



Microsoft Security Labs

Microsoft Modern Work Team

Dicker Data

February 2024



Notable information

Demo labs via your MPN (cdx.transform.microsoft.com)
Contact: microsoft.presales@dickerdata.com.au

We are recording the session – We will share a link to the recording AFTER the event – you cannot download it directly from Teams.

Series Agenda



Part 1 (Today, 27th February)

- Security Foundations
- Identity Security
- Email Protection
- Defender for Business

Part 2 (Tuesday, 5th March)

- Autopilot
- Intune & Security
- Endpoint Management

Part 3 (Tuesday, 12th March)

- Introduction to Copilot for Microsoft 365
- Copilot Readiness
- Information Governance
- Purview

Defender for Endpoint Demo

- Simulated Attacks
- Power Automate Flow for Device Isolation

Security foundation

 ASCEND

Cyberthreats – primer

Phishing Fraud in which an attacker masquerades as a reputable person. It's often easier to trick someone than to hack in.

Ransomware Malicious encryption software that blocks access to systems and demands a sum of money to unlock. An infected PC can spread the ransomware to other computers on your network.

Fileless attacks use malicious scripts that hijack legitimate software and load malware into memory, without saving to the file system. This makes the malware harder to detect.

Live off the land attacks use trusted software and system tools to carry out their work. Examples are administrative shells, antivirus programs, RMM software, etc. This makes it difficult to detect and/or determine who is behind the activity.

Why should SMB customers care about security?



Perception

I am too small a business for hackers to attack me...only large enterprises need to worry about security...

Reality

"Someone was **fooled by the email from the CEO** and used his Corp card to send the iTunes gift cards. We lost about \$5,000."

— *Adam A., equipment rentals, 150 employees*

"The only reason **we caught it** was that it was a 6-digit sales order and our sales orders are 7 digits."

— *Joe B, food distribution, 250 employees*

"They **got someone's password**, and sent an email to our CFO, who sent the \$40,000 wire transfer."

— *Bob K., property management, 150 employees*

Security is top of mind for SMB customers

+300%

Ransomware attacks in the past year, with more than 50% targeted at small businesses ¹



1 in 4

Nearly one in four SMBs state that they had a security breach in the last year²

70%

Over 70% of SMBs think cyber threats are becoming more of a business risk²

90%

SMBs would consider hiring a new MSP if they offered the right cybersecurity solution²

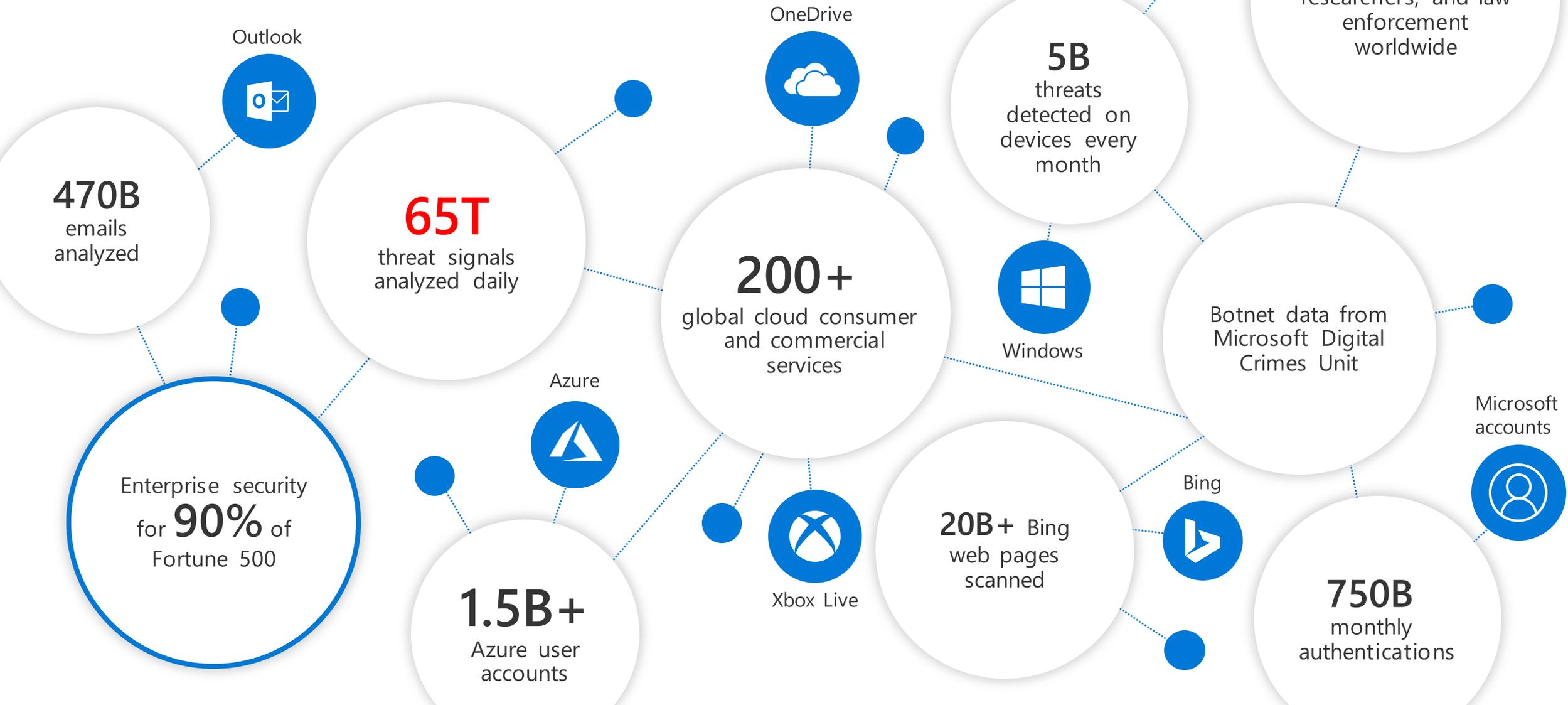


60%

of businesses close permanently within six months of an attack.³

1. [Homeland Security Secretary Alejandro Mayorkas, 06 May 2021 ABC report](#)
2. [Microsoft commissioned research, April 2022, US SMBs 1-300 employees](#)
3. [Why small businesses are vulnerable to cyberattacks, May 2022](#)

Microsoft has competitive advantage in Security





Microsoft Security— a Leader in 5 Gartner Magic Quadrant reports

*Gartner “Magic Quadrant for Access Management,” by Henrique Teixeira, Abhyuday Data, Michael Kelley, November 2021

*Gartner “Magic Quadrant for Cloud Access Security Brokers,” by Craig Lawson, Steve Riley, October 2020

*Gartner “Magic Quadrant for Enterprise Information Archiving,” by Michael Hoech, Jeff Vogel, October 2020

*Gartner “Magic Quadrant for Endpoint Protection Platforms,” by Paul Webber, Rob Smith, Prateek Bhajanka, Mark Harris, Peter Firstbrook, May 2021

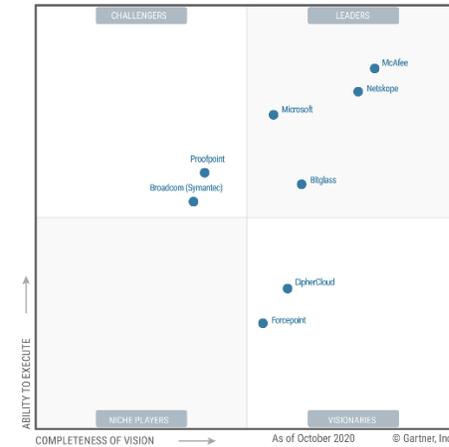
*Gartner “Magic Quadrant for Unified Endpoint Management,” by Dan Wilson, Chris Silva, Tom Cipolla, August 2021

These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.



Source: Gartner (November 2021)

Access Management



Source: Gartner (October 2020)

Cloud Access Security Brokers



Source: Gartner (October 2020)

Enterprise Information Archiving



Source: Gartner (May 2021)

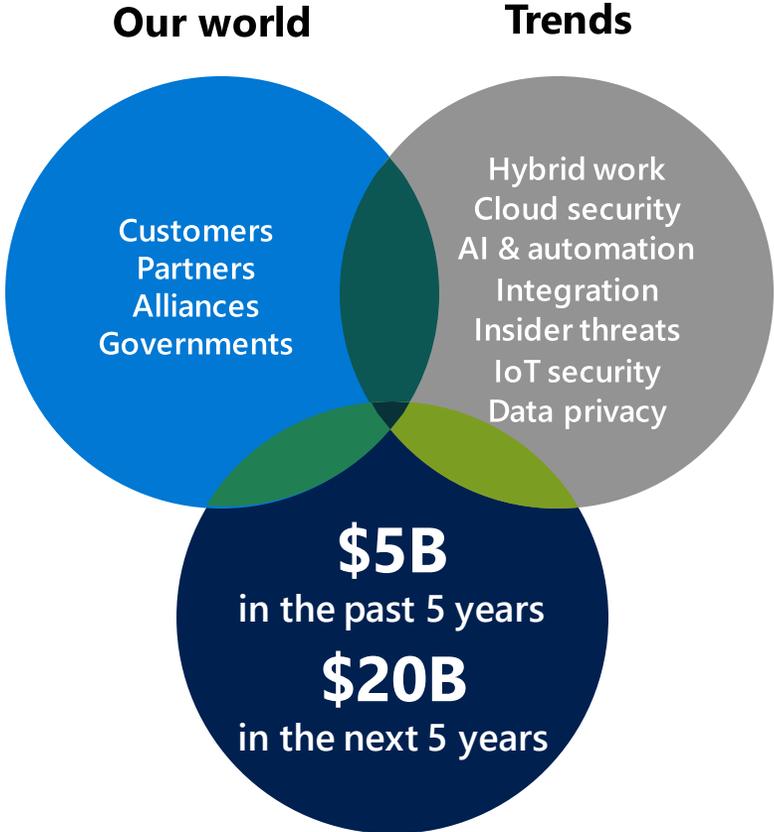
Endpoint Protection Platforms



Source: Gartner (August 2021)

Unified Endpoint Management

Continual innovation to increase your advantage against bad actors



- 2004 Endpoint antimalware
- 2005 Email protection
- 2013 Multifactor authentication
- 2015 Cloud security
Information protection and governance
Machine learning (security-specific)
- 2019 Cloud native SIEM
XDR
- 2020 Integrated SIEM and XDR
Agentless IoT/OT security monitoring
Insider risk management
- 2021 Decentralized identity
Unified privileged access & cloud entitlement management
- 2022 Identity governance
- 2023 Threat intelligence platform
Attack surface management
Generative AI (security-specific)

> many more to come...

What is Microsoft 365 Business Premium?

A comprehensive security solution that is integrated with Office 365



**Defend against
cyberthreats**



**Protect
business data**



**Secure
your devices**

**All the capabilities of Microsoft 365 Business Standard, plus
advanced cybersecurity, data protection, and device management**

Security built into Microsoft 365

Microsoft 365 includes built-in security protections

- ✓ Encryption of data at rest and in transit
- ✓ Continuous data backup via replication to geo-redundant servers
- ✓ Robust spam and virus filtering
- ✓ “Red team / Blue team” exercises
- ✓ Microsoft invests \$4B per year on security

Protections are on by default; no action necessary



Check your Secure Score

The problem:

You want to improve your customer's security, but don't know where to start

The solution:

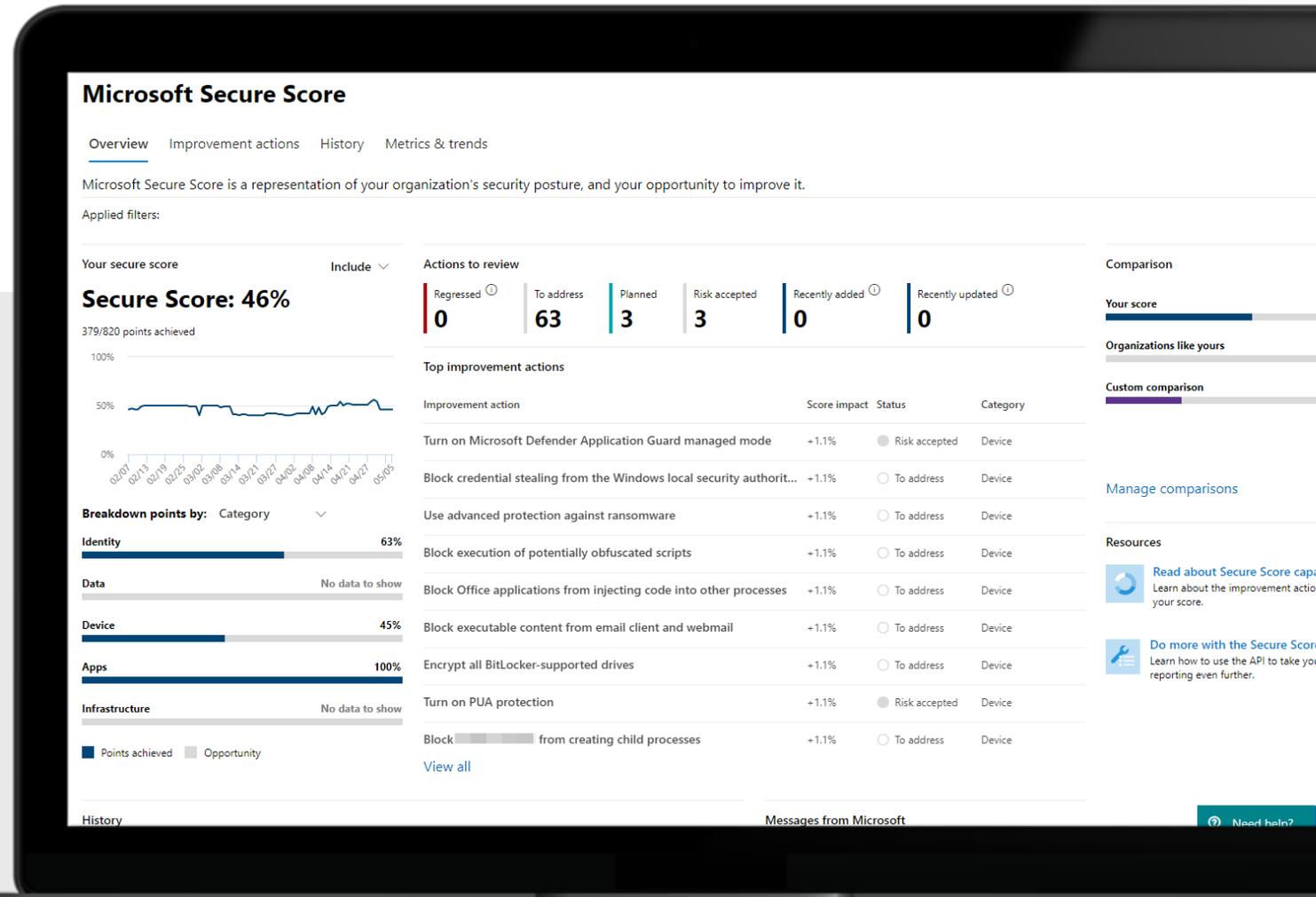
Check Microsoft Secure Score

What it is:

Microsoft Secure Score analyzes your Microsoft 365 overall security and assigns a score. Secure Score also recommends next steps to consider in order to improve security.

How to access:

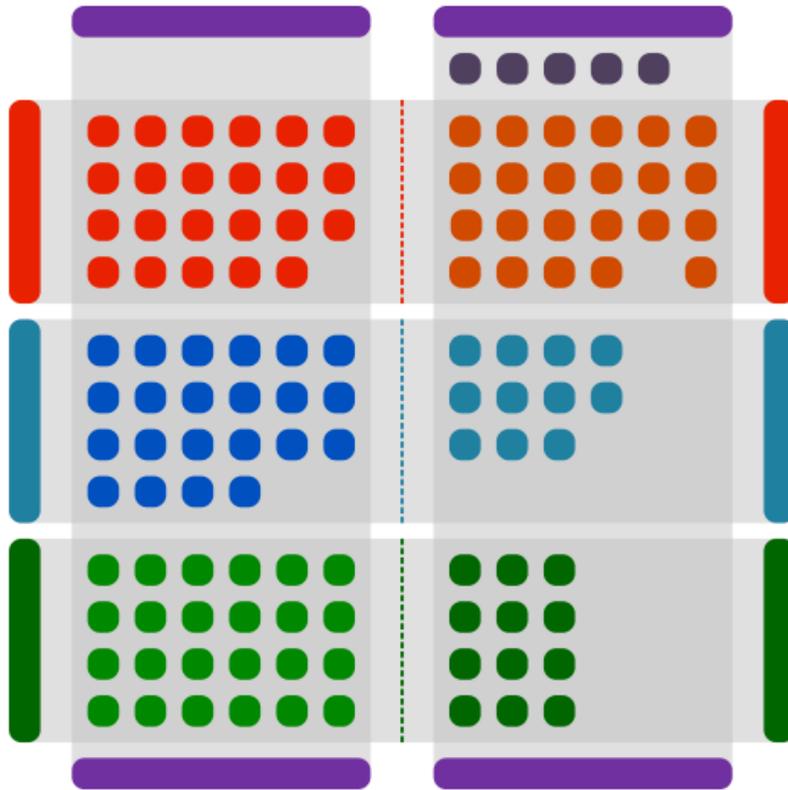
<https://security.microsoft.com/securescore>





M365 Maps

ASCEND



Microsoft 365 Licensing

By Aaron Dinnage

Microsoft 365 Enterprise, Business, Education, Frontline, and Consumer

Office 365, Enterprise Mobility + Security, Windows, Project, and Visio

m365maps.com

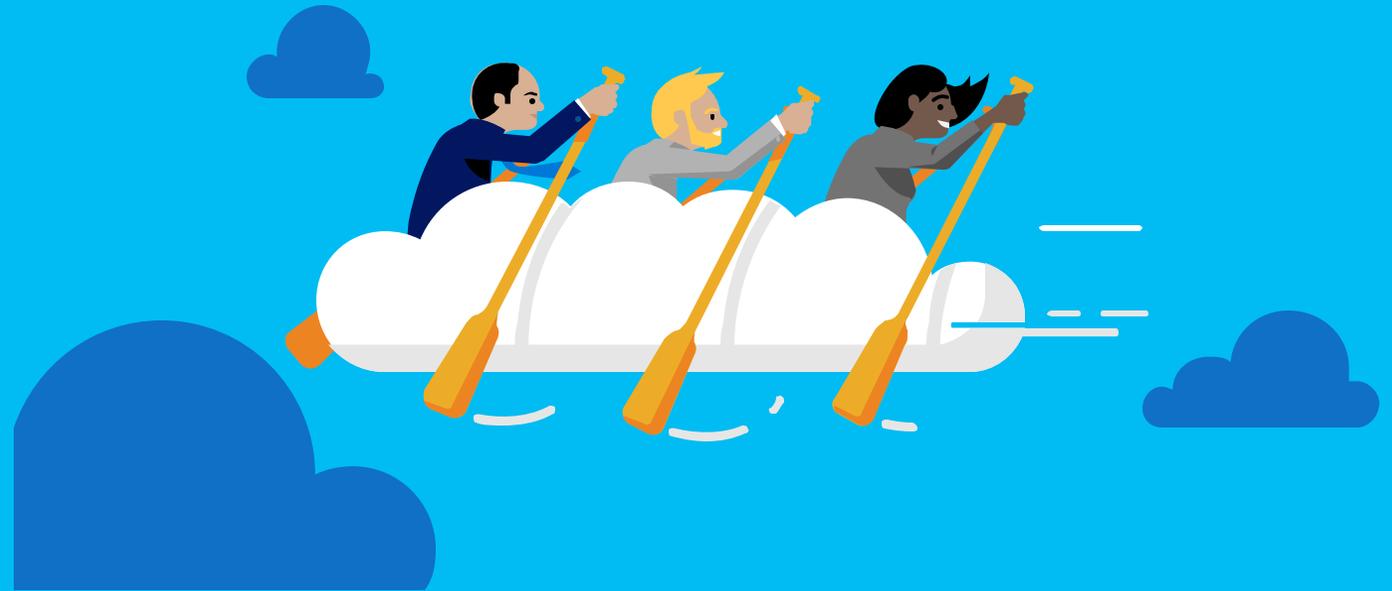
Pop quiz

01

As you implement security for your customer their Secure Score should go up. When should we expect to see changes reflected in Secure Score?

Immediately

Tomorrow



Defender for Business & Endpoint

Microsoft Defender for Business

Elevate your security

Elevate your security with enterprise-grade endpoint protection specially built for businesses with up to 300 employees.



Enterprise-grade protection

Security for all your devices with next-gen protection, endpoint detection and response, and threat and vulnerability management.



Easy to use

Streamline onboarding with wizard-driven set up and recommended security policies activated out-of-the-box to quickly secure devices.



Cost-effective

Endpoint security that keeps you productive and works with your IT without compromising budget.

How to purchase Microsoft Defender for Business

Microsoft 365 Business Premium

Comprehensive productivity and security solution

Per user license

Microsoft 365 Business Standard (\$22.44)
Office apps and services, Teams



Microsoft Defender for Business
Microsoft Defender for Office 365 Plan 1
Intune
Azure AD Premium Plan 1
Azure Information Protection Premium P1
Exchange Online Archiving
Autopilot
Azure Virtual Desktop license
Windows 10/11 Business
Shared Computer Activation

Microsoft Defender Business →
Enterprise-grade
endpoint security

Per user license

- ✓ Next generation protection
- ✓ Cross Platform support (iOS, Android, Windows, MacOS)
- ✓ Endpoint Detection and Response
- ✓ Threat and Vulnerability Management
- ✓ ...and more

1) As standalone SKU, *up to 300 users*
Entitlement for use on up to 5 devices

2) Included as part of Microsoft 365
Business Premium, *up to 300 users*

Microsoft 365 Offerings for SMBs

Microsoft 365 Business Basic

Cloud Services



\$10.80 per user/month

Microsoft 365 Business Standard

Cloud Services



Desktop Apps



\$22.44 per user/month

Microsoft 365 Business Premium

Cloud Services



Desktop Apps



Comprehensive Security



\$39.40 per user/month

Price is subject to change based on subscription term and is excluding GST

Note: Not all features/product logos shown.

Cost Savings With Microsoft 365 Business Premium

Reduce operation costs



Reduce license costs

- 35% • Reduction in the likelihood of a data breach
- 23% • Cut spending on employee devices
- 25% • Cut time deploying, managing new software
- 75% • Cut endpoint configuration times
- 15% • Cut help desk tickets and resolution time
- 25% • Cut costs on travel and expenses
- 60h • Improvement of end-user productivity

\$150+ per user/month



\$39.40 per user/month

Communication e.g., Zoom, Webex
Collaboration e.g., Slack, Google Meet / Hangouts
File Sharing e.g., Box, Confluence
Endpoint Mgmt. e.g., Workspace ONE, MaaS360
Email e.g., Gmail, MDAemon
Storage e.g., Box, Dropbox
Mobile Device Mgmt. e.g., Mobile Iron, Airwatch
Identity & Access e.g., Okta, Hennge
Labeling & Encrypt e.g., SolarWinds, CoSoSys
Endpoint Protection e.g., CrowdStrike, Fortinet

Microsoft
365 Business
Premium
\$39.40

Savings of **\$100+** user/month

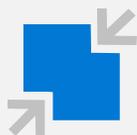


Microsoft Defender for Business

→ Elevate your security ←



Threat & Vulnerability
Management



Attack Surface
Reduction



Next Generation
Protection



Endpoint Detection
& Response



Auto Investigation
& Remediation



Simplified Onboarding
and Administration



APIs and Integration

Threat & Vulnerability Management



A risk-based approach to mature your vulnerability management program



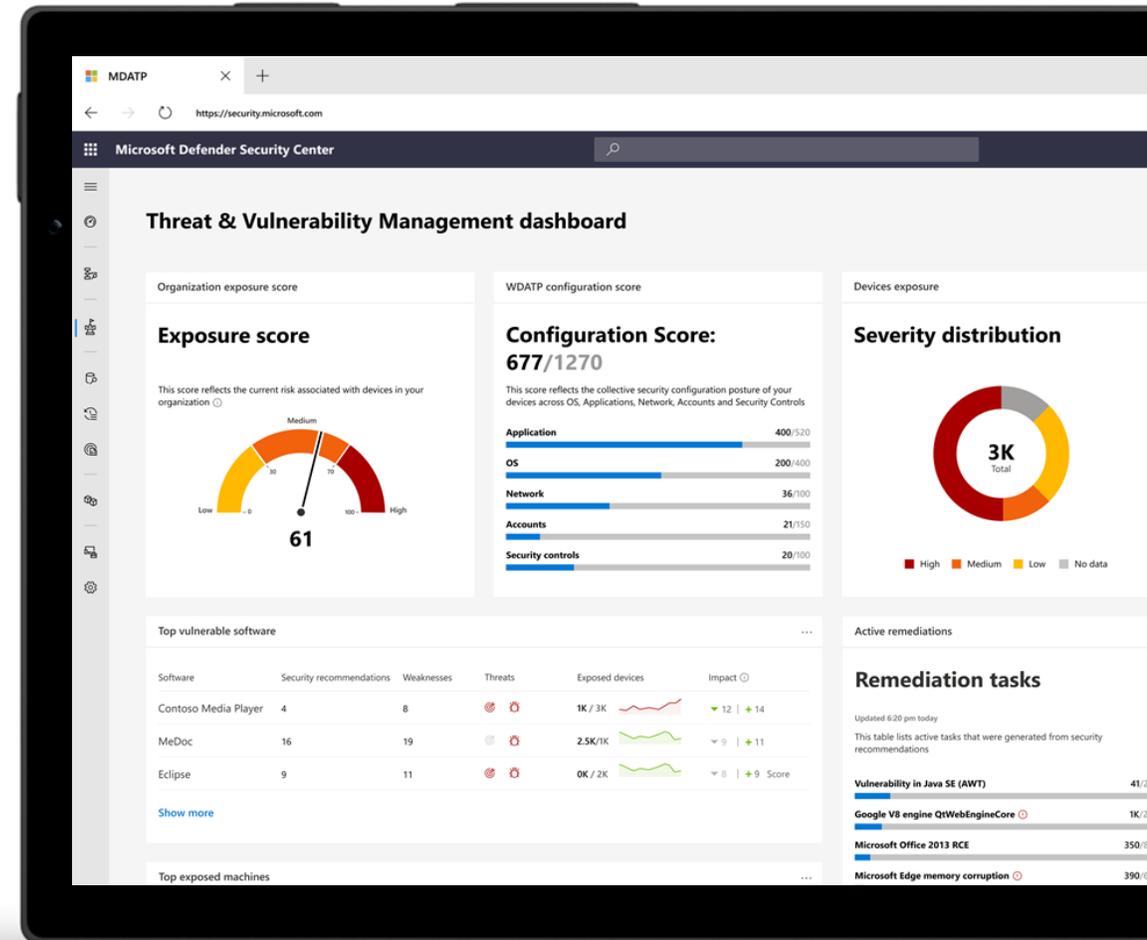
Continuous real-time discovery



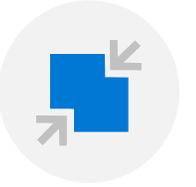
Context-aware prioritization



Built-in end-to-end remediation process



Attack Surface Reduction



Protect against risks by reducing the surface area of attack



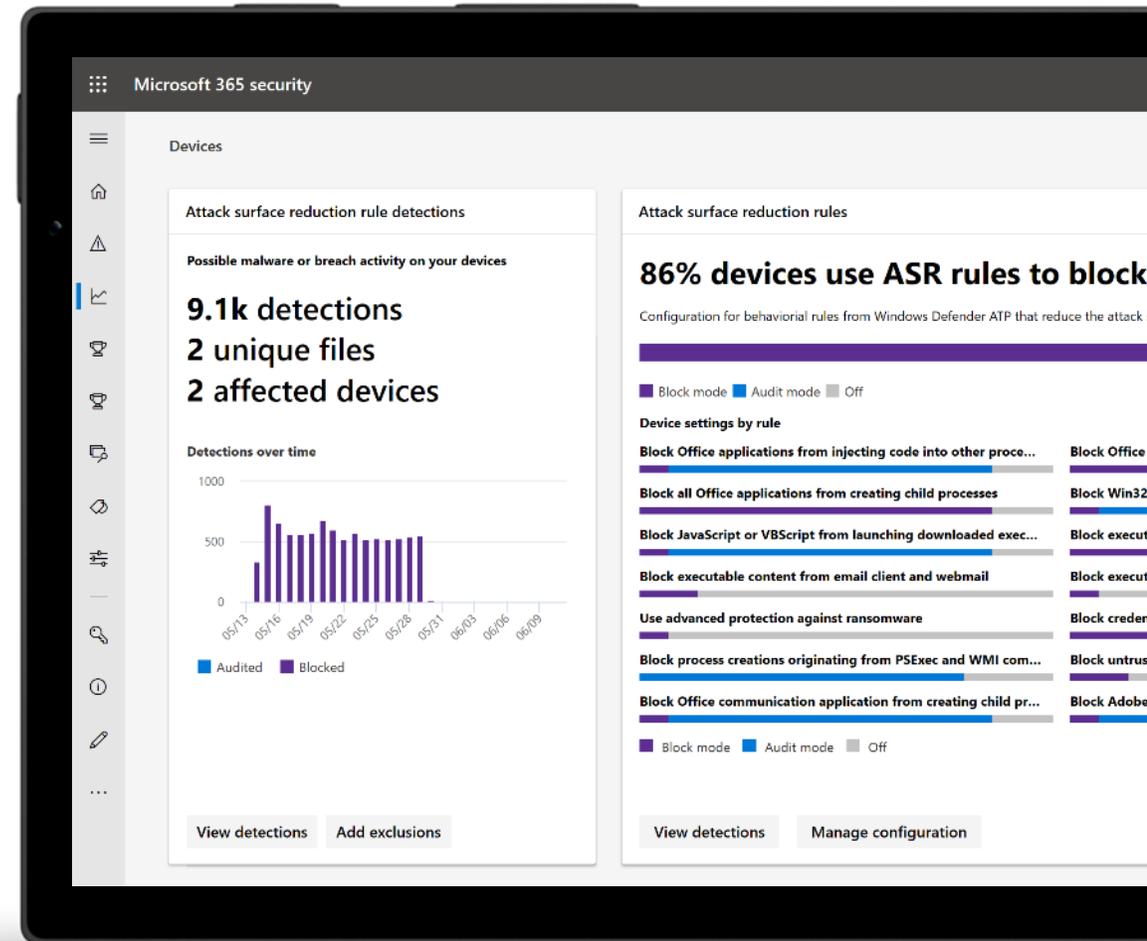
System hardening without disruption



Customization that fits your organization



Visualize the impact and simply turn it on



Next Generation Protection



Helps block and tackle sophisticated threats and malware



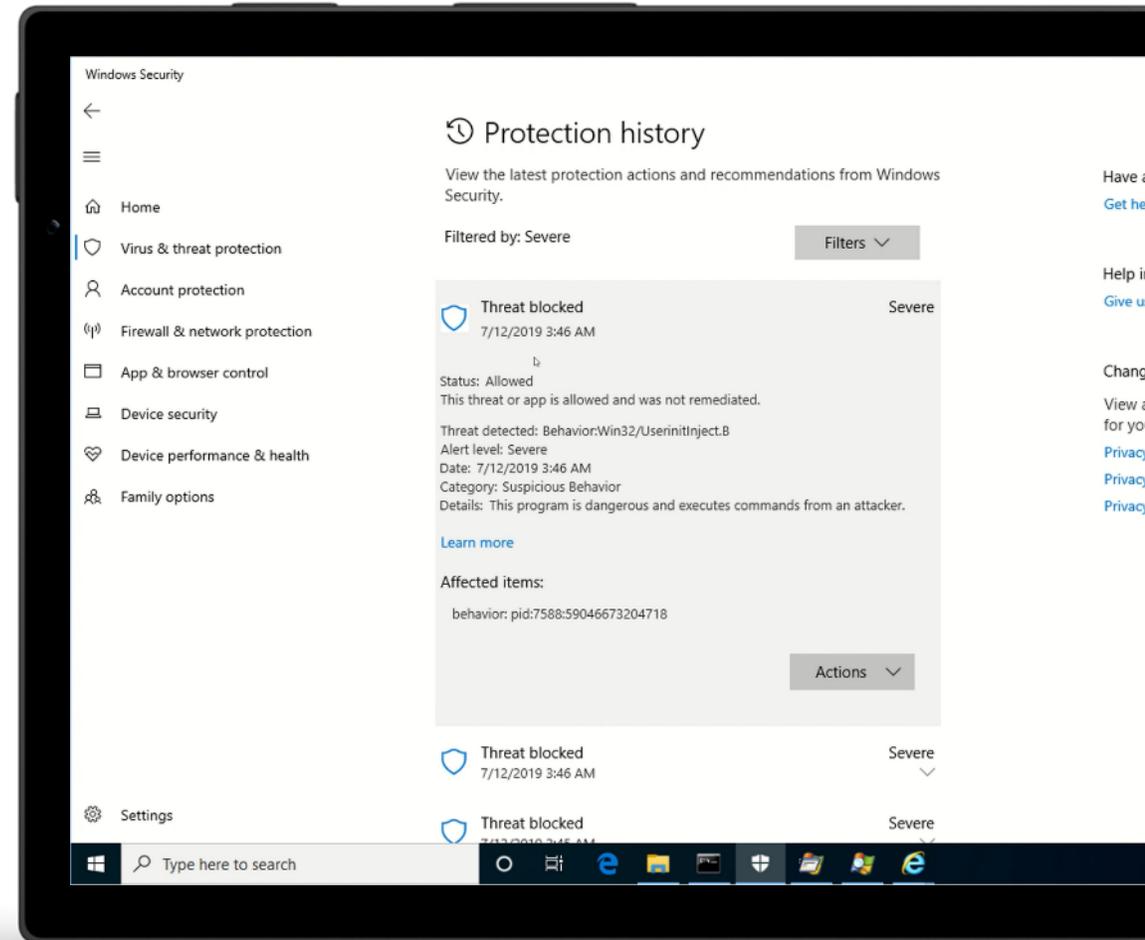
Behavioral based real-time protection



Blocks file-based and fileless malware



Stops malicious activity from trusted and untrusted applications



Endpoint Detection & Response



Detect and investigate advanced persistent attacks



Behavioral-based detection



Manual response actions for a device or file



Live response to gain access to devices

The screenshot displays the Windows Defender Security Center interface. The main section is titled "Incidents" and shows a list of security events. The table below summarizes the visible incidents:

Incident name	Severity	Category	Alerts	Machines	Users	Last activity	Classification
2195	Medium	General, Persistence, Suspicious Activity, Delivery	11	1	1	10/17/18, 5:25 PM	Not set
2195	Medium	Installation	1	1	1	10/17/18, 4:04 PM	Not set
2191	Medium	General, Suspicious Activity	2	1	1	10/16/18, 8:57 AM	Not set
2194	Low	Suspicious Network Traffic	1	1		10/16/18, 7:31 AM	Not set
2192	Low	Suspicious Network Traffic	1	1		10/16/18, 7:12 AM	Not set
2193	Low	Suspicious Network Traffic	1	1		10/16/18, 7:25 AM	Not set
2190	Low	Suspicious Network Traffic	1	1		10/16/18, 5:59 AM	Not set
2189	Low	Suspicious Network Traffic	1	1		10/16/18, 6:30 AM	Not set
2188	Low	Suspicious Network Traffic	1	1		10/16/18, 2:04 AM	Not set
2183	Low	Suspicious Network Traffic	1	1		10/15/18, 5:52 PM	Not set
2187	Low	Suspicious Network Traffic	1	1		10/15/18, 5:55 PM	Not set
2185	Low	Suspicious Network Traffic	1	1		10/15/18, 5:48 PM	Not set
2184	Low	Suspicious Network Traffic	1	1		10/15/18, 5:26 PM	Not set
2185	Low	Suspicious Network Traffic	1	1		10/15/18, 5:19 PM	Not set
2182	Low	Suspicious Network Traffic	1	1		10/16/18, 2:59 PM	Not set
2181	Low	Suspicious Network Traffic	1	1		10/16/18, 2:27 PM	Not set
2180	Low	Suspicious Network Traffic	1	1		10/16/18, 2:30 PM	Not set
2178	Low	Suspicious Network Traffic	1	1		10/16/18, 2:22 PM	Not set
2179	Low	Suspicious Network Traffic	1	1		10/15/18, 11:08 PM	Not set

Auto Investigation & Remediation



Automatically investigates alerts and helps to remediate complex threats



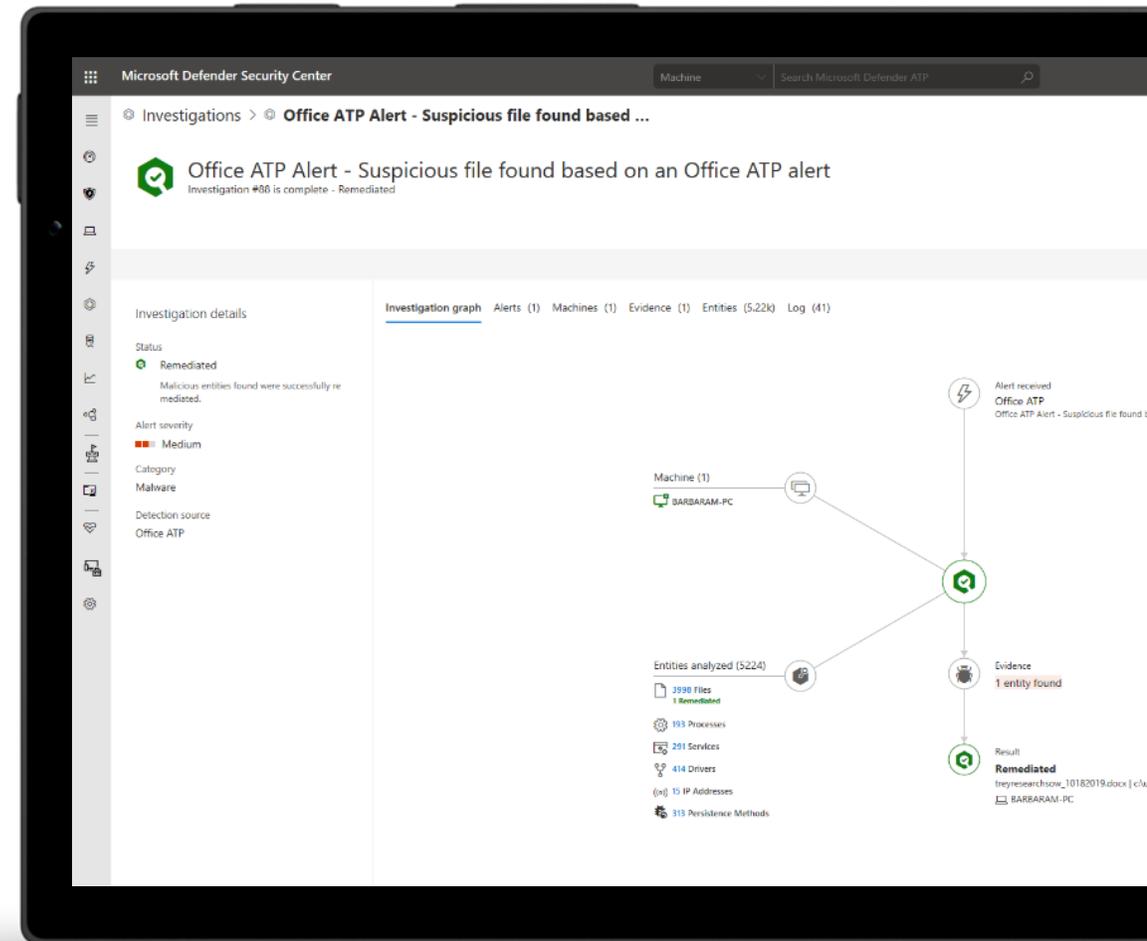
Mimics the ideal steps analysts would take



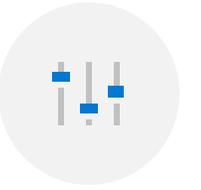
Tackles file or memory-based attacks



Scales security operations with 24x7 automated responses



Simplified Onboarding and Administration

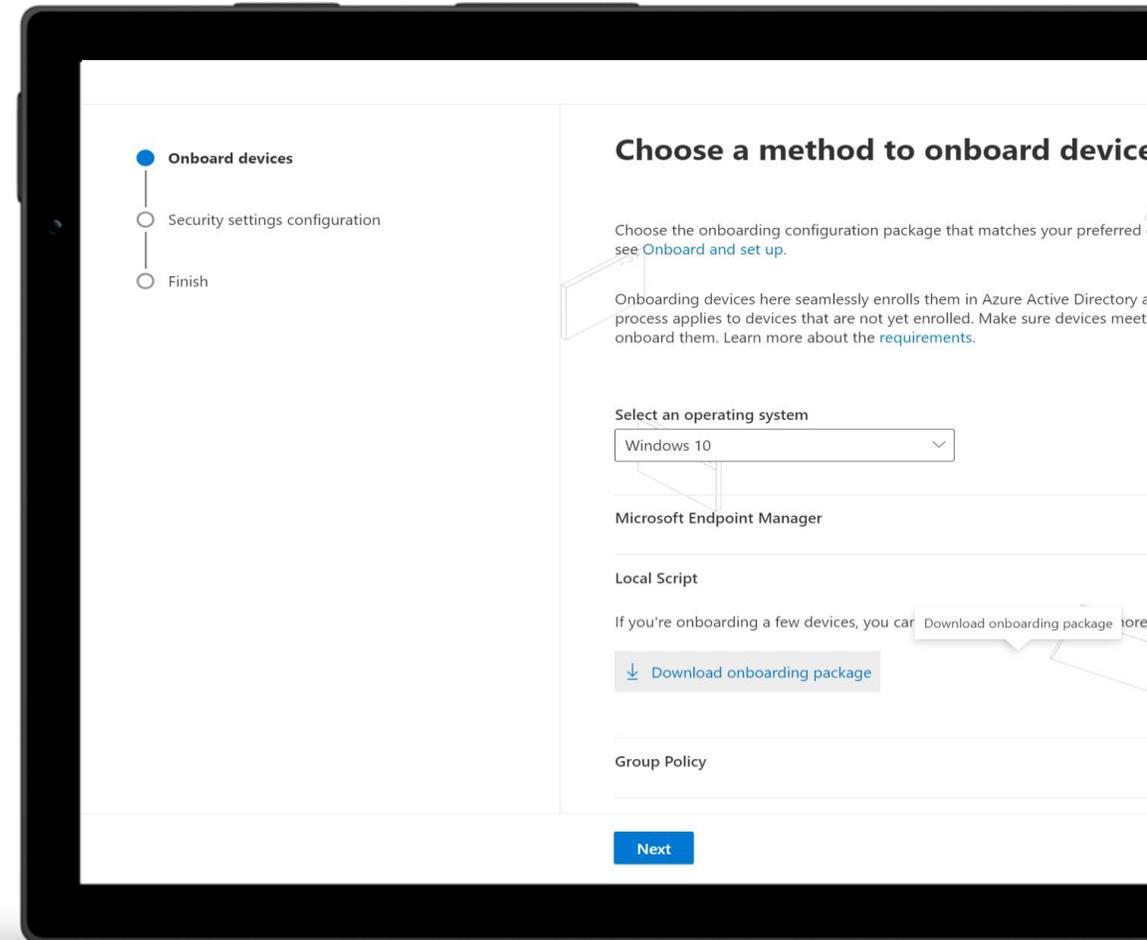


Wizard-driven onboarding and easy to use management controls

 Onboard new devices in a few simple steps

 Recommended security policies activated out-of-the-box

 Action-oriented dashboard help prioritize tasks



Delivering endpoint security across platforms



Windows

macOS



iOS



Windows 365

Azure Virtual Desktop

Endpoints

Mobile device OS

Virtual desktops

Product Comparison: Defender for Business brings enterprise-grade capabilities to SMBs

Customer size	< 300 seats	> 300 seats	
Endpoint capabilities\SKU	Microsoft Defender for Business (currently in preview, will be included with M35BP post GA)	Microsoft Defender for Endpoint Plan 1 (Included with M365 E3, currently in preview)	Microsoft Defender for Endpoint Plan 2 (Included with M365 E5)
Centralized management	✓	✓	✓
Simplified client configuration	✓		
Threat and Vulnerability Management	✓		✓
Attack Surface Reduction	✓	✓	✓
Next-Gen Protection	✓	✓	✓
Endpoint Detection and Response	✓ ²		✓
Automated Investigation and Response	✓ ²		✓
Threat Hunting and 6-months data retention			✓
Threat Analytics	✓ ²		✓
Cross platform support for Windows, MacOS, iOS, and Android	✓	✓	✓
Microsoft Threat Experts			✓
Partner APIs for exporting to SIEM	✓	✓	✓
Microsoft 365 Lighthouse for partners for viewing security incidents across customers	✓ ³		

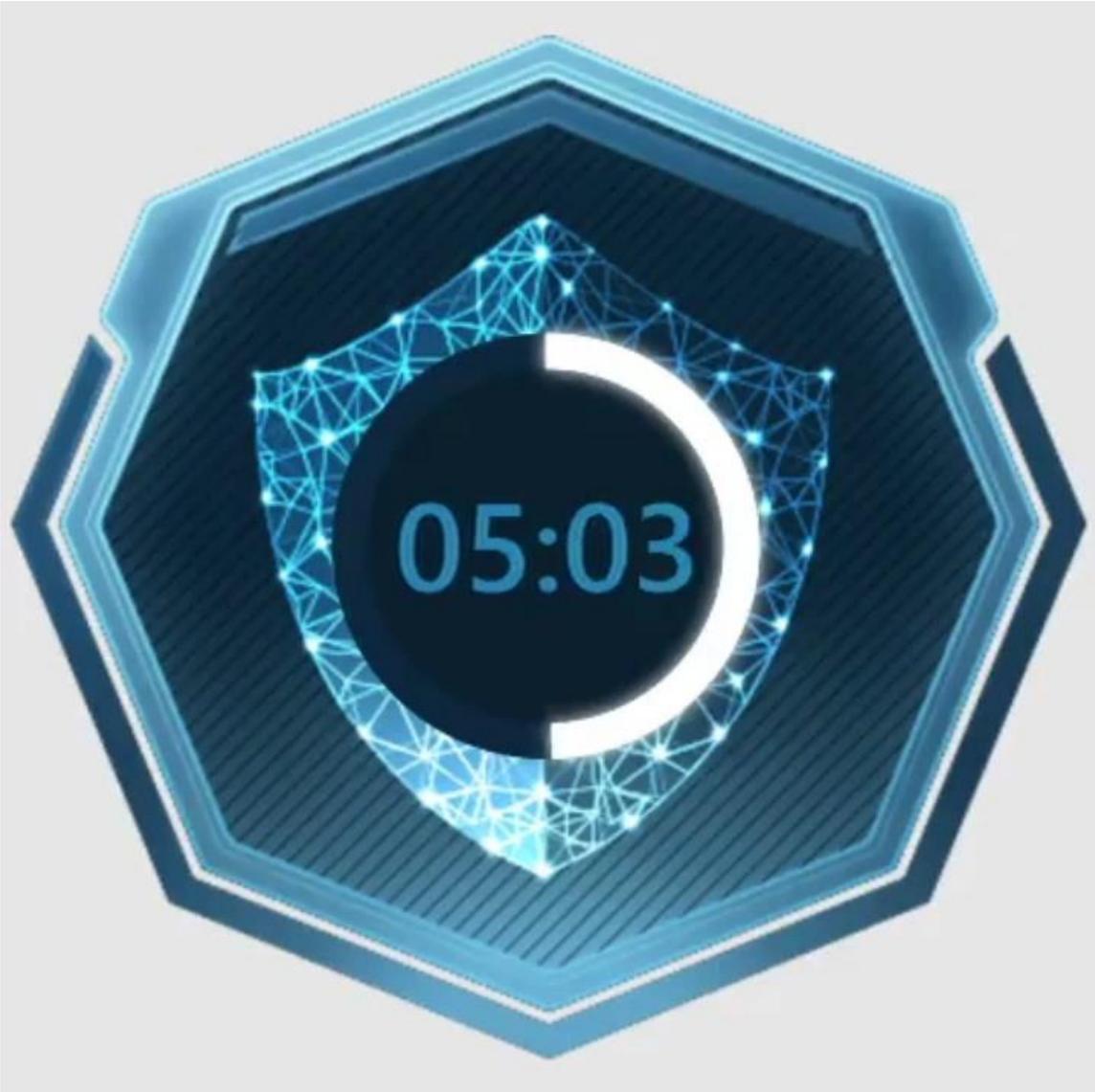
Demonstration



DICKER
DATA



5 Minute break



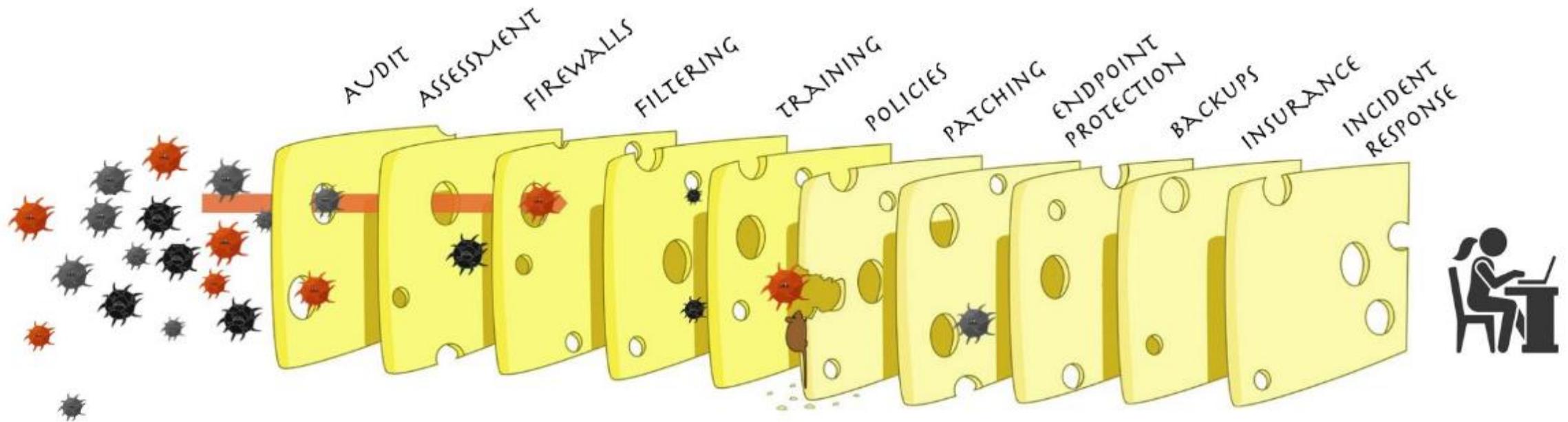
Mastering Microsoft Assessments

 ASCEND

THE SWISS CHEESE

CYBERSECURITY DEFENSE-IN-DEPTH MODEL

RECOGNIZING THAT NO SINGLE INTERVENTION IS SUFFICIENT TO PREVENT HARM



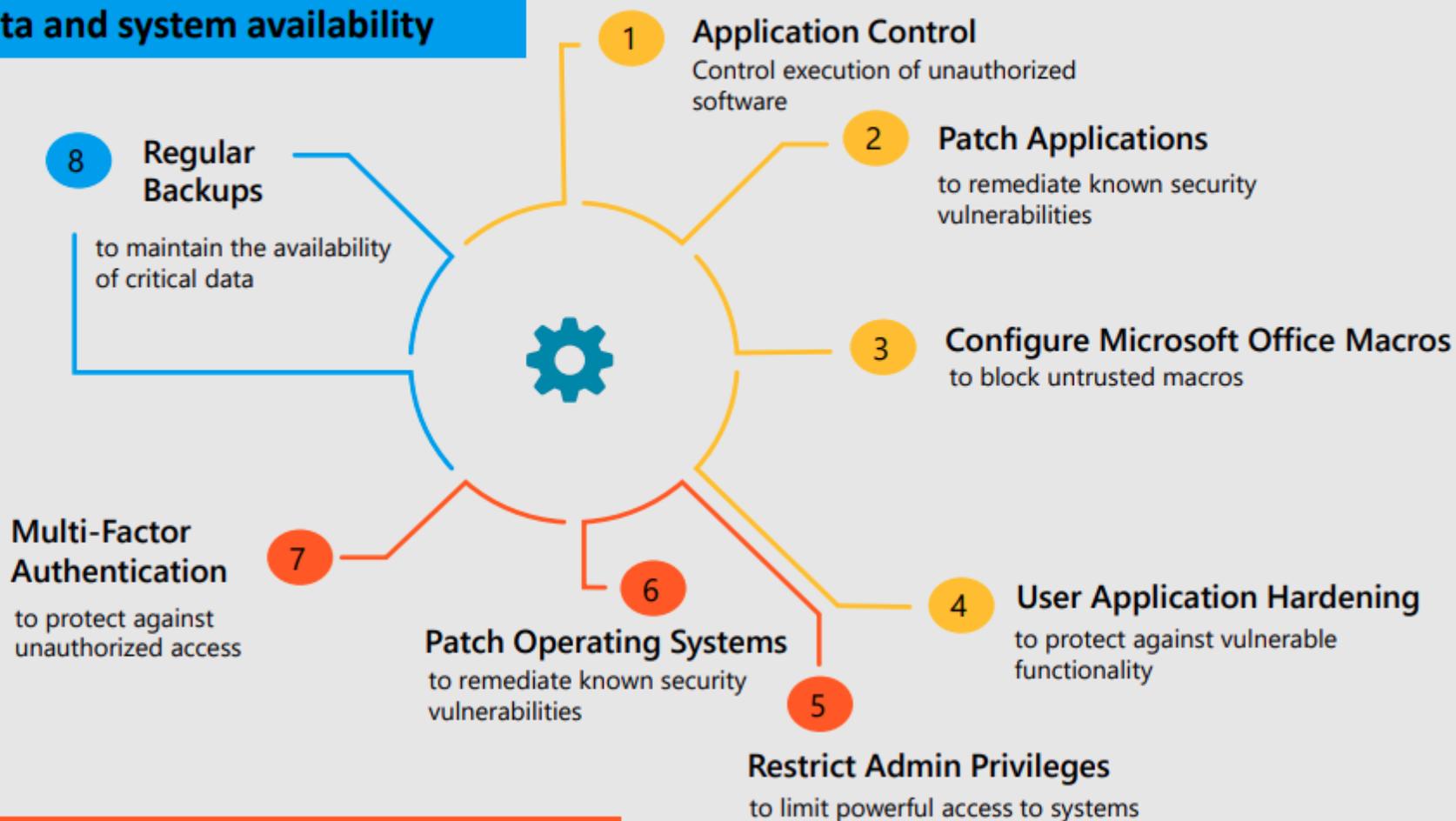
EACH INTERVENTION (LAYER) HAS IMPERFECTIONS (HOLES).
MULTIPLE LAYERS IMPROVE SUCCESS.

ADAPTED FROM THE SWISS CHEESE RESPIRATORY VIRUS
PANDEMIC DEFENSE
IAN M. MACKAY VIROLOGYDOWNUNDER.COM

The Essential Eight Controls are segmented into 3 groups

Prevent Malware Delivery and Execution

Recover data and system availability



Limit the extent of Cyber Security Incidents



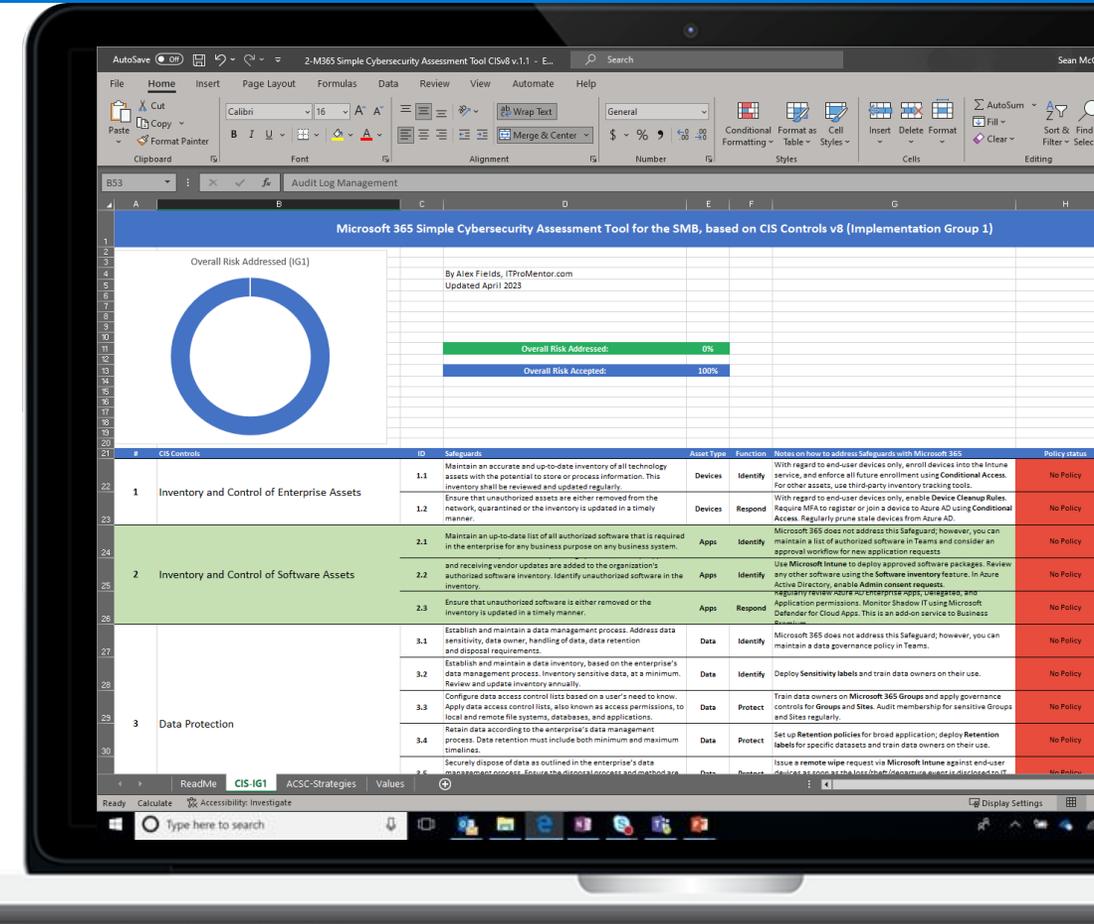
Evolving Role of MSPs: Managed Security Services



Security Managed Services Partner Kit

- Step by step guidance on how to begin with services
- Practical guidance on expanding from IT management to security
- Integration with security frameworks and key partner tools.

Security Managed Services Partner Kit



Microsoft 365 Partner Playbook

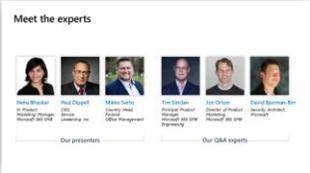
Microsoft 365 Partner Playbook: Practical Guidance across the partner journey

Understand business opportunity



Partner opportunity

Build profitable managed services



Managed services best practices from experts

Train your team

Technical



Technical Training

Sales GTM



Customer Conversation aids

Manage and deploy solutions



IT Checklist



Deployment Guide



Decks and docs



Webinars



Videos



Tools and templates

M365 Business Premium Partner Playbook
<https://aka.ms/M365BPPlaybook>

Practical Guidance for partners for building a profitable managed service practise with M365BP– including managed services offers that meet today’s customer needs, technical and sales training and go to market content. Built in partnership with Industry and Microsoft experts. Companion tools and online training.

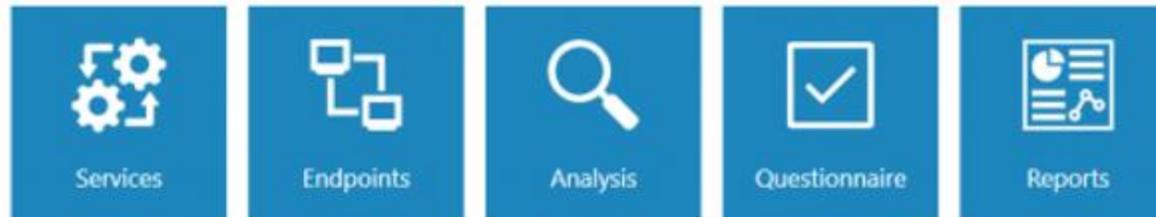


The Power of Microsoft Assessments

ASCEND



CSAT Components



[Cyber Security Assessment Tool](#)

Security Assessment Types

SMB Focus

	CSAT Self Service Assessment	CSAT QuickScan Assessment	CSAT FullScan Assessment
Target Group	SMB – Open to all customers	SMB (30-300 Endpoints)	Enterprise, Corporate and Top SMB (300+ Endpoints)
Purpose of Assessment	<ol style="list-style-type: none"> 1. Lead Generation for full-service assessments. 2. Show customers they need a more detailed assessment to identify all cybersecurity risks. 3. Based on a limited number of controls of the Zero Trust Architecture 4. Limited datasets and concise report. Allow for first improvement actions while sparking interest for a full assessment 	<ol style="list-style-type: none"> 1. Do a quick check on the cybersecurity hygiene 2. Propose improvement actions based on actual data 3. Quick report and few customizations 4. Based on the CIS controls IG1 	<ol style="list-style-type: none"> 1. Comprehensive cybersecurity assessment 2. Align Business and IT management 3. Help to decide on new security initiatives based on facts 4. Deployment and implementation plan 5. Based on the CIS controls IG 1-3
Outcomes of Assessment	Positioning of Microsoft's Security solutions in M365 and Azure. Customer will be interested in a comprehensive assessment	Upsell to Microsoft 365 Business Premium, Azure migrations and increase of Azure Consumed Revenue by adding Azure Security	Upsell to Microsoft 365 E3+E5 and Sentinel, Azure migrations and increase of Azure Consumed revenue by adding Azure Security
Scan Sources in Scope	<ul style="list-style-type: none"> • Manual Endpoint Scan of Windows OS • Local Active Directory • Email DNS check • Limited datasets of Microsoft 365 environment • Limited datasets from the Azure tenant • Questionnaire on basic security controls – no official framework 	<ul style="list-style-type: none"> • Basic Automated Endpoint Scan • Local Active Directory • Email DNS check • Microsoft 365 environment • Limited datasets from the Azure tenant • Checked against CIS IG1 (basic security hygiene controls) 	<ul style="list-style-type: none"> • Comprehensive Automated Endpoint Scan including Linux machines and network devices • Local Active Directory • Email DNS check • Microsoft 365 environment • Comprehensive scan of the Azure tenant • SharePoint on-premises • Google Workspace and AWS included • Checked against the full CIS18 controls

Rapid Security Assessment | Estimated Timeline

Assessment Stages

Assessment Planning

CSAT QuickScan

Report Generation and Delivery

Post-Assessment

Nomination submitted via MS website, validated between Ops and Partner

Nomination approved, TC assigned, and Pre-deployment call scheduled

Pre-Deployment call discussing process and tool requirements

Customer Deploys CSAT Scan Wizards

Customer submits CSAT Questionnaire

Report Generated and Internal Review Call

Assessment Report Review Call with Partner and Customer

Assessment Follow-Up and Migration Planning with Partner

3 Days

1-7 Days

3 Days

1-3 Days

1-3 Days

1-3 Days

Variable

Total Estimated Time from Nomination approval to Report Delivery: **1-3 weeks**

Rapid Security Assessment

Objective: Provide Microsoft partners and customers with Rapid Security Assessments that can help **drive data-driven implementations** of security policies, procedures, and tools using built-in reports to support **migration plans** to improve security based on CIS Controls and the Zero Trust framework.

1

CSAT Scan and Analysis

- Scans an organization's endpoints via CSAT QuickScan, as well various additional data sources in a customer's on-premise and cloud environments.
- Collects and analyzes data from the hybrid IT environment with a 4-6 hour scan to provide data-driven recommendations.
- Classification of security threats identified during the scan based on Microsoft's Zero Trust framework.

2

CSAT Questionnaire

- Collection of additional information about the customer security-related policies and procedures that cannot be gathered from the CSAT scan.
- Asks questions to evaluate customer's security-related policies, process, procedures, identity and data management, among others.

3

CSAT Report

The SMB Desk will provide a report outlining key findings and high-level recommendations in support of improving the organization's cybersecurity posture, including:

- An organizational security maturity score based on CIS Controls v8
- Data-based recommendations ranked by level of urgency and probability of a security issue – i.e. quick wins and longer term actions.
- Identification of MS security products associated with recommendations to upsell and/or deploy additional licenses, products, and services.



The Power of Microsoft Assessments

ASCEND

CSAT

The Cyber Security Assessment Tool is developed by a team of seasoned security experts. It collects relevant data from:



Endpoints



Microsoft 365,
Google Workspace,
SharePoint and
Azure



Active Directory
Azure AD



Questionnaire,
Interview

[Microsoft Presales Email](#)

Compliance Manager

Manage your compliance from one place

Ongoing risk assessment

An intelligent score reflects your compliance posture against regulations or standards



Actionable insights

Recommended actions to improve your data protection capabilities

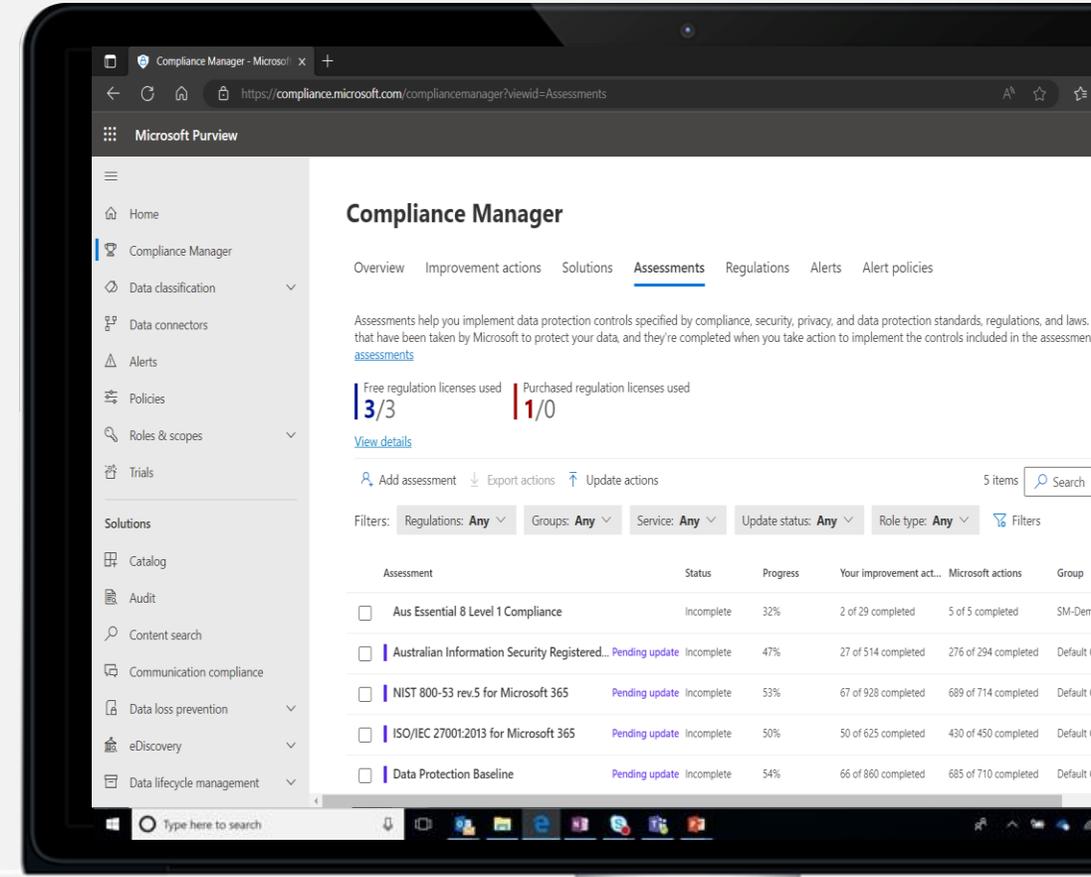


Simplified compliance

Streamlined workflow across teams and richly detailed reports for auditing preparation



Compliance Manager is a dashboard that provides the Compliance Score and a summary of your data protection and compliance stature as well as recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.



Demonstration



DICKER
DATA



Microsoft 365 Lighthouse

 ASCEND

Microsoft 365 Lighthouse overview

Helps **Managed Service Providers** to secure devices, data, and users for customers that have up to 2500 licensed users and 365 subscriptions



Customer management at scale

Monitor and manage customers centrally to easily identify gaps in end-customer configuration, target improvements, and drive adoption.



Proactive risk management

Realize efficiencies in customer management to support business scale and growth



Improved security

Secure and protect devices, data, and users across customer environments using recommended best practices.



Standardize configuration

Benefit from deployment plans to drive standardization, upsell across customer base, and reduce risk

Enable least privilege access in Microsoft 365 Lighthouse with Granular Delegated Administrative Privileges (GDAP) now [available for securing Lighthouse](#).

Technical release of Granular Delegated Admin Privileges (GDAP)

Enable least privilege access

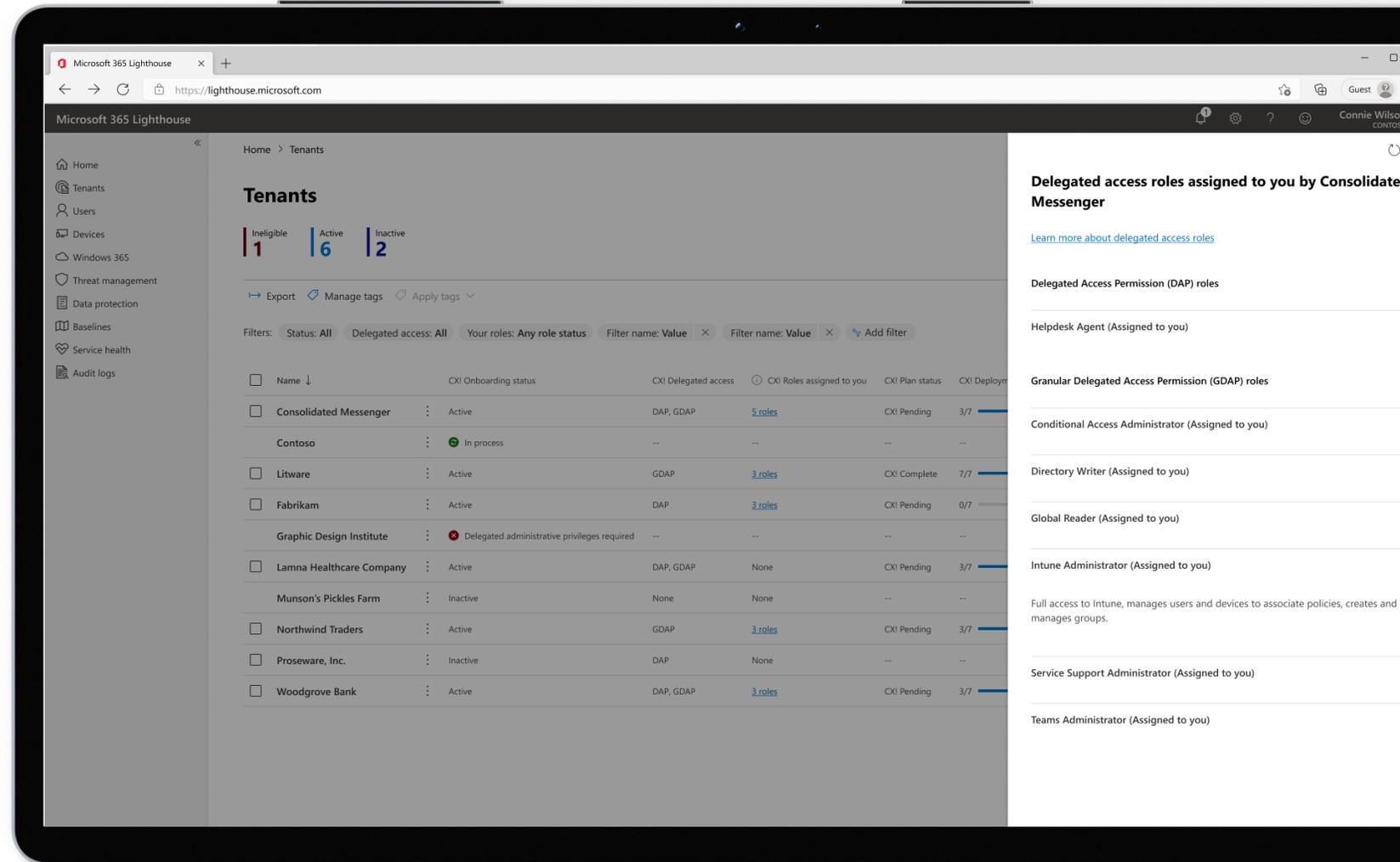
Right size permissions across your technicians to the tasks they need to perform.

Data Security

Address concerns about data security, reduce the likelihood of security incidents, and help make your ecosystem more secure.

Time-bound access per customer at workload level

Restrict access per customer at the workload level for your employees who are managing your customers' services and environments.



Set up GDAP in Lighthouse: [Set up roles to manage customer tenants](#)

Learn more about GDAP: [Granular delegated admin privileges \(GDAP\) introduction](#)

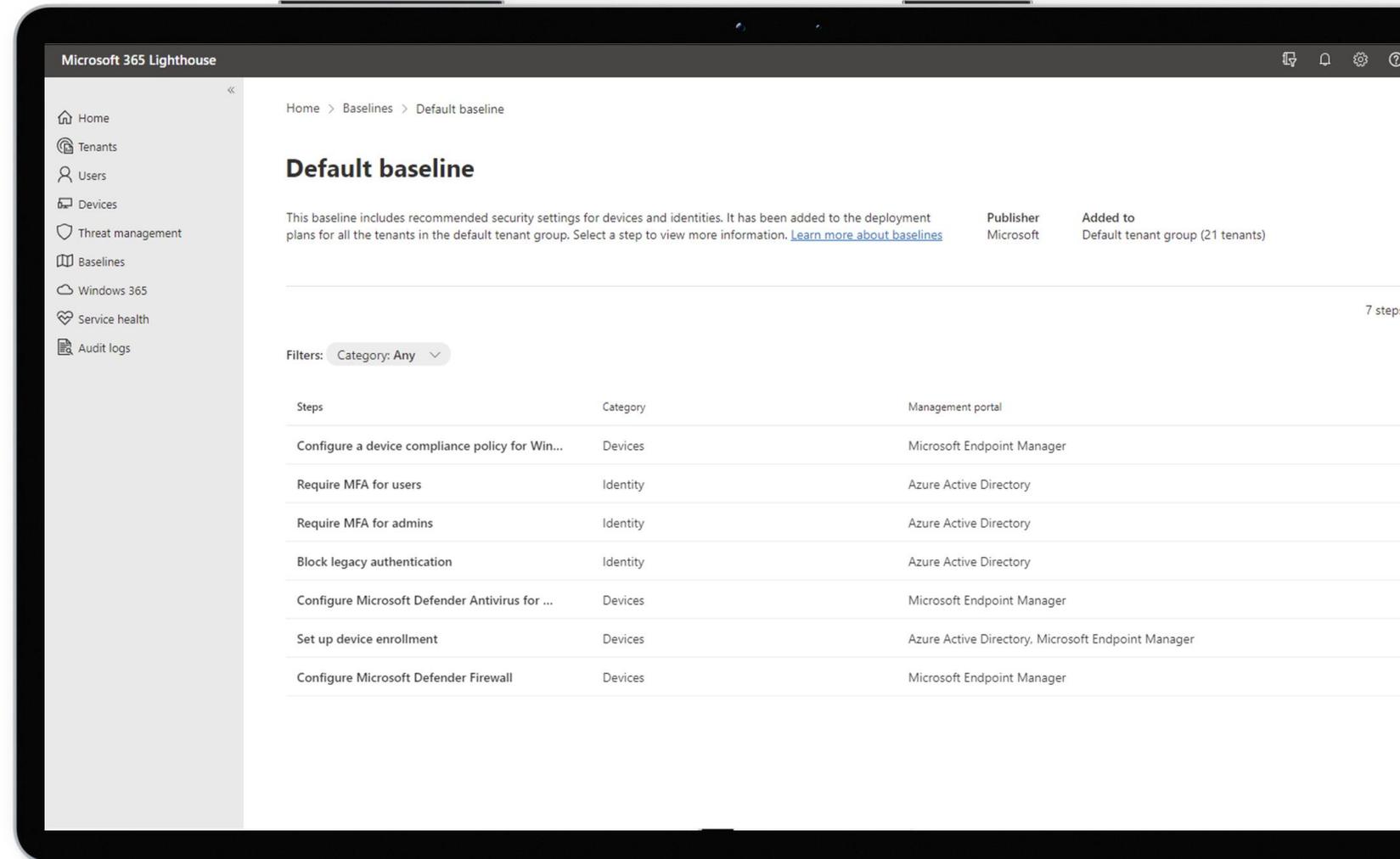
Standardize configuration

Recommended settings

Baselines are Microsoft's recommended settings and policies optimized for small and medium sized businesses.

Consistent deployment

Move beyond monitoring by deploying consistent security standards across new and existing customers using Deployment plans.



- Home
- Tenants
- Users
- Devices
- Threat management
- Baselines
- Service health

Home > Baselines > Default baseline

Default baseline

This baseline includes recommended security settings for devices and identities. It has been added to the deployment plans for all the tenants in the default tenant group. Select a step to view more information.

Publisher
Microsoft

Added to
Default tenant group (4 tenants)

6 templates

Filters: Category: Any

Steps	Category	Management portal
Require MFA for admins	Identity	Azure Active Directory
Require MFA for end-users	Identity	Azure Active Directory
Block legacy authentication	Identity	Azure Active Directory
Set up customer device enrollment	Devices	Azure Active Directory, Microsoft Endpoint Manager
Set up Windows 10 antivirus policy	Devices	Microsoft Endpoint Manager
Require device compliance	Devices	Microsoft Endpoint Manager

- Home
- Tenants
- Users
- Devices
- Threat management
- Baselines
- Windows 365
- Service health
- Audit logs

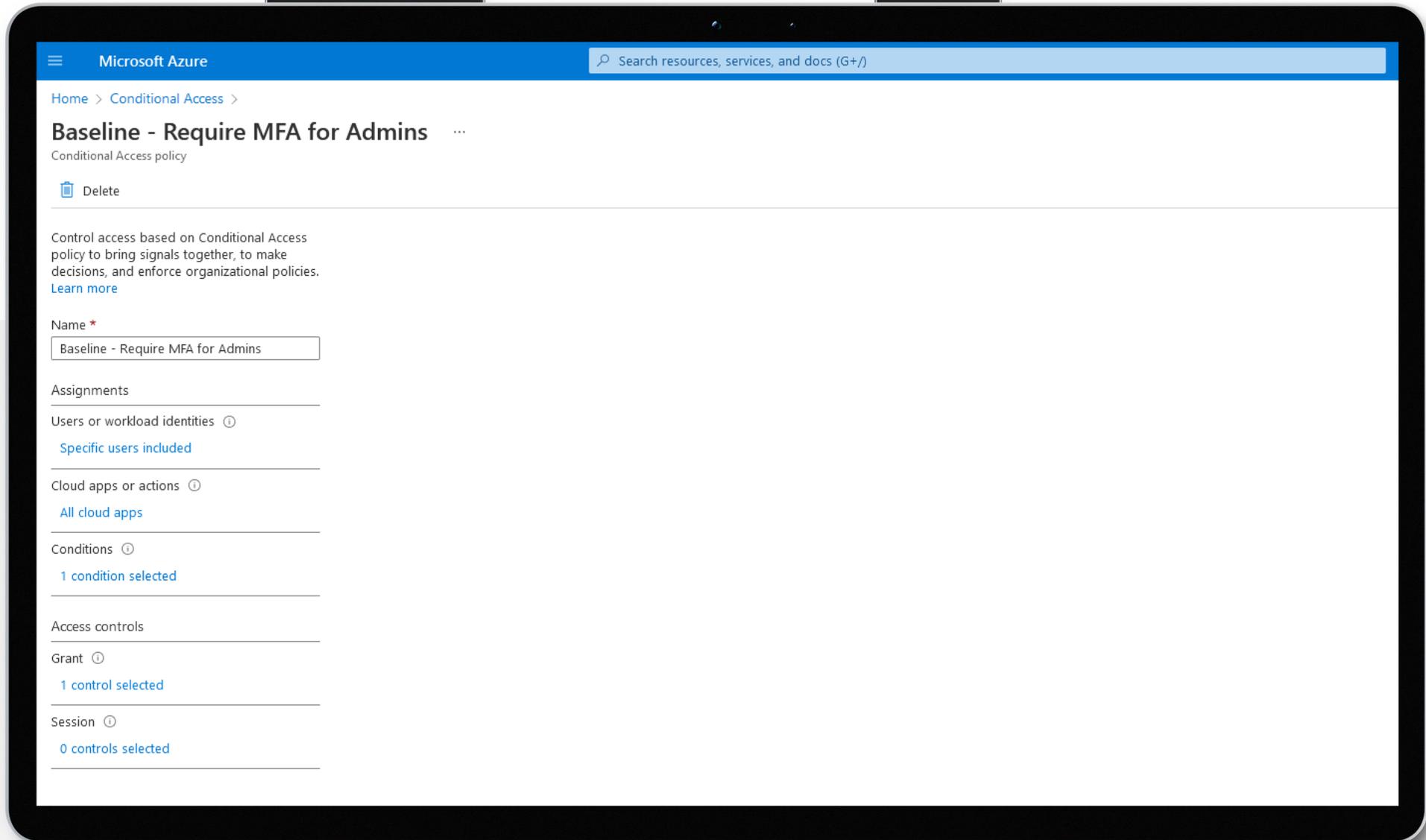
Home > Tenants > Consolidated Messenger

Consolidated Messenger

Overview Deployment Plan[Export](#) [Refresh](#)7 steps

Deployment step	Status	Baseline	Category	Last updated
Configure a device compliance policy for Windows 10 and later	<input type="radio"/> To address	Default baseline	Devices	3/16/2022
Require MFA for users	<input checked="" type="checkbox"/> Complete	Default baseline	Identity	3/16/2022
Require MFA for admins	<input type="radio"/> To address	Default baseline	Identity	3/16/2022
Block legacy authentication	<input checked="" type="checkbox"/> Complete	Default baseline	Identity	3/16/2022
Configure Microsoft Defender Antivirus for Windows 10 and later	<input checked="" type="checkbox"/> Complete	Default baseline	Devices	3/16/2022
Set up device enrollment	<input type="checkbox"/> Manual Steps	Default baseline	Devices	3/16/2022
Configure Microsoft Defender Firewall	<input checked="" type="checkbox"/> Complete	Default baseline	Devices	3/16/2022

Microsoft 365 Lighthouse Deployment Plan



[View policy in Azure Active Directory](#)



Managing your Customer Tenants

- Home
- Tenants
- Users
- Devices
- Threat management
- Baselines
- Service health

Welcome to Microsoft 365 Lighthouse

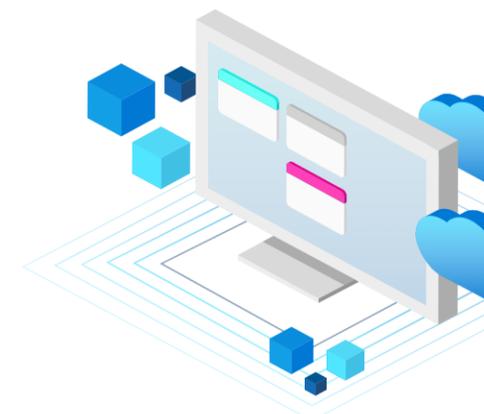
Get started Feedback

Welcome to Microsoft 365 Lighthouse, a new experience that makes it easier for you to deliver managed services at scale to small and medium-sized customers. [Learn more about Microsoft 365 Lighthouse](#)

Before you get started, there are a few things you should do to get the full Lighthouse experience. [Learn how to turn on features in Microsoft 365 Lighthouse](#)

[Next](#) [Close](#)

Tenants: All



Microsoft Defender Antivirus threat landscape

4 threats blocked across ...

Data reflects threats detected on Windows 10 devices running Microsoft Defender Antivirus over the past 30 days.



Mitigated Resolved Allowed

[View all threats](#)

[View all active threats](#)

Microsoft Defender Antivirus protection

0 devices need antivirus ...

Data reflects Windows 10 devices only



Not protected Protected

Tenant Devices not protected

Contoso 0 / 4

[View full report](#)

Risky users

3 users flagged for risk

Tenant Risky users

Contoso 3

[View risky users](#)

Daily Security Health Check

Organize tiles to show information most critical to you, first

The screenshot shows the Microsoft 365 Lighthouse dashboard. The top navigation bar includes the product name, user profile, and various utility icons. A left-hand navigation menu lists sections like Home, Tenants, Users, Devices, Threat management, Baselines, Windows 365, and Service health. The main content area, titled 'Home', features a 'Tenants: All' dropdown and three prominent security health check tiles. The first tile, 'Windows 365', reports '3 Cloud PCs have failed provision...'. The second, 'Device compliance', shows '18 of 110 devices are not compli...' with a progress bar and a table of non-compliant tenants. The third, 'Security incidents', reports '1 active incidents detected amon...'. Each tile includes a 'View' button for further details.

Microsoft 365 Lighthouse

Home

Tenants: All

Windows 365

3 Cloud PCs have failed provision...

View Cloud PCs with failed provisioning

Device compliance

18 of 110 devices are not compli...

Not compliant In grace period Not evaluated Compliant

Tenant	Not compliant
Fourth Coffee	18 / 29
Consolidated Messenger	0 / 15
Contoso	0 / 66

View full report View devices

Security incidents

1 active incidents detected amon...

View all incidents

Tenant Status

Status	Description
Active	Onboarding and data flow has started.
Inactive	Tenant is no longer active.
In process	Tenant discovered, but not fully onboarded.
Ineligible, Delegated access required	Delegated Admin Privileges (DAP) setup is required.
Ineligible, Missing required license	Tenant does not have required license.
Ineligible, User count exceeded	Tenant has more users than allowed.
Ineligible, Contract type	Tenant does not have a contract.

Microsoft 365 Lighthouse

Home > Tenants

Tenants

Ineligible 8 | Active 7 | Without DAP 0 | Inactive 1

Export Manage Tags Assign Tags

Filters: Status: Any Delegated administrative privilege: Any Tags: Any

Name ↑	Status	Delegated administrative privilege	Tags
AdventureWorks Cycles	Active	Yes	
Allure Bays Corp	Ineligible, Missing required license	Yes	
Blue Yonder Airlines	Ineligible, Missing required license	Yes	
City Power & Light	Ineligible, Missing required license	Yes	
Consolidated Messenger	Active	Yes	GOLD LEVEL IMPORTANT
Contoso	Active	Yes	SUPPORT
Contoso	Inactive	Yes	
Fourth Coffee	Active	Yes	
FusionTomo	Active	Yes	
Graphic Design Institute	Ineligible, Missing required license	Yes	
Parnell Aerospace	Active	Yes	SUPPORT ONBOARDING

Tenant Tagging

Update the Home Screen information to show only tenants with the selected tag

Home

Tenants: 🏆 Gold Level ▾ ✕

[Back](#)

🔍 Filter by tag...

Tags

- 🔗 !! Important
- 🔗 🛎 Support
- ✓ 🔗 🏆 Gold Level
- 🔗 🥈 Silver Plus
- 🔗 📦 More cool stuff
- 🔗 🚀 Onboarding

Home

Tenants: 🏆 Gold Level ▾ ✕

Risky users

2 users flagged for risk

Tenant	Risky users
Consolidated Messenger	2

[View risky users](#)

Device compliance

0 of 15 devices are not compliant

■ Not compliant ■ In grace period ■ Not evaluated ■ Compliant

Tenant	Not compliant
Consolidated Messenger	0 / 15

[View full report](#)

[View devices](#)

Filter Tenants by Tag

The screenshot shows the Microsoft 365 Lighthouse interface. The main page displays a 'Tenants' overview with a summary of 8 Ineligible, 7 Active, 0 Without DAP, and 1 Inactive tenants. Below this are links for 'Export', 'Manage Tags', and 'Assign Tags'. A filter bar at the bottom of the main page shows 'Status: Any', 'Delegated administrative privilege: Any', and 'Tags: Any'. A modal overlay is shown in the foreground, where the 'Tags' filter is set to 'Gold Level'. The modal displays a table of filtered tenants.

Name ↑	Status	Delegated administrative privilege	Tags
<input checked="" type="checkbox"/> Consolidated Messenger	Active	Yes	GOLD LEVEL !!! IMPORTANT
Woodgrove Bank	Active	Yes	GOLD LEVEL

Background table (partially visible):

Name	Status	Delegated administrative privilege	Tags
Fourth Coffee	Active	Yes	
FusionTomo	Active	Yes	
Graphic Design Institute	Ineligible, Missing required license	Yes	
Parnell Aerospace	Active	Yes	SUPPORT ONBOARDING

Risky Users

Microsoft 365 Lighthouse

- Home
- Tenants
- Users
- Devices
- Threat management
- Baselines
- Windows 365
- Service health

Home > Tenants > Consolidated Messenger

Consolidated Messenger

Overview | Deployment Plans

Tenant overview

Headquarters: Redmond, WA, United States

Industry:

Website: <http://getconsolidated.com>

Customer domain: consolidatedmessenger001.onmicrosoft.com

Total users: 9

Total devices: 15

Contacts

Select a contact for more options

Name	Title	Phone	Email
Bob Smith	IT Wizard	555-328-4988	Copy

Home > Users

Users

Tenants: Consolidated Messenger

Search users | **Risky Users** | Multifactor Authentication | Password reset

Tenants without an Azure AD Premium License aren't reported here.

Investigate users flagged for risk and reset passwords. It may take a while for risk status to be updated. [Learn how to investigate risk](#)

Confirmed compromised | 0 | At risk | 2 | Remediated | 0 | Dismissed | 2

Export | Refresh | Confirm user(s) compromised | Dismiss user(s) risk | Reset password | Block sign-in

Filter: Risk state: Any | User status: Any | Risk last updated: Any

Name	Username	Tenant	Risk state
Graham Strong	Graham@consolidatedmessenger001.onmicrosof	Consolidated Messenger	Dismissed
Mike Ross	miker@consolidatedmessenger001.onmicrosof	Consolidated Messenger	Dismissed
Chris Green	chris@consolidatedmessenger001.onmicrosof.c	Consolidated Messenger	At risk
Ina Anthony	ianthony@consolidatedmessenger001.onmicrosof	Consolidated Messenger	At risk

Product	Count	Percentage
Azure Active Directory Premium	--	--
Azure Advanced Threat Protection	--	--
Intune	5	-44%
Microsoft Defender Advanced Threat Protection	--	--
Office 365 Advanced Threat Protection	--	--

Multifactor Authentication

Home > Users

Users

Tenants: Consolidated Messenger

Search users Risky Users **Multifactor Authentication** Password reset

i Tenants without an Azure AD Premium License aren't reported here.

Tenants without recommended MFA enablement

0 tenants don't have MFA enabled through recommended methods

We recommend using Azure AD conditional access or security defaults to enable Azure MFA. [Learn more about MFA](#)

Users not capable of MFA

4 users aren't capable of MFA in this tenant

Registered Not registered

Export Refresh

Filter: MFA enablement: All

Consolidated Messenger

MFA enablement Conditional Access policies **Users not capable of MFA**

Select users to send them an email reminder to register for MFA using their allowed verification options.
[Download sample email templates](#)

[View Consolidated Messenger overview page to find a direct contact to email](#)

Export Create email 4 users

User	Create email	Jusername	Methods registered
<input checked="" type="checkbox"/> Carey Richard	<input type="checkbox"/>	crichard@consolidat	
<input type="checkbox"/> Graham Strong	<input type="checkbox"/>	Graham@consolidat	
<input type="checkbox"/> Ina Anthony	<input type="checkbox"/>	ianthony@consolida	
<input type="checkbox"/> package_5c6b66c8-031...	<input type="checkbox"/>	package_0abfc9cd-1	

Manage MFA Exclusions

The screenshot displays the Microsoft 365 Lighthouse interface. The top navigation bar includes the title 'Microsoft 365 Lighthouse', a user profile for 'Enrique@testtest11092...', and various utility icons. A left-hand navigation pane lists categories such as Home, Tenants, Users, Devices, Threat management, Baselines, Windows 365, and Service health. The main content area is titled 'Require MFA for users' and includes a breadcrumb trail: 'Home > Tenants > Consolidated Messenger > Require MFA for users'. Below the title, there is a descriptive paragraph about MFA and a 'Review and apply' button. A status indicator shows 'Not started' with a dropdown arrow, and a 'Share' button is also present. A section titled 'What does this deployment do?' explains that selecting 'Apply' will execute certain processes. A table below this section shows the process 'Create conditional access policy to require MFA for users' with a status of 'Not started'. A 'Next steps' section suggests assigning the policy to end-users in Azure Active Directory. An overlay panel on the right, titled 'Edit exclusions', provides instructions on selecting groups for policy exceptions. It features a search bar and a list of groups: 'All Users', 'Device Group 1', and 'Test group 1'. The 'Test group 1' group is currently selected, and a 'Save exclusions (1)' button is located at the bottom of the panel.

Microsoft 365 Lighthouse

Home > Tenants > Consolidated Messenger > Require MFA for users

Require MFA for users

Multi-factor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised.

[Review and apply](#) Not started [Share](#)

What does this deployment do?

When you select Apply, the following processes will be executed automatically:

Process	Activity
Create conditional access policy to require MFA for users	<input type="radio"/> Not started

Next steps

Assign policy to end-users in Azure Active Directory

Edit exclusions

Exclusions are exceptions to policies. Select groups in the list below to define your policy exclusions.

Search for groups

- Display name
- All Users
- Device Group 1
- Test group 1

[Save exclusions \(1\)](#)

Threat Management

The screenshot displays the Microsoft 365 Lighthouse Threat Management interface. The main view shows a list of devices under the 'Antivirus protection' tab, filtered by 'Gold Level' tenants. A detailed view for device 'messenger03' is overlaid on the right, showing its status and available actions.

Microsoft 365 Lighthouse

Home > Threat management

Threat management

Tenants: Gold Level

Data displayed is only for devices running Windows 10 or later.

Overview Threats **Antivirus protection**

Devices with warnings: 0 | Need threat protection enabled: 0 | Need antivirus updates: 3 | Need full scan: 0 | Need real-time protection: 0

Export Refresh Update antivirus Run full scan Run quick scan Reboot device

Filter set: Clear all Device state: Threat protection: Antivirus updates: Need updates

Device name	Tenant	Device state	Threat protection	Antivirus updates	Real-time protection
messenger02	Consolidated Messenger	Clean	Enabled	Need updates	Enabled
messenger03	Consolidated Messenger	Clean	Enabled	Need updates	Enabled
messenger04	Consolidated Messenger	Clean	Enabled	Need updates	Enabled

messenger03
Device

Run quick scan Run full scan Reboot device Update antivirus

Overview Current threats Device action statuses

View device in Microsoft Endpoint Manager

Assigned to: -- Tenant: Consolidated Messenger

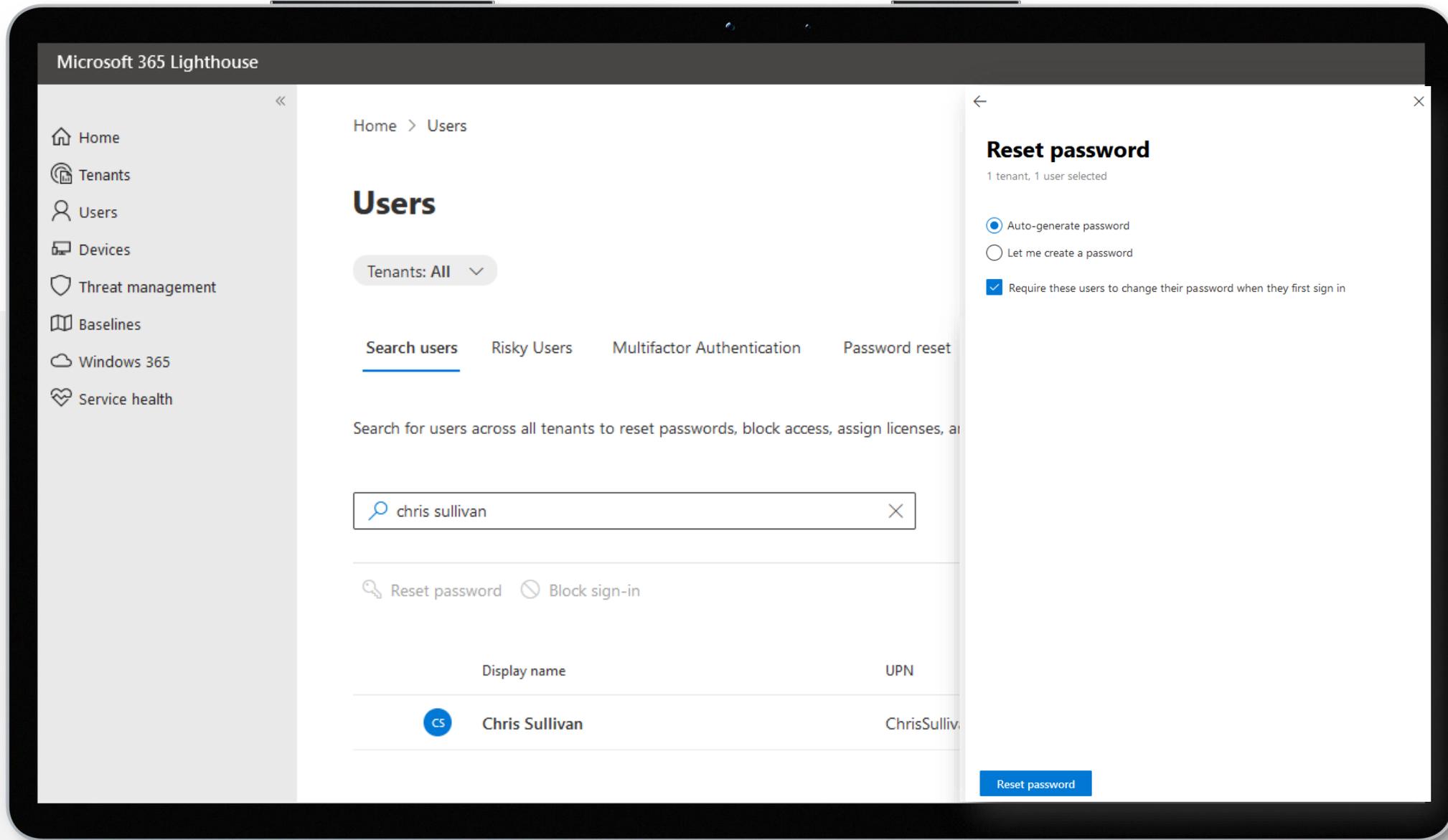
Active threats: 0 Device action statuses: No actions pending

Threat protection: Enabled, Updated 1/27/2022, 2:33:31 PM Real-time protection: Enabled, Updated 1/27/2022, 2:33:31 PM

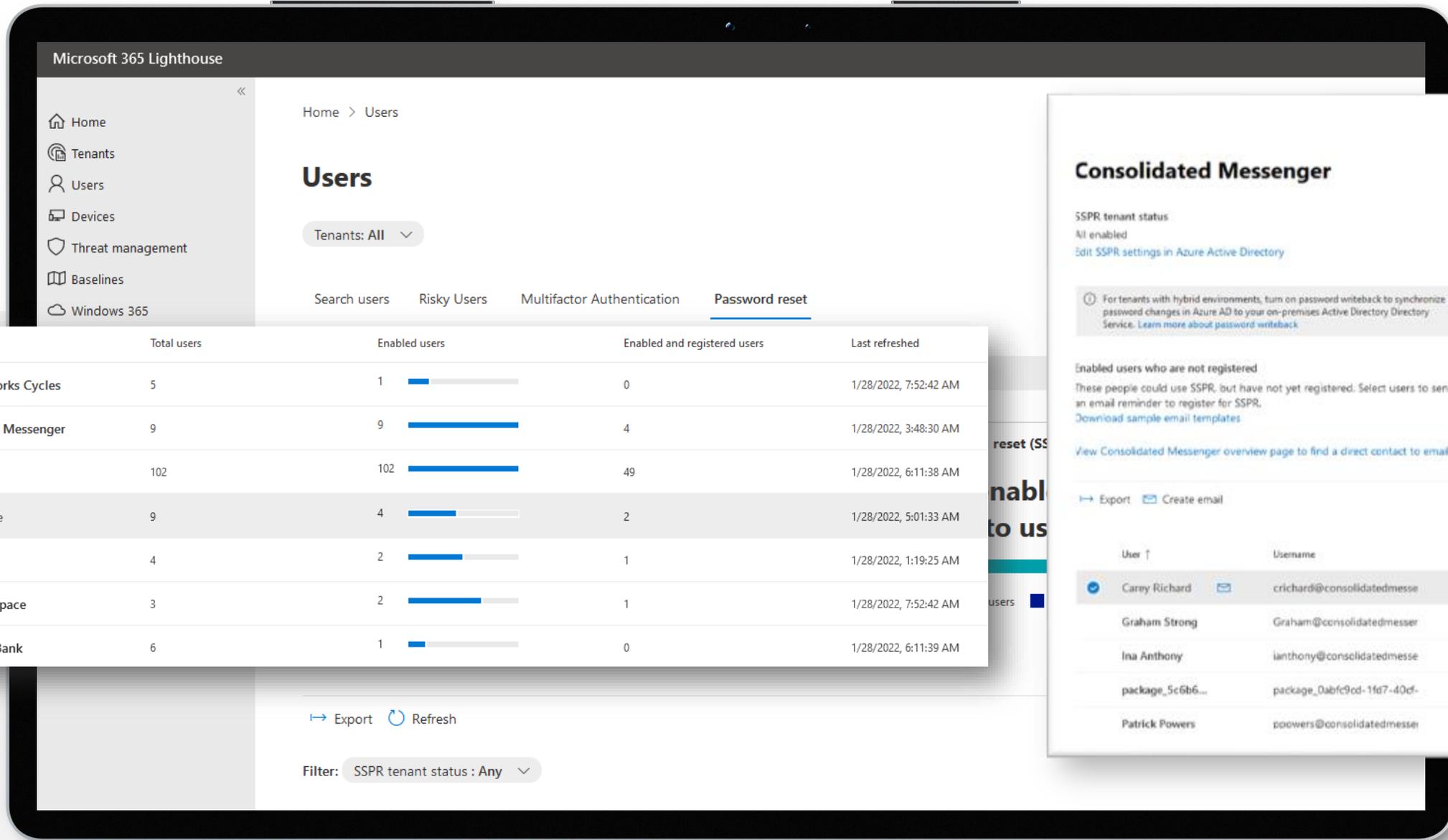
Quick scan: On schedule, Updated 1/26/2022, 8:08:28 PM Full scan: On schedule

Antivirus updates: Need updates, 1.355.1697.0

Password Reset



Self-Service Password Reset



Tenant name ↑	Total users	Enabled users	Enabled and registered users	Last refreshed
AdventureWorks Cycles	5	1	0	1/28/2022, 7:52:42 AM
Consolidated Messenger	9	9	4	1/28/2022, 3:48:30 AM
Contoso	102	102	49	1/28/2022, 6:11:38 AM
Fourth Coffee	9	4	2	1/28/2022, 5:01:33 AM
FusionTomo	4	2	1	1/28/2022, 1:19:25 AM
Parnell Aerospace	3	2	1	1/28/2022, 7:52:42 AM
Woodgrove Bank	6	1	0	1/28/2022, 6:11:39 AM

Consolidated Messenger

SSPR tenant status
All enabled
[Edit SSPR settings in Azure Active Directory](#)

For tenants with hybrid environments, turn on password writeback to synchronize password changes in Azure AD to your on-premises Active Directory Directory Service. [Learn more about password writeback](#)

Enabled users who are not registered
These people could use SSPR, but have not yet registered. Select users to send them an email reminder to register for SSPR.
[Download sample email templates](#)

[View Consolidated Messenger overview page to find a direct contact to email](#)

Export Create email 5 users

User ↑	Username
Carey Richard	crichard@consolidatedmesse
Graham Strong	Graham@consolidatedmessa
Ina Anthony	ianthony@consolidatedmesse
package_5c6b6...	package_0abfc9cd-1fd7-40cf-
Patrick Powers	ppowers@consolidatedmesse

Service Health & Status

[Check Microsoft 365 Service Health](#)

Microsoft 365 Lighthouse

Home
Tenants
Users
Devices
Threat management
Baselines
Windows 365
Service health

Service health

Total incidents: 3 | Total advisories: 7 | Services with incidents: 1

All services | All issues

Service

Exchange Online

Some users' Exchange Online outgoing messages are delayed or stuck in the Drafts or Sent Items folder after sending

Some users' Exchange Online outgoing messages are delayed or stuck in the Drafts or Sent Items folder after sending

EX305387, Exchange Online. Last updated: January 24, 2022 11:28 AM
Start time: December 14, 2021 11:30 AM, End time: December 14, 2021 6:35 PM

Overview | Tenants affected

Export 7 items Filter Search

Tenant	Status
AdventureWorks Cycles	Restoring service
Consolidated Messenger	Extended recovery
Contoso	Restoring service
Fourth Coffee	Extended recovery
FusionTomo	Restoring service
Parnell Aerospace	Extended recovery
Woodgrove Bank	Extended recovery

Admins' web protection reports via the Microsoft Defender 365 portal don't include events from Microsoft Edge | Advisory | 7 | DZ30

Microsoft 365 Lighthouse with Defender for Business and Microsoft Business Premium

View security incidents, alerts and devices from Defender for Business in the dashboard and get the detail from the Incidents queue*. Additional security management capabilities are planned on the roadmap.

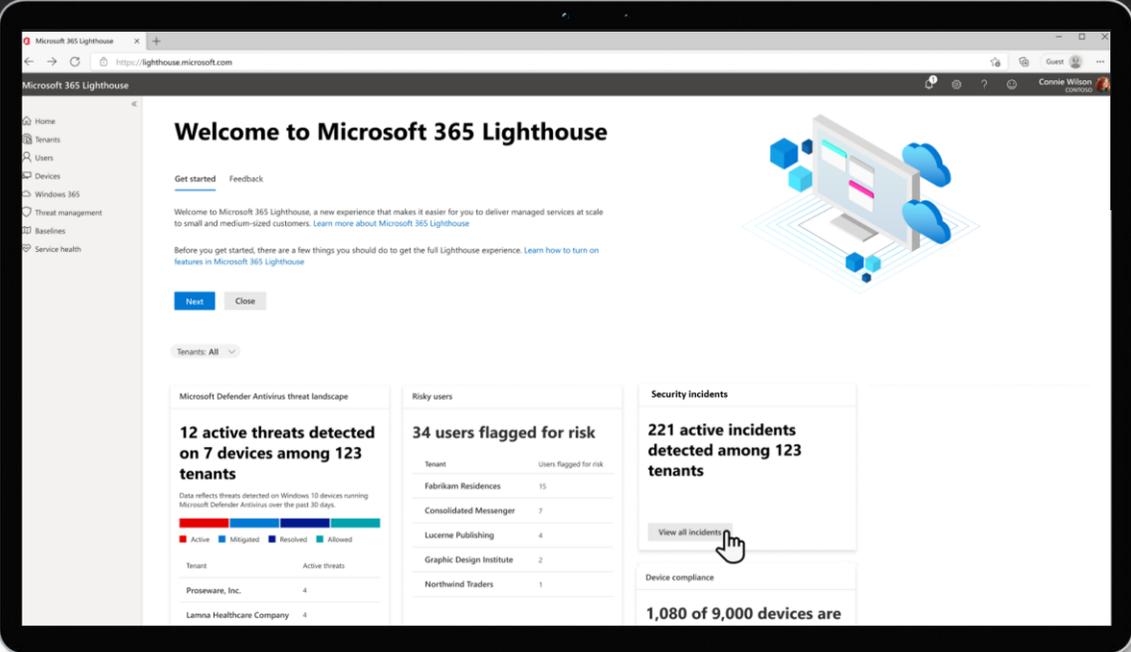


Image 1: Security incident summary on the Home dashboard

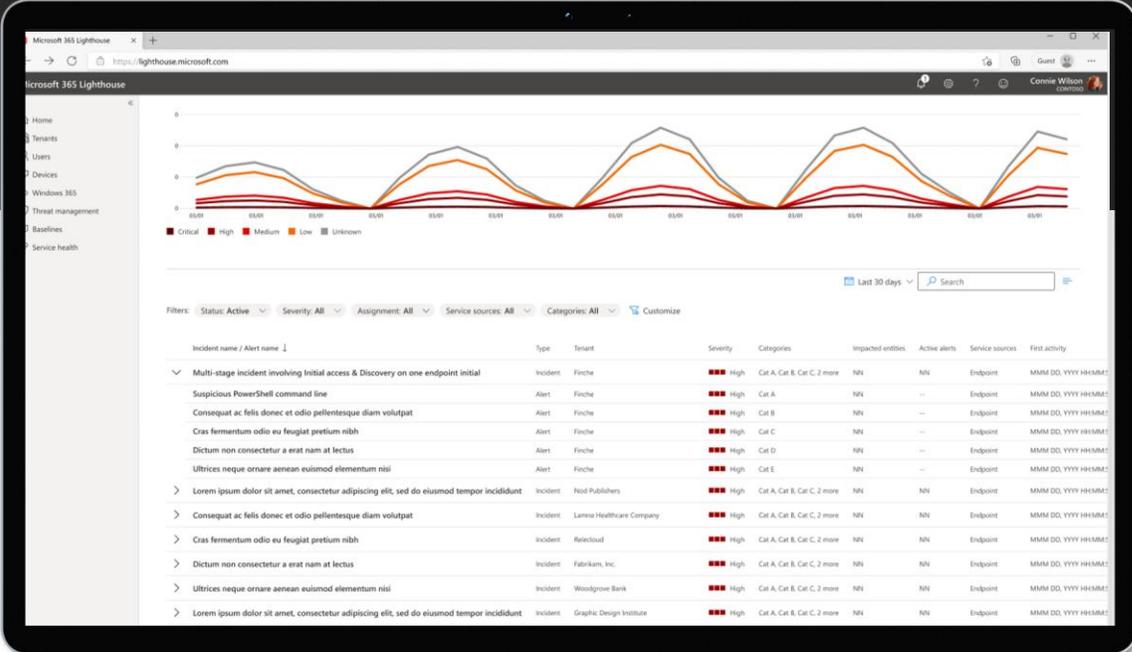


Image 2: Incident queue highlighting security incidents and alert details

Microsoft 365 Lighthouse

Introducing the new Sales Advisor feature with AI-powered actionable insights and recommendations

The improved Microsoft 365 Lighthouse tool offers a solution that's transforming the way CSPs engage with their customers. With advanced features to proactively manage SMB customer relationships on a larger scale, Lighthouse simplifies tenant management, minimizes risks, and now delivers personalized recommendations with AI-driven insights from the new Sales Advisor (formerly Project Orland) capability.

Help your customers maximize their Microsoft 365 investment and deliver value consistently through every stage of the customer lifecycle with Microsoft 365 Lighthouse.



Sales Advisor helps deliver value at every stage of the customer journey



Acquire

Increase customer acquisition by utilizing trials and conversion conversations to effectively sell Microsoft 365.



Retain

Sales Advisor gives timely alerts to prevent potential churn, allowing for direct engagement to improve customer satisfaction and retention.



Grow

Identify customers ready for their digital transformation's next phase by analyzing their usage patterns and comparing them to similar customers.

Onboard to Lighthouse

Unlock the full potential of cutting-edge customer management and engagement tools today!

Additional resources for partners:

- [Microsoft 365 Lighthouse Partner page](#)
- [Overview of Microsoft 365 Lighthouse](#)
- [Microsoft 365 Lighthouse Sales Advisor partner datasheet](#)

Get Started with Microsoft 365 Lighthouse

Criteria

Managed Service Providers enrolled in the Cloud Solution Provider (CSP) program

Established **Granular Delegated Administration** privileges with customers

Customers must have **at least one** Microsoft 365, Office 365, Exchange Online, Windows 365 Business, or Microsoft Defender for Business subscription.

A customer tenant must not have more than 2500 licensed users in total

Device Compliance and **Threat management** capabilities require device enrolment with Microsoft Intune.

Learn more at

<https://aka.ms/M365Lighthouse>

Technical documentation available

<https://aka.ms/M365LighthouseDocs>

Demo content

<https://aka.ms/M365Lighthouse-OverviewGuide>

<https://aka.ms/M365Lighthouse-BestPracticeGuide>

[Microsoft 365 Lighthouse Help & Support](#)

[Microsoft 365 Lighthouse Documentation](#)

aka.ms/m365lighthouseonboard

aka.ms/m365lighthousefeedback

Identity security



**Microsoft
Entra ID**

Best practice tips

Always use Security Defaults *or* Conditional Access for MFA

Do not enable MFA on a per user basis

Always exclude an admin account from MFA

Start with one target group of users

Ensure your users know what to expect

Test your policies with a test user before rolling out

- Consider Geo Blocking
- Use Passwordless or above
- Try Conditional Access Templates
- Use strong MFA for ANY privileged access



**Microsoft
Entra ID**

**Recommended
tasks**

Enable SSPR in ~~Azure AD~~ Entra ID

Enable Combined Security Information Registration in Entra ID

Create an emergency access admin account

Enable common conditional access policies

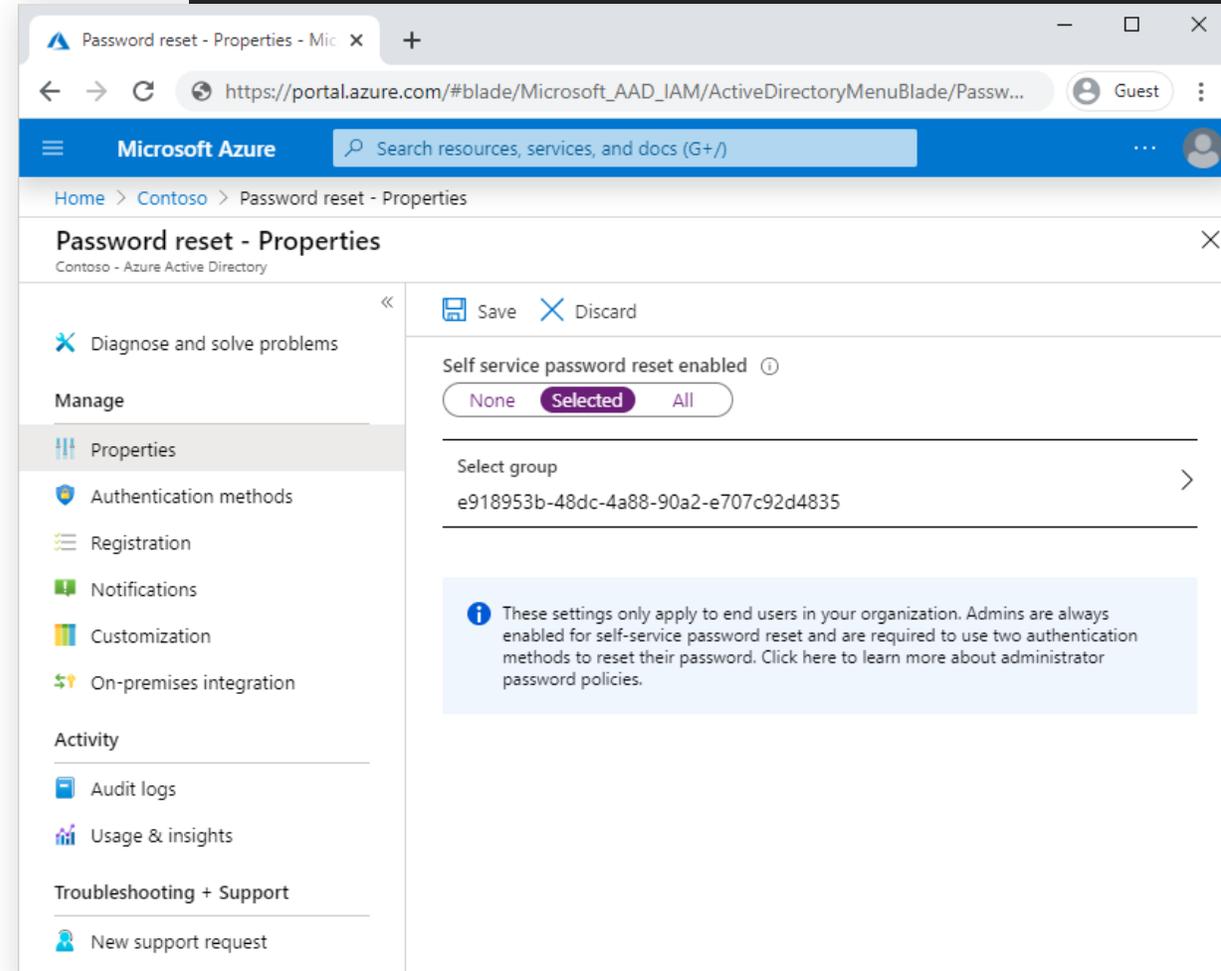
- Block Legacy Authentication
- Require MFA for admins
- Require MFA for all users
- Secure security info registration
- Block access by location (geo blocking)
- Require compliant devices

Self Service Password Reset

Enable Self Service Password Reset:

1. Sign into the Azure portal using an account with global administrator permissions.
2. Search for and select **Azure Active Directory**, then choose **Password reset** from the menu on the left-hand side.
3. From the Properties page, under the option Self service password reset enabled, choose **All**
4. Select **Save**.

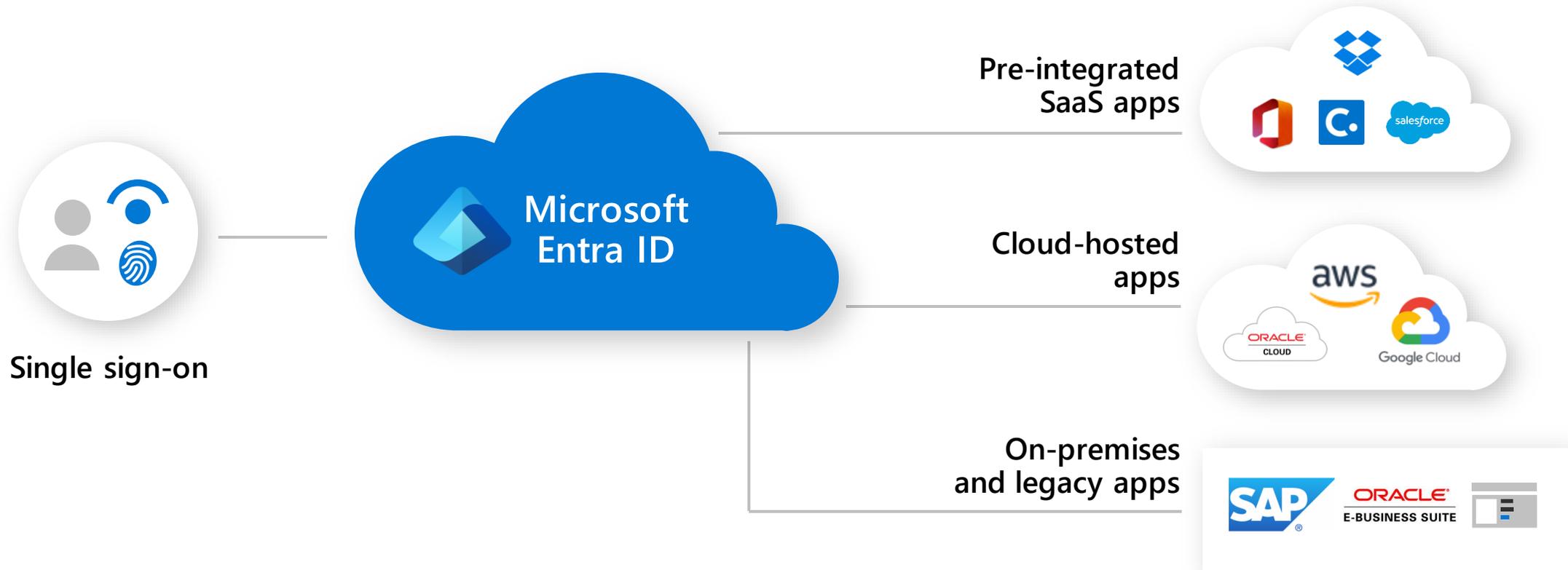
To learn more, see [Enable Azure Active Directory self-service password reset - Microsoft Entra](#)



The screenshot shows the Azure portal interface for the 'Password reset - Properties' page. The breadcrumb navigation is 'Home > Contoso > Password reset - Properties'. The page title is 'Password reset - Properties' with a subtitle 'Contoso - Azure Active Directory'. The left-hand navigation pane includes options like 'Diagnose and solve problems', 'Manage', 'Properties', 'Authentication methods', 'Registration', 'Notifications', 'Customization', 'On-premises integration', 'Activity', 'Audit logs', 'Usage & insights', 'Troubleshooting + Support', and 'New support request'. The main content area shows the 'Self service password reset enabled' setting, which is currently set to 'Selected' (with 'None' and 'All' also visible as options). Below this, there is a 'Select group' dropdown menu with the value 'e918953b-48dc-4a88-90a2-e707c92d4835'. A blue information box at the bottom states: 'These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.'

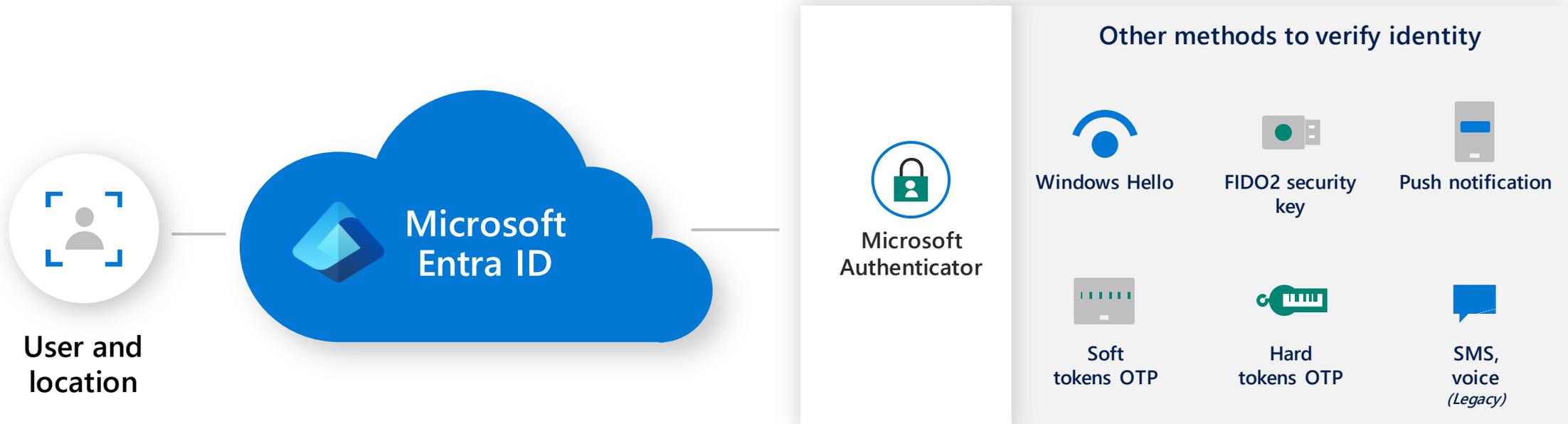
Securely access all apps using Single-Sign On

From cloud to on-premises apps



Enable MFA to keep remote employees protected

Verify user identities to establish trust

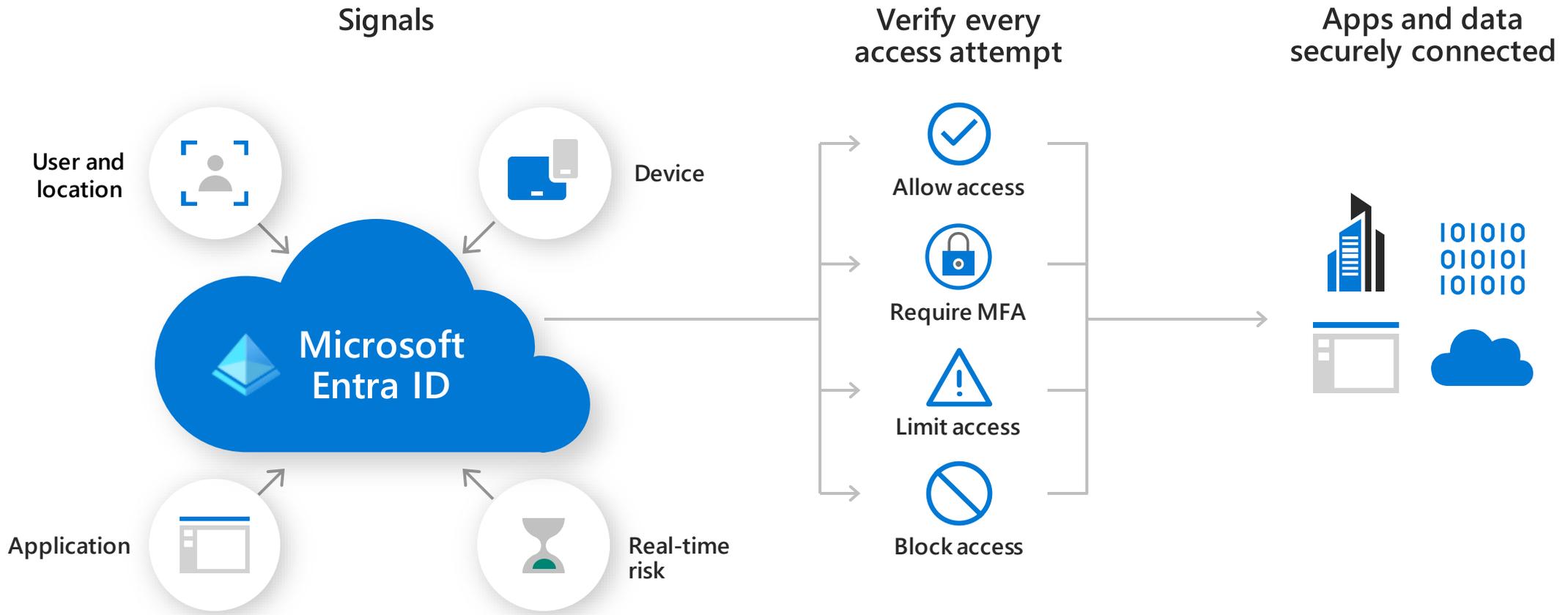


Multi-factor authentication prevents 99.9% of automated identity attacks.



Protect access for any user from anywhere

Apply consistent risk-based policies with Conditional Access



Pop quiz

02

Can I use Security Defaults to enable MFA if my customer **also** requires Conditional Access policies?

YES

NO



Email Protection

The basics



Exchange Online Protection (EOP)

Blocks commodity spam and malware



Transport Rules

Block auto-forward

Add warnings



DNS records

MX, SPF, DKIM, & DMARC



Defender for Office 365 (Formally ATP)

Analyzes email & files for anything suspicious



EOP & Defender for O365

Does not address endpoint or network security

Email Protection



Exchange Online Protection (EOP)

Blocks commodity spam and malware



Transport Rules

Block auto-forward

Add warnings

The basics



DNS records

MX, SPF, DKIM, & DMARC

The basics



Defender for Office 365

Extends to Teams & SharePoint

Analyzes email & files for anything suspicious

Safe Attachments

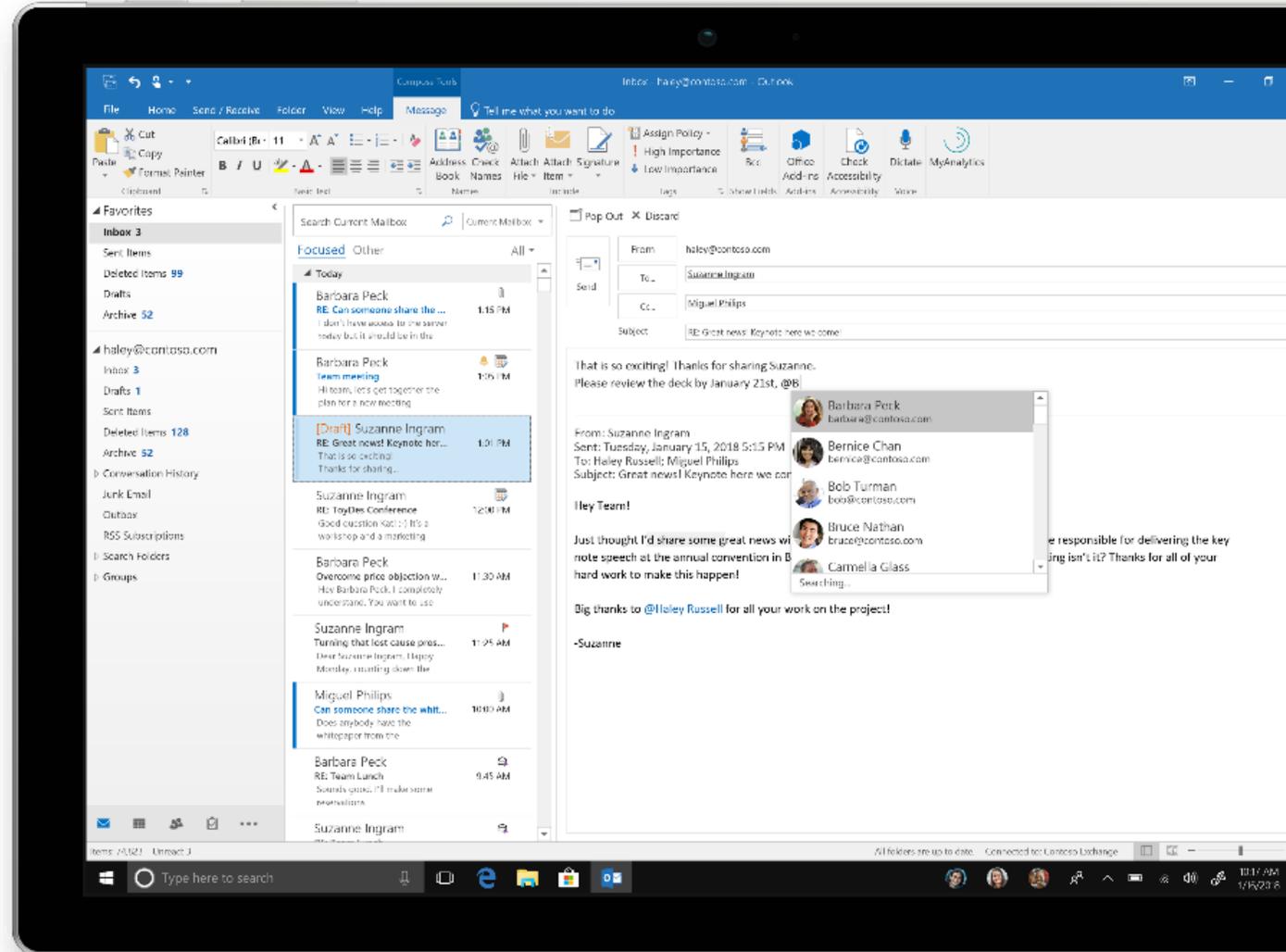
Set policies to **identify if email attachments are malicious**

Catch identified threats in corporate mail before they reach the inbox

Extend protection to files in SharePoint Online, OneDrive for Business, and Microsoft Teams

View ATP reports in the **Office 365 Security and Compliance Center dashboard**

How it works: Email attachments are opened and tested in a virtual environment. If malicious, the attachment is blocked. Protection also applies to attachments shared via SharePoint Online, OneDrive or Teams.

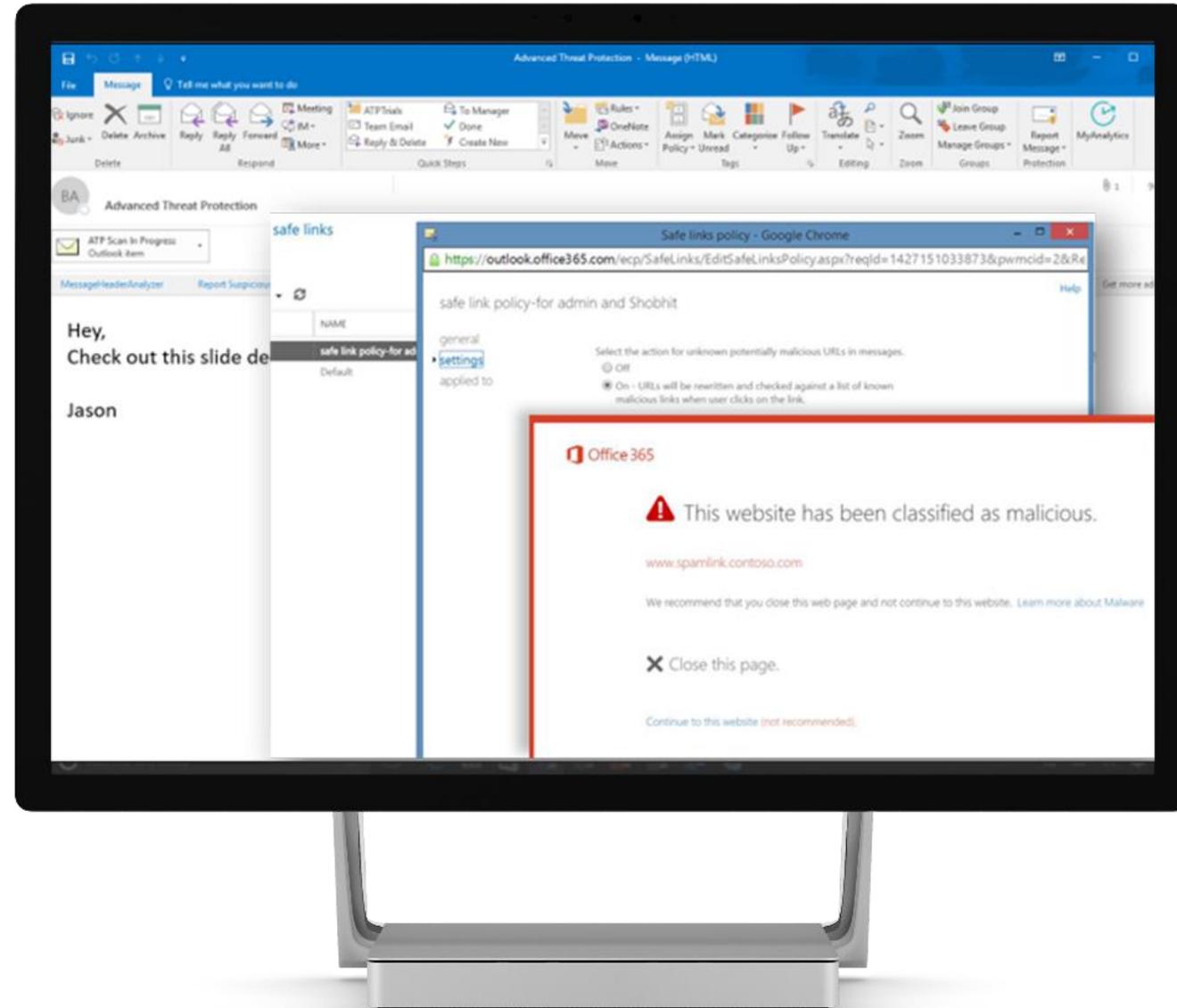


Safe Links & URL Detonation

Prevent users from being compromised by files linked to malicious URLs

Safe Links policy can allow users to bypass warnings and enable tracing

How it works :Each time a user clicks on a URL, the link is checked by ATP Safe Links before redirecting to the website.



Anti-phishing

What it is:

Mitigation against spoofing attacks / forged domains

Identifies senders that fail authentication

How it works:

An array of techniques, updated as threats evolve, help block sophisticated impersonation attempts.

- Detection of forgery of the 'From: header'
- Understanding the history of the source's email infrastructure
- Machine learning algorithms that understand a user's normal patterns of contact with others

Emails may be blocked, sent to junk mail, quarantined, or have a Safety Tips displayed

Examples:

Cóntoso.com instead of Contoso.com

meganb@**conotos**.com instead of meganb@**contoso**.com)

Bringing it all together:
Resources that can help

Practical security resources

Microsoft Secure Score

<https://security.microsoft.com/securescore>

Secure Remote Work Kit

[Guide & Checklist](#)

IT ProMentor CIS based Security Assessment tool

<https://www.itpromentor.com/cis-controls-4m365>

CIS Controls v8.1

<https://cissecurity.org>

NIST CSF

<https://www.nist.gov/cyberframework/framework>