StepUp Technical Training

Microsoft 365 Business (Security) 1 of 4
Analyze customer risk with Secure Score

Todd Sweetser
Partner Technology Strategist

Pamela Johnson
Senior Partner/Channel Marketing Manager

StepUp Technical

Register for these upcoming StepUp events!		
Microsoft 365 Business (Security) 2 of 4: Guard against online threats and keep data secure	Oct 18	Register
Microsoft 365 Business (Security) 3 of 4: Leverage the newest capabilities to protect from security threats	Oct 25	Register
Microsoft 365 Business (Security 4) of 4: Protect and classify sensitive documents	Nov 1	Register
Spin up a VM with Disaster Recovery	Oct 16	Register
Leverage SQL Server by Moving to Azure VM	Nov 8	Register

Microsoft

aka.ms/MSStepUpTechnical

Ready to launch your Microsoft 365 Business campaign?

The Great American Campaign Competition starts October 19

Choose from *Why Cloud* or *Security* scenarios

- We'll provide all the content and images and help you create new content
- Learn the best way to measure your campaign
- Win weekly prizes
- Need extra support? We're on it. Just ask.

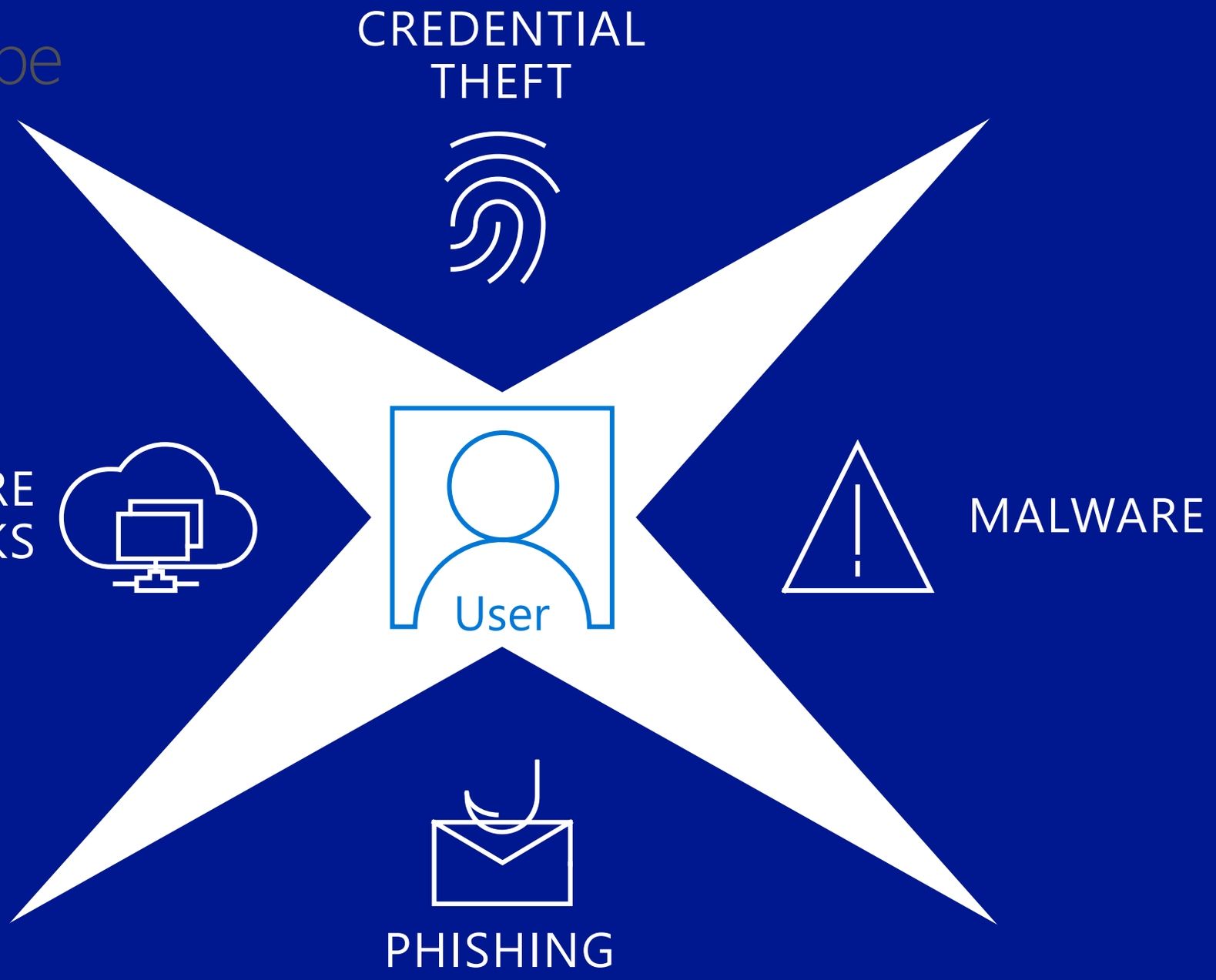
aka.ms/mssworkshops

Oct 19	Kickstart your campaign	Register
Oct 26	Campaign best practices	Register
Nov 2	Meet the content creators	Register
Nov 9	Wrap up, prizes and results	Register

StepUp Microsoft 365 Business Security 1 of 4 - Analyze customer risk with Secure Score

Todd Sweetser
Partner Technology Strategist

Threat landscape



Traditional IT security tools have problems

Complexity

Initial setup, fine-tuning, creating rules, policies, thresholds, and baselines can take a long time.

Prone to false positives

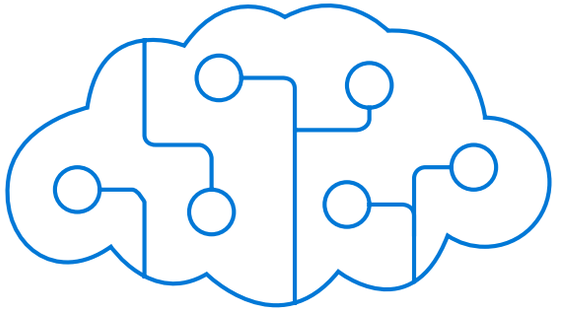
You receive too many reports in a day with several false positives that require valuable time you don't have.

Designed to protect the perimeter

When attackers successfully compromise a user, your current defenses provide limited detection and protection.

Technological shifts for defenders

User and entity behavior analytics (UEBA)



Machine Learning

Big Data

Microsoft 365 Business Overview

Technology challenges faced by small and midsized businesses today

Keeping technology up-to-date

Mobile, distributed workforce

Protecting sensitive data

Cyber threats & phishing schemes

INTRODUCING

Microsoft 365 Business

Microsoft 365 Business

Securely run and grow your business

Get more done

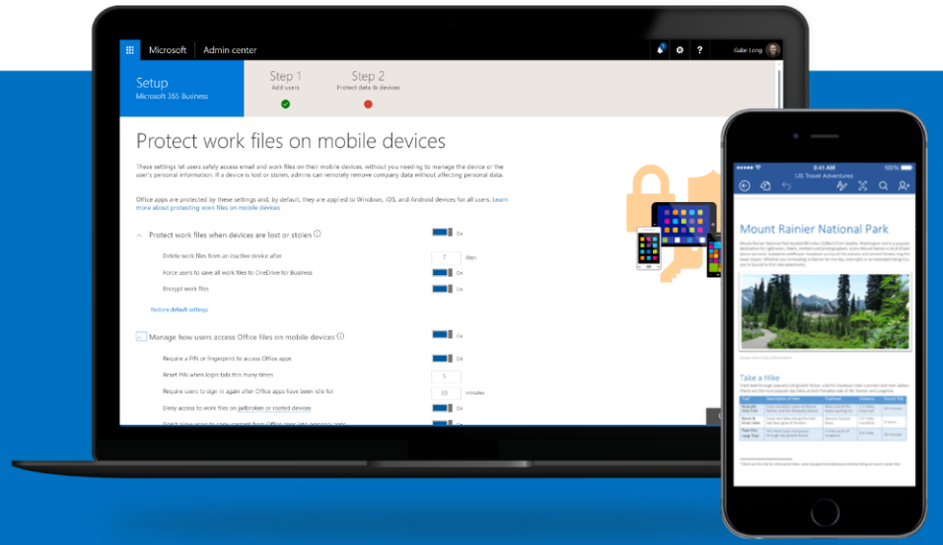
Increase productivity with intelligent tools built into the Office you love along with enterprise grade email and file storage.

Work better together

Collaborate, share, and communicate with flexible tools that go where your team goes.

Build your business

Get more customers and improve the efficiency of your business operations



Safeguard your business

Help protect your company against external threats and data leaks with built-in privacy compliance tools.

Simplified for you

Easily setup and manage your users, devices and data, giving you more time to focus on your business.

What's new?

We've recently added advanced security features to Microsoft 365 Business to help businesses protect against cyberthreats and safeguard sensitive information.

Cyber Threats

1. Office 365 Advanced Threat Protection

   Attachment scanning & ML detection to catch suspicious attachments

   Link Scanning/Checking to prevent users from clicking suspicious links

2. Windows Exploit Guard Enforcement

   Preventing devices from ransomware and malicious websites at device end points

Safeguard Sensitive Information

1. Data Loss Prevention

   Does Deep Content Analysis to easily identify, monitor, and protect sensitive information from leaving org

2. Azure Information Protection

   Controls & Manages how sensitive content is accessed

3. Intune Availability

   Protecting data across devices with E2E Device and app management

4. Exchange Online archiving

   100GB Archiving & preservation policies to recover data or remain compliant

5. BitLocker Enforcement

   Encrypt Data on devices to protect data if device lost or stolen

Comparison of Microsoft 365 Business and Office 365 E3

	Features (new in blue)	Office 365 E3	Microsoft 365 Business
	Estimated retail price per user per month $USD (with annual commitment)	$20	$20
	Maximum number of users	unlimited	300
Office Apps	Install Office on up to 5 PCs/Macs + 5 tablets + 5 smartphones per user (Word, Excel, PowerPoint, OneNote, Access), Office Online	ProPlus	Business
Email & Calendar	Outlook, Exchange Online	100GB	50GB
Chat-based Workspace, Meetings	Microsoft Teams, Skype For Business	●	●
File Storage	OneDrive for Business,	Unlimited	1 TB
Social, Video, Sites	Stream, Yammer, Planner, SharePoint Online[1], Power Apps[1], Flow[1]	●	●
Business Apps	Scheduling Apps – Booking, StaffHub	●	●
	Business Apps – Outlook Customer Manager, MileIQ[1] Business center[2], Listings[2], Connections[2], Invoicing[2]		●
Threat Protection	Office 365 Advanced Threat Protection		●
	Windows Exploit Guard Enforcement		●
Identity & Access Management	Azure Active Directory - SSPR Cloud Identities, MFA, SSO >10 Apps		●
Device & App Management	Office 365 MDM	●	●
	Microsoft Intune, Windows AutoPilot, Windows Pro Management		●
	Upgrade rights to Windows 10 Pro for Win 7/8/8.1 Pro licenses		●
Information Protection	100 GB Exchange Archiving, Office 365 Data Loss Prevention[4]	●	●
	Azure Information Protection Plan 1, BitLocker Enforcement		●
On-Prem CAL Rights	ECAL Suite (Exchange, SharePoint, Skype)	●	
Compliance	Litigation Hold, eDiscovery, Compliance Manager, Data Subject Requests	●	●

[1] Indicates Office 365 has Plan 2 and Microsoft 365 Business has Plan 1 of the functionality
[2] Available in US, UK, Canada
[3] Currently in public preview in US, UK, Canada
[4] Data Loss Prevention Features will be available summer 2018

Safeguard your data

Protect your company against external threats and data leaks

Protection from threats

Protection from data leaks

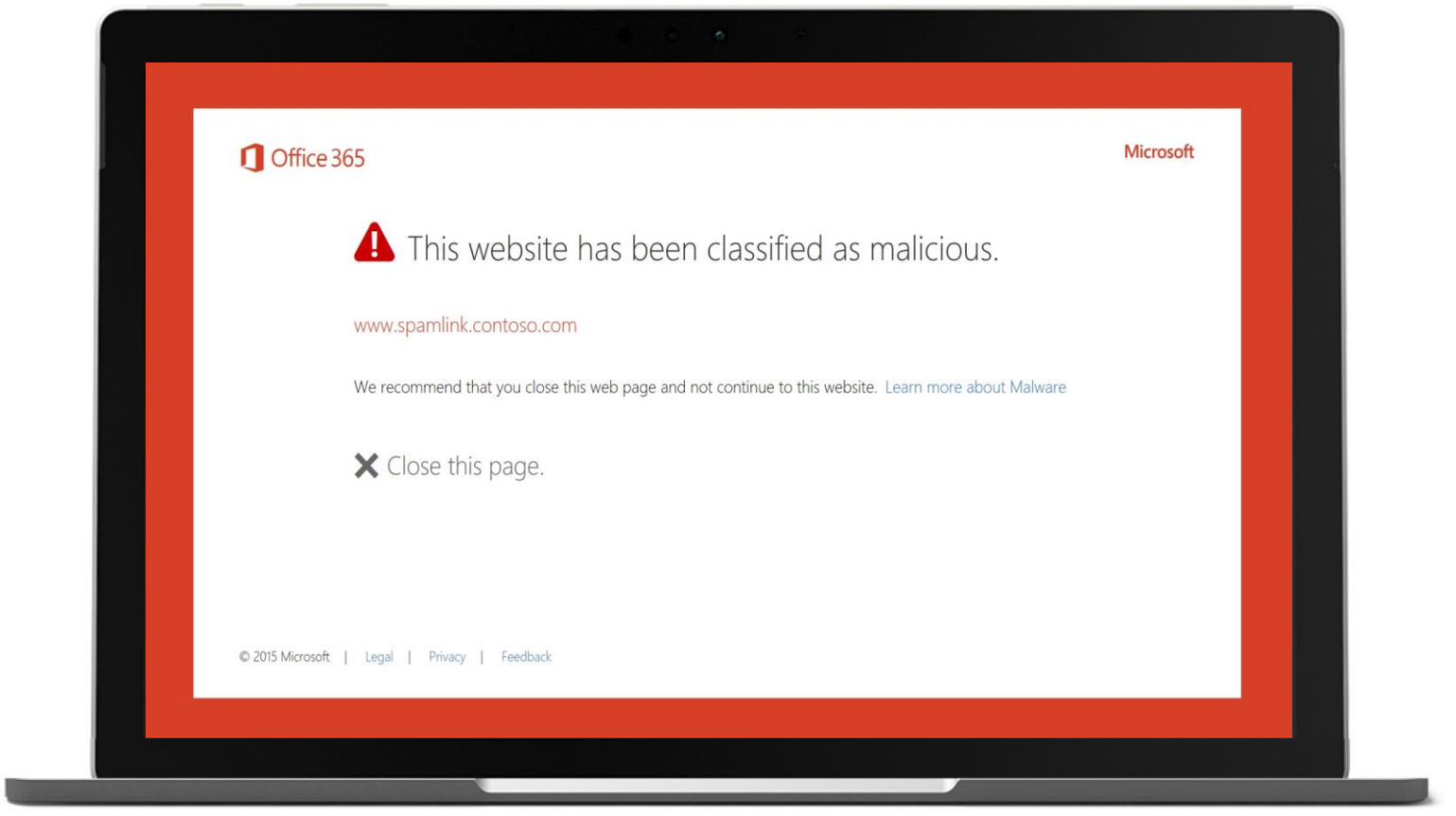
Control data access

Safeguard your data:
Protection from threats

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

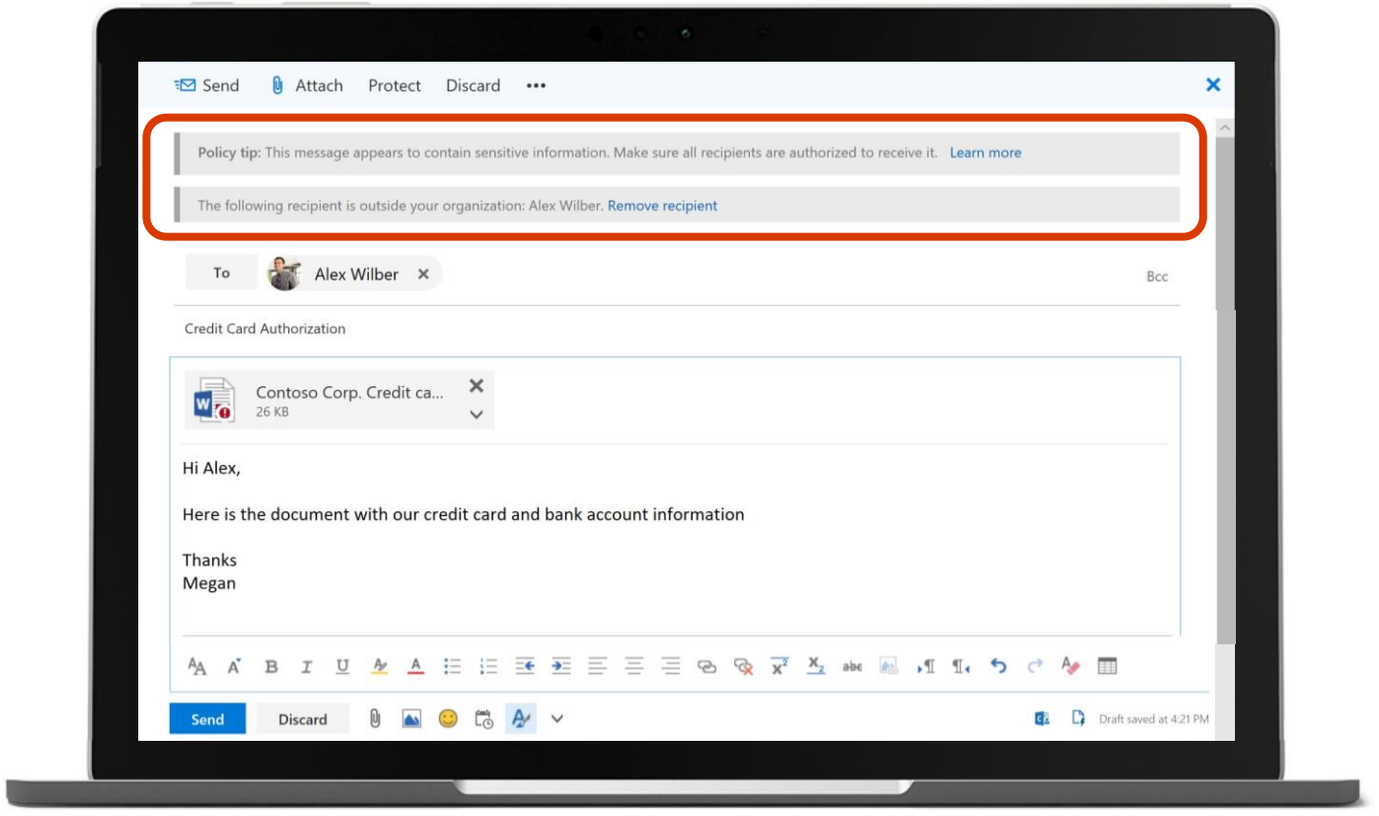
AI-powered attachment scanning detects malware previously not seen

Windows devices are **monitored for suspicious processes** like ransomware



Safeguard your data:

Protection from data leaks



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

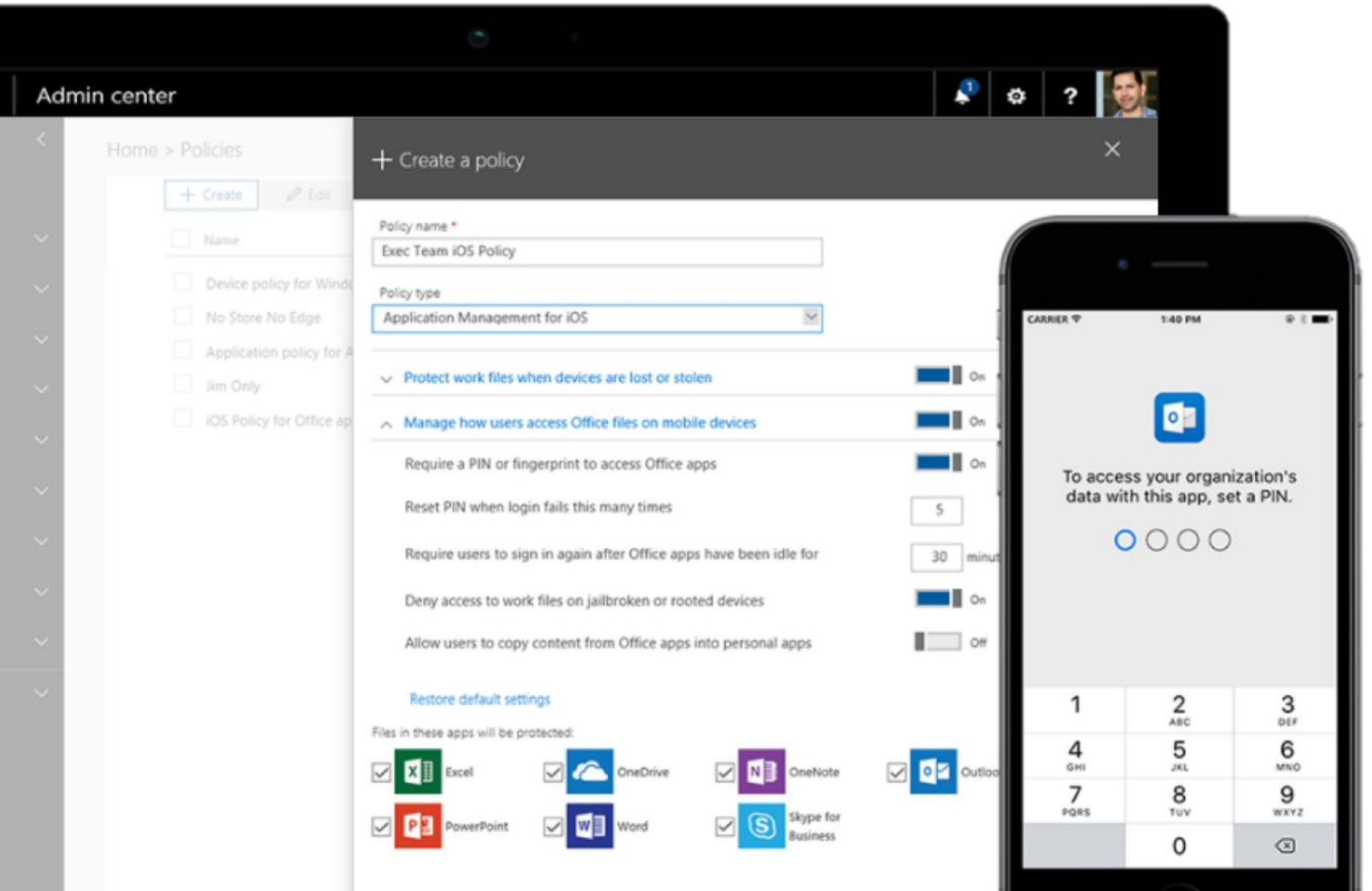
Enforce **BitLocker device encryption to** protect data if a computer is lost or stolen

Manage all your devices—PCs, Mac, iOS, and Android—with full-featured **Intune management**

*Data Loss Prevention will be available in Microsoft 365 Business in summer 2018

Safeguard your data:

Control data access



Require PIN or fingerprint to access business documents and data

Remotely wipe business data without affecting personal information

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

Security that travels with you

Protect your data and devices against malware, malicious attacks, and device loss or theft. **BitLocker, BitLocker to Go,** and **Windows Information Protection** help protect business data on mobile devices by ensuring all business data is encrypted and accessible only by authorized users.

Further protect Windows 10 devices from unauthorized access using **Windows Hello multi-factor authentication** to strengthen your users' device credentials.

Perform a remote **Selective Wipe** of company data easily on lost or stolen devices.

Reduce your security risk

Centralize control of your company data on personal devices.

Reduce your risk profile with security features for SMB customers.

Apply a consistent security configuration profile, across managed devices.

Establish a baseline of security policies across managed devices.

Configure devices consistently to help ensure that your data and devices are protected from malware and external threats.

Help protect your devices, data, and people

Know that lost or stolen devices are protected with Windows 10 built-in encryption capabilities like **BitLocker** and **BitLocker to Go**.

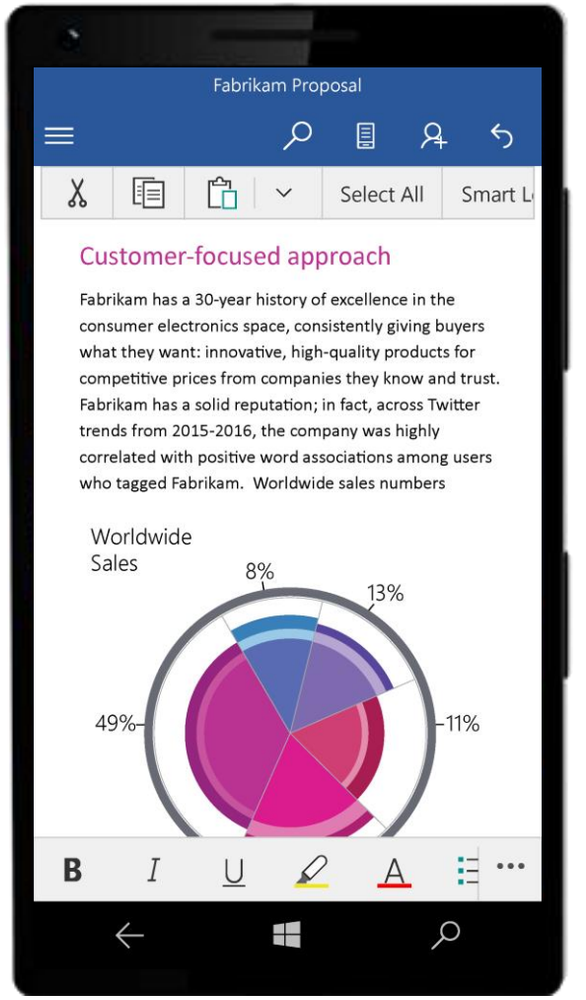
Help prevent accidental data leaks by securely separating business information from personal information with **Windows Information Protection**, and perform a remote **Selective Wipe** of business data on demand while leaving personal data untouched.

Make sure employees always have access to files while confining company information to Office apps, using **App Protection for Office mobile apps** capabilities for personal iOS, and Android devices.

Make accessing Windows 10 devices more convenient, simple, and secure by using **Windows Hello** biometric authentication2 to unlock devices with a look or a touch.

Help make sure that devices boot securely and that only trusted software can run during start-up with **Windows Trusted Boot** used in combination with the PC industry hardware standard, UEFI Secure Boot.

Enforce **Windows Defender** to always be on from within the admin console.



Technology Overview

Technical Overview Agenda

Windows Defender Exploit Guard
Antivirus/antimalware detection and protection enhanced by cloud-based analysis and insights.

Office 365 Advanced Threat Protection
Detection of—and protection against—malware and malicious links for your Office 365 email and productivity apps.

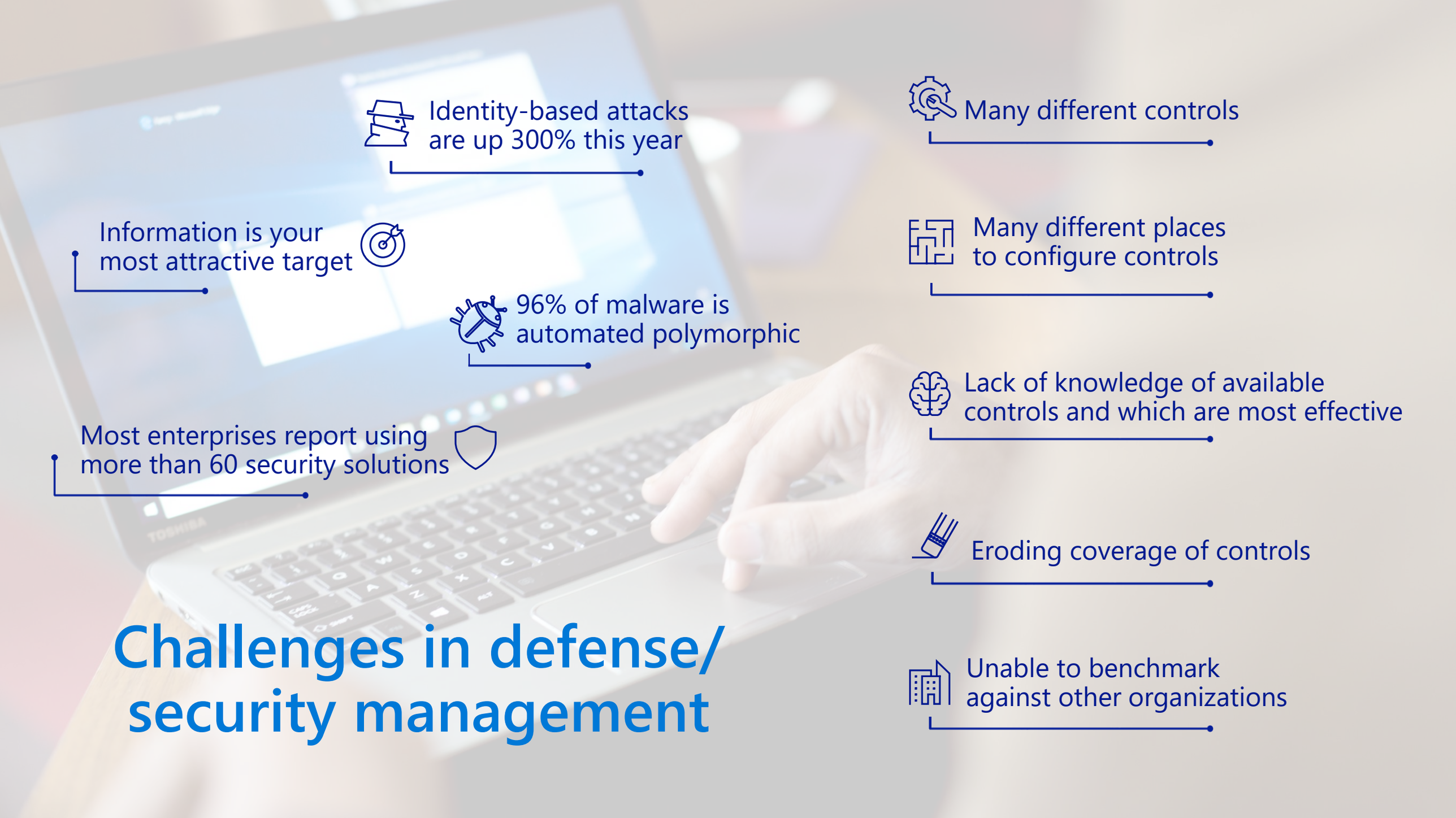
Data Loss Prevention
Identify and protect sensitive information

Device Management Policies
Protect & secure devices and the business data access by and stored on devices

Azure Information Protection
Classify, label, and protect files no matter where they are or where they go

Microsoft

Microsoft Secure Score



Challenges in defense/ security management

Identity-based attacks are up 300% this year

Information is your most attractive target

96% of malware is automated polymorphic

Most enterprises report using more than 60 security solutions

Many different controls

Many different places to configure controls

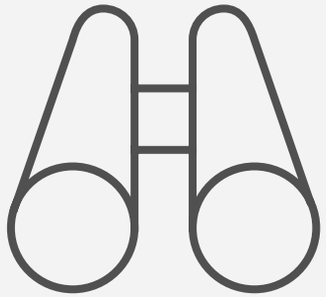
Lack of knowledge of available controls and which are most effective

Eroding coverage of controls

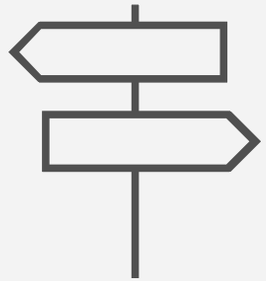
Unable to benchmark against other organizations

Microsoft Secure Score

Visibility into your Microsoft security position and how to improve it



Insights into your security position



Guidance to increase your security level

Insights

One place to understand your security position and what features you have enabled.

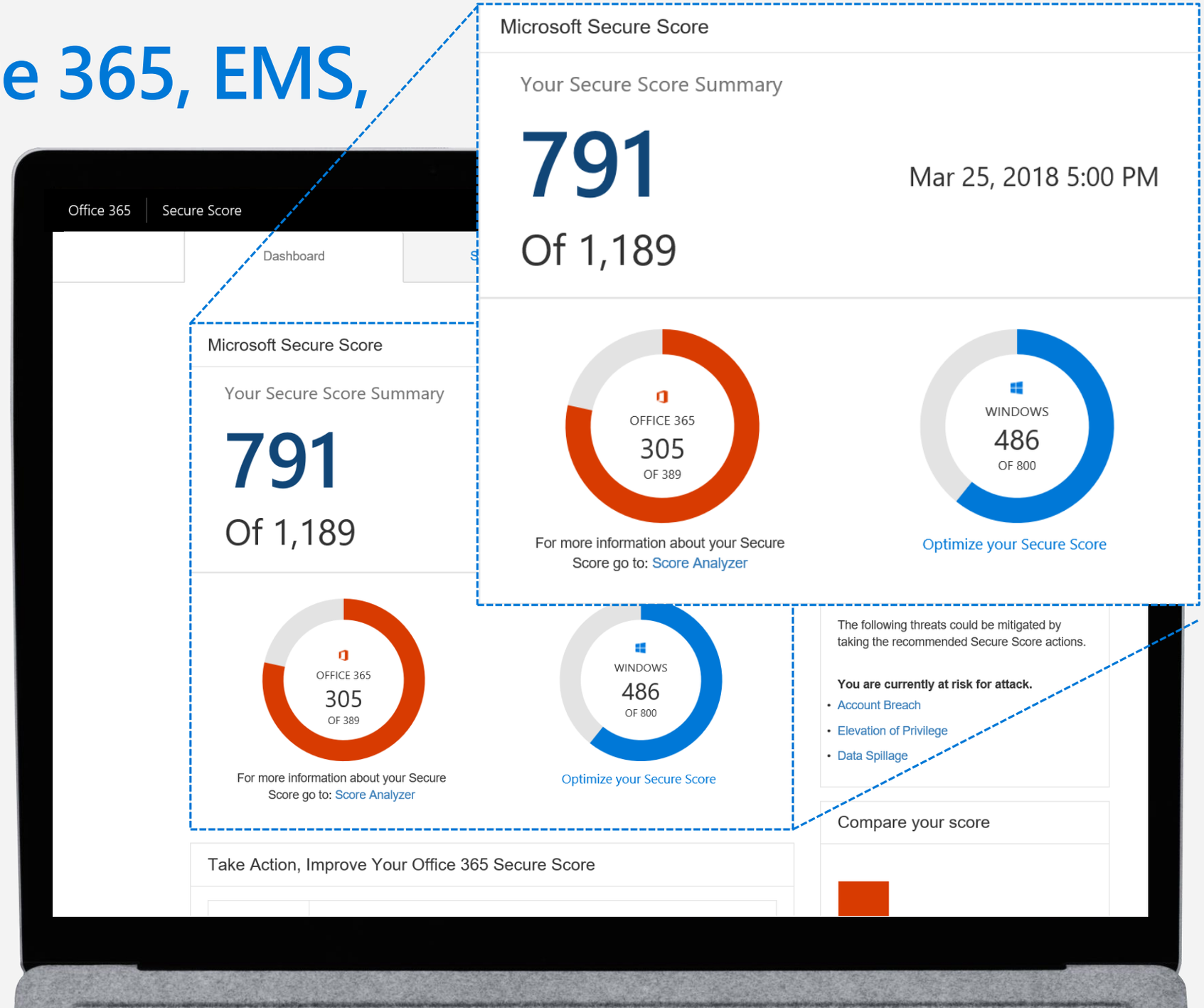
- Visibility into Office 365, EMS, and Windows 10.
- View historical score and trends.
- Easily compare score against other days and other organizations.

Support for Office 365, EMS, & Windows 10

Office 365 and Windows 10 scores part of summary

Azure Active Directory and Intune controls supported

59 controls supported

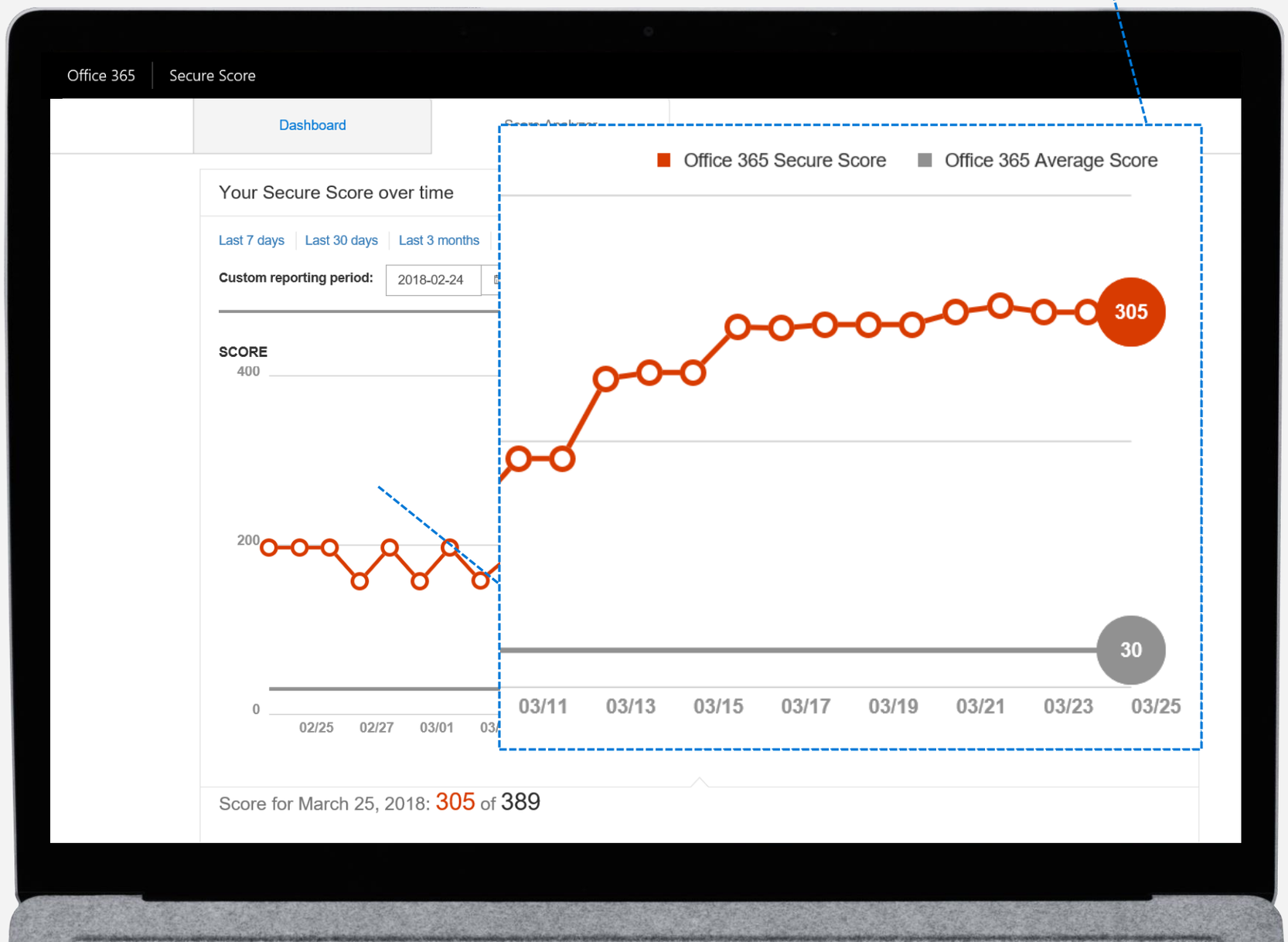


Historical score and trends

View score over the past 7, 30, or 90 days, or select a custom range

Detailed list of how you obtained points

Export data to pdf, csv, or via API



Secure Score API

Report to downstream tools like SIEM

Historical data using the Microsoft Graph API framework using REST

90 days of data on controls used and score

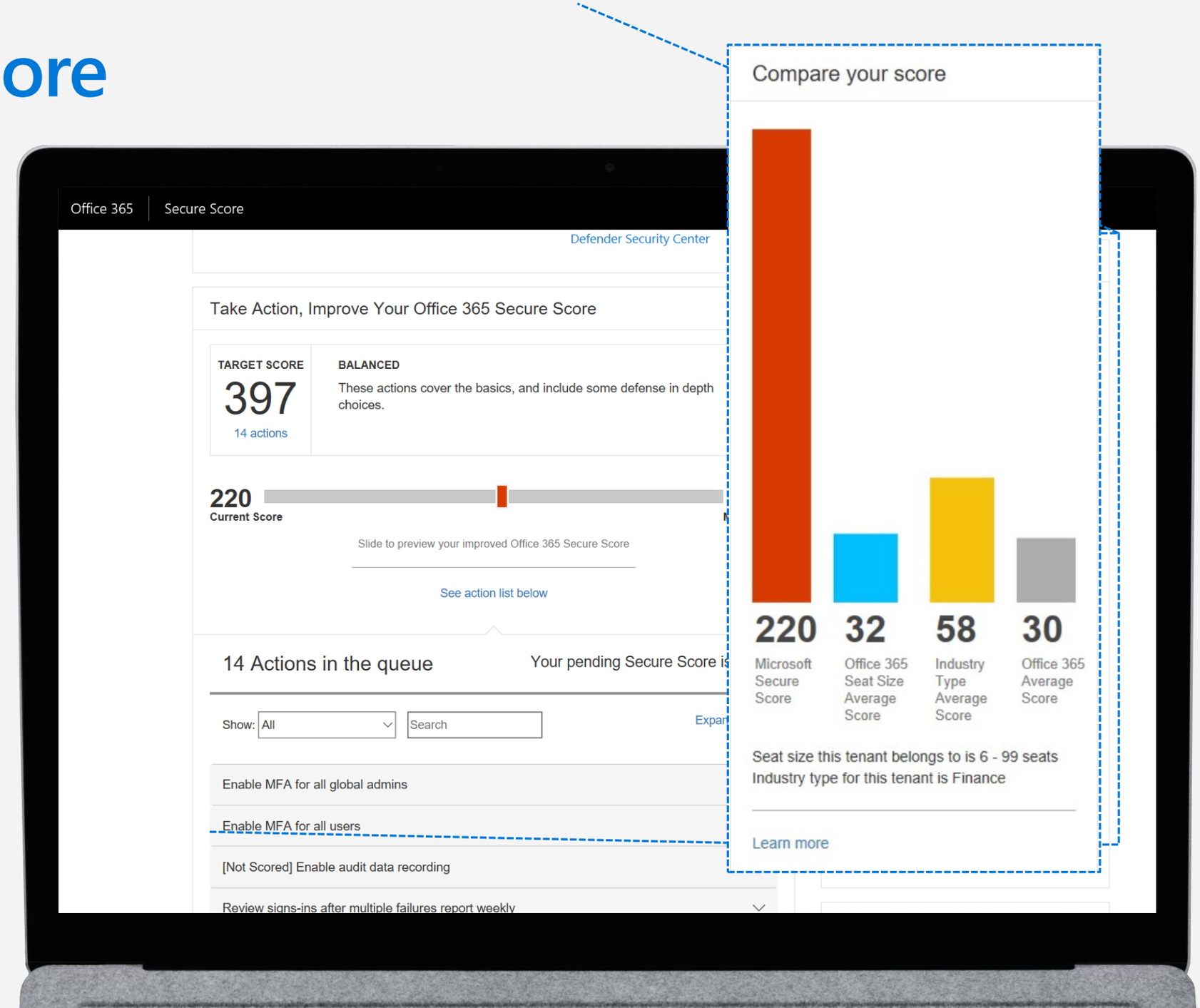
Learn more at: https://blogs.technet.microsoft.com/office365security/using-the-office-365-secure-score-api/


```
PS C:\WINDOWS\system32> HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
{
"value":[
{
"tenantId":"15f504b9-3b10-42a4-8777-3acf17064422",
"createdDateTime":"2018-03-23T00:00:00+00:00",
"licensedUsersCount":28,
"activeUsersCount":0,
"secureScore":115,
"organizationMaxScore":243,
"accountScore":33,
"dataScore":45,
"deviceScore":37,
"enabledService":[
“exchange”,
“lync”,
“sharepoint”,
“OD4B”,
“Yammer”
],
"controlScores":[{
"AdminMFA":[
{"score":"21"},
},

{"maxScore":"50"
},

{"count":"9"
},

{"total":"16"
}

],
"averageSecureScore":16.5588017,
"averageMaxScore":237.017166,
"averageAccountScore":3.69947028,
"averageDataScore":12.7047329,
"averageDeviceScore":0.154599056
}],
}]
}
```

Compare your score

Compare score from previous days to see what exactly changed

Benchmark against other organizations based on Office 365 average, size, and industry



Guidance

Learn what security features are available to reduce risk while helping you balance productivity and security.

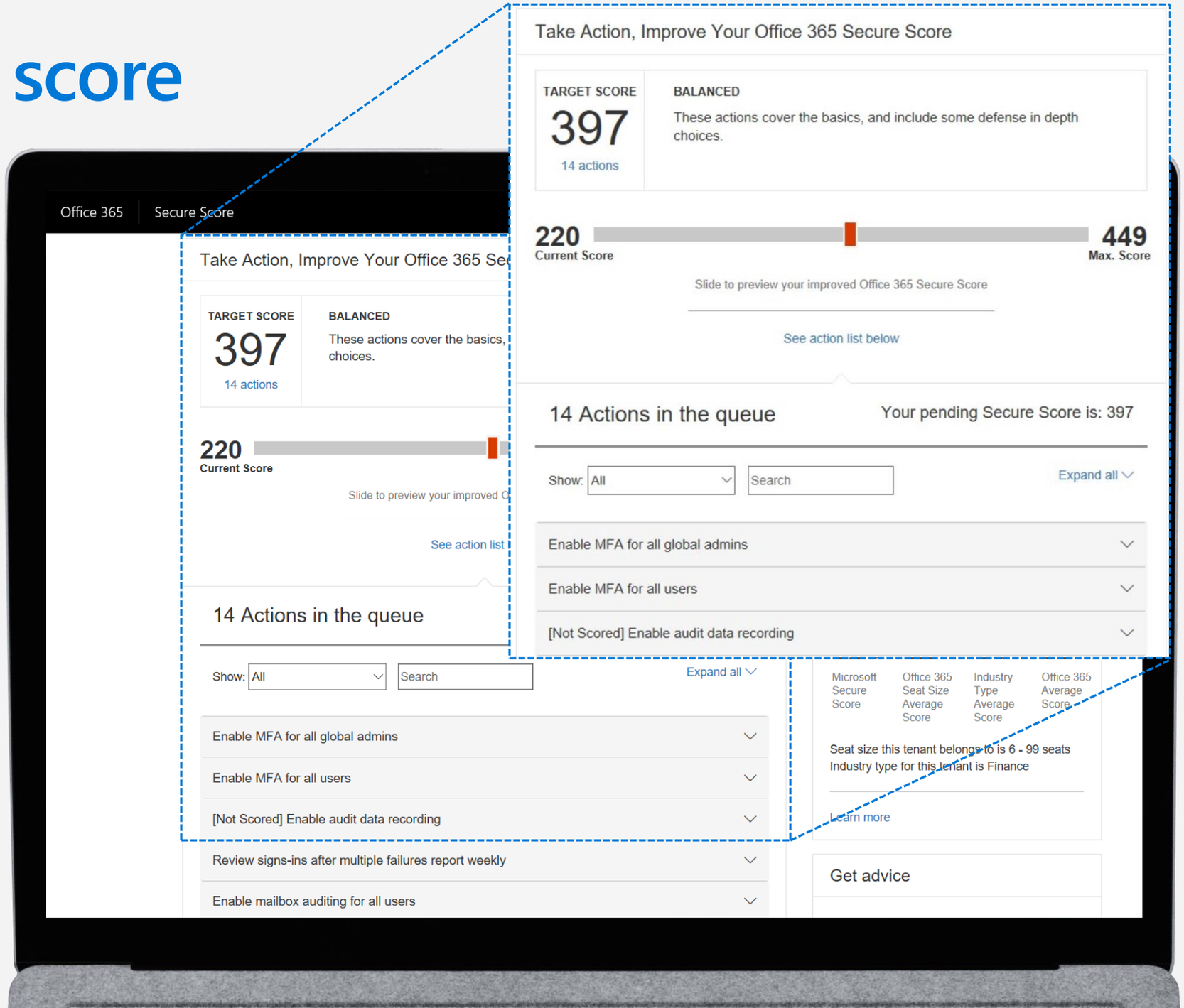
- Model your ideal score.
- Filter actions that meet your criteria.
- Ignore controls that are not valid for you.
- 3rd party product support.

Model your ideal score

Find the right balance of productivity and security

Prioritized actions based on effectiveness

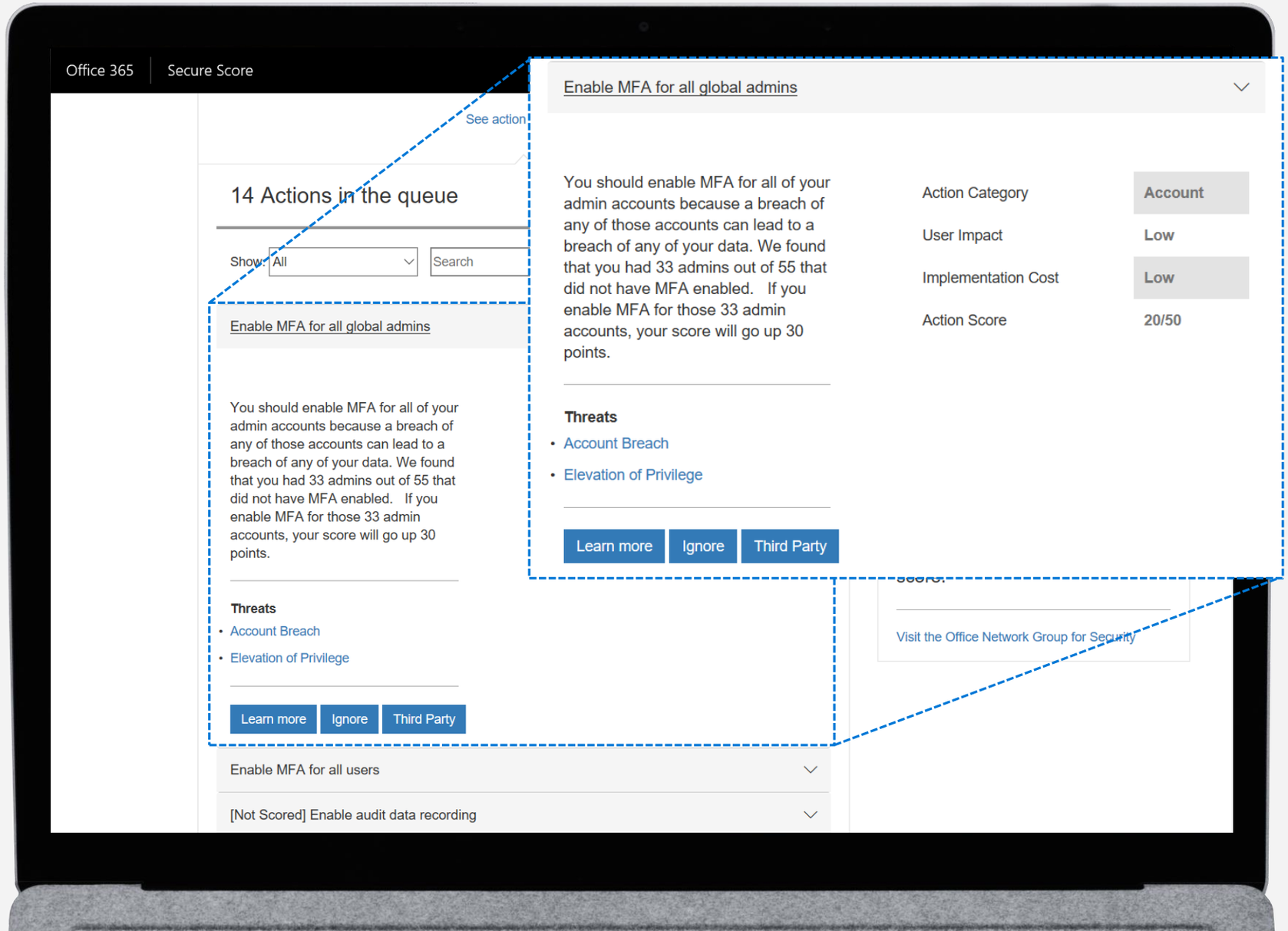
Filter and search for specific controls



Enable controls through Secure Score

Short description when you expand action

Get more details and enable control or take you to where you can enable

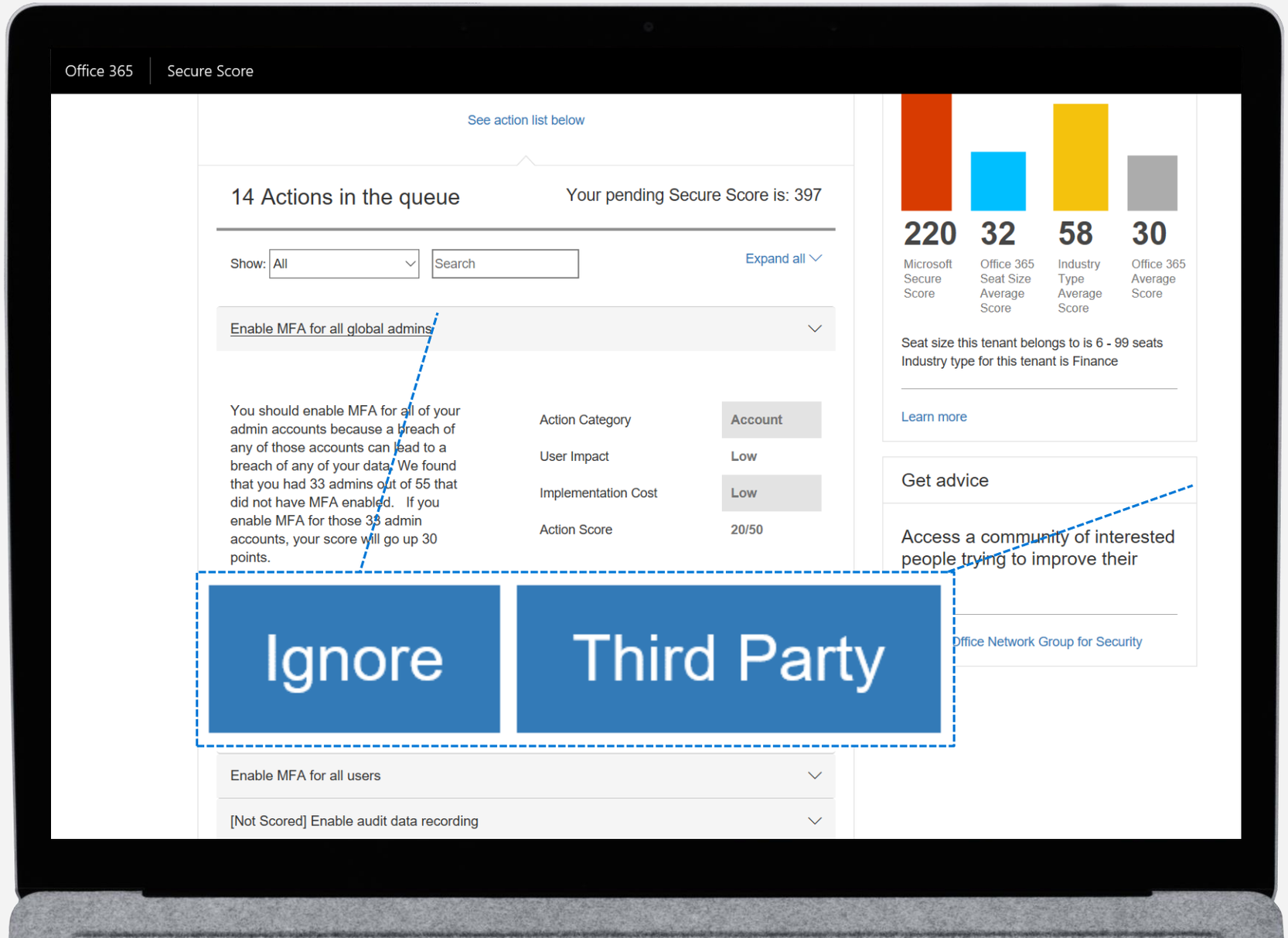


Getting credit for 3rd party solutions

Third party button provides points for controls meet though other solutions

Ignore controls that are not valid for you

Can remove designation though Score Analyzer



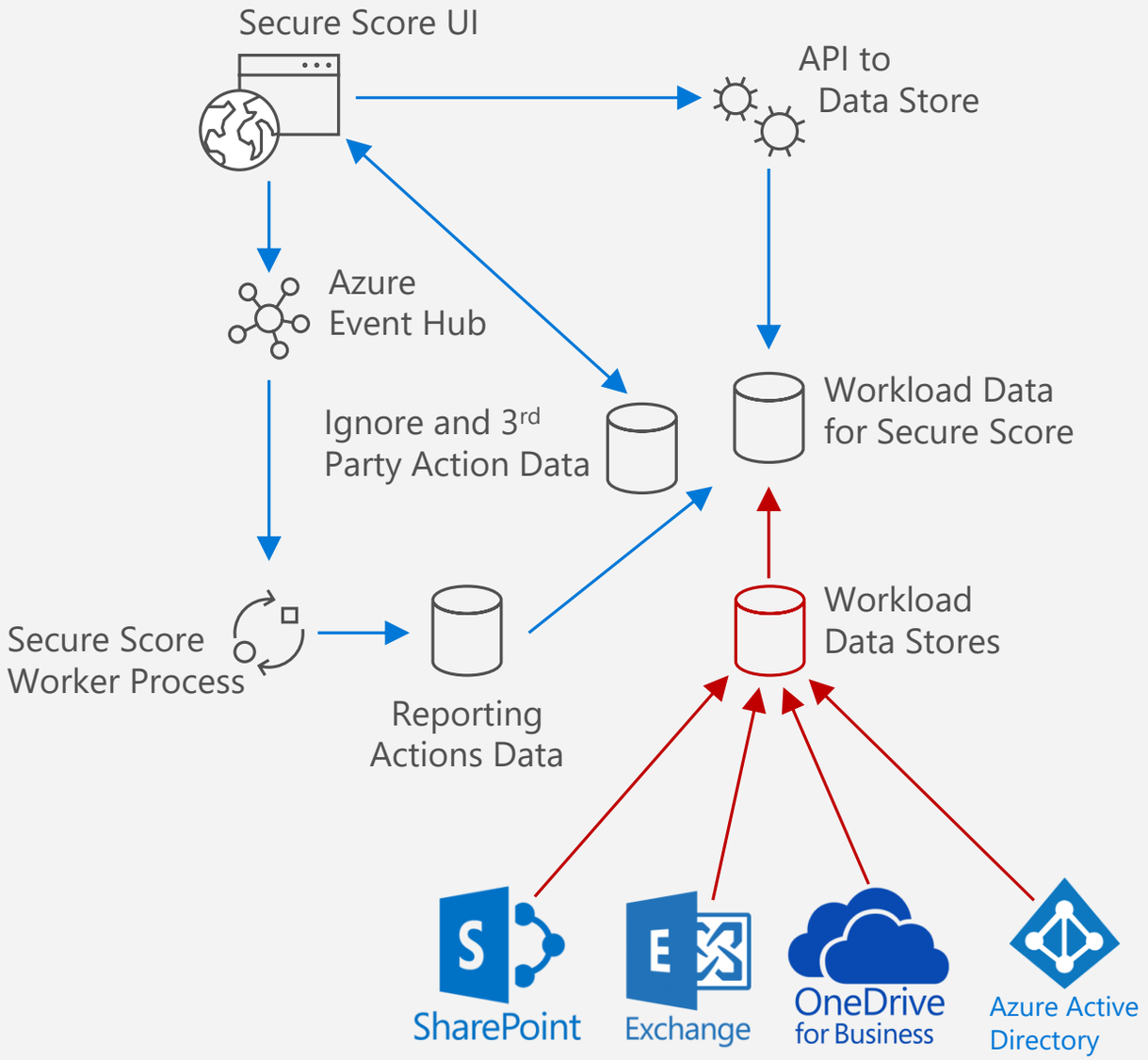
Demo

How scores get calculated

Nightly process collects telemetry from workloads

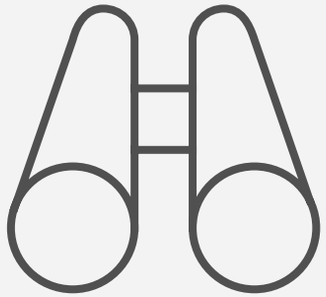
Ignore and 3rd party information is stored in another location

Reviewing report data is anonymized and store separately

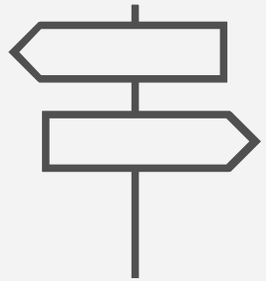


Microsoft Secure Score

Visibility into your Microsoft security position and how to improve it



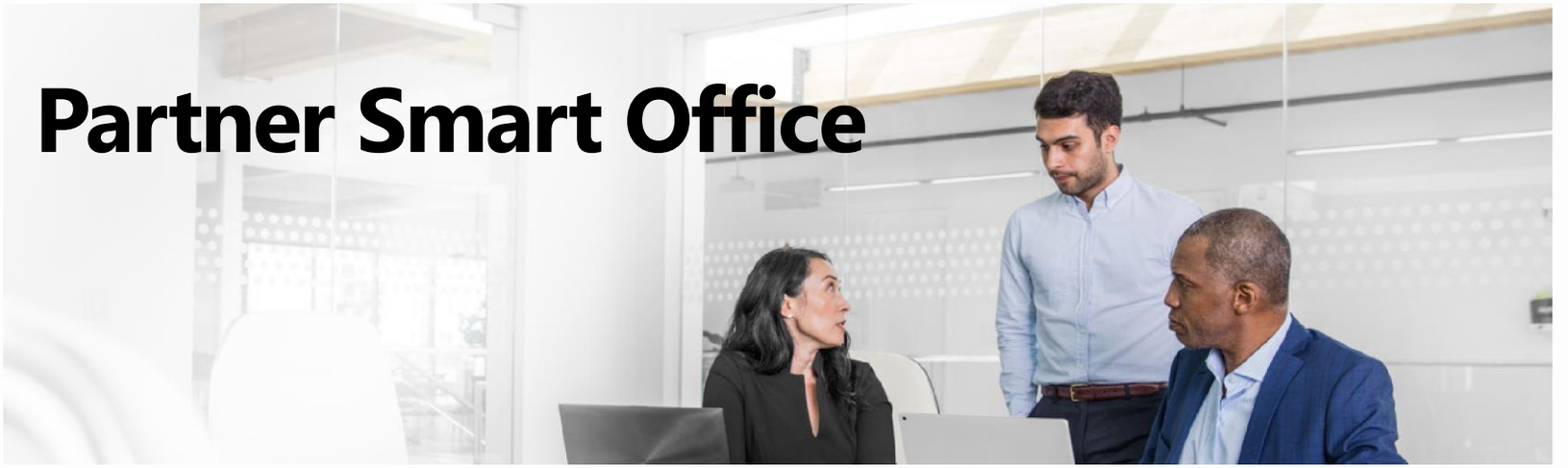
Insights into your security position



Guidance to increase your security level

Partner Smart Office

Partner Smart Office



An open source toolkit that empowers partners to better understand a customer's security posture.

Security is a primary concern for Microsoft, partners, and customers.

Office 365 customers are provided with many tools to help improve their security practices; however, many don't take advantage of the tools. To help customers manage security threats, Microsoft partners need a way to streamline and aggregate security information across their entire customer base. **A new open source solution called Partner Smart Office facilitates aggregation of information on customers with subscriptions obtained through an Enterprise Agreement or the Cloud Solution Provider (CSP) program.**

Partner Smart Office imports and aggregates information obtained from the Intelligent Security Graph and Office 365 Secure Score, enabling partners to take advantage of advanced analytics. These analytics are able to link threat intelligence and security data to provide insights that can strengthen a customer's organizational security. **Now, partners can also view security data across all of their customers at once**.

Customer

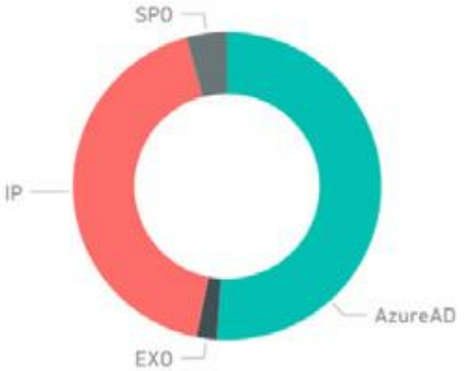
Forth Coffee

DISCLAIMER - Secure Score does not express an absolute measure of how likely you are to get breached. It expresses the extent to which you have adopted controls which can offset the risk of being breached. No service can guarantee that you will not be breached, and Secure Score should not be interpreted as a guarantee in any way

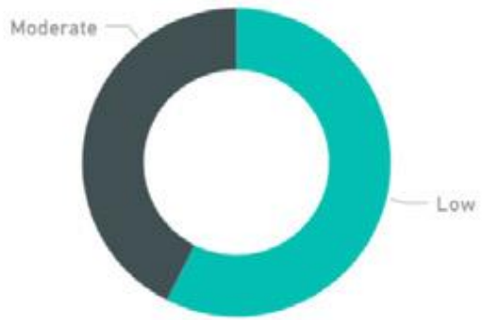
Secure Score

Score by Category

Score by Workload



Score by Implementation Cost



Licensed Users

1

Active Users

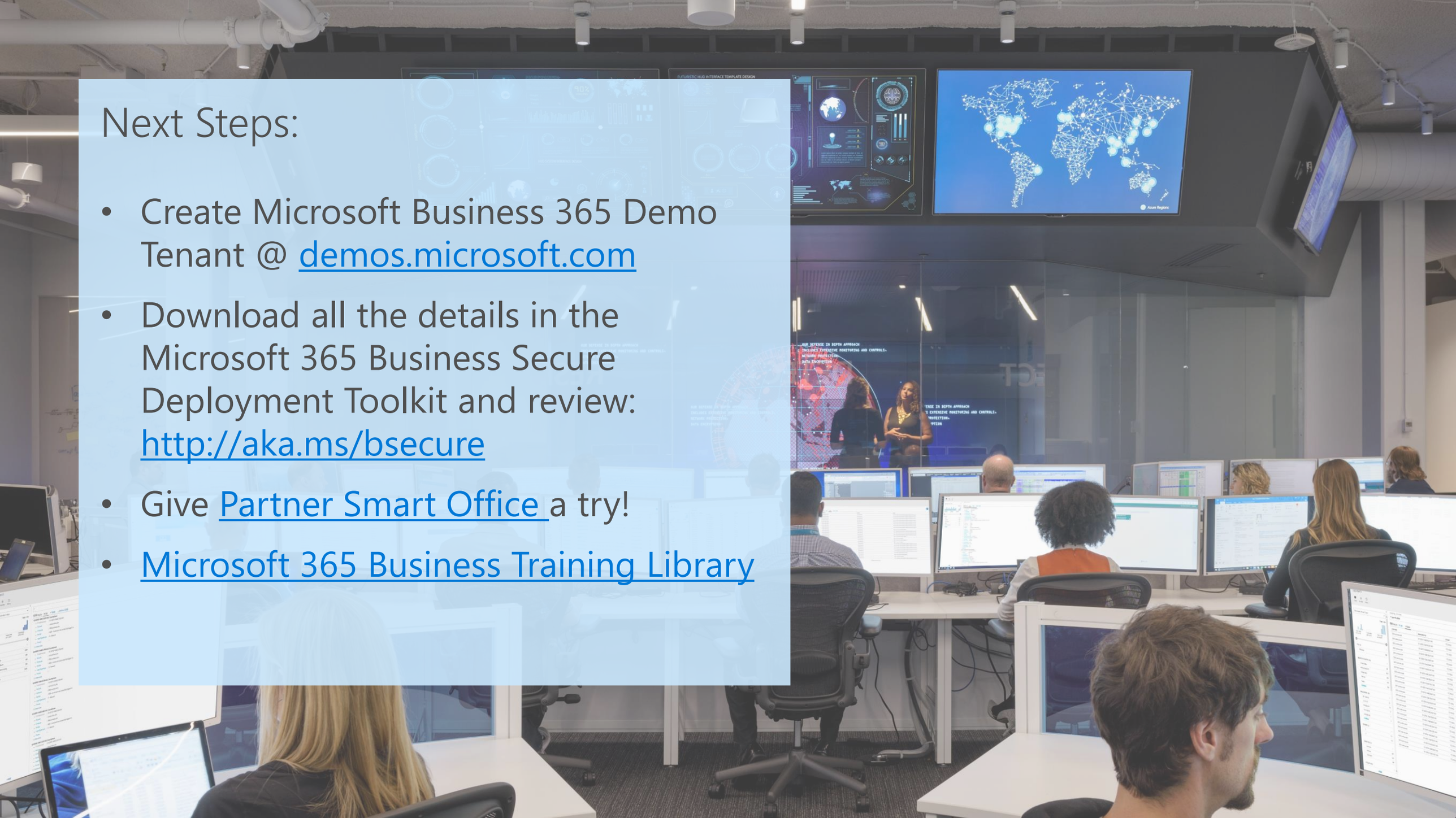
0

Outstanding Actions

36

Recommended Actions

Action Category	Name	Score	Max Score	Implementation Cost	User Impact	Workload	Action URL
Account	Disable accounts not used in last 30 days	0	1	Low	Moderate	AzureAD	https://portal.office.com/Admin/Defa
Account	Enable MFA for all global admins	0	50	Low	Low	AzureAD	https://account.activedirectory.windo
Account	Enable MFA for all users	0	30	Low	Moderate	AzureAD	https://account.activedirectory.windo
Account	Review account provisioning activity report weekly	0	5	Low	Low	AzureAD	https://portal.azure.com/#blade/Micr
Account	Review non-global administrators weekly	0	5	Low	Low	AzureAD	https://portal.office.com/Admin/Defa
Account	Review role changes weekly	0	10	Low	Low	AzureAD	https://portal.office.com/Admin/Defa
Account	Review signs-ins after multiple failures report weekly	0	45	Low	Low	AzureAD	https://portal.azure.com/#blade/Micr
Account	Use non-global administrative roles	0	1	Low	Low	AzureAD	https://portal.office.com/Admin/Defa
Data	Allow anonymous guest sharing links for sites and docs	0	1	Low	Moderate	SPO	https://%initialdomainshort%-admin.s
Data	Configure expiration time for external sharing links	0	2	Low	Moderate	SPO	https://%initialdomainshort%-admin.s
Data	Enable Advanced Threat Protection safe attachments policy	0	15	Low	Moderate	IP	https://portal.office.com/AdminPortal
Data	Enable Advanced Threat Protection safe links policy	0	15	Low	Moderate	IP	https://portal.office.com/AdminPortal
Data	Enable Client Rules Forwarding Block	0	20	Moderate	Moderate	EXO	https://outlook.office.com/ecp/RulesE
Data	Enable customer lockbox feature	0	5	Moderate	Moderate	EXO	https://portal.office.com/AdminPortal
Data	Enable Data Loss Prevention policies	0	20	Moderate	Moderate	IP	https://outlook.office365.com/ecp/?R
Data	Enable mailbox auditing for all users	0	10	Low	Low	EXO	https://github.com/OfficeDev/O365-I
Total		**0**	**315**				



Next Steps:

- Create Microsoft Business 365 Demo Tenant @ demos.microsoft.com
- Download all the details in the Microsoft 365 Business Secure Deployment Toolkit and review: http://aka.ms/bsecure
- Give Partner Smart Office a try!
- Microsoft 365 Business Training Library

Start today on your Microsoft 365 Business technical learning path

Start with:

1. Product service description
2. Partner technical overview
3. Licensing overview and Microsoft 365 Plans

Move to:

1. Start a demo tenant @ demos.microsoft.com
2. Secure deployment guide
3. Assessing current environments
4. Understanding cloud identity
5. Workload migration

Finish with:

1. Secure deployment kit
2. Android and IOS device management
3. Windows 10 management
4. Advanced Windows 10 deployment
5. Windows application deployment
6. Office 365 Business Premium deployment
7. Autopilot overview

Join:

- Join the Modern Workplace Technical Yammer Community
- Join the StepUp Technical Yammer Community

Hot off the Press:
New! Watch these short, on-demand videos to enable your technical practice – less than 17 minutes each

ANSWER OUR SURVEY FOR A CHANCE TO WIN!*

Take the survey here:
https://aka.ms/stepupsession1

The prize: Technology Travel Kit.
We will announce the winner
in November.

*Terms and Conditions on Yammer here or email SMBIn@microsoft.com.
One winner/one prize total, for four-session event series.

Thank you!