inherent operational complexity. Partners can become privacy consultants or implementers to support the customer privacy journey.

The significant fines imposed for non-compliance could put many companies out of business. This means customers should be motivated to achieve compliance. With those motivators in mind, here are 4 opportunities for partners:

GLOBAL & US-MARKET IMPACT	OPERATIONAL COMPLEXITY	SIGNIFICANT FINES	NEED FOR PRIVACY PROFESSIONALS
GDPR applies to companies that trade products or services with European customers or in European market. CCPA applies to companies that do business in CA.	Requires privacy-by-design and by-default. Partners can become privacy consultants or implementers to support customer privacy journey.	Fines for non-compliance can be up to 4% of global revenues or €20 million, whichever is greater. CCPA can result in class action statutory damages between $100 to $750 per CA resident; and $7,500 ***for each*** intentional violation and $2,500 ***for each*** unintentional violation (note that a violation is ***per CA resident***). Fines of these magnitudes could be an existential threat to many of the organizations covered by the regulations.	There will be a serious resource shortfall of privacy professionals. Professional services vendors will pick up the slack.

To plan accordingly, here are five Microsoft-recommended steps to provide effective services to customers:

GLOBAL MANDATE	The large number of firms doing business in the European and US markets or covered constituents are tackling privacy rules. Microsoft cloud services and a partner's privacy-related services can be critical to compliance.
PRIVACY-BY-DESIGN	Partners can work closely with security leaders to provide privacy assessments and determine how Microsoft cloud services and partner services can enable customers to meet privacy-by-design requirements.
DATA BREACH NOTIFICATION	With 72-hour data breach notification, partners can utilize Microsoft cloud services to become an incident response (IR) orchestrator through managed services or professional services.
DATA PRIVACY OFFICER (DPO)	The demand for privacy officers is creating a serious shortfall of privacy skills. Partners can consider providing "Privacy Officer as a Service" to customers.
EVIDENCE OF RISK MITIGATION	Organizations must demonstrate that they have implemented appropriate measures to mitigate privacy risks. Partners and customers can use Microsoft cloud services to build evidence of mitigation strategies and controls.

Five key reasons

Why should partners utilize Microsoft Solutions for Privacy Compliance

1. Microsoft was the first major cloud services provider to pledge GDPR compliance
2. Microsoft has been an industry leader on Model Clauses, HIPAA, ISO 27018, and is taking a similar lead on GDPR and CCPA compliance
3. Microsoft offers the most comprehensive set of compliance capabilities of any major cloud service provider and has the best baseline to build from
4. Microsoft provides a single stack solution—all pieces work well together
5. Microsoft's compliance solutions enable multi-cloud compliance to integrate with customers' existing security and compliance investments

RESOURCES:

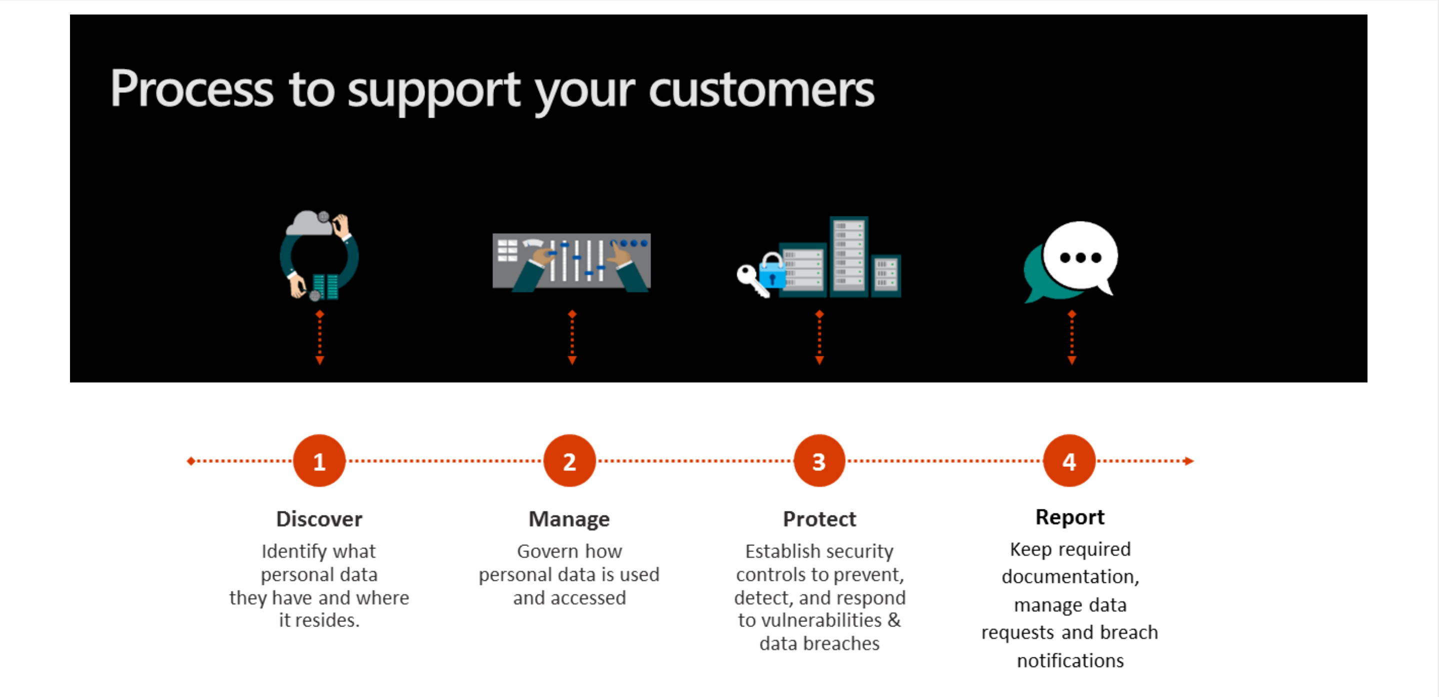
- GDPR accountability checklists
- Beyond GDPR: How to respond to ever-changing regulatory requirements (eBook)
- Get a compliance score with Compliance Manager
- GDPR frequently asked questions

TAKE A PLATFORM APPROACH

Rather than track the controls required by individual standards or regulations on a case-by-case basis, a best practice is to identify an overall set of controls and capabilities to meet these requirements. Likewise, rather than assessing individual technologies and solutions against a comprehensive regulation, taking a platform view—such as one encompassing Windows, Microsoft SQL Server, SharePoint, Exchange, Microsoft 365, Azure, and Dynamics 365—can provide a clearer path to ensure a customer complies not only with relevant privacy regulations, but also with other data protection requirements important to the customer as well.

THE PROCESS FOR SUPPORTING CUSTOMERS WITH PRIVACY COMPLIANCE

The following illustration summarizes a step-by-step process that can be used as a foundation helping customers towards privacy compliance.



Process to support your customers

1 **Discover**
Identify what personal data they have and where it resides.

2 **Manage**
Govern how personal data is used and accessed

3 **Protect**
Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches

4 **Report**
Keep required documentation, manage data requests and breach notifications

NEXT STEPS FOR PARTNERS

Follow this checklist:

☑ Determine if privacy compliance is needed. If so, act now.

☑ Learn more about the technology ramifications of privacy regulations and Microsoft Security offerings using the Trust Center.

☑ Pilot services and offerings with a few customers before going broad.

Support as a managed service

No matter how well a cloud or hybrid environment is planned, provisioned, operated, or monitored, problems will arise, and those problems will need to be remediated. It's the managed service provider's job to offer support to customers to deal with outages, breaches, inefficiencies, and disaster scenarios. Managed service providers need to consider the level of support that makes sense for their practice—in terms of resources and revenue—as well as what makes sense to customers.

KEY SERVICES FOR THIS OFFERING

- **User support:** Provide support for frequently asked questions, setup and usage, best practices, questions around billing and invoicing, break-fix support for developers, architecture design, and solution design support for architects.
- **System support:** Provide customers with information on any service interruption, and relay expectations on when the system will be back online.
- **Product support:** Provide support when the Microsoft product is not working as expected or the service stops working. Escalate to Microsoft when the issue cannot be resolved with existing documentation and/or training.
- **Extended support hours:** Many customers need the ability for 24/7 support but cannot justify the overhead internally.
- **Account management:** Offering an account manager that is responsible for reporting service consumption and ultimately minimizing time to resolution is a service that can be offered at a premium.
- **Dedicated support:** The value add of a dedicated support team cannot be understated. Engineering resources that already know the customers' environment, including the business and technical reasons for how a solution was implemented can add a tremendous value over the lifetime of an agreement.

Cloud monitoring services

While Azure offers many monitoring capabilities built within the platform, there is still a place for partners who provide additional, deeper monitoring tooling, triage the false positives from the real alerts and proactively act upon the alerts before any measurable loss in performance.

KEY SERVICES FOR THIS OFFERING

SYSTEM HEALTH MONITORING	LOG ANALYTICS AND ALERTING	DATABASE MONITORING	APP PERFORMANCE MONITORING
Complete monitoring of VMs, CPU utilization, memory usage, storage IOPs, and OS performance. Includes monitoring of application performance and operation health, and dashboards and reports on system health.	Every client, device, and user accessing a network produces data that is logged. Analyzing those logs can offer deep insight into performance, security, resource consumption, and several other meaningful metrics.	A view into the customer's database that helps MSPs ensure high availability of database servers. The process involves keeping logs of size, connection time and users of databases, analyzing use trends, and leveraging data to proactively remediate issues.	End-to-end tracking of all aspects of an application (or webpage). App monitoring involves watching every part —from shopping carts to registration pages—of a customer's app(s) for performance issues to provide the best user experience possible.

RESOURCES

- Azure Advisor
- Azure Application Insights
- Azure Diagnostics
- Azure Monitor Log Analytics
- System Center
- Automation

THIRD-PARTY RESOURCES

- App Dynamics
- Nagios
- New Relic
- Science Logic
- Splunk
- Logic Monitor

Creating intellectual property in a security practice

Productizing IP and creating repeatable processes has been a very successful strategy for many partners. Some partners are achieving gross margins higher than 70% by productizing IP and selling it to customers on a recurring revenue basis. Productizing IP helps create stickiness with customers and opens opportunities to sell solutions through the partner channel.

Review successful projects to see if there are repeatable elements that can be productize. Repeatable elements can be about a partner's unique vertical or process best practices, or even focus on common customer pain points. Start small. The IP can be a simple template or just a few lines of code that automates a function in a way the market typically needs.

Partners who do not create IP can look to the partner ecosystem for incremental solutions that can be bundled with Microsoft's offerings to round out the total solution. There are multiple opportunities for building intellectual property that can be used to expedite engagements, or even as an entire engagement.

INTEGRATE SECURITY APIs TO DELIVER HIGH-VALUE INTELLECTUAL PROPERTY

Consider providing customized solutions that provide experiences for customers integrating the Microsoft Graph API (which provides access to data about emails, security events, users, files, and groups), the Office 365 Service Communications API (for reporting on service status), the Office 365 Management Activity API (to retrieve information about user, admin, system, and policy actions and events from Microsoft 365 and Azure AD activity logs), the Microsoft Graph Security API (for monitoring and reporting the secure score), the Azure Consumption API (to monitor usage of Azure resources), and the Azure REST API (for integrating data from and managing Azure services). Use these APIs together to create solutions that provide integrated visualization, customized monitoring, and remediation workflows, and handle vertical-specific workloads.

PACKAGE PROCESSES

Another way that partners are creating IP in security practices is by packaging assessments, documents, and processes into proprietary, reusable components that only they own and can deliver. For example, package a service around security monitoring that relies on the ongoing application and review of Secure Score.

In the Microsoft Cloud Practice Development Study, partners were asked which intellectual property offerings they provide within their practice. The results indicate that partners are customizing key security solutions and providing better user experiences through automation, portals, and dashboards.

Intellectual property services

INTELLECTUAL PROPERTY SERVICES (n=224)	
Threat Detection, Monitoring, and Mitigation Solutions	46%
Identity & Access Control Solutions	42%
Information Protection Solutions	42%
Mobility Solutions	40%
Automation and Scripting	40%
Customer Self-Serve Portals	37%
Auditing Solutions	34%
Pre-Configured Dashboards	23%
Turnkey BI Portals	14%
We do not offer any of these intellectual property services	20%

Security intellectual property services by region

	Total (n=224)	AU (n=11*)	CEE (n=11*)	Germany (n=22*)	LATAM (n=18*)	MEA (n=24*)	UK (n=20*)	US (n=43)	WE (n=40)
Threat Detection, Monitoring, and Mitigation Solutions	46%	45%	45%	36%	28%	75%	60%	49%	35%
Identity & Access Control Solutions	42%	45%	45%	27%	33%	42%	50%	49%	38%
Information Protection Solutions	42%	36%	64%	23%	28%	42%	60%	44%	43%
Mobility Solutions	40%	36%	55%	32%	11%	42%	65%	47%	35%
Automation and Scripting	40%	27%	36%	50%	33%	33%	50%	44%	33%
Customer Self-Serve Portals	37%	45%	27%	27%	17%	50%	40%	44%	35%
Auditing Solutions	34%	36%	45%	18%	33%	33%	50%	35%	25%
Pre-Configured Dashboards	23%	27%	18%	27%	11%	33%	15%	26%	25%
Turnkey BI Portals	14%	9%	18%	14%	6%	25%	10%	16%	10%
We do not offer any of these intellectual property services	20%	27%	9%	32%	28%	8%	10%	21%	25%

Source: Microsoft Cloud Security Practice Development Study, MDC Research, July 2020.

THE MICROSOFT AZURE IP ADVANTAGE

Microsoft Azure IP Advantage program represents the industry's most comprehensive protection against intellectual property (IP) risks. The Microsoft Azure IP Advantage program includes the following benefits:

- Best-in-industry intellectual property protection with uncapped indemnification coverage will now also cover any open source technology that powers Microsoft Azure services, such as Hadoop used for Azure HD Insight.
- Makes 10,000 Microsoft patents available to customers that use Azure services for the sole purpose of enabling them to better defend against patent lawsuits against their services that run on top of Azure. These patents are broadly representative of Microsoft's overall patent portfolio and are the result of years of cutting-edge innovation by our best engineers around the world.
- Microsoft is pledging to Azure customers that if Microsoft transfers patents in the future to non-practicing entities, they can never be asserted against them.

With these changes, Microsoft now offers our customers industry-leading protection against intellectual property risk in the cloud. Learn more at aka.ms/AzureIPAdvantage.

> “
>
> Don't be an ostrich. Cloud makes software your competitive advantage. We have packaged repeatable projects that are focused around rapidly demonstrating value within the cloud and identifying the big transformational opportunities.
>
> **ALEX BROWN,**
>
> CEO, 10th Magnitude

Stay informed on security and compliance matters

The Microsoft Trust Center, Microsoft 365 Security Center, and Microsoft 365 Compliance Center are three resources to be familiar with when defining a security, compliance and identity practice strategy.

Microsoft Trust Center

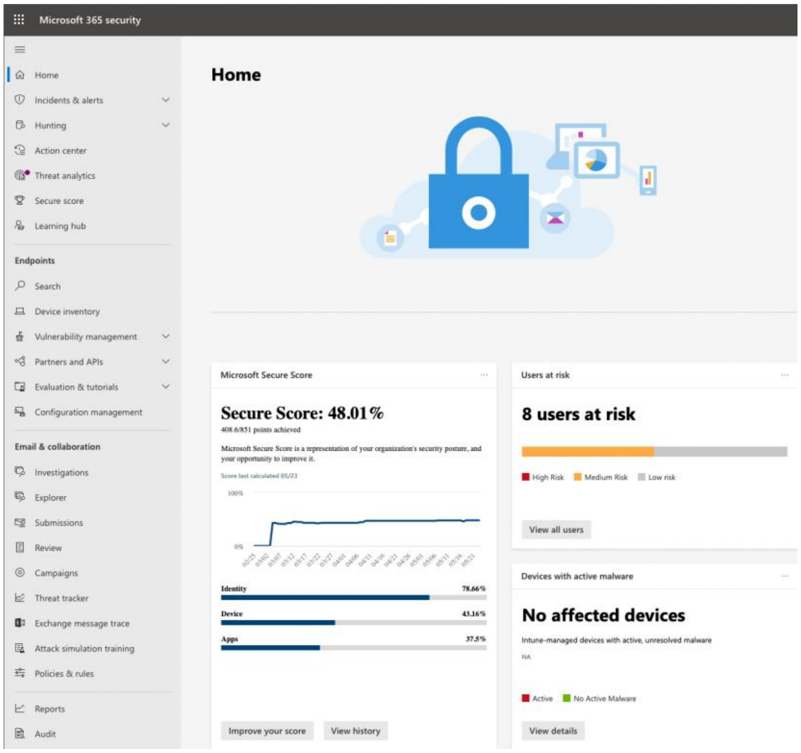
Microsoft Trust Center is a resource for learning how Microsoft implements and support security, privacy, compliance, transparency in its cloud products and services. The Trust Center is an important part of the Microsoft Trusted Cloud initiative and provides support and resources for the legal and compliance community.

THE TRUST CENTER SITE PROVIDES:

- In-depth information about security, privacy, and compliance offerings, policies, features, and practices across Microsoft cloud products.
- Recommended resources, a curated list of the most applicable and widely used resources for each topic.
- Information specific to key organizational roles, including business managers, tenant admins or data security teams, risk assessment and privacy officers, and legal compliance teams.
- Direct guidance and support, including options for contacting Microsoft.

Microsoft 365 Security Center

The Microsoft 365 Security Center is the one-stop portal for securing Microsoft 365. Use it to help get an overview of the security of Microsoft 365, manage & secure endpoints, audit user activity, and ensure services in Microsoft 365 remain secured. Use the Microsoft 365 Security Center to manage security for all services and devices across Microsoft 365 and run attack simulations, track treats, inventory devices, and more.



Secure Score: 48.01%

408.6/851 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 05/23

Identity	78.66%
Device	43.16%
Apps	37.5%

8 users at risk

No affected devices

Intune-managed devices with active, unresolved malware

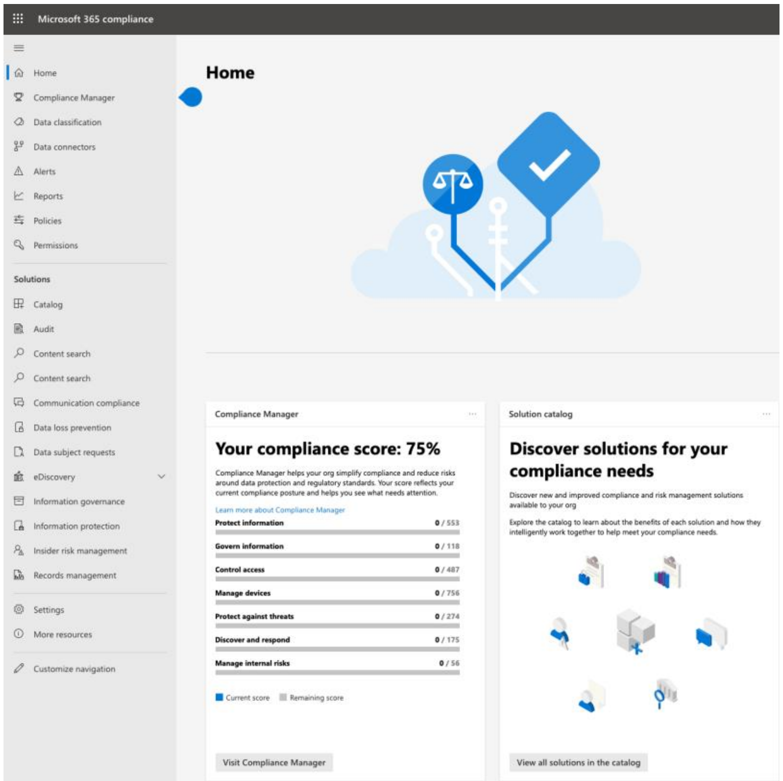
NA

THE SECURITY CENTER INCLUDES CAPABILITIES FOR:

- **Alerts:** View and manage alerts for a Microsoft 365 organization, including Advanced Security Management alerts.
- **Hunting:** Query audit logs to help identify and investigate break activity.
- **Threat analytics:** Manage alerts for any devices compromised by a known threat.
- **Endpoint management:** Device inventory, vulnerability management, connected applications, and configuration management.
- **Investigate and explorer:** Automate investigation and response capabilities as a response to well-known threats and explore logs in near real-time to investigate and respond to threats.
- **Attack simulation training:** Train users by launching various simulated attacks including phishing, brute force, and password spray attacks.
- **Permissions:** Grant permissions to people who perform compliance tasks like device management, data loss prevention, eDiscovery, and retention.

Microsoft 365 Compliance Center

The Microsoft 365 Compliance Center is the one-stop portal for protecting data in Microsoft 365. Use it to help address data compliance needs and to audit user activity in an organization. Use the Microsoft 365 Compliance Center to manage compliance for all data across Microsoft 365 and manage eDiscovery searches and holds, maintain compliance in communications, and more.



Your compliance score: 75%

Compliance Manager helps your org simplify compliance and reduce risks around data protection and regulatory standards. Your score reflects your current compliance posture and helps you see what needs attention.

Learn more about Compliance Manager

Protect information 0 / 553
Govern information 0 / 118
Control access 0 / 487
Manage devices 0 / 756
Protect against threats 0 / 274
Discover and respond 0 / 175
Manage internal risks 0 / 56

■ Current score ■ Remaining score

Discover solutions for your compliance needs

Discover new and improved compliance and risk management solutions available to your org

Explore the catalog to learn about the benefits of each solution and how they intelligently work together to help meet your compliance needs.

THE COMPLIANCE CENTER INCLUDES CAPABILITIES FOR:

- **Alerts:** View and manage alerts for a Microsoft 365 organization, including compliance focused alerts.
- **Permissions:** Grant permissions to people who perform compliance tasks like data loss prevention, eDiscovery, and retention.
- **Search & investigation:** Search for content and review user activity. Use eDiscovery to manage cases and set up supervisory review policies to help capture communication for review.
- **Data loss prevention:** Identify, monitor, and protect sensitive and secure content stored in Microsoft 365 to insure it isn’t shared with the wrong person.
- **Information governance:** Import email from other systems. Enable archive mailboxes or set policies for retaining email and other content within an organization.
- **Information protection:** Label files, emails, sites, and groups that contain sensitive company information to ensure content is protected based on its classification.
- **Records management:** Control the content lifecycle by classifying and retaining required records while regular disposing of records that are no longer required to be retained.
- **Service assurance:** View details about how Microsoft keeps Microsoft 365 customer data safe, and how Microsoft 365 helps customers meet industry compliance requirements.

Microsoft

Hire & Train

Security, Compliance, and Identity

aka.ms/practiceplaybooks

Microsoft Partner Network

Introduction

The previous section looked at the various services that partners can pursue as they set up or build their cloud practice. With avenues of partner success identified, the next step is building and training a team.

This section will offer role definitions and guidance on the skills needed for an application development-focused practice. It will cover the necessary technical, sales, and marketing training, which starts with an assessment of current skills, and a plan for filling the gaps, whether through new hires, contractors, partnering, or training.

To start the hiring processes, there are detailed job descriptions, tips on where to look for resources, the factors to consider in a candidate's skill set, and what to expect to pay by role and region.

A big focus of this section is ensuring all practice resources are trained and continue to receive ongoing training.

RECRUIT, HIRE, ONBOARD, AND RETAIN TALENT PLAYBOOK AND HIRE AND TRAIN GUIDE

Leverage the Microsoft resources available in the Recruit, Hire, Onboard, and Retain Talent playbook and the Hire and Train guide for comprehensive job descriptions and to learn best practices to find the right people, grow their skills, and retain talent.

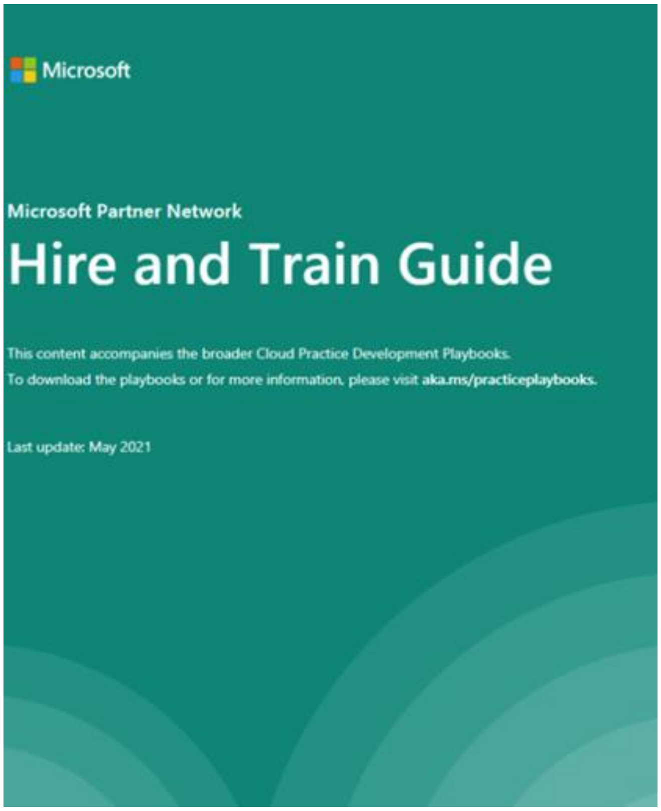
Microsoft

Recruit, Hire, Onboard, and Retain Talent

Microsoft Practice Development Playbook

Published: July 2021

aka.ms/practiceplaybooks



Microsoft

Microsoft Partner Network

Hire and Train Guide

This content accompanies the broader Cloud Practice Development Playbooks.
To download the playbooks or for more information, please visit **aka.ms/practiceplaybooks.**

Last update: May 2021

RESOURCES

- Recruit, Hire, Onboard and Retain Talent Playbook
- Hire and Train Guide

Hire, build, and train the team

Sales resources

Even the best products need a sales strategy to gain maximum market traction. Consider hiring for the following sales positions for broad reach.

ROLE	DESCRIPTION
Solution Sales Manager	A senior leader within the enterprise sales organization that leads, develops, and manages a team of high-performing sales and technical pre-sales/post-sales resources to drive solution opportunity revenue and market share by leveraging the Microsoft cloud offerings to meet their customers' needs. Read the full job description at https://aka.ms/solutionsalesmgr.

Technical resources

These roles form the heart of a partner solution. Hiring the right people can turn vision into reality.

ROLE	DESCRIPTION
Cloud Architect	Drives customer initiatives in collaboration with customers. This role is a technical, customer-facing role that is accountable for the end-to-end customer cloud deployment experience. This role owns technical customer engagement, including architectural design sessions, specific implementation projects, and/or proof of concepts. Read the full job description at https://aka.ms/cloudarchitect.
Mobility Solution Engineer	Responsible for the design, implementation, integration, support, and monitoring of enterprise mobility solutions. The candidate must have prior experience formulating, planning, and implementing a mobile strategy, including formulating policies for the "bring your own device" (BYOD) policy and remote access. Read the full job description at https://aka.ms/mobsolutioneng.
Identity Solutions Engineer	Responsible for securing organizational identities. This includes integration with internal and external applications. This role is responsible for configuring trusts and federation and understanding the various standard authentication protocols like OpenID and OAuth. This role is also responsible for what and how profile information is exposed to applications. Read the full job description at https://aka.ms/idsolutioneng.
Security Architect	The first line of defense in the prevention of hackers, malware, viruses, and other malicious activities. This role is responsible for setting up policies, procedures, guidelines for system access, and ensuring that SIEM systems are monitoring all business-critical applications. This role will interact with the Compliance Officer and Legal team to provide technical guidance on security incidents. Read the full job description at https://aka.ms/secarchitect.

Management

Consider the following management positions if development effort will involve eight or more technical staff. In smaller teams, senior-level employees sometimes take on management duties along with their other responsibilities, removing the need for dedicated managers.

ROLE	DESCRIPTION
Product Manager	Establishes and sustains the business case for the project and plays a key role in identifying and setting priorities across the target audience. This includes ensuring that business expectations are clearly articulated and understood by the project team and that the functional specifications respond to business priorities. This role owns the vision statement for the project. Read the full job description at https://aka.ms/productmgr.
Program Manager	Owns the specification for a solution's features and functionality and coordinates the day-to-day communication required to develop the solution effectively and consistently within organizational standards. This role has a key communication and coordination role with input from other team leads and assists Product Management in articulating the vision for the project. Read the full job description at https://aka.ms/programmgr.

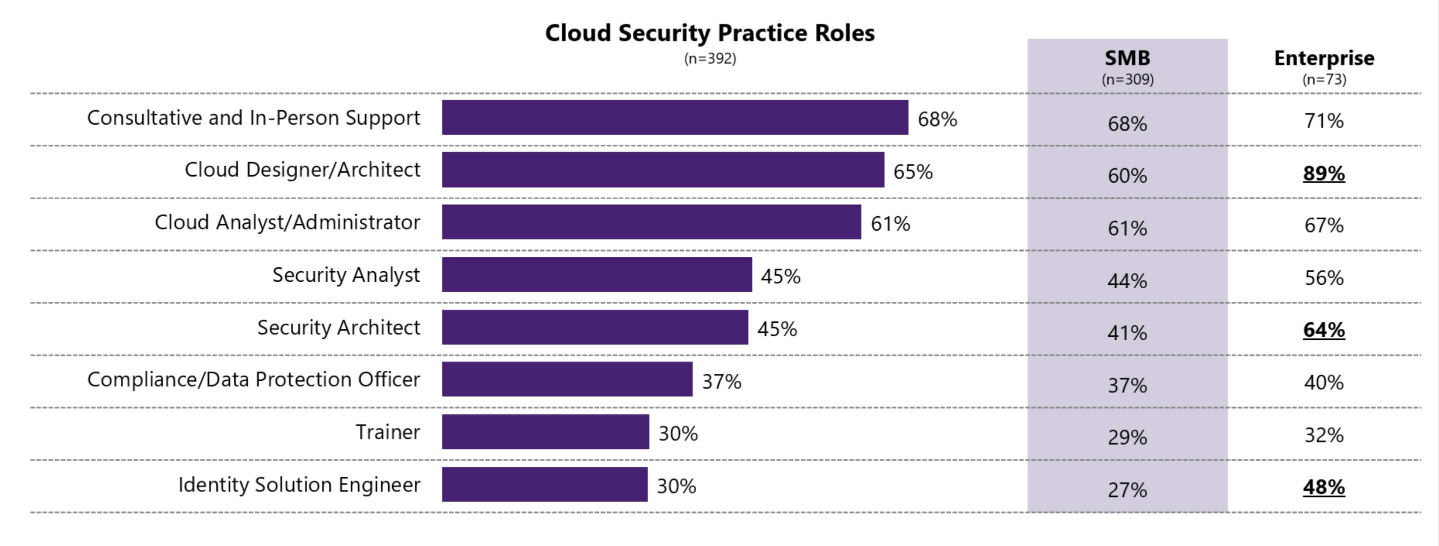
Support resources

A lot of effort goes on behind the scenes, or in positions that involve post-sales customer engagement. To ensure long-term success of projects, consider hiring some of these support roles.

ROLE	DESCRIPTION
Cloud Support Engineer	Assists both internal and external customers who are having technical issues with the product or who need help to realize the full benefit of the solution to help them deliver their cloud-based workloads. Training this role on both the product and the infrastructure on which it is built is paramount to their success, and ultimately, the customers' satisfaction. Read the full job description at https://aka.ms/supporteng.
Security Analyst (Information Security Analyst)	Assess and provide security advice on cloud infrastructure, including network, service, and application components. This role conducts risk assessments, architectural reviews, provides cybersecurity subject matter expertise, and assists in the building and design of secure solutions. Additional duties may include network and application penetration testing, support for cybersecurity investigations, and on-call responses to cybersecurity incidents. Read the full job description at https://aka.ms/security-analyst.
Quality Assurance/ Test Technician	The primary goal of this role is to help avoid defects in the final product or solution. This role will be involved throughout the development process to problem solve and identify technical, procedural, and usability concerns. This role will also coordinate with technical and management teams to ensure that the correct measures are put into place to align the final product with the initial goal. Read the full job description at https://aka.ms/testtechnician.
Support Specialist	Assists customers who are having technical issues with the product, or who need help to realize the full benefit of the solution in delivering their cloud-based workloads. They will likely be able to help customers navigate the operational challenges of cloud computing, so thoroughly training them in both products and the infrastructure is paramount to their success, and ultimately, customers' satisfaction. Read the full job description at https://aka.ms/supportspecialist.
Compliance Officer (Data Protection Officer)	Ensures that data is kept safe and secured throughout the various technology solutions. This role works with internal and external data processors to ensure that legal regulations are followed. This role works with legal bodies and the internal and external legal teams when litigations via lawsuits are involved. This role will also work hand in hand with Security Architects and Analysts to discover, remediate and resolve compliance issues and unauthorized data breaches. Read the full job description at https://aka.ms/compofficer.

Recruiting resources

Consultative/In-Person Support and Cloud Designer/Architect roles exist in two thirds of cloud security practices.



Source: Microsoft Cloud Practice Development Study, MDC Research, June 2020.

Now, what are the most important factors to look for in a potential hire's skillset? Partners were asked this question in a recent practice development playbook survey. The three most important factors were work history, cultural fit, and years of experience.

	TOTAL (n=1136)	**SMB** (n=886)	**ENTERPRISE** (n=250)
Work history	71%	71%	71%
Cultural fit	43%	37%	49%
Years of experience	39%	41%	37%
Referrals	31%	30%	33%
Professional certifications	28%	24%	33%
Professional training received	18%	18%	18%
Contract to hire or other means to test skills "hands-on"	17%	22%	12%
Reputation through community	13%	13%	14%
Formal education	12%	12%	12%
Publications	3%	4%	2%
Awards received	2%	2%	3%
Other	3%	4%	2%

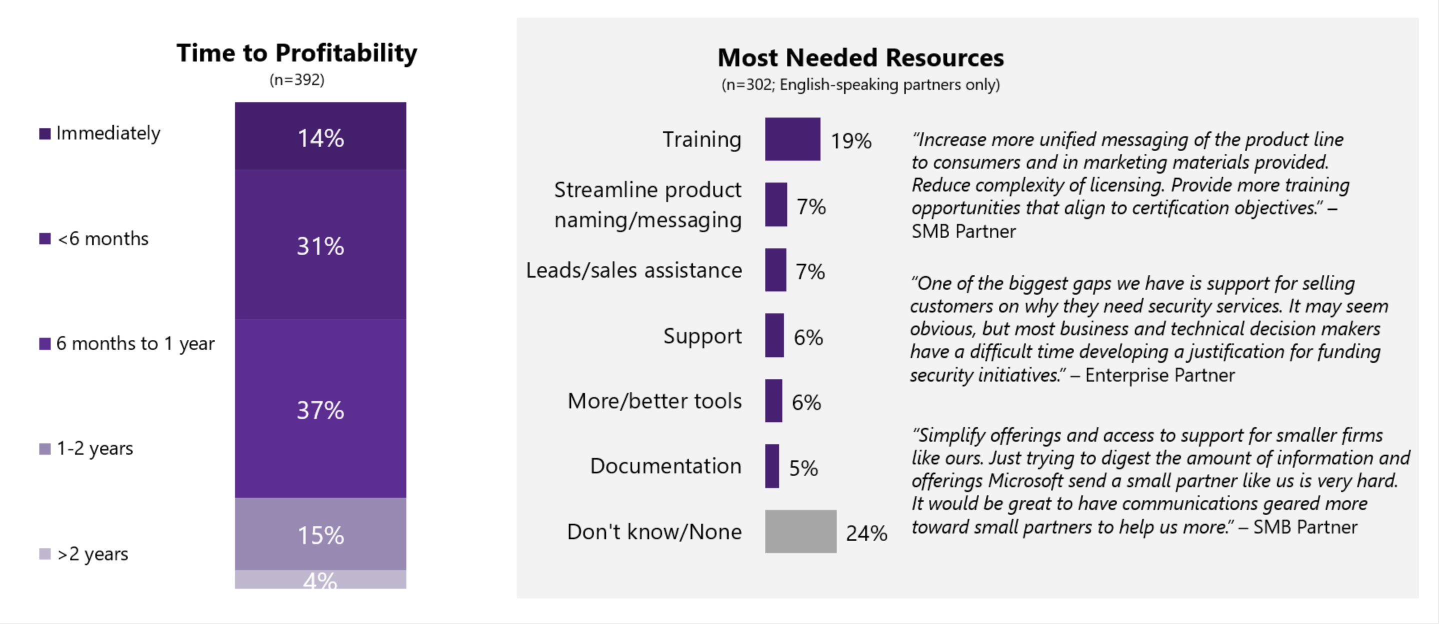
Source: Cloud Application Development and Modernization Playbook Survey, MDC Research, May 2020

Training and readiness

Follow a learning curriculum to build the skills most needed to stay relevant. Fill a skills gap or improve a team’s skill surface area with sales and technical training.

Suggested resources to help onboard employees for training success are available in this section. This includes a range of on-line learning resources for self-paced learning, as well as options for instructor-led training for rapid technology adoption.

One in seven reach profitability on new security offerings immediately; training is the biggest need.



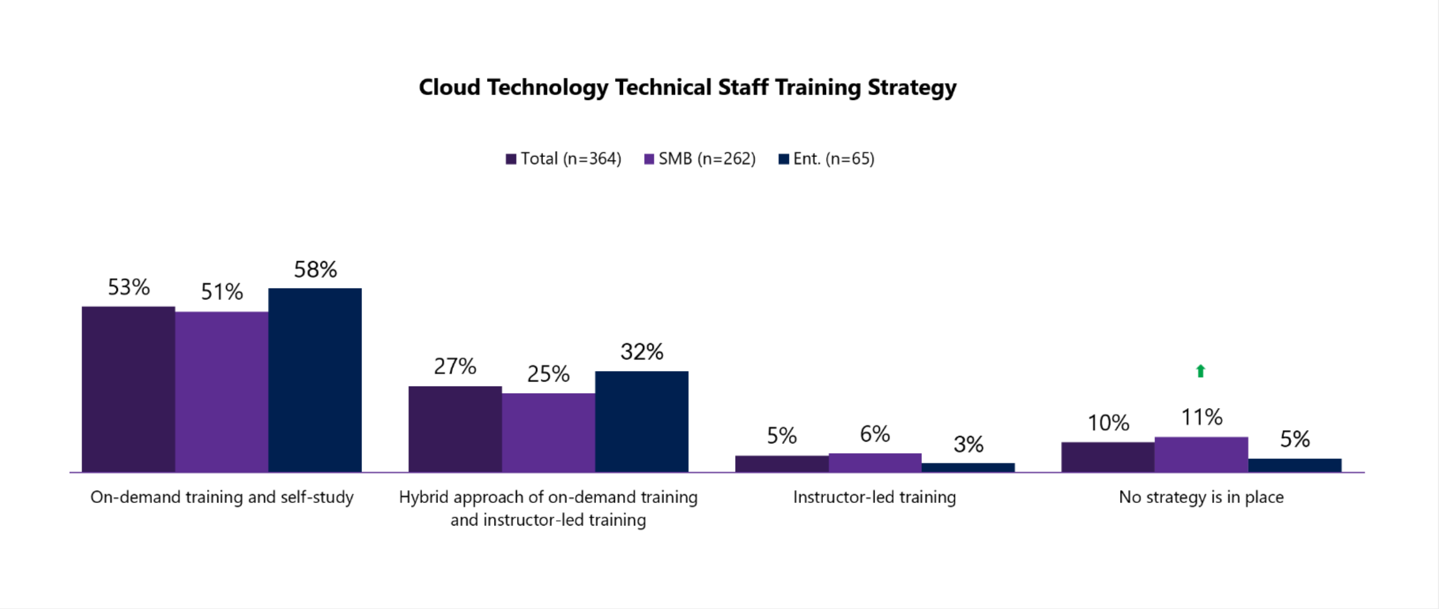
“Increase more unified messaging of the product line to consumers and in marketing materials provided. Reduce complexity of licensing. Provide more training opportunities that align to certification objectives.” – SMB Partner

“One of the biggest gaps we have is support for selling customers on why they need security services. It may seem obvious, but most business and technical decision makers have a difficult time developing a justification for funding security initiatives.” – Enterprise Partner

“Simplify offerings and access to support for smaller firms like ours. Just trying to digest the amount of information and offerings Microsoft send a small partner like us is very hard. It would be great to have communications geared more toward small partners to help us more.” – SMB Partner

Source: Microsoft Azure Migration eBook, MDC Research, June 2020

An MDC Research study found that most partners trained staff using on-demand and self-study, with a smaller percentage using a mix of on-demand and instructor-led training.



Source: Microsoft Azure Migration eBook, MDC Research, January 2018

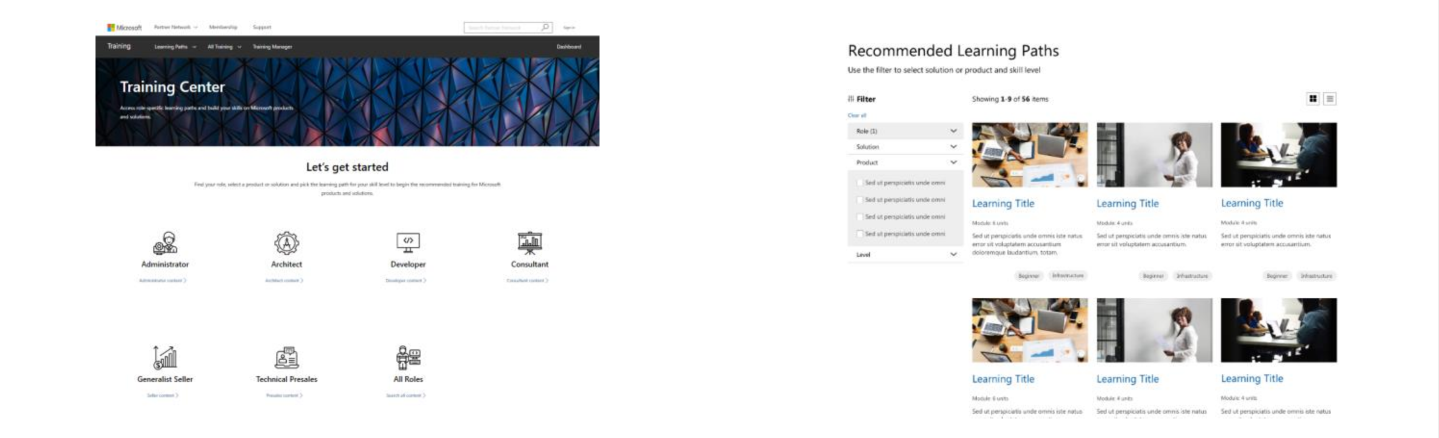
> “
>
> #1 challenge for the cloud adoption is access to talent. Building a learning culture inside the organization is the success mantra for keeping our azure rockstars up-to-date on the ever improving azure platform.
>
> **ANIL SINGH,**
>
> CEO, Hanu Software

Increase readiness and marketability with learning paths and assessments, competencies, and certifications

There are numerous assessments and certifications employees should consider as motivation for advancing their skills, creating proof points for the organization's practice, and achieving Microsoft Partner Network competencies.

PARTNER TRAINING CENTER

The MPN Partner Training Center that provides a simplified experience that offers new role-based learning paths with curated training recommendations based on technical role, skill level, and solutions being developed.


Training Center

Access role-specific learning paths and build your skills on Microsoft products and solutions

Let's get started

Find your role, select a product or solution and pick the learning path for your skill level to begin the recommended training for Microsoft products and solutions.

Recommended Learning Paths

Use the filter to select solution or product and skill level

Showing 1-9 of 56 items

Learning Title

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam.

Learning Title

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium.

Learning Title

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium.

Learning Title

Sed ut perspiciatis unde omnis iste natus

Learning Title

Sed ut perspiciatis unde omnis iste natus

Learning Title

Sed ut perspiciatis unde omnis iste natus

GENERAL TECHNICAL TRAINING

Whether partners need to fill a skills gap or are looking to improve their team's skill surface area, technical training is critical to success.

MICROSOFT 365 SECURITY TRAINING

The Microsoft 365 Security Track offers online curated training for individual certifications and partner competencies, including and advanced partner workshop and M365 Administration Certification prep.

AZURE SECURITY COMPASS ON GITHUB

Microsoft's Cybersecurity Solutions Group has a GitHub page on Azure Security Compass with download files including presentations, best practices, videos, and tracking worksheets.

MICROSOFT CONFERENCE RECORDINGS

For those who missed the annual live event, the Microsoft Inspire and Microsoft Ignite conferences provide many of its sessions as on-demand recordings—no conference pass required.

PARTNER COMMUNITY EVENTS, CALLS & WEBINARS

The Microsoft Partner Enablement Blog maintains a schedule of trainings available to partners. Visit often and plan a training calendar.

MICROSOFT 365 COMPLIANCE TRAINING

Micosoft Learn has several courses for the compliance learning journey. There are courses for Information Protection in Microsoft 365, Information Protection and Governance , Insider risk in Microsoft 365, Advanced eDiscovery & Advanced Audit, and Protect enterprise infmration with Microsoft 365. New training offerings that become available can be found by visiting https://aka.ms/mwpartnerenablement.

Competencies and certifications

Build and verify technical expertise

Competencies

A Microsoft Partner Network competency demonstrates to customers a company's expertise in a specific product or solution. Among the first steps to achieving a competency is to meet technical skills requirements. One of the next steps is for partners to ensure they align the technical team to the MPN competency for their practice.

The competencies most applicable to the security, compliance, and identity practice are:

- Security
- Cloud Productivity
- Small and Midmarket Cloud Solutions
- Enterprise Mobility Management
- Cloud Platform Competency

Each competency has a gold or silver level that define specific requirements and provide differentiated benefits. Partners can always find the latest competency requirements and benefits available on the Microsoft Partner Network competencies portal.

Advanced specializations

Partners with an active gold competency who demonstrate deep knowledge in a specific area may seek an advanced specialization. An advanced specialization will increase a partner's visibility to customers through prioritized ranking in searches and assures potential customers that the partner meets the highest standards for service delivery and support.

Advance specializations for security include:

- Cloud Security
- Identity Access and Management
- Information Protection and Governance
- Threat Protection

Certifications

Certification is a way to demonstrate to customers that partner organization has the skills to create solutions that enable the design and implementation of secure solutions. Security certifications are industry-aligned to meet specific job roles and market needs. They don't just assess what individual know, but also their ability to apply what they know to solve real business challenges.

- SC-900: Microsoft Security, Compliance, and Identity Fundamentals
- SC-200: Microsoft Security Operations Analyst
- SC-300: Microsoft Identity and Access Administrator
- SC-400: Microsoft Information Protection Administrator
- AZ-500: Microsoft Azure Security Technologies
- MS-500: Microsoft 365 Security Administration

Microsoft

Operationalize

Security, Compliance, and Identity

aka.ms/practiceplaybooks

Microsoft
Partner
Network

Introduction

This section outlines the steps to operationalize a security practice. Leverage the resources available in the Operationalize guide for details on preparing for launch with systems, tools, and processes in place. The guide contains the following additional sections:

LEVERAGE INTERNAL USE BENEFITS

Internal use benefits provide complimentary software licenses and subscriptions for use within a partner organization and resell it as well as part of an overall package along with custom software, creating a new revenue stream for the business.

IMPLEMENT INTELLECTUAL PROPERTY

Find tips for implementing intellectual property in a service offering.

PREPARE KEY CONTRACTS

Support the sales and marketing efforts with guidance on building the materials to support sales and marketing efforts and the key contracts to put in place.

SET UP SUPPORT PROCESSES AND SYSTEMS

Implement tools and systems with this guidance. Partner success may be impacted by the ability to manage customer records, projects, and support trouble tickets.

SET UP SOCIAL OFFERINGS

Increase visibility for a practice by reviewing the Microsoft marketplaces and how to get listed on them. Find guidance on the social offerings a practice should consider setting up.

STANDARDIZE ENGAGEMENTS USING CHECKLISTS

Leverage checklists and templates to standardize customer engagement process.

PROVIDE PLANNING AND DEPLOYMENT SERVICES FOR PROTECTING IDENTITIES

Passwords are a burden on users and a liability to the enterprise. Enable enterprise customers to modernize authentication by helping them plan and deploy Windows Hello for Business.

Once authenticated on a device, without any additional measures, the tokens that device uses to authenticate with other enterprise assets can be compromised and reused, effectively giving an attacker the privileges of the user without knowing the password.

Windows Hello for Business provides users a natural approach to multi-factor authentication and in a way in which they will never forget their password because the user's own biometrics (via facial recognition or fingerprints) and device (via a certificate issued to the device during setup) combined constitute the password.

AUGMENT CREDENTIAL PROTECTION WITH CREDENTIAL GUARD

Credential Guard prevents attackers from being able to retrieve credentials from operating system memory by maintaining them in a virtualized environment that is only accessible by privileged system software and is not directly accessible by privileged users.

Partners should guide their customers to combine Credential Guard with Windows Hello for Business and Windows Server 2019 for comprehensive credential protection. Use of Windows Hello ensures that there are no usernames or passwords to phish and protects private keys from extraction.

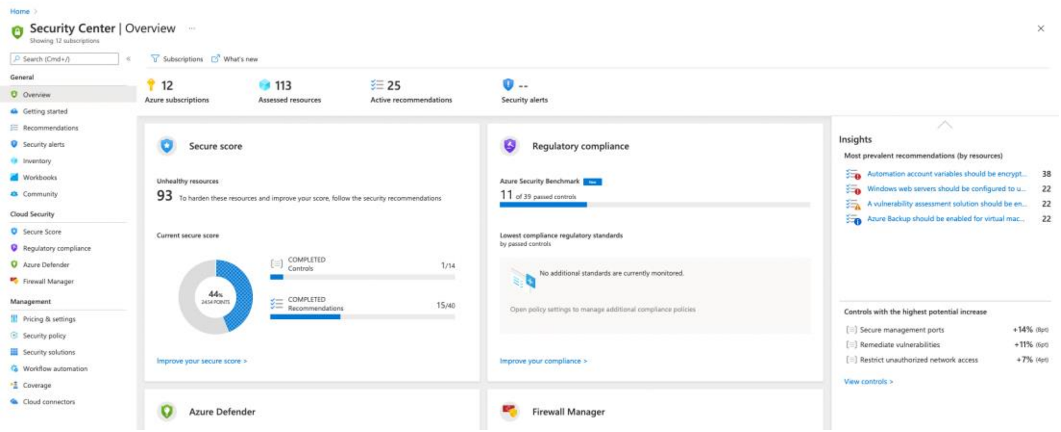
Manage and support an Azure deployment

Support resources

Supporting an Azure deployment involves transitioning from deployment focus to ongoing health and occasional troubleshooting. Microsoft Azure offers several services to help manage and monitor workloads running in Azure, as well as documentation for troubleshooting practice services.

AZURE SECURITY CENTER

Security Center helps prevent, detect, and respond to threats with increased visibility into and control over the security of Azure resources. It provides integrated security monitoring and policy management across Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions. Azure Security Center should be part of any managed service practice to assist with monitoring and support.



12 Azure subscriptions
113 Assessed resources
25 Active recommendations
-- Security alerts

Unhealthy resources
93 To harden these resources and improve your score, follow the security recommendations

Current secure score
COMPLETED Controls 1/14
COMPLETED Recommendations 15/40

Azure Security Benchmark
11 of 39 passed controls

Lowest compliance regulatory standards by passed controls
No additional standards are currently monitored.
Open policy settings to manage additional compliance policies

Most prevalent recommendations (by resources)

Automation account variables should be encrypt...	38
Windows web servers should be configured to u...	22
A vulnerability assessment solution should be en...	22
Azure Backup should be enabled for virtual mac...	22

Controls with the highest potential increase

Secure management ports	+14% (8pt)
Remediate vulnerabilities	+11% (6pt)
Restrict unauthorized network access	+7% (4pt)

Security Center delivers easy-to-use and effective threat prevention, detection, and response capabilities that are built into Azure. Some of its key capabilities are:

- Monitor the security state of Azure resources.
- Defines policies for Azure subscriptions and resource groups based on a company’s security requirements, the types of applications used, and the sensitivity of data.
- Uses policy-driven security recommendations to guide service owners through implementing needed controls.
- Rapidly deploy security services and appliances from Microsoft and partners
- Automatically collect and analyze security data from Azure resources, the network, and partner solutions like antimalware programs and firewalls
- Leverages global threat intelligence from Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds.
- Apply advanced analytics, including machine learning and behavioral analysis.
- Provides prioritized security incidents/alerts.
- Offers insights into the source of the attack and impacted resources.
- Suggests ways to stop the current attack and help prevent future attacks.

Azure Security Center enables partners to offer cloud security posture management (CSPM) and cloud workload protection platform (CWPP) as services. For instance, Microsoft partner BUI is a dedicated cyber security facility that leverages Azure Sentinel to offer threat detection, investigation and response in its BUI Cyber SoC service. BUI offers the service in three packages (Bronze/Gold/Silver) and bills monthly on a consumption model and uses our Tier One Microsoft CSP.

To help customers understand the benefits of adopting ASC, consider performing a proof-of-concept to validate specific scenarios. This how-to article walks through the steps of performing an Security Center proof-of-concept.

AZURE ADVISOR

Azure Advisor analyzes an organization's resource configuration and usage telemetry to detect risks and potential issues. It then draws on Azure best practices to recommend solutions that will reduce cost and improve the security, performance, and reliability of applications.

AZURE MONITOR

For those who are not offering Azure Monitor in its entirety as part of a core offering, using Log Analytics for support and monitoring can be a huge time saver. Log Analytics can help collect and analyze data generated by resources in cloud and on-premises environments. It gives real-time insights using integrated search and custom dashboards to readily analyze millions of records across all workloads and servers regardless of their physical location.

ENGAGING MICROSOFT SUPPORT

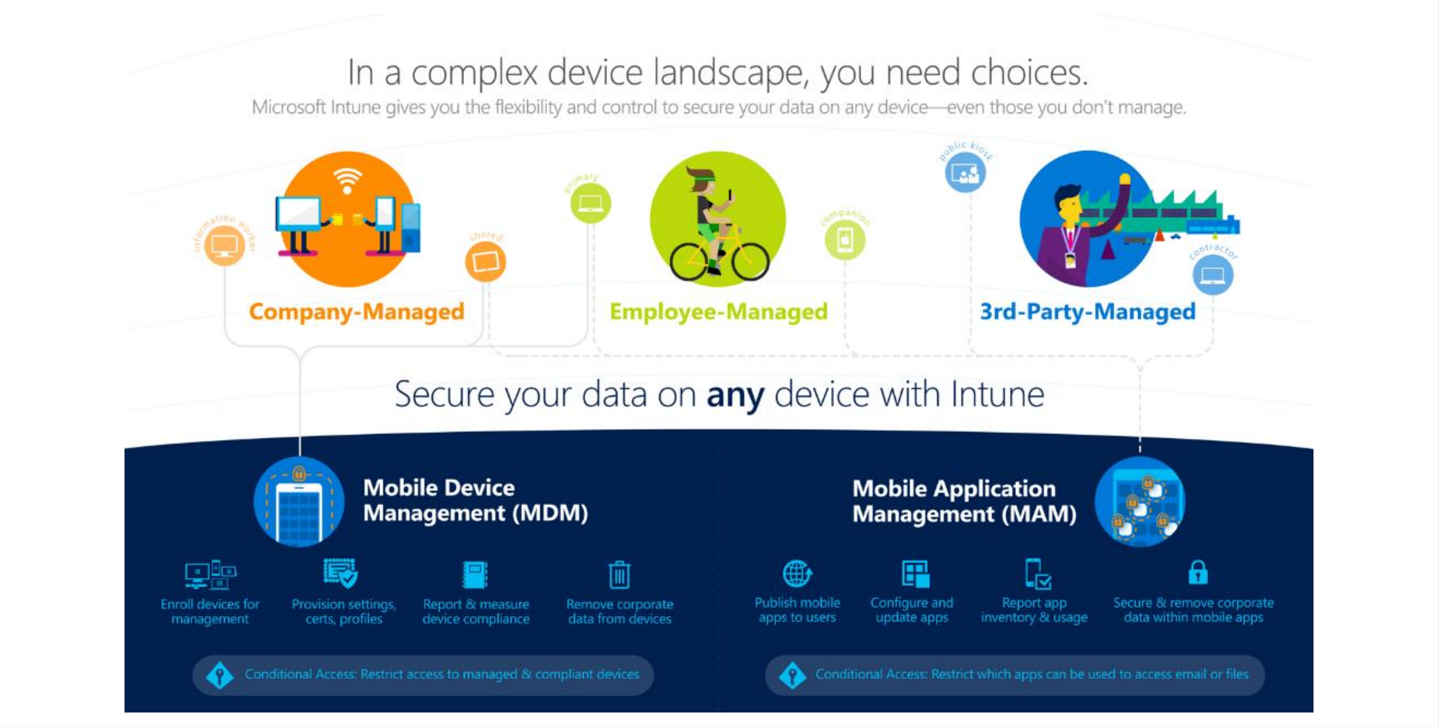
Partners who are Cloud Solution Providers (CSPs) or have sold support as part of their managed services solution, they are the front-line support for their customer. At some point, they may need to contact Microsoft to escalate an issue. Microsoft offers several options via forum support or paid options as discussed in the "Support options from Microsoft" section of this playbook.

RESOURCES

- Azure Security Center Overview
- Azure Advisor
- Azure Forum Support Resources
- Log Analytics
- Partner Support Resources

Deploy Microsoft Endpoint Manager

Microsoft Endpoint Manager is a cloud-based service that helps provide endpoint security, device management, and intelligent cloud actions within a unified management platform by leveraging Microsoft Intune and Configuration Manager.



In a complex device landscape, you need choices.

Microsoft Intune gives you the flexibility and control to secure your data on any device—even those you don't manage.

information worker
shared
Company-Managed
primary
companion
Employee-Managed
public kiosk
contractor
3rd-Party-Managed
Secure your data on any device with Intune
Mobile Device Management (MDM)
Enroll devices for management
Provision settings, certs, profiles
Report & measure device compliance
Remove corporate data from devices
Conditional Access: Restrict access to managed & compliant devices
Mobile Application Management (MAM)
Publish mobile apps to users
Configure and update apps
Report app inventory & usage
Secure & remove corporate data within mobile apps
Conditional Access: Restrict which apps can be used to access email or files

MOBILE DEVICE MANAGEMENT

Intune helps provide secure management of personal and corporate-owned devices across the most popular platforms, including Windows, Windows Phone, iOS, and Android. Users can be given the ability to enroll their own devices for management, as well as install corporate applications from the self-service company portal. In the case of large-scale device deployments, it is possible to simplify enrollment using Apple Configurator or an Intune service account. With Intune's resource access policies, users can be restricted from accessing corporate resources on an unenrolled or noncompliant device. Device settings can be applied that can enable remote actions such as passcode reset, device lock, data encryption, or full wipe of a lost or stolen device.

MOBILE APPLICATION MANAGEMENT

Microsoft Intune enables control of corporate data at the app level without having to lock down the entire device. This is commonly an issue with employees using their own personal devices who feel IT is intruding on their device when locking it down. With Intune, manageability and data protection is built directly into the Office mobile apps employees are most familiar with, helping prevent leakage of company data by restricting actions such as copy, cut, paste, and save between Intune-managed apps and personal apps. Intune provides the flexibility to extend these capabilities to existing line-of-business apps with the Intune App Wrapping Tool and offers secure content viewing using the Intune Managed Browser, PDF Viewer, AV Player, and Image Viewer apps. Administrators also can deny specific applications or URL addresses from being accessed on a mobile device and can push required apps automatically during enrollment. To further protect corporate information, wipe managed apps and related data on devices that are unenrolled can be selectively wiped, no longer compliant, lost, stolen, or retired from use.

CLOUD CONFIGURATION

Cloud configuration includes various capabilities to empower better management and security of the various devices accessing corporate data. With cloud configuration, endpoints are remotely managed no matter where they may be located. Within cloud configuration deeper insights can be gained about the devices, the software they have installed, and their readiness for updates and patch deployments. Software updates as well as OS deployments can be done remotely insuring devices always have the most recent security updates installed. Not only can security updates be applied, but with Cloud Configuration compliance settings can be used to configure various features and security settings. Another aspect of Cloud Configuration is the ability to provide security, antimalware, and Windows Firewall management for all the computers within the organization and integration with the Windows Defender suite. Lastly, inventory of both hardware and software is included to always know the details of the hardware accessing corporate data as well as the software and files stored on the endpoints.

Deploy Microsoft Defender for Identity

From detecting known malicious attacks to uncovering abnormal activity with machine learning and behavioral analytics, identify advanced persistent threats to the enterprise quickly—and act swiftly—with Microsoft Defender for Identity.

Microsoft Defender for Identity is a cloud-based security solution that uses signals from your on-premises Active Directory environment to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions.

It addresses the following:

MALICIOUS ATTACKS	ABNORMAL BEHAVIOR	SECURITY ISSUES & RISKS
Microsoft Defender for Identity detects known malicious attacks almost as instantly as they occur. • Pass-the-Ticket (PtT) • Pass-the-Hash (PtH) • Overpass-the-Hash • Forged PAC (MS14-068) • Golden Ticket • Malicious replications • Reconnaissance • Brute Force • Remote code execution • Malicious Data Protection API (DPAPI)	Behavioral analytics leverage machine learning to uncover questionable activities and abnormal behavior. • Anomalous logins • Unknown threats • Password sharing • Lateral movement	Microsoft Defender for Identity identifies known security issues using world-class security research. • Broken trust • Weak protocols • Known protocol vulnerabilities

HOW IS MICROSOFT DEFENDER FOR IDENTITY UNIQUE?

The constant reporting of traditional security tools and sifting through them to locate the important and relevant alerts can get overwhelming. Microsoft Defender for Identity provides a timeline view of events. The attack timeline is a clear, efficient, and convenient feed that surfaces the right things on a timeline, giving the power of perspective on the who, what, when, and how. Microsoft Defender for Identity also provides recommendations for investigation and remediation for each suspicious activity.

For a complete list of the detections and their descriptions, please see What Suspicious Activities can Microsoft Defender Identity Detect?

HOW IS MICROSOFT DEFENDER FOR IDENTITY DEPLOYED?

Microsoft Defender for Identity is deployed directly on the domain controllers without the added overhead of additional servers. Once deployed, Microsoft Defender for Identity automatically starts analyzing and detecting suspicious activities.

Deploy Azure Sentinel

For security information and event management in the cloud.

Performing security operations for digitally transforming customers can be complex and costly as these operations typically have hybrid or multi-cloud environments. Existing enterprise-level security information and event management systems (SIEMs) can't keep pace at cloud scale. Security operations teams are inundated with threat alerts, resulting in a high volume of time-wasting false positives and uninvestigated alerts.

Azure Sentinel is the first SIEM+SOAR (Security information and event management + Security Orchestration and Automated response) solution built into a public cloud platform to deliver intelligent security analytics across the enterprise and automatic scalability to meet ever evolving needs.

With native integration of machine learning, and User and Entity Behavioral Analysis (UEBA) models, Azure Sentinel can help detect threats quickly and reduce the noise and alert fatigue by up to 90%.

A BIRD'S-EYE VIEW ACROSS THE ENTIRE DIGITAL ESTATE

Azure Sentinel is a software-as-a-service solution for SIEM and security orchestration and automated response (SOAR). It uses Azure Monitor which is built on a proven and scalable log analytics database that ingests more than 10 petabytes every day and provides a very fast query engine that can sort through millions of records in seconds. With built-in connectors for collecting data, Azure Sentinel ingests security data from a wide range of data sources including Azure, SaaS applications including Microsoft 365, networks, and on-premises systems, Linux, Windows, Amazon Web Services (AWS), other Microsoft services, and hardware.

It features native integration of Microsoft signals and support for industry standard log formats, SYSLOG, CEF, event forwarding, and API ingestion. It also allows partners to enrich signals and filter out false positives using known malicious IP addresses derived from the context of the trillions of diverse signals in the intelligent security graph. Azure Sentinel can also leverage Microsoft's Graph Security API to integrate existing threat intelligence sources and tools.

Key benefits for partners and their customers include:

- Cloud-native with no infrastructure set-up and maintenance
- Intelligence from decades of Microsoft security experience
- Machine learning to make threat detection, analysis and response smarter and faster
- Integrated security orchestration and automation (SOAR) capabilities
- Real world investigation and remediation playbooks built by analysts in Microsoft's SOC
- Ingest Microsoft 365 data for free, and analyze and draw correlations to deepen threat intelligence
- Rapidly spot anomalies without a mountain of false positives and respond to the real threats in minutes, not days

With an expected shortfall of 3.5M security professionals by 2021, partners will need a solution that empowers their SecOps team to see the threats clearer and eliminate the distractions. To go even further into Sentinel, download the Azure Sentinel Technical Playbook for MSSPs.

USE AZURE LIGHTHOUSE TO MANAGE SENTINEL WORKSPACES ACROSS MULTIPLE TENANTS

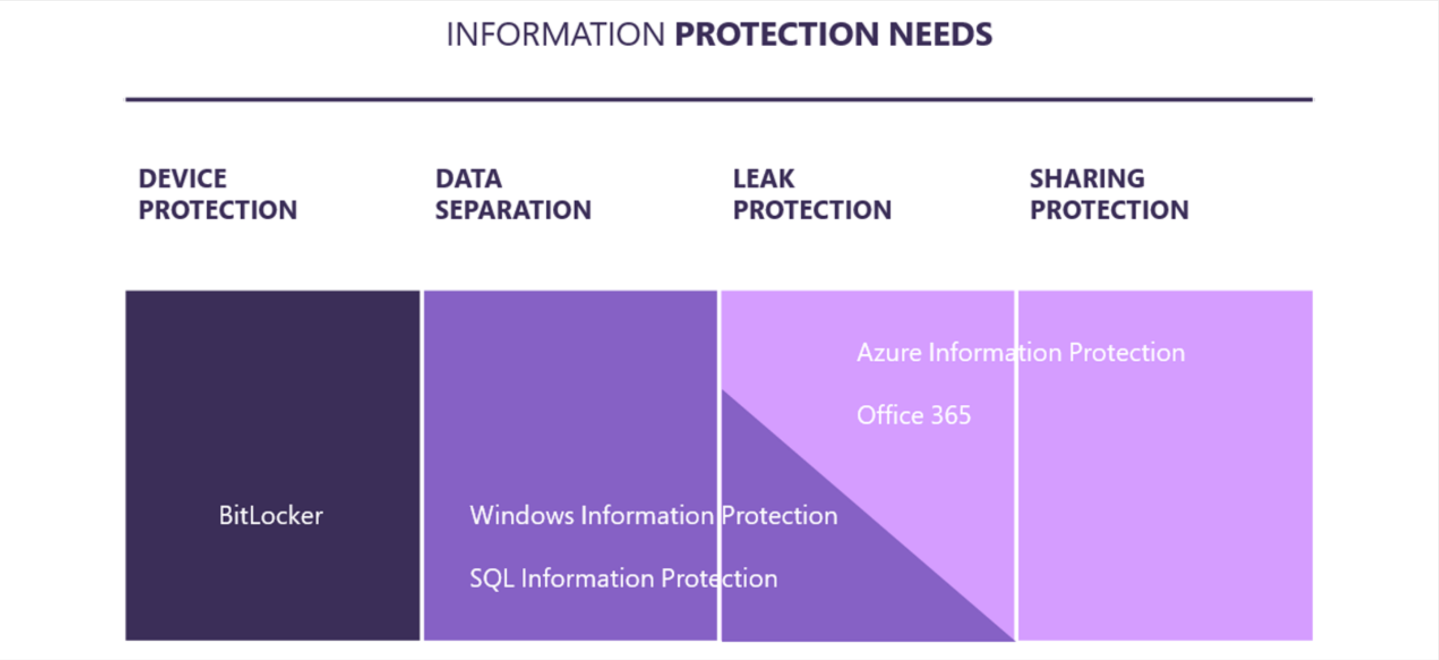
Azure Lighthouse provides capability for cross-tenancy management of Azure services for Managed Service Providers (MSPs) and organizations with multiple Azure tenants, all from a single Azure portal. Azure Lighthouse can be used to investigate an attack that targets several customers at once.

Deploy Information Protection

Information security starts with device protection, meaning a solution is needed that can protect data while it is at rest, even if the device is lost or stolen. Windows includes BitLocker for this scenario. BitLocker is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. BitLocker achieves this by encrypting all user files and system files on the operating system drive, including the swap files and hibernation files, and checking the integrity of early boot components and boot configuration data.

THE FOLLOWING REQUIREMENTS ARE FUNDAMENTAL TO INFORMATION PROTECTION:

- Provide the means to identify personal versus corporate data, such that corporate data can be contained and securely wiped on demand.
- Provide the ability to prevent business data from leaking in an unauthorized way. For instance, with a solution that can prevent data from being copied from corporate documents into non-corporate locations.
- Ensure that business data can be securely shared with others within and outside of their organization.


INFORMATION PROTECTION NEEDS
DEVICE PROTECTION
DATA SEPARATION
LEAK PROTECTION
SHARING PROTECTION
BitLocker
Windows Information Protection
SQL Information Protection
Azure Information Protection
Office 365

MICROSOFT INFORMATION PROTECTION

Microsoft Information Protection (MIP) is a cloud-based solution that helps an organization classify, label, and protect its documents and emails. This can be done automatically by administrators who define rules and conditions, manually by users, or a combination in which users are given recommendations.

CLASSIFICATION AND LABELING

Classify data based on source, context, and content at the time of creation or modification, either automatically or manually. Once classified, a persistent label is embedded in the data and actions such as visual marking and encryption can be taken based on the classification and label.

PROTECTION AND USE RIGHTS

Protect sensitive data by encrypting it and allowing only authorized users access to the data. The protection is persistent to ensure data is always protected, regardless of where it is stored or with whom it is shared.

TRACKING AND REPORTING

Track activities on shared files and revoke access if they encounter unexpected activities. The solution provides rich logs and reporting that can be leveraged for compliance and regulatory purposes.

KEY CUSTOMER CHALLENGES AND QUESTIONS

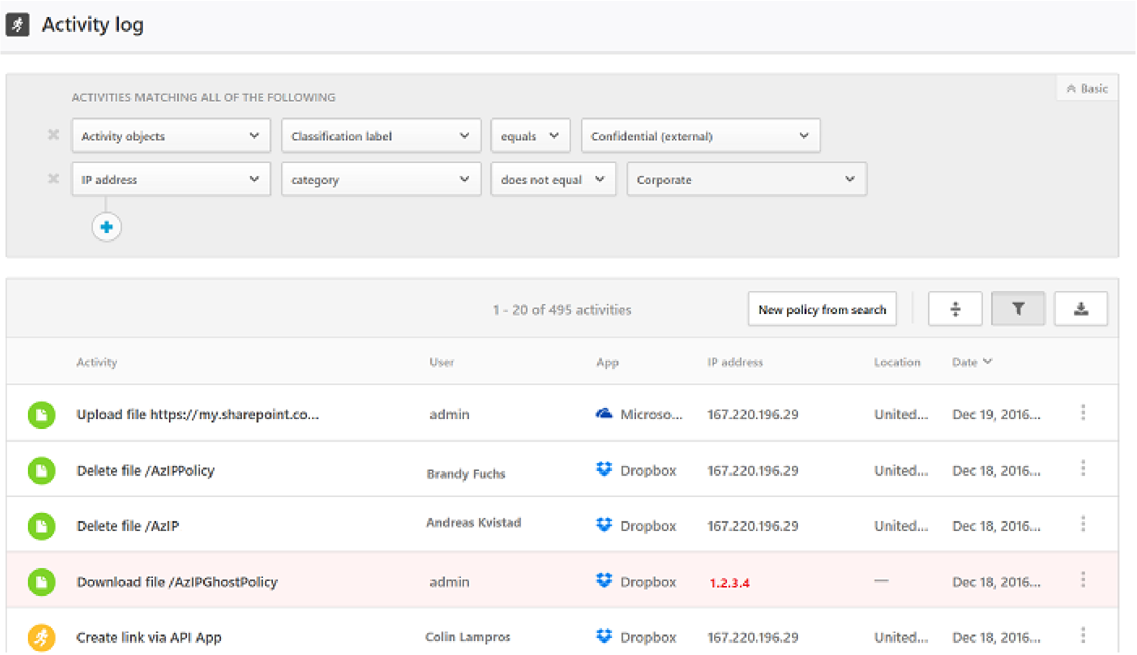
- How should I classify data?
- How does Azure Information Protection help protect sensitive data?
- How can we securely collaborate inside and outside of our organization?

RESOURCES

- Microsoft Information Protection
- Data Classification for Microsoft Information Protection

THREAT PROTECTION

Users can track activities on shared files and revoke access if they encounter unexpected activities. The solution provides rich logs and reporting that can be leveraged for compliance and regulatory purposes.



ACTIVITIES MATCHING ALL OF THE FOLLOWING

Activity objects | Classification label | equals | Confidential (external)

IP address | category | does not equal | Corporate

1 - 20 of 495 activities

Activity	User	App	IP address	Location	Date
Upload file https://my.sharepoint.co...	admin	Microso...	167.220.196.29	United...	Dec 19, 2016...
Delete file /AzIPPolicy	Brandy Fuchs	Dropbox	167.220.196.29	United...	Dec 18, 2016...
Delete file /AzIP	Andreas Kvistad	Dropbox	167.220.196.29	United...	Dec 18, 2016...
Download file /AzIPGhostPolicy	admin	Dropbox	1.2.3.4	—	Dec 18, 2016...
Create link via API App	Colin Lampros	Dropbox	167.220.196.29	United...	Dec 18, 2016...

DEPLOY MICROSOFT CLOUD APP SECURITY

Bring the security capabilities traditionally available to on-premises systems to SaaS cloud applications like DropBox, Microsoft 365, G Suite and Salesforce, and get deeper visibility, comprehensive controls, and enhanced protection against cloud security issues.

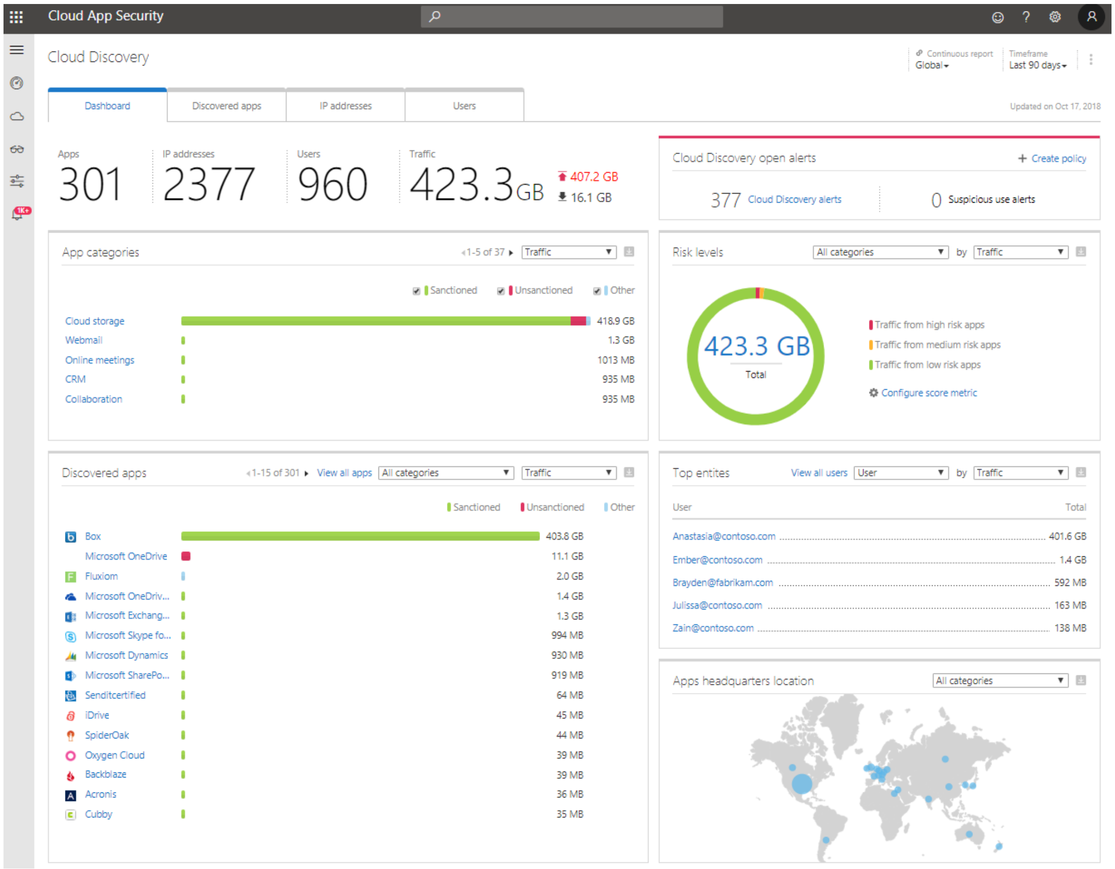
KEY CUSTOMER CHALLENGES AND QUESTIONS

- How do I identify applications in use by employees?
- How do I ensure that sensitive data is protected?
- How do I track access to shared files and compliance issues?

How Cloud App Security helps

APP DISCOVERY

Discover all the cloud apps in a network, gain visibility into Shadow IT, and assess risk without installing agents. All information is gathered directly from the network firewalls and proxies by a log collector that runs on that network and receives logs over Syslog or FTP and uploads them to Cloud App Security.



Updated on Oct 17, 2018

Apps 301 | IP addresses 2377 | Users 960 | Traffic 423.3GB (⬆ 407.2 GB, ⬇ 16.1 GB)

Cloud Discovery open alerts: 377 Cloud Discovery alerts; 0 Suspicious use alerts

App categories (1-5 of 37) — ☑ Sanctioned ☑ Unsanctioned ☑ Other

Category	Traffic
Cloud storage	418.9 GB
Webmail	1.3 GB
Online meetings	1013 MB
CRM	935 MB
Collaboration	935 MB

Risk levels: 423.3 GB Total
- Traffic from high risk apps
- Traffic from medium risk apps
- Traffic from low risk apps

Discovered apps (1-15 of 301) — Sanctioned, Unsanctioned, Other

App	Traffic
Box	403.8 GB
Microsoft OneDrive	11.1 GB
Fluxiom	2.0 GB
Microsoft OneDriv...	1.4 GB
Microsoft Exchang...	1.3 GB
Microsoft Skype fo...	994 MB
Microsoft Dynamics	930 MB
Microsoft SharePo...	919 MB
Senditcertified	64 MB
iDrive	45 MB
SpiderOak	44 MB
Oxygen Cloud	39 MB
Backblaze	39 MB
Acronis	36 MB
Cubby	35 MB

Top entites

User	Total
Anastasia@contoso.com	401.6 GB
Ember@contoso.com	1.4 GB
Brayden@fabrikam.com	592 MB
Julissa@contoso.com	163 MB
Zain@contoso.com	138 MB

Apps headquarters location

DATA CONTROL

Protect sensitive data by encrypting it and allowing only authorized users access to the data. The protection is persistent to ensure data is always protected, regardless of where it is stored or with whom it's shared. This is performed via the integrated app connectors to SaaS cloud application APIs. The following table illustrates the security capabilities available with each supported cloud application.

	Microsoft 365	Box	Okta	G Suite	Service Now	Salesforce	Dropbox	AWS
List accounts	✓	✓	✓	✓	✓	✓	✓	✓
Group	✓	✓	✓	✓	✓	✓	✓	✓
Privileges	✓	✓	Not supported by provider	✓	✓	✓	✓	
User governance	✓	✓		✓	Coming soon	Coming soon	Coming soon	
Log on activity	✓	✓	✓	✓	✓	✓	✓	✓
User activity	✓	✓	✓	✓ Requires Google Unlimited	Partial	Supported with Salesforce Shield	✓	Not applicable
Administrative activity	✓	✓	✓	✓	Partial	✓	✓	✓
Periodic file scan	✓	✓	Not applicable	✓	✓	✓	✓	Coming soon
Near-real time file scan	✓	✓	Not applicable	✓ Requires Google Unlimited			Coming soon	
Sharing control	✓	✓	Not applicable	✓	Not applicable		✓	
Quarantine	✓	✓	Not applicable	Coming soon			Coming soon	
View app permissions	✓	Not supported by provider	Not applicable	✓		✓	Not supported by provider	
Revoke app permissions	✓		Not applicable	✓		✓	Not applicable	

Cloud App Security is available as a part of the Identity & Threat Protection offering for customers with the Windows 10 Enterprise E3 plan and as a part of EMS E5. Learn more at https://www.microsoft.com/cloud-platform/cloud-app-security.

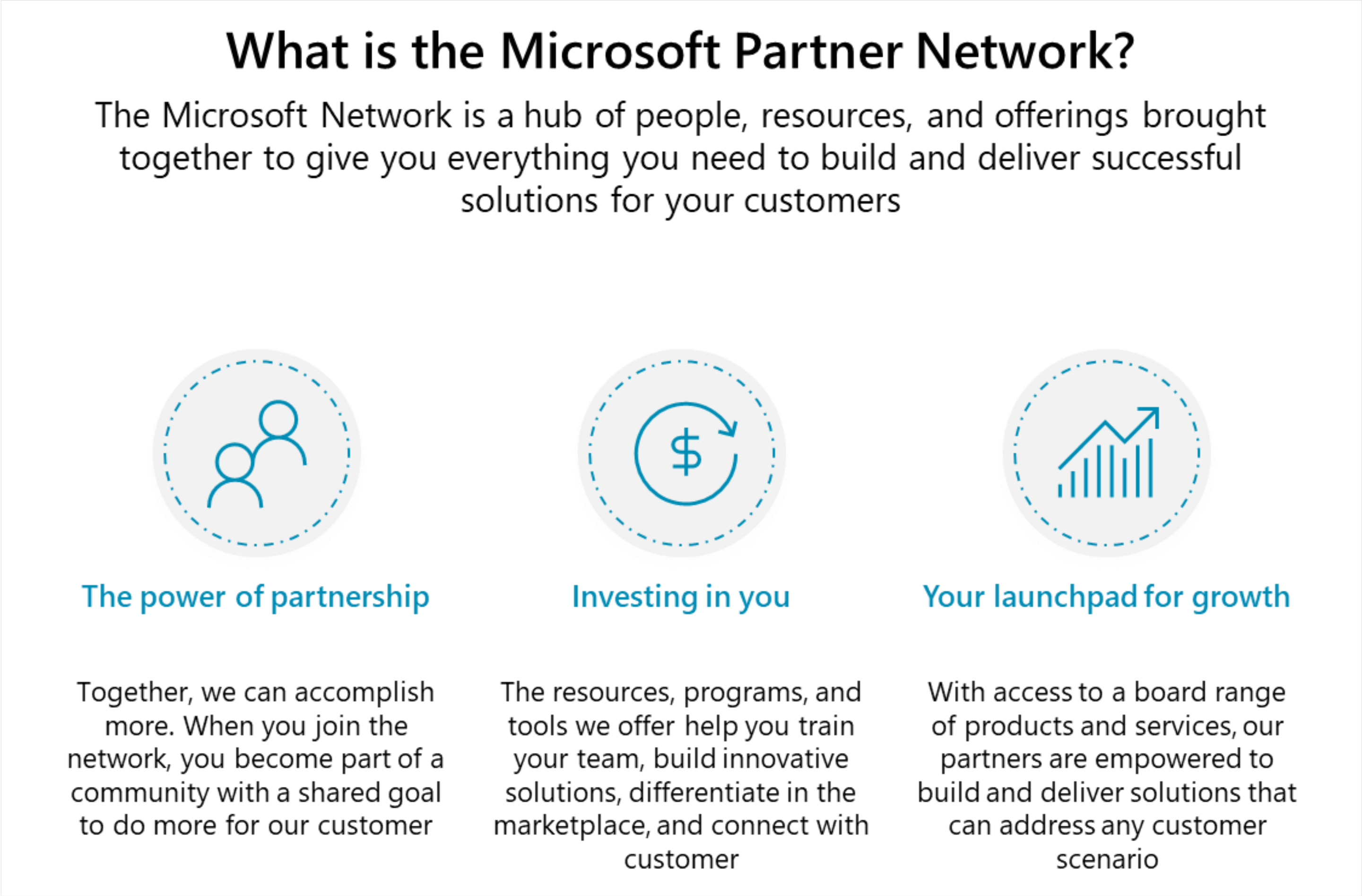
Partnering with Microsoft

One of the first steps to partnering with Microsoft is to join the Microsoft Partner Network. Partners gain access to resources like training, whitepapers, and marketing material described in this playbook. It is also where partners set up their users to gain Microsoft Partner competencies and access to other partner benefits.

TO BECOME A MICROSOFT PARTNER

The Microsoft Partner Network provides three types of memberships. Partners can participate in the program at the level that suits their unique needs.

- **Network Member:** Receive a set of no-cost introductory benefits to help save time and money. Use our resources to help build business and discover the next steps.
- **Microsoft Action Pack (MAP):** This affordable yearly subscription is for businesses looking to begin, build, and grow their Microsoft practice in the cloud-first, mobile-first world through a wide range of software and benefits.
- **Competency:** Demonstrate the capability with a specific product or solutions and receive increased support, software, and training.



What is the Microsoft Partner Network?

The Microsoft Network is a hub of people, resources, and offerings brought together to give you everything you need to build and deliver successful solutions for your customers

The power of partnership

Together, we can accomplish more. When you join the network, you become part of a community with a shared goal to do more for our customer

Investing in you

The resources, programs, and tools we offer help you train your team, build innovative solutions, differentiate in the marketplace, and connect with customer

Your launchpad for growth

With access to a board range of products and services, our partners are empowered to build and deliver solutions that can address any customer scenario

Microsoft

Go-To-Market and Close Deals

Security, Compliance, and Identity

aka.ms/practiceplaybooks

Microsoft
Partner
Network

Introduction

This section lays out the unique considerations for marketing to a security buyer and details the steps for bringing partner solutions to market, from, creating a good value proposition to building marketing and sales materials.

It starts with building foundational marketing materials and campaigns, and the co-selling and co-marketing opportunities in the Microsoft partner ecosystem.

Find partner best practices for attracting new customers and see why integrated marketing campaigns work the best.

GO-TO-MARKET AND CLOSE DEALS GUIDE

Leverage the Microsoft resources available in the Go-to-Market and Close Deals guide, for these additional sections:

Marketing to the Cloud Buyer

Technology buyers buy differently than in the past. By the time they engage with sales, they have already made some decisions.

Align Marketing Goals with Business Goals

What should the marketing efforts try to accomplish?

Creating Marketing for Every Phase of the Journey

Messaging and content should be available at each stage of the customer journey.

Marketing Tactics

Understand strategies for websites, SEO and SEM, social media, email, blogs, and webinars.

Sales

Find selling tips, sales training materials, best practices, sales incentives, and sales compensation advice.

Closing the Sale

Write winning proposals and negotiate the offer.

Marketing to the security buyer

Plan the customer's journey to buying

The cloud changes the partner business model. Buyers buy differently than in the past. With all the information on the internet, buyers tend to research and self-educate long before they engage with salespeople. By the time they do engage with sales, they have already made some decisions.

And, while cloud buyers are often eager to move to a SaaS model, with predictable monthly pricing, there are still concerns about the security of the cloud, and therefore, a partner's cloud services. Businesses are seeking out more advanced security solutions inscluding threat management, vulnerability management, firewalls, and anti-malware.

CONSIDER THE FOLLOWING

- In 2020, the IC3 received over 2,000 complaints per day of cyber crime *
- Victim losses from the crimes were approximate $4.2 billion *

* 2020 FBI Internet Crime Report

DOs and DON'Ts for marketing to the security buyer

DO target existing customers with envisioning sessions and PoCs before marketing to win new customers.

DO engage the CISO early to remove security blockers.

DO help them envision the possibilities enabled by whiteboarding the security story.

DO describe the benefits in terms of the business needs.

DO emphasize intelligence as differentiator, Microsoft Intelligent Security Graph draws upon insights from billions of emails analyzed, user authentications, device protection, and web pages.

DO provide realistic benefits based on previous experience with the solution.

DO be prepared to answer key customer concerns and challenger questions.

DON'T compartmentalize security, have the all-up security discussion that emphasizes Microsoft's end-to-end security built into the platform.

DON'T overpromise the capabilities of security.

RESOURCES

- Go to Market Guide
- The Microsoft Digital Transformation Series – Part 2: Engaging Customers

Pre-sales, post sales, and support

Define the technical effort required before the sale (pre-sales), after the sale (post-sales), and in support of the sale. Understand the technical pre-sales and post-sales requirements for a solution offer.

PRE-SALES

- Discussing the customer requirements and address their objections.
- Developing technical pitch decks.
- Providing a technical demo. This demo may be generic or may need customization to the better meet the requirements of the customer. The goal of the technical demo is to inspire confidence in the partner's ability to deliver the desired solution by demonstrating they have "already done something like it before."

POST-SALES

- Addressing follow-on customer concerns about the technology or implementation.
- Providing training to increase awareness of the solution that will be implemented.
- Providing a more customized technical demo for the customer to better understand their needs before moving on to the next phase of the project.
- Following up with the customer to ensure implementation is on track and meeting expectations.

For guidance with sales efforts, consider the learning paths available in the Microsoft Partner Network Training Center.

Leverage these presentations which can be used for technical briefings or sales pitches:

- Microsoft Security and Identity partner practice page
- Microsoft Compliance partner practice page

Partners should customize each presentation to explain how their unique offering makes the overall solution a true differentiator.

Leverage Partner Technical Services available from Microsoft to help build technical capabilities faster to accelerate sales, deployments, and app development.

Consultative selling and technical pre-sales

Discovering the art of the possible

From the very start of an engagement with a prospect, partners should be aware of the need for technical pre-sales assistance. Many times, they are dealing with business decision makers during the buying cycle. In that case, they are less likely to have a need for technical assistance. However, more than ever before, technical staff are a part of decision making with security practices as they help envision a solution to solve a customer need.

The technical pre-sales staff should be very experienced users of a company's products and services. These employees need training or experience as a user of those products. Former support employees often make good technical pre-sales staff. The technical pre-sales staff is in place to explain technology, how it works, how it meets a business need and to answer any other questions. They should excel at the more complex issues that come from prospects, and be focused on pre-sales, working together with sales and marketing, who address the business benefits. One without the other cannot be effective. The sales staff needs to speak to business decision makers and envision the art of the possible, with security solutions this often occurs jointly with technical expertise.

Examples of technical probing questions to ask during pre-sales conversations supporting a security practice:

- What are the challenges you are looking to solve?
- Are you looking to improve communication, learn from your data (such as predicting future events)?
- Do you have the data to help you approach these challenges? In what formats?
- Is the data generated and captured with your system or is it external and provided by 3rd parties?
- What application development and technologies are within your existing team's comfort zone? Do you have any data scientists on the team?
- What application platforms would you like to target? Web, mobile, desktop, IoT, etc.
- Are there any compliance or regulatory requirements that pertain to the handling of data?
- How does data enter the system and how it is ultimately consumed?
- Is Office on-premises or delivered as Microsoft 365?
- Does your company allow workers to bring their own devices?
- How are corporate and personal devices managed today? Is corporate data being loaded on to personal devices?
- How do you ensure that internal documents are protected and not sent out to your competition?
- How do you ensure that if an employee leaves that corporate data does not leave on their personal devices?
- How do you manage user experience and security for SaaS applications?
- Does your IT/Helpdesk have problems or heavy cost with password resets?

BEST PRACTICES – CONSULTATIVE SELLING:

Rather than just promoting an existing product, the salesperson focuses on the customer's problems and addresses the issue with appropriate offerings (products and services). The problem resolution is what constitutes a "solution".

The best reps combine solution selling with insights. To gain credibility in the eyes of the buyer, the solutions sales rep must introduce content and data that adds value to the sales call.

Ask good questions. The successful solutions seller remains sensitive to the buyer’s needs and asks important questions at the right moment.

Listen actively. Solution selling requires considerable understanding of the buyer’s needs, which will only come from listening attentively. Solution sellers should actively listen as the buyer details their organizational needs, taking notes and asking considerate questions in the process.

Offer guidance. Solution sellers must guide the buyer towards the solution being offered. This guidance comes as the solution seller adopts something of a teaching role, helping the buyer to overcome business challenges by utilizing their deep knowledge of industry pain points and trends.

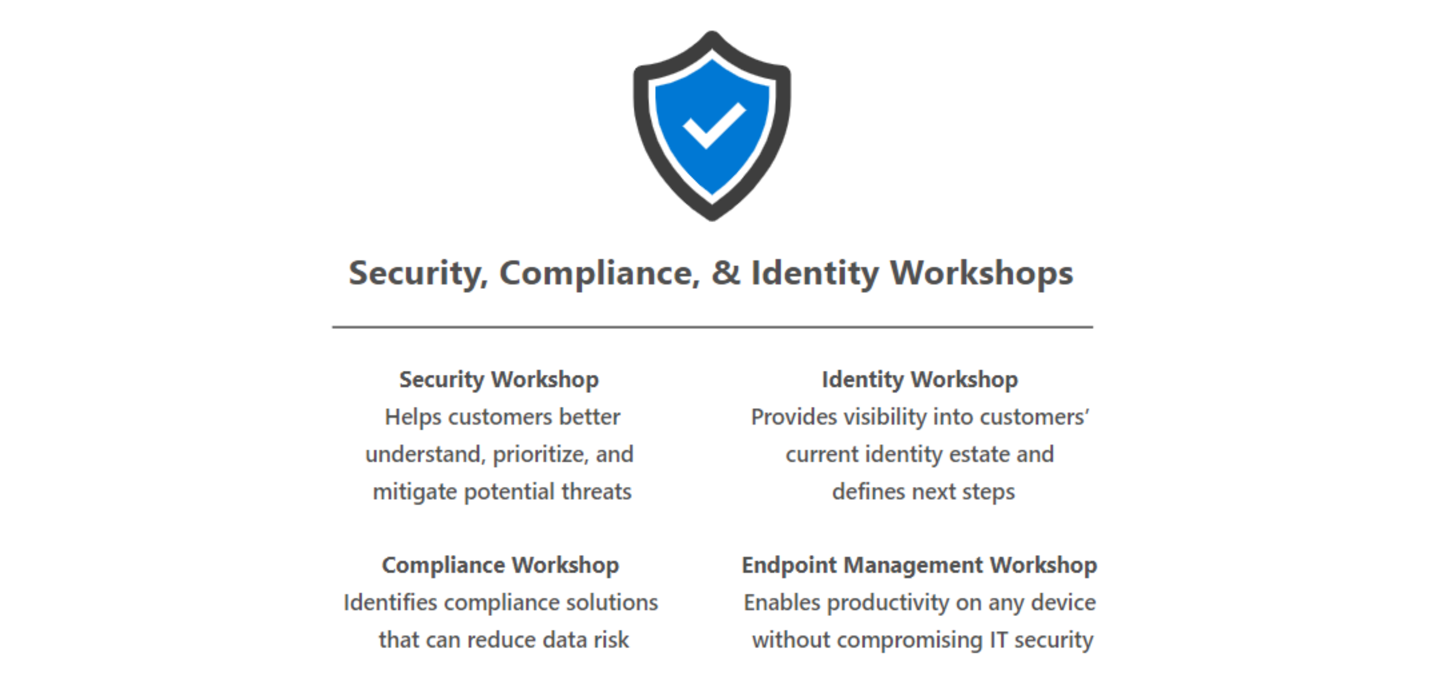
RESOURCES

- Azure Pre-Sales Resources
- Engagement Offerings

Microsoft Cloud Accelerators

Microsoft Cloud Accelerators provide a set of pre-made workshops that enable partners to accelerate the customer journey, including a rapid deployment program to address a customers' current needs for business continuity. Leveraging these accelerators allow partners to facilitate more productive customer conversations, help customers envision the possibilities, and more efficiently realize opportunities.

The Security, Compliance, and Identity Workshops are designed to assist in conducting effective discussions with customers about their baseline and advanced security and compliance strategy, priorities, initiatives, and key influences.



Security, Compliance, & Identity Workshops

Security Workshop
Helps customers better understand, prioritize, and mitigate potential threats

Identity Workshop
Provides visibility into customers' current identity estate and defines next steps

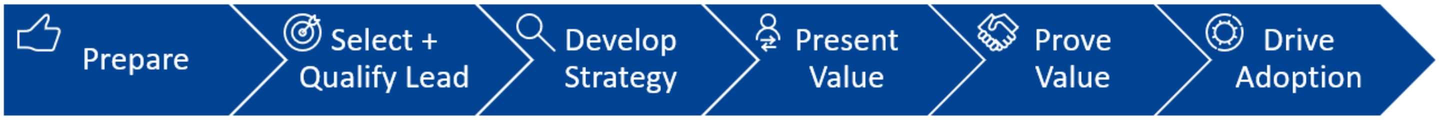
Compliance Workshop
Identifies compliance solutions that can reduce data risk

Endpoint Management Workshop
Enables productivity on any device without compromising IT security

The Microsoft 365 Security Sales Formula

To get to the sale tipping point for Microsoft 365 security features, it is important that partners know and understand how to showcase the customer value and benefits.

Most effective advanced security sales start early and with an assessment. Sales cycles can be long, so start as early as possible. Ensure the right partner solution specialists are fully engaged as part of the end-to-end sales process. Security workloads are complex; be sure to leverage the most strategic sellers and consultants as part of the wider team.



Prepare → Select + Qualify Lead → Develop Strategy → Present Value → Prove Value → Drive Adoption

	RESOURCES FOR USE DURING SELLING	STEPS FOR SELLING TO CUSTOMER
Prepare	Know the product, programs, tools, training and research to get ready.	Discuss with customers their security needs, identify how best to deliver a Security Assessment Workshop
Select + Qualify Lead	Target the right industry verticals to maximize effort. Explore customers who have existing Exchange Online deployments or EMS customers. Have a CISO discussion to drive engagement and possible security assessment workshop.	Understand the customer landscape and define positioning of the advanced security workload post Security Assessment Workshop
Develop Strategy	Learn the Digital Transformation vision presentation and the advanced security and Secure Score demos.	Create Security Assessment Workshop strategy, publish security offerings, baseline offering strategy, land with customers.
Present Value	Utilize partner success stories and customer success stories to showcase customers leveraging Microsoft 365 security.	Showcase the value of Microsoft 365 security through proof points and demos.
Prove Value	Show economic value and value of security assessments by leveraging Secure Score.	Use customer evidence to demonstrate the ROI and business impact
Drive Adoption	Drive advanced security workloads by realizing the benefits identified in the security assessment workshop and bringing customer security environments up to the customer desired level.	Build security into the Customer Success Plan and help customers realize the value of security identified in the Security Assessment Workshop

Microsoft

Optimize & Grow

Security, Compliance, and Identity

aka.ms/ practiceplaybooks

Microsoft
Partner
Network

Optimize and Grow Guide

Leverage the Microsoft resources available in the Optimize and Grow guide, for details on optimization strategies, engaging customers for life, and monitoring and measuring results. The guide contains the following additional sections:

Optimize through Bottom-Line Efficiencies
Optimize for operational excellence, using bottom-line levers.

Measure Results
Benchmark and create scorecard to measure improvement against key performance indicators.

Understanding Customer Lifetime Value
A lifelong customer is of far greater value than any one-off transaction. And not all customers are equal in value.

Customer Experience and Satisfaction
Continually improve the customer experience by establishing CX related metrics.

Collect Feedback
Solicit feedback from customers on a regular basis and act on that feedback.

Perform a Post-Mortem
Establish a formal process for evaluating a project.

Growth through Top-Line Strategies
Without a strategic plan for growth and revenue generation, the impact will be felt on the bottom line.

Post-Sale Activities
Building and nurturing positive customer outcomes post-deployment is critical to secure recurring and renewal-based revenue.

Grow Partnerships
Identify partnership opportunities, assess readiness, and grow relationships to differentiate offers, expand markets, or enter verticals.

Security Playbook Summary

Thank you for taking the time to review this playbook. The goal is to provide new insight on how to successfully build a security practice by taking advantage of the resources, guidance and partner best practices outlined herein.

Our objective was to organize resources and provide insight that can be used to quickly accelerate or optimize a security practice.

The first section, **Define the strategy**, offered guidance on how to define the strategy upon which the practice will be built.

In the second section, **Hire & train**, it focused on the importance of hiring the right team, and then providing appropriate and ongoing training.

The third section, **Operationalize**, shifted to the solution delivery process, the Microsoft-provided support options, and tips for implementing IP in a security offering. It concluded with a customer engagement checklist to use for creating repeatable processes.

The fourth section, **Go-To-Market and Close Deals**, covered the sales and marketing process, finding new customers, and then nurturing and investing in them to build lasting relationships.

The final section, **Optimize & Grow**, stressed the importance of building customer lifetime value and the key elements of a customer adoption approach.

FEEDBACK

Share feedback on how this and other playbooks can be improved by emailing playbookfeedback@microsoft.com.