Microsoft

DICKER DATA

Microsoft Security Labs

Microsoft Modern Work Team

Dicker Data

February 2024

Microsoft

ASCEND

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 year[2]

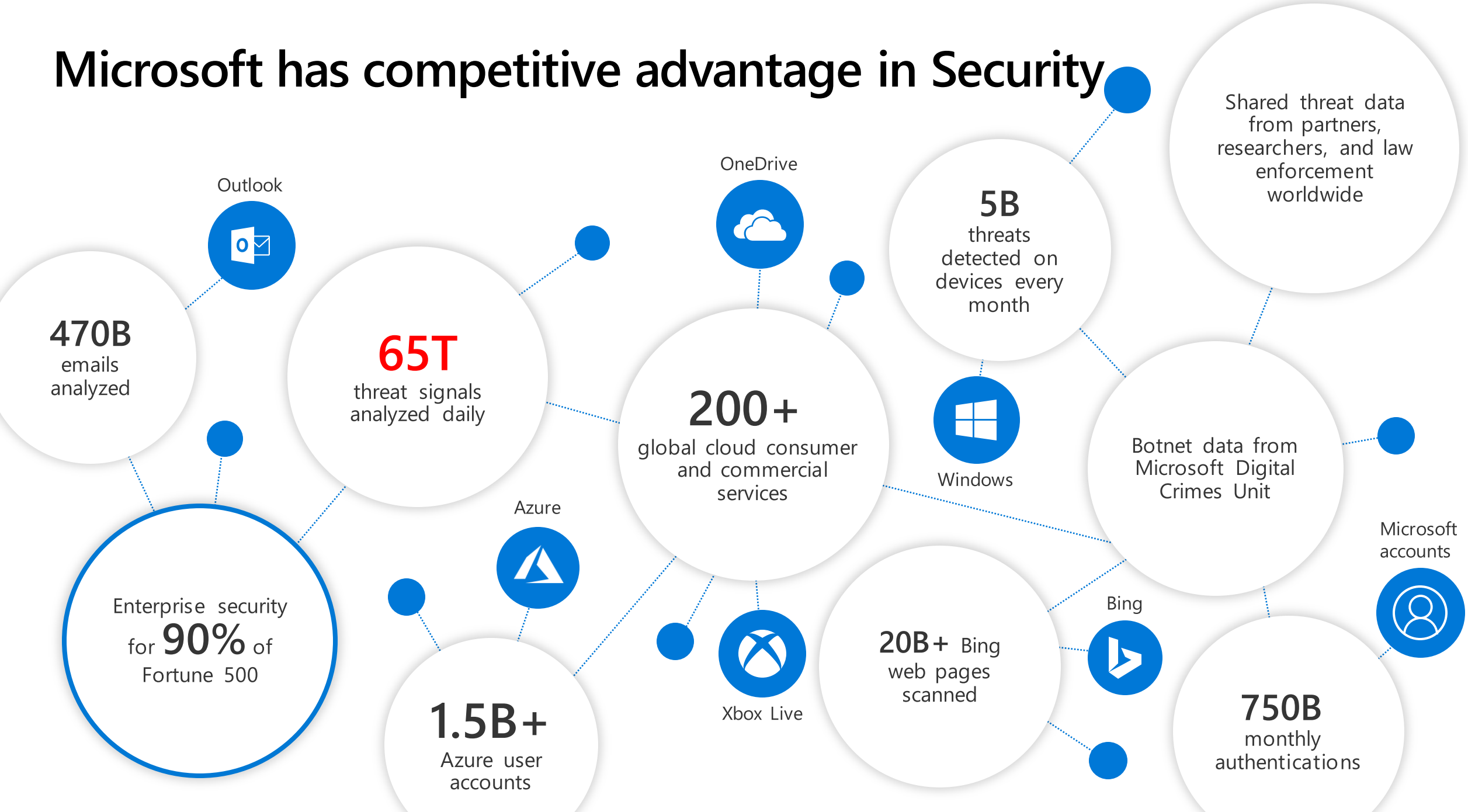
70% Over 70% of SMBs think cyber threats are becoming more of a business risk[2]

90% SMBs would consider hiring a new MSP if they offered the right cybersecurity solution[2]

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



Gartner®

Microsoft Security—a Leader in 5 Gartner Magic Quadrant reports

Access Management

Cloud Access Security Brokers

Enterprise Information Archiving

Endpoint Protection Platforms

Unified Endpoint Management

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

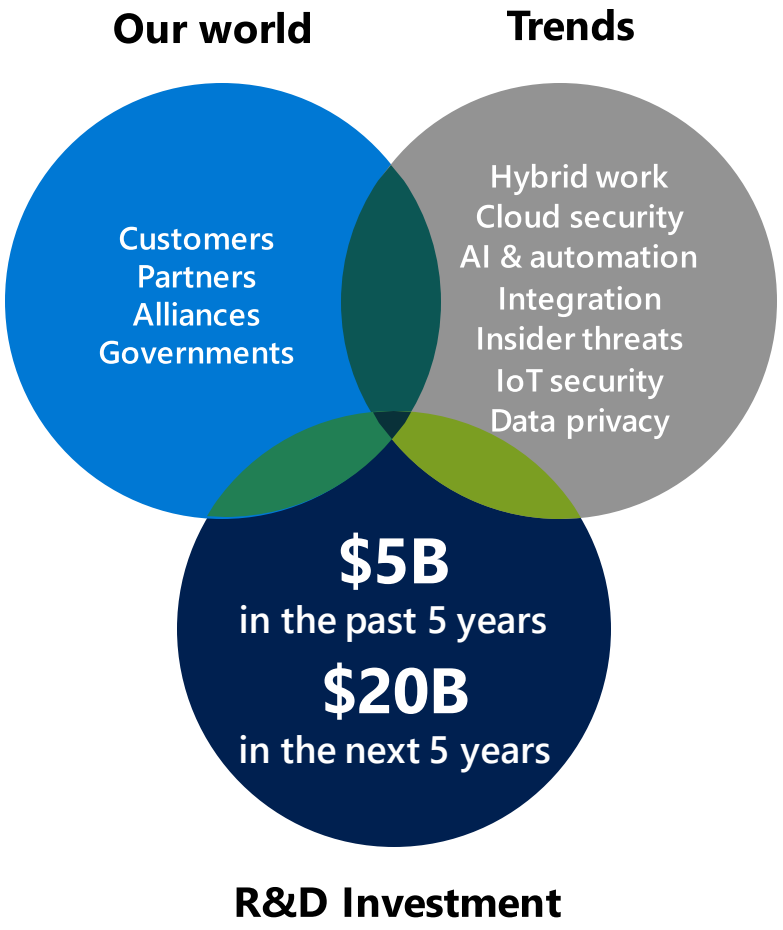
*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Craig Lawson, Steve Riley, October 2020

*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

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:

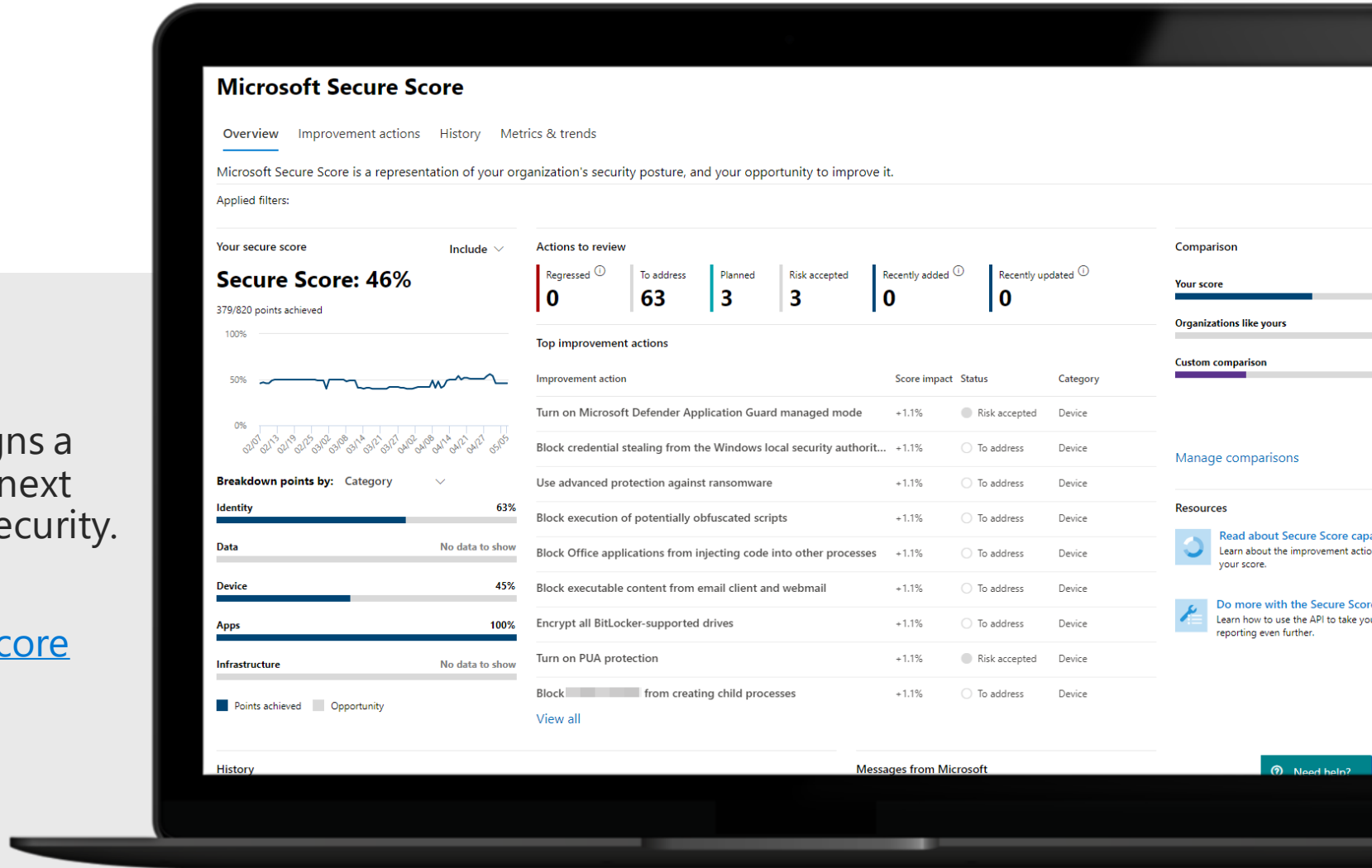
Check Microsoft Secure Score

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.

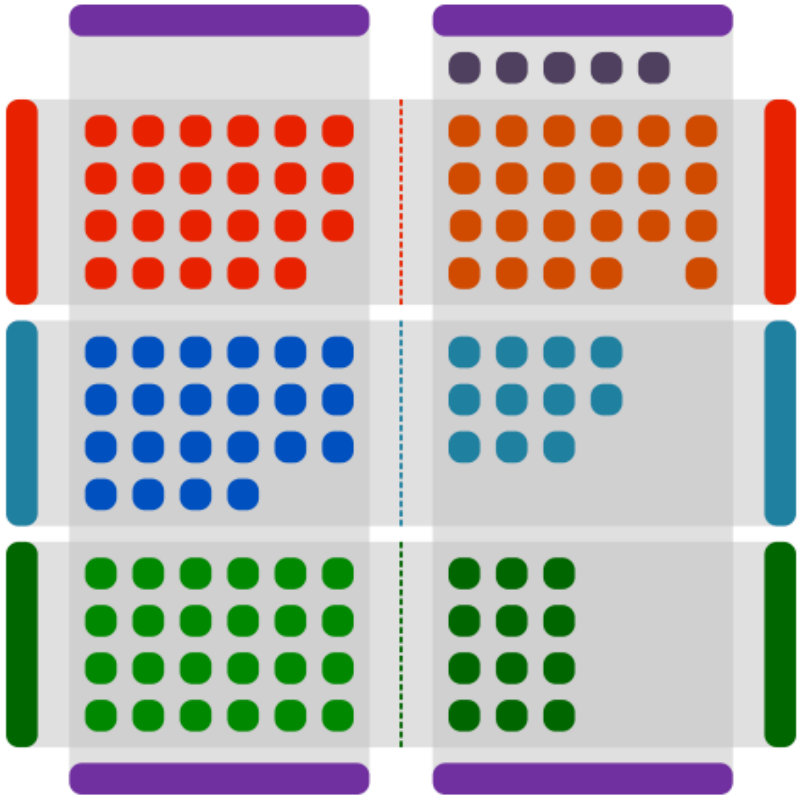
How to access:

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

DICKER DATA | Microsoft

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

ASCEND

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 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

→

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

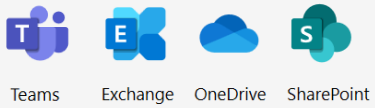
1) As standalone SKU, *up to 300 users*
Entitlement for use on up to 5 devices

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

Microsoft 365 Offerings for SMBs

Microsoft 365 Business Basic

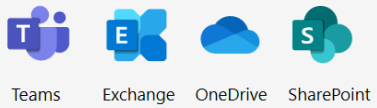
Cloud Services



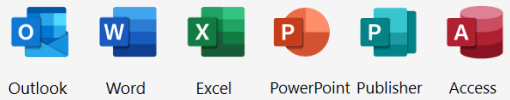
$10.80 per user/month

Microsoft 365 Business Standard

Cloud Services



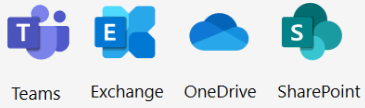
Desktop Apps



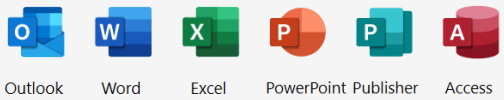
$22.44 per user/month

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

- **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

+

Reduce license costs

$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

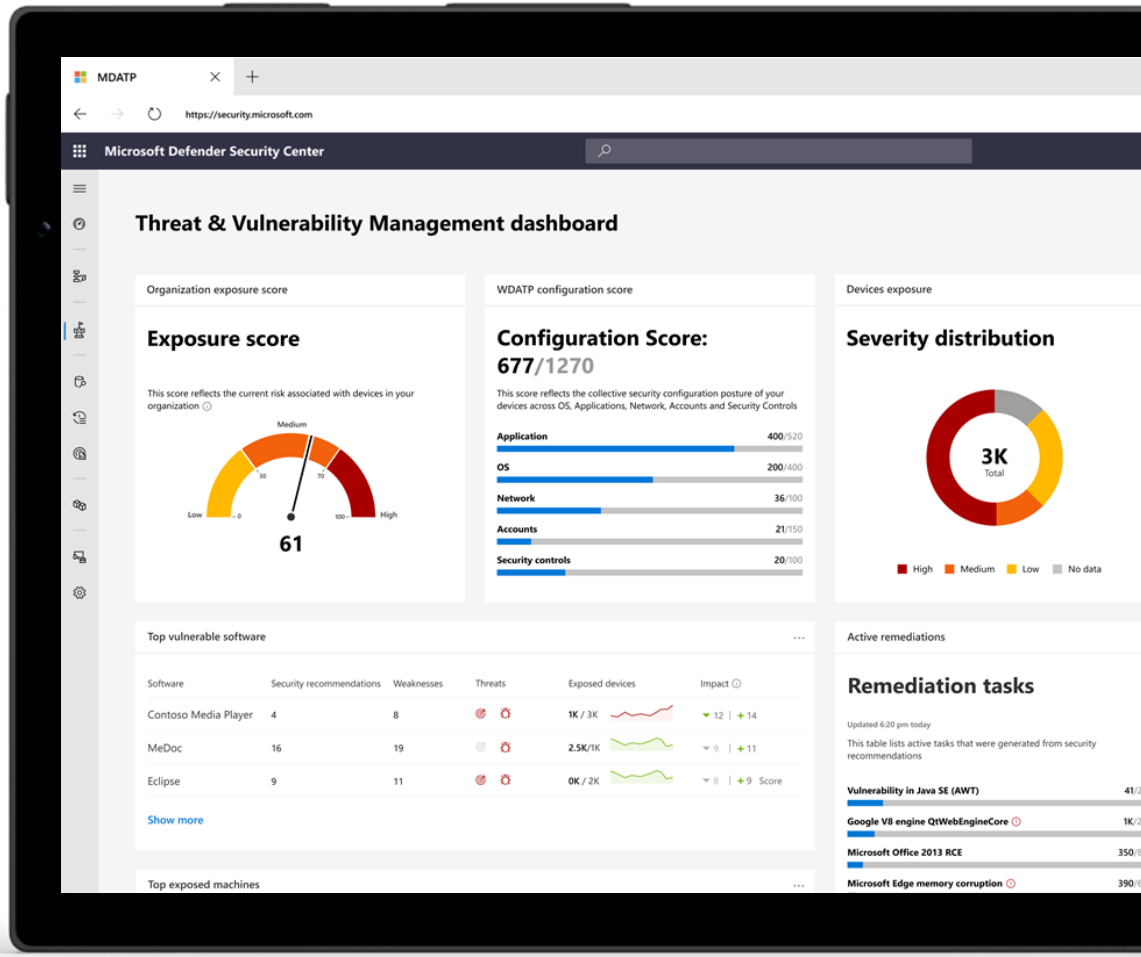
Simplified Onboarding and Administration

APIs and Integration

Threat & Vulnerability Management

A risk-based approach to mature your vulnerability management program

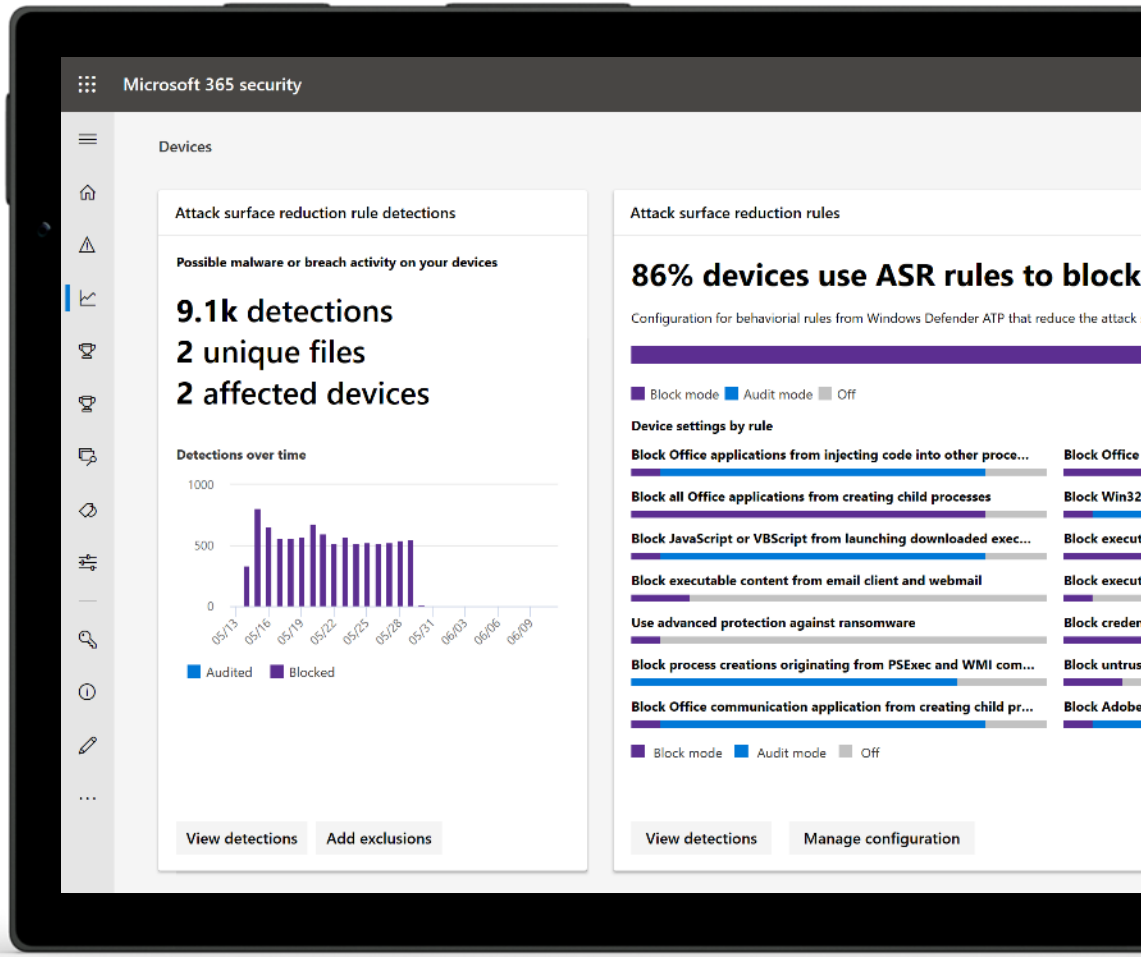
- Continuous real-time discovery
- Context-aware prioritization
- Built-in end-to-end remediation process



Attack Surface Reduction

Protect against risks by reducing the surface area of attack

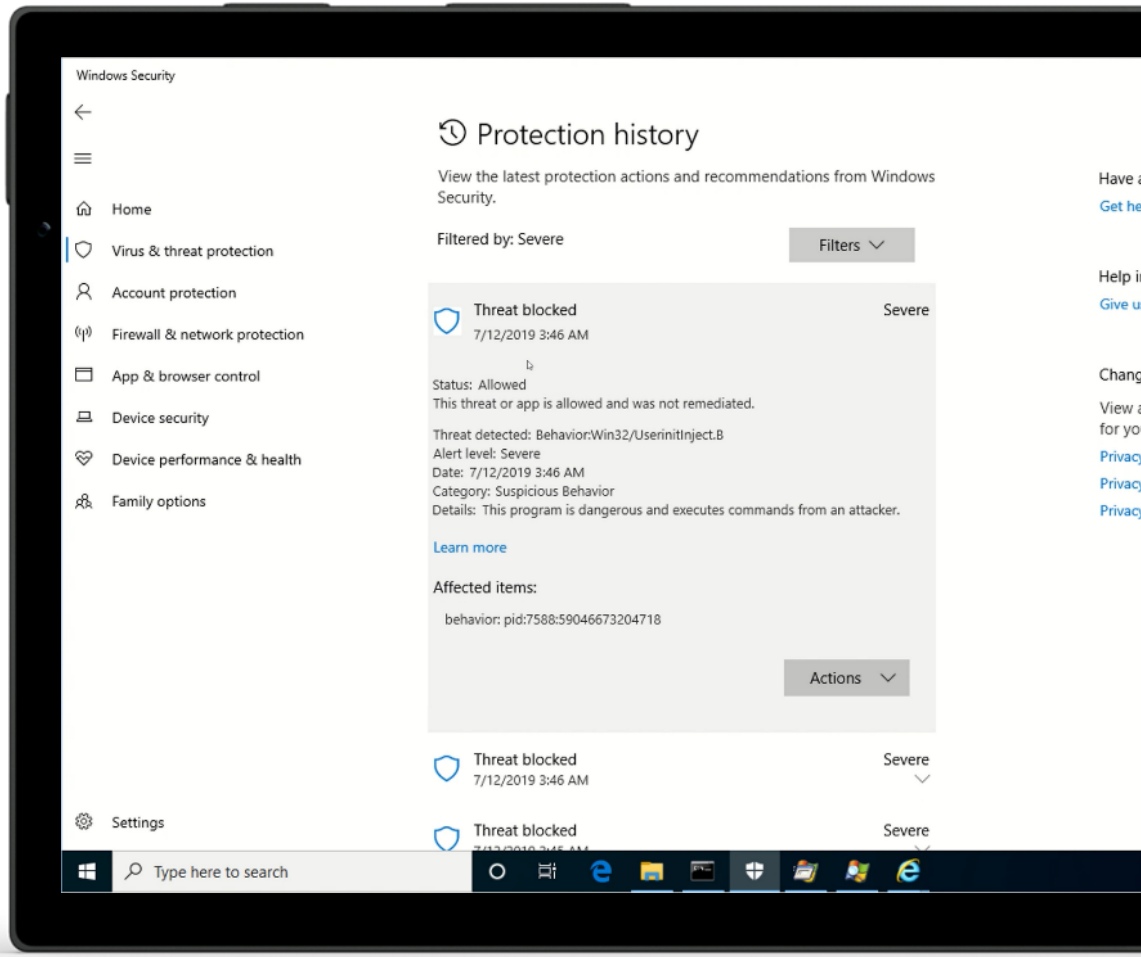
- System hardening without disruption
- Customization that fits your organization
- Visualize the impact and simply turn it on



Next Generation Protection

Helps block and tackle sophisticated threats and malware

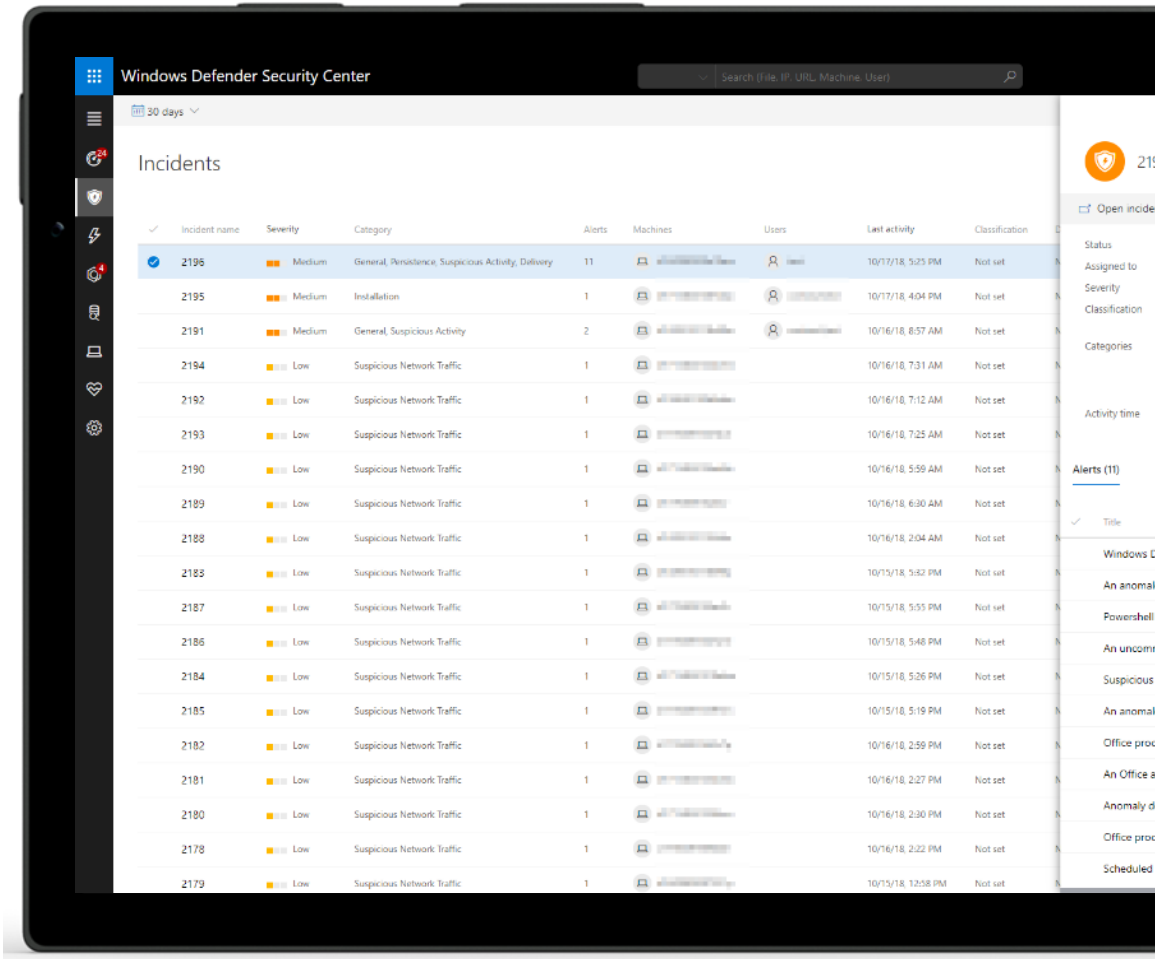
- Behavioral based real-time protection
- Blocks file-based and fileless malware
- Stops malicious activity from trusted and untrusted applications



Endpoint Detection & Response

Detect and investigate advanced persistent attacks

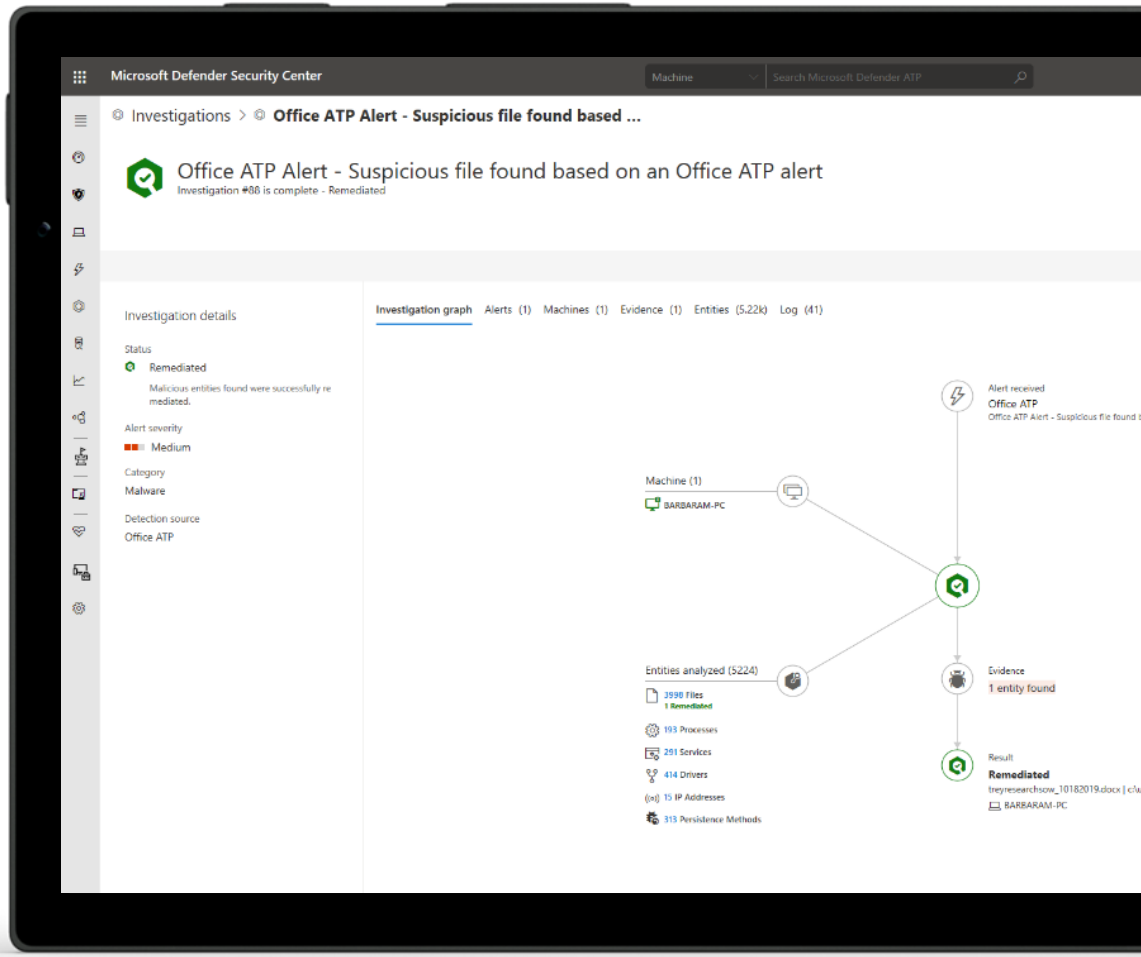
- Behavioral-based detection
- Manual response actions for a device or file
- Live response to gain access to devices



Auto Investigation & Remediation

Automatically investigates alerts and helps to remediate complex threats

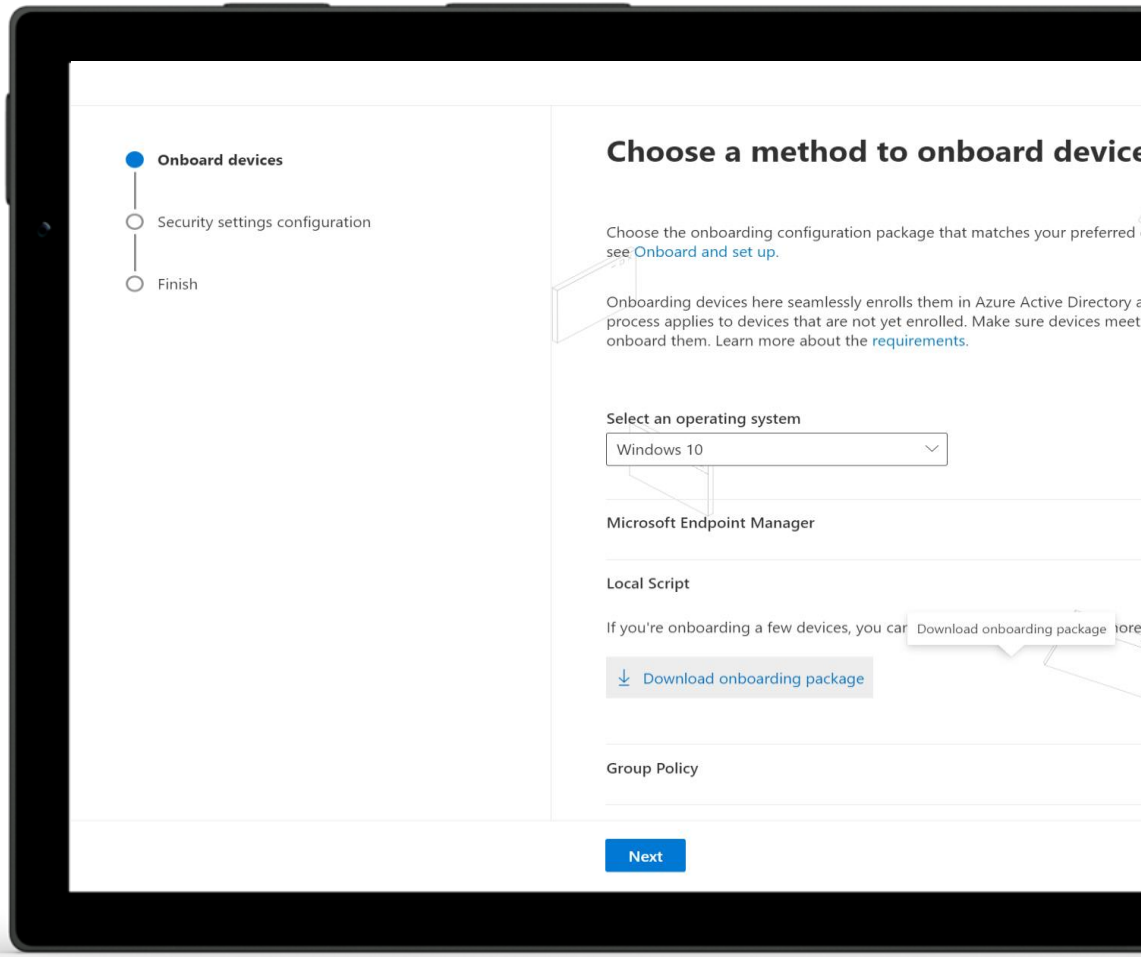
- Mimics the ideal steps analysts would take
- Tackles file or memory-based attacks
- Scales security operations with 24x7 automated responses



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

Endpoints

iOS

Mobile device OS

Windows 365

Azure Virtual Desktop

Virtual desktops

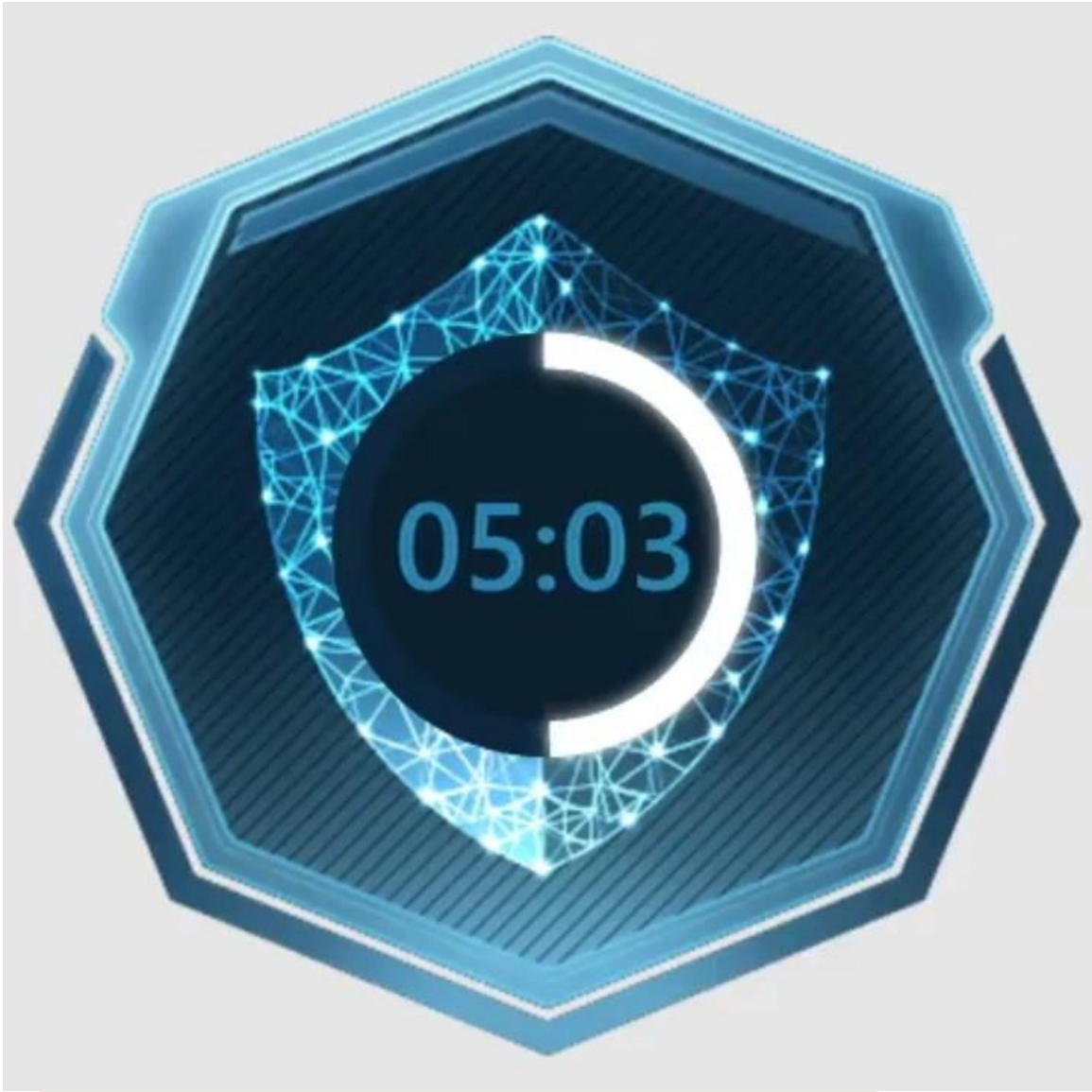
Product Comparison: Defender for Business brings enterprise=grade capabilities to SMBs

Customer size	< 300 seats	> 300 seats	
Endpoint capabilities\SKU	**Microsoft Defender for Business (currently in preview, will 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]		

[1]Limited. [2] Optimized for SMB. [3] Additional capabilities planned

Demonstration

5 Minute break

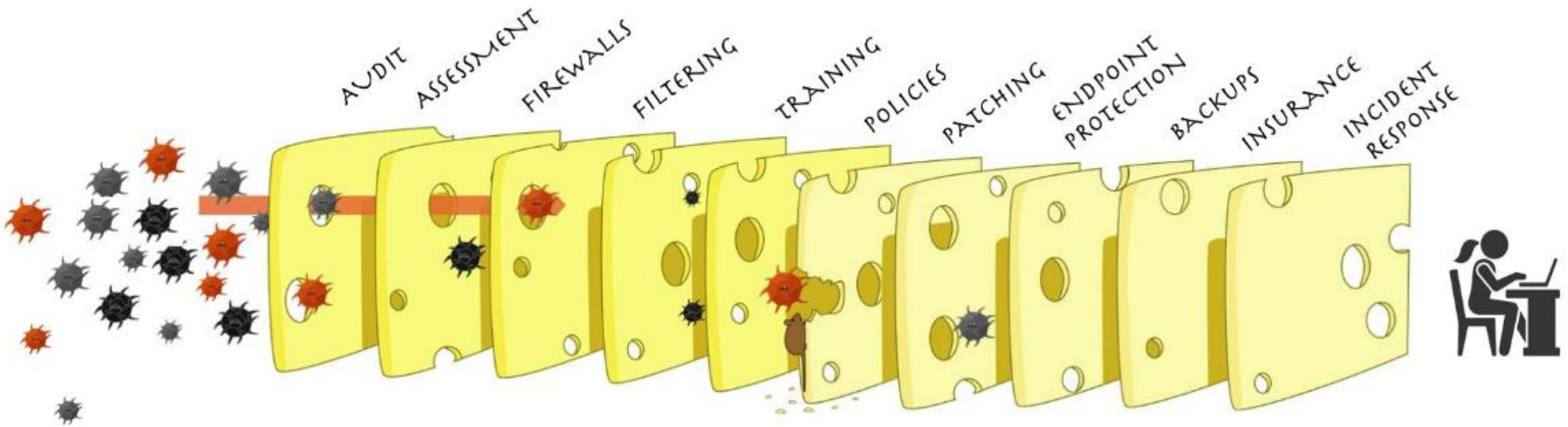


Mastering Microsoft Assessments

ASCEND

THE SWISS CHEESE CYBERSECURITY DEFENSE-IN-DEPTH MODEL

RECOGNIZING THAT NO SINGLE INTERVENTION IS SUFFICIENT TO PREVENT HARM



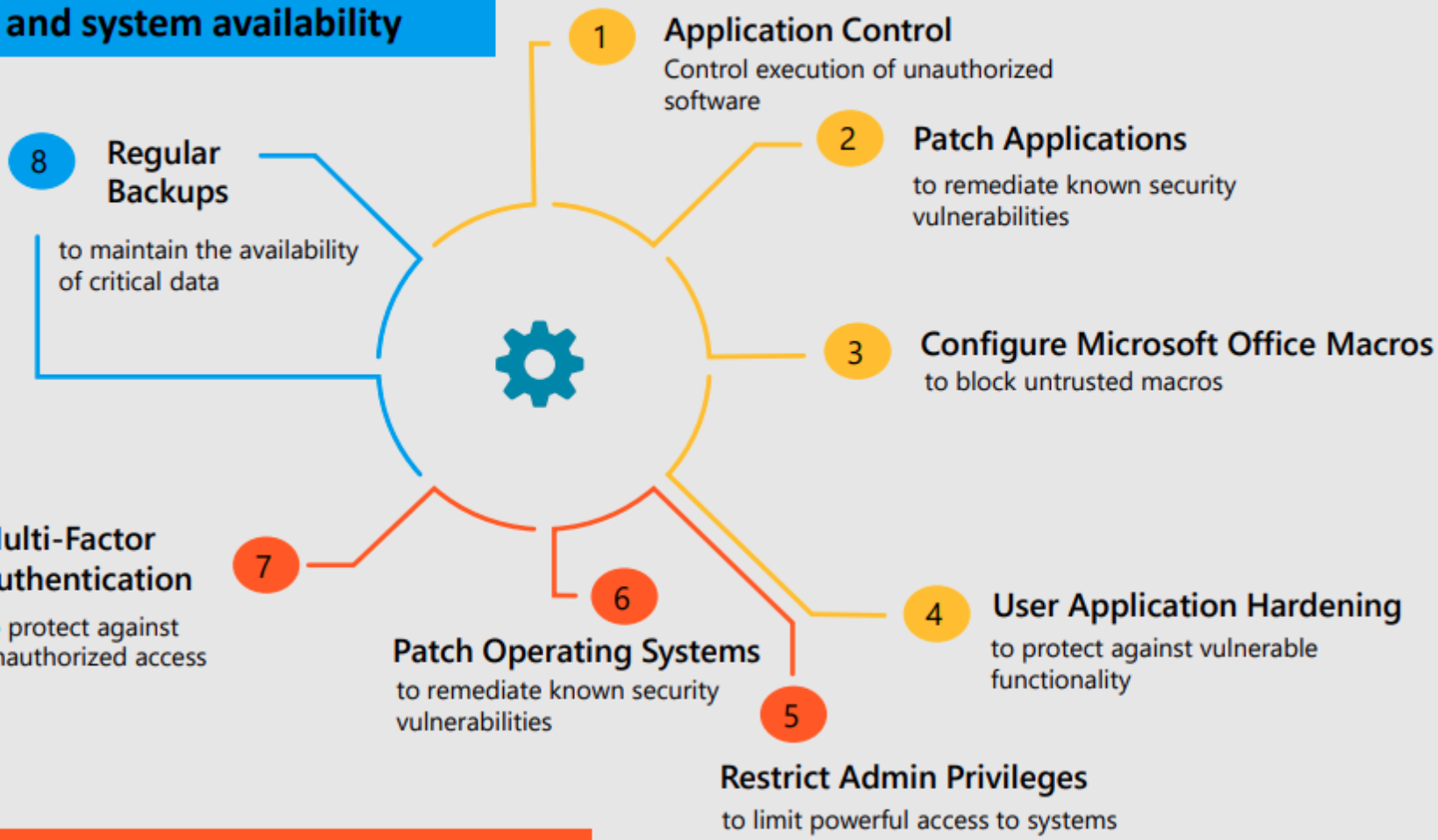
EACH INTERVENTION (LAYER) HAS IMPERFECTIONS (HOLES).
MULTIPLE LAYERS IMPROVE SUCCESS.

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

Microsoft

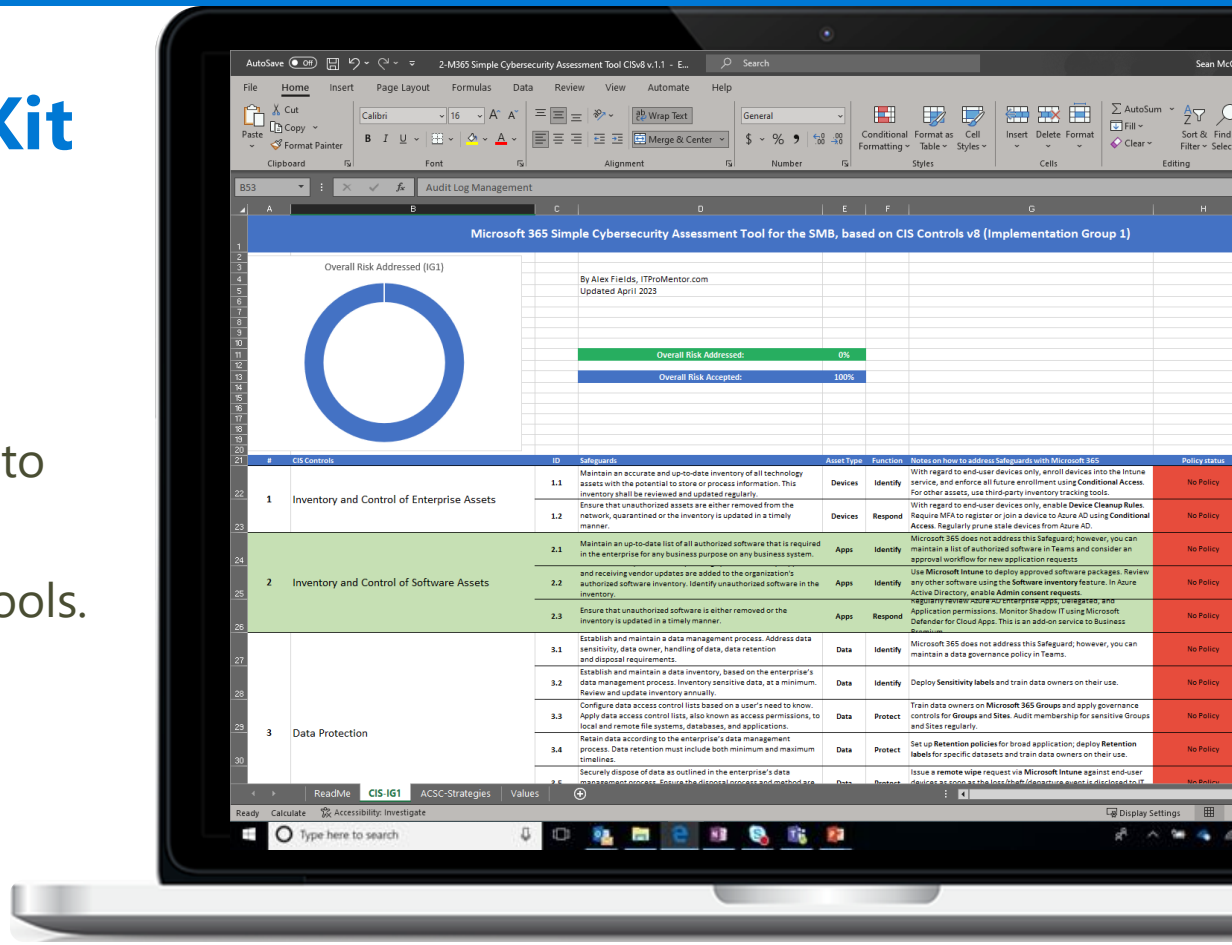
Evolving Role of MSPs: Managed Security Services

ASCEND

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]

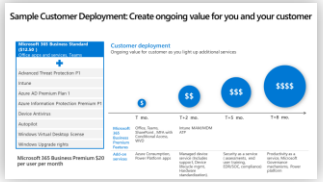


DICKER DATA | Microsoft

Microsoft 365 Partner Playbook

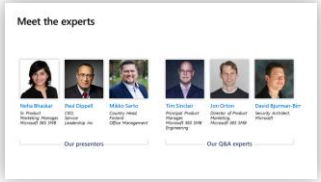
Microsoft 365 Partner Playbook: Practical Guidance across the partner journey

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

Cyber Security Assessment Tool

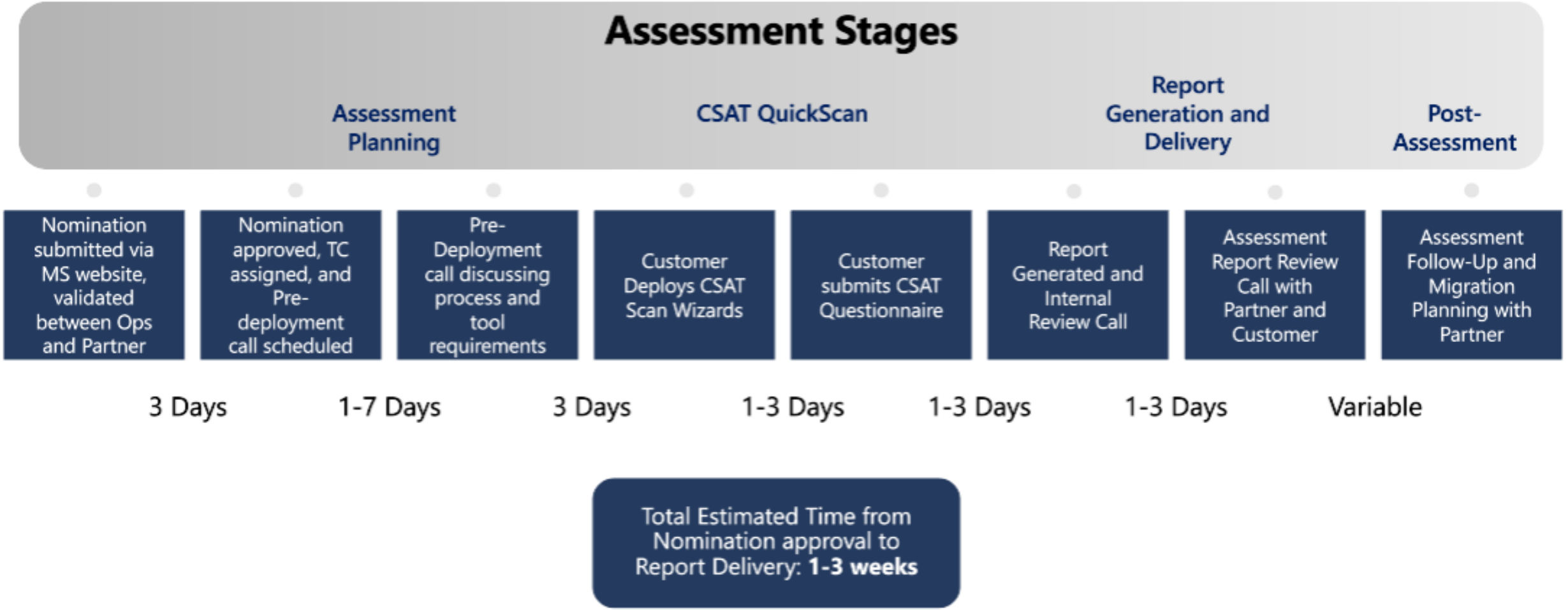
DICKER DATA | Microsoft

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	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	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	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	• 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	• 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)	• 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



DICKER DATA | Microsoft

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.

DICKER DATA | Microsoft

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]

DICKER DATA | Microsoft

Compliance Manager

Manage your compliance from one place

Ongoing risk assessment

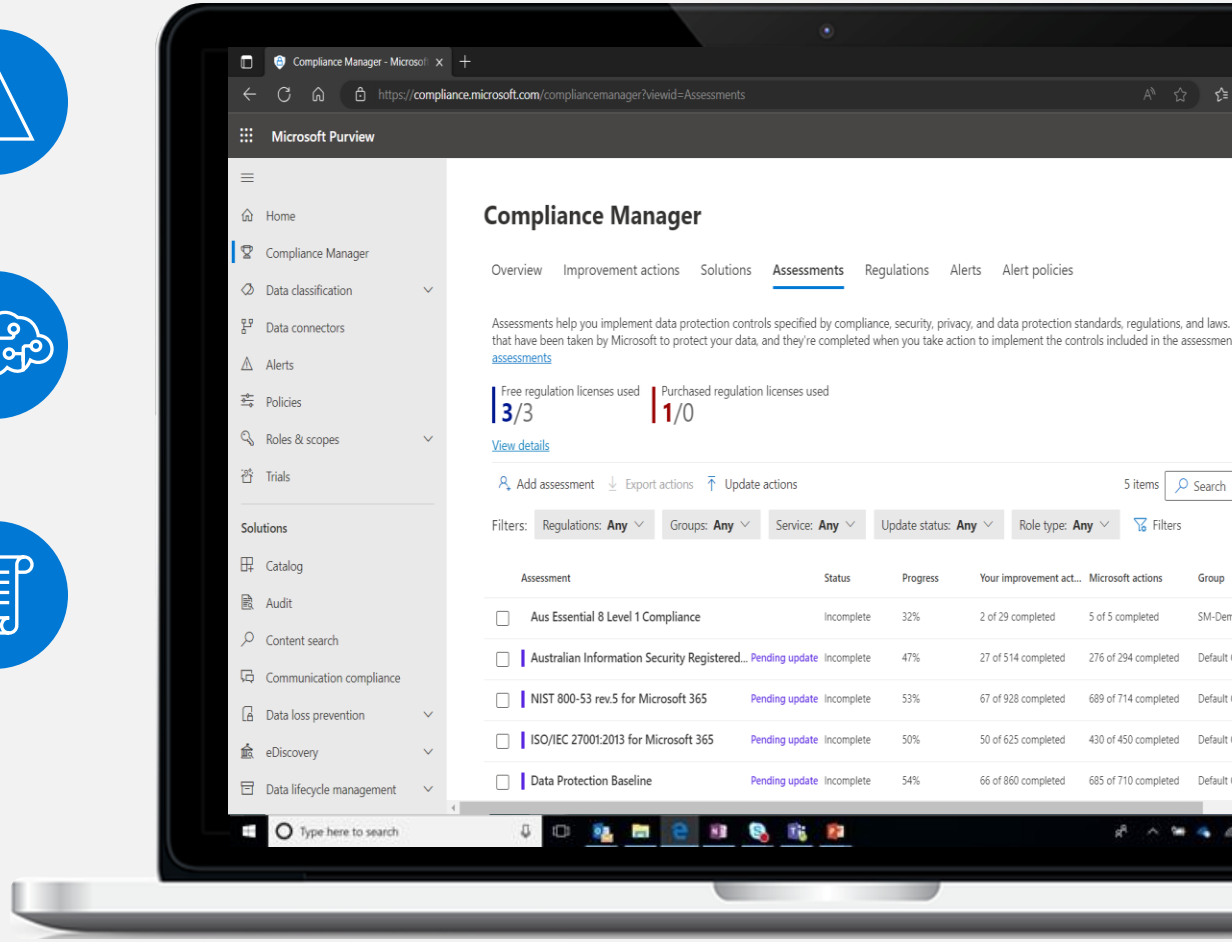
An intelligent score reflects your compliance posture against regulations or standards

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

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

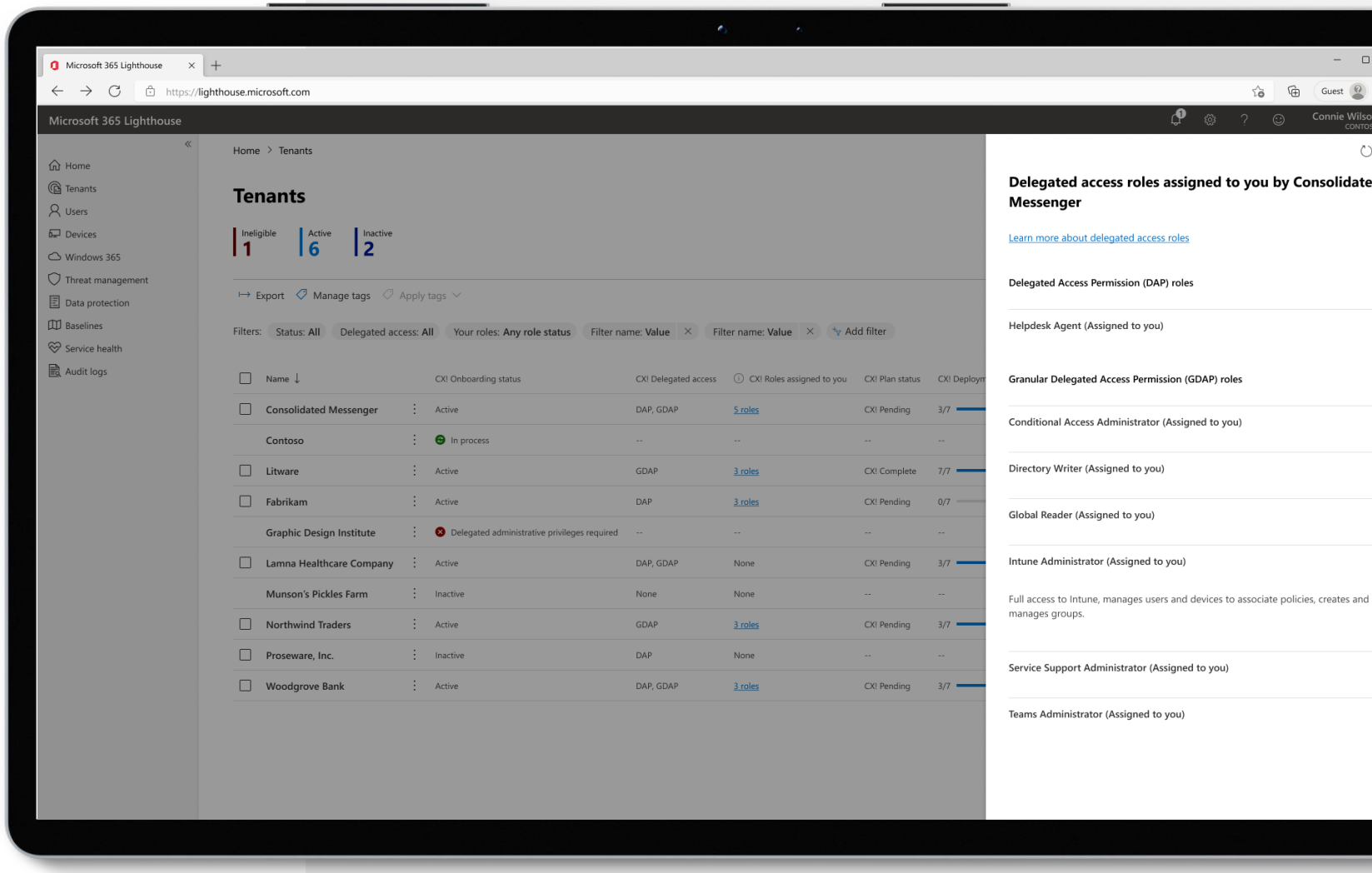
Right size permissions across your technicians to the tasks they need to perform.

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]

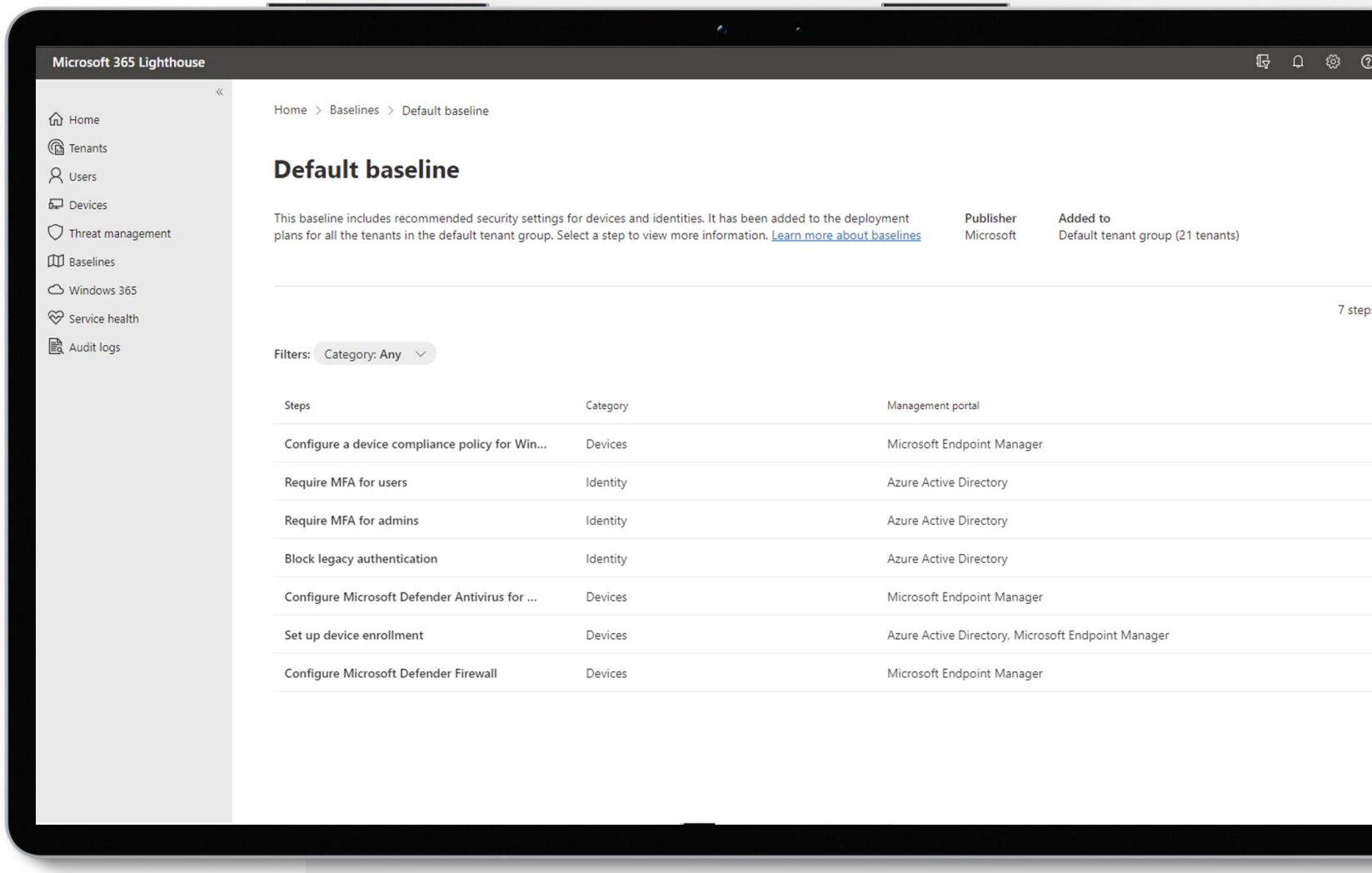
Standardize configuration

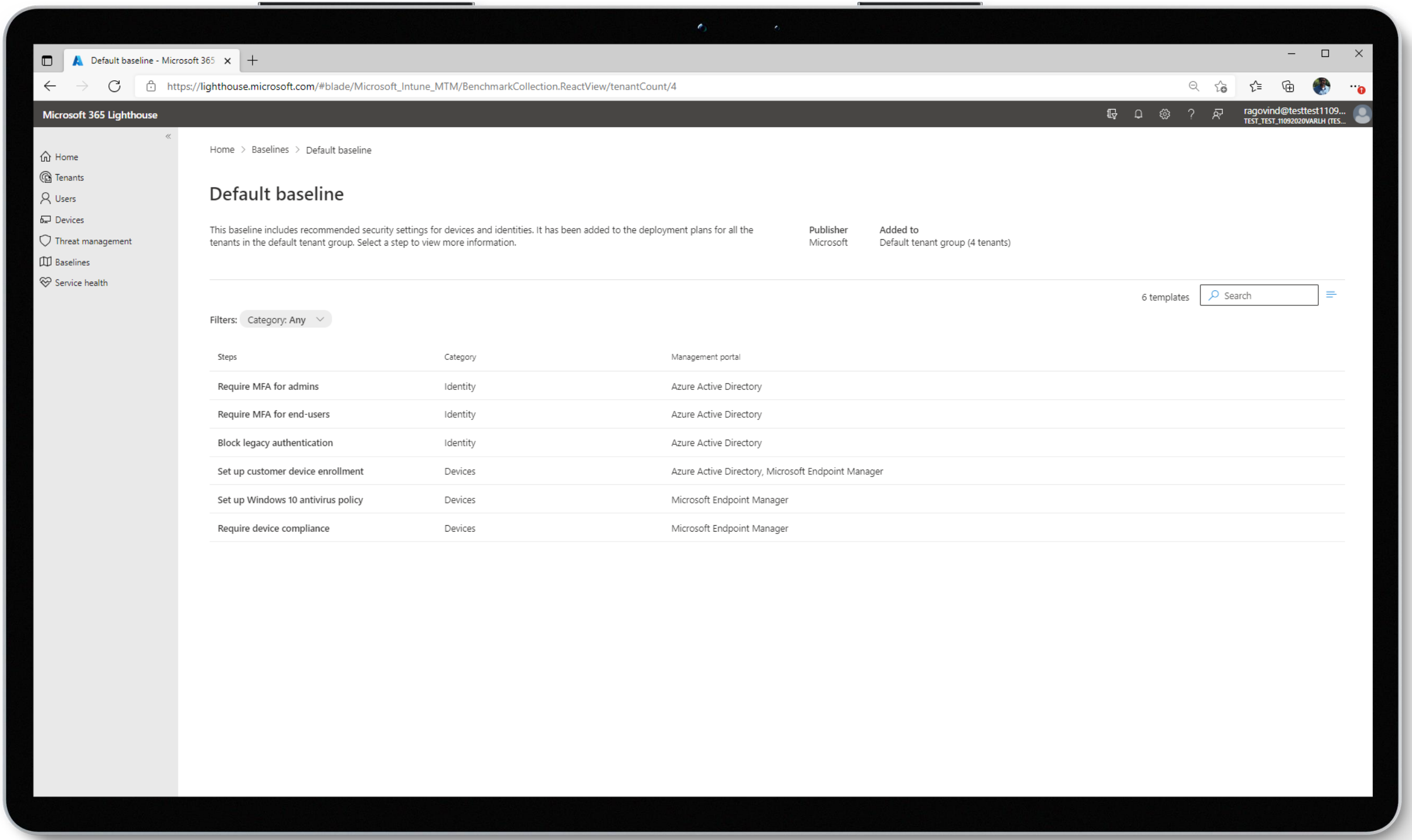
Recommended settings

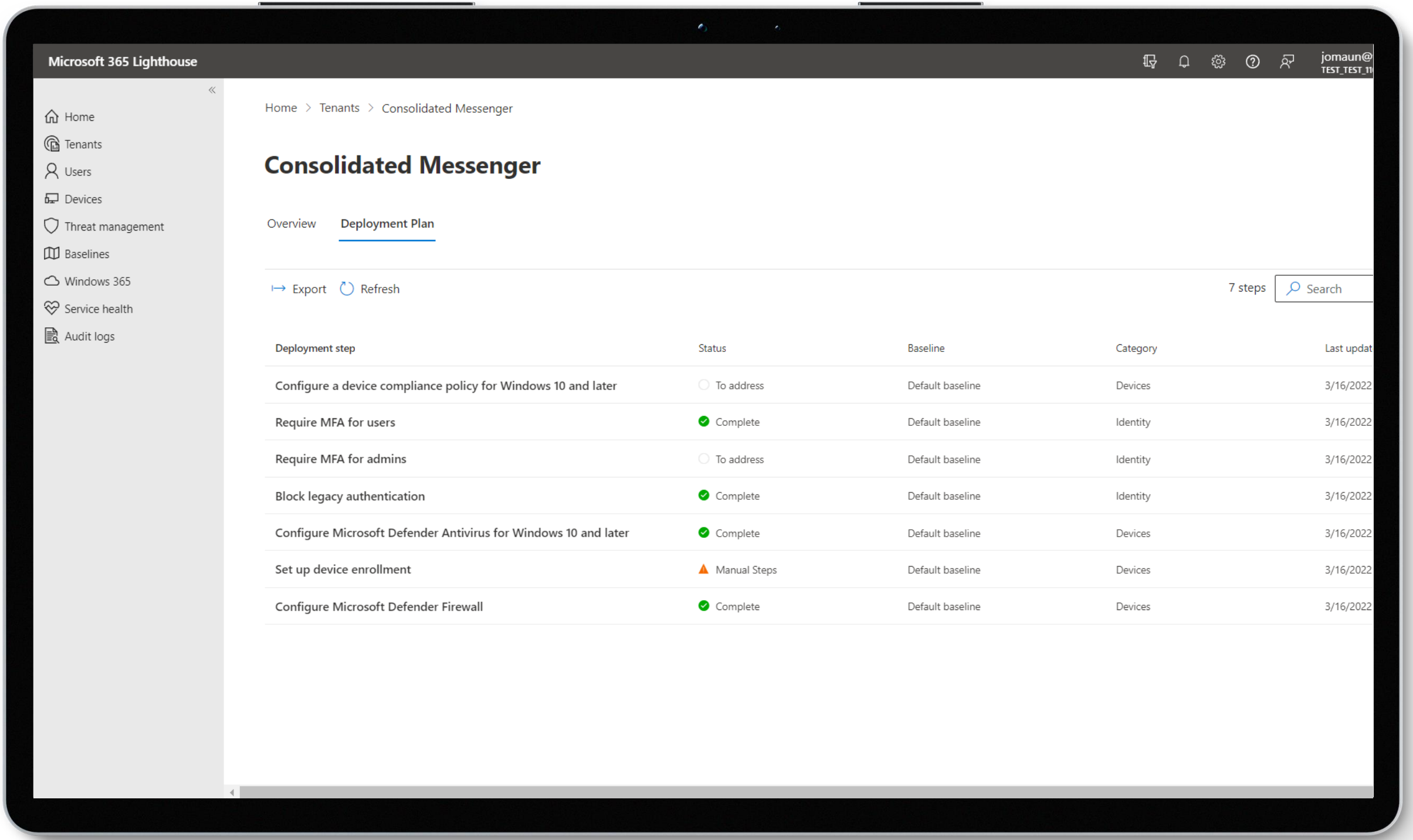
Baselines are Microsoft's recommended settings and policies optimized for small and medium sized businesses.

Consistent deployment

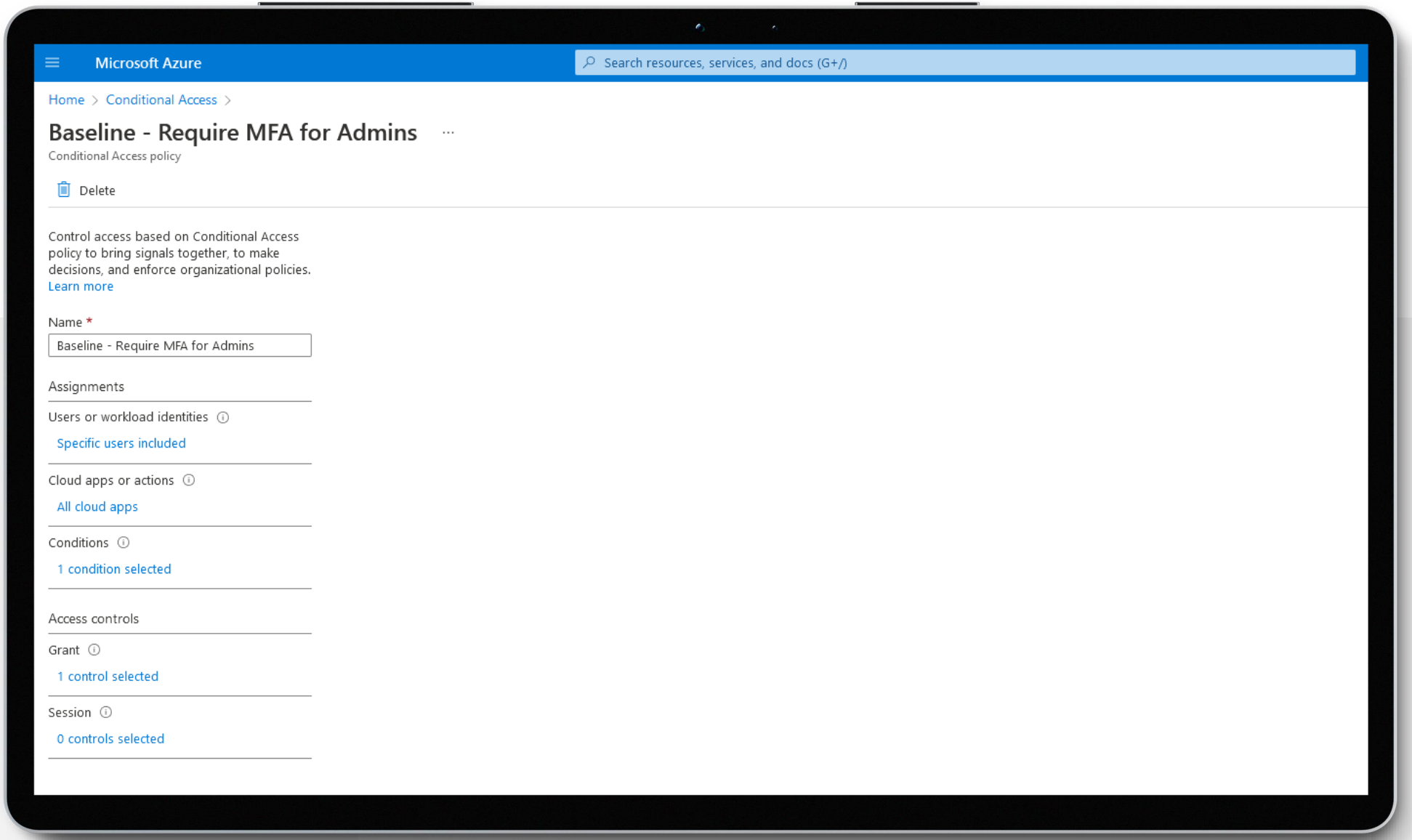
Move beyond monitoring by deploying consistent security standards across new and existing customers using Deployment plans.




Default baseline - Microsoft 365
https://lighthouse.microsoft.com/#blade/Microsoft_Intune_MTM/BenchmarkCollection.ReactView/tenantCount/4
Microsoft 365 Lighthouse
ragovind@testtest1109...
TEST_TEST_11092020VARLH (TES...
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
Search
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


Microsoft 365 Lighthouse
jomaun@
TEST_TEST_11
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
Search
Deployment step
Status
Baseline
Category
Last updat
Configure a device compliance policy for Windows 10 and later
To address
Default baseline
Devices
3/16/2022
Require MFA for users
Complete
Default baseline
Identity
3/16/2022
Require MFA for admins
To address
Default baseline
Identity
3/16/2022
Block legacy authentication
Complete
Default baseline
Identity
3/16/2022
Configure Microsoft Defender Antivirus for Windows 10 and later
Complete
Default baseline
Devices
3/16/2022
Set up device enrollment
Manual Steps
Default baseline
Devices
3/16/2022
Configure Microsoft Defender Firewall
Complete
Default baseline
Devices
3/16/2022

Microsoft 365 Lighthouse Deployment Plan



Microsoft

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.

View all threats | View all active threats

Microsoft Defender Antivirus protection

0 devices need antivirus ...

Data reflects Windows 10 devices only

Tenant	Devices not protected
Contoso	0 / 4

View full report

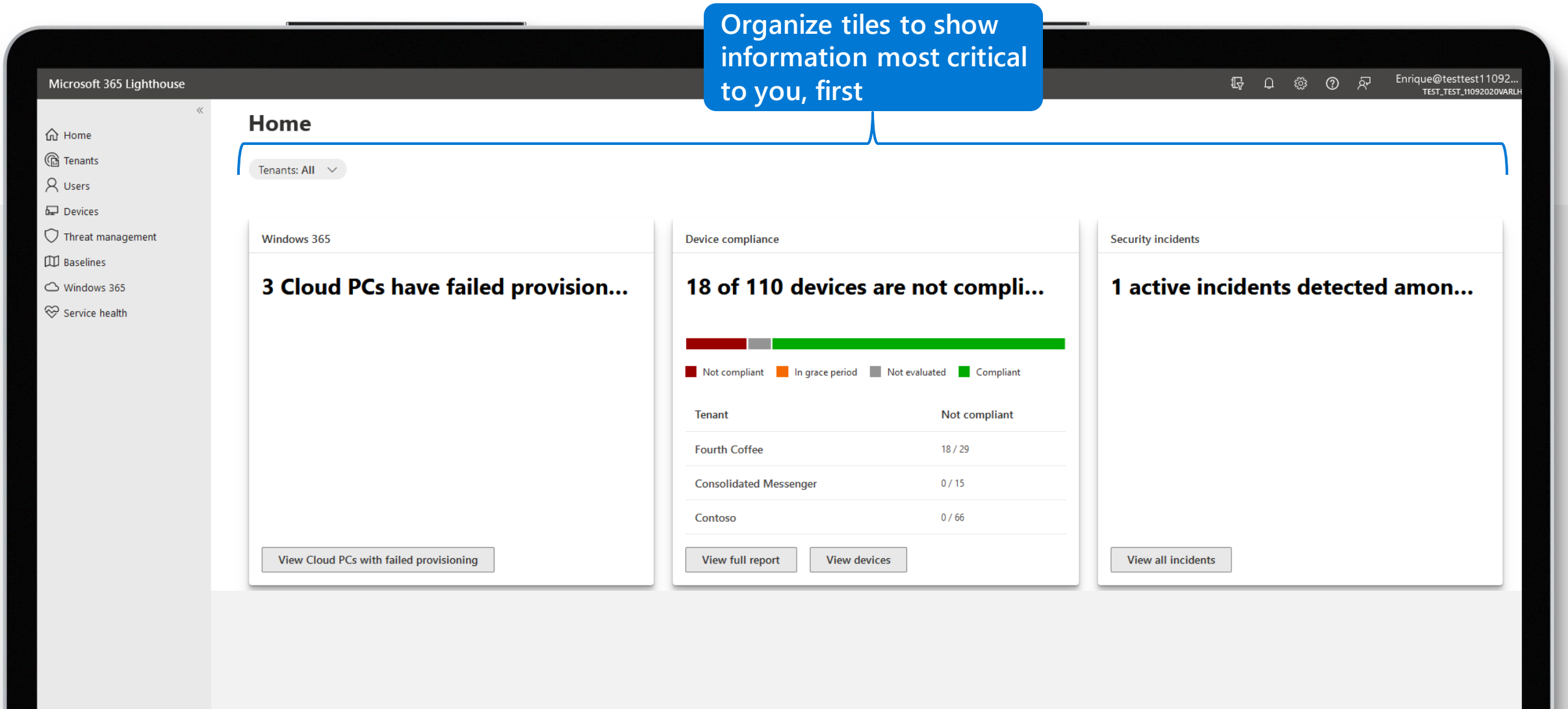
Risky users

3 users flagged for risk

Tenant	Risky users
Contoso	3

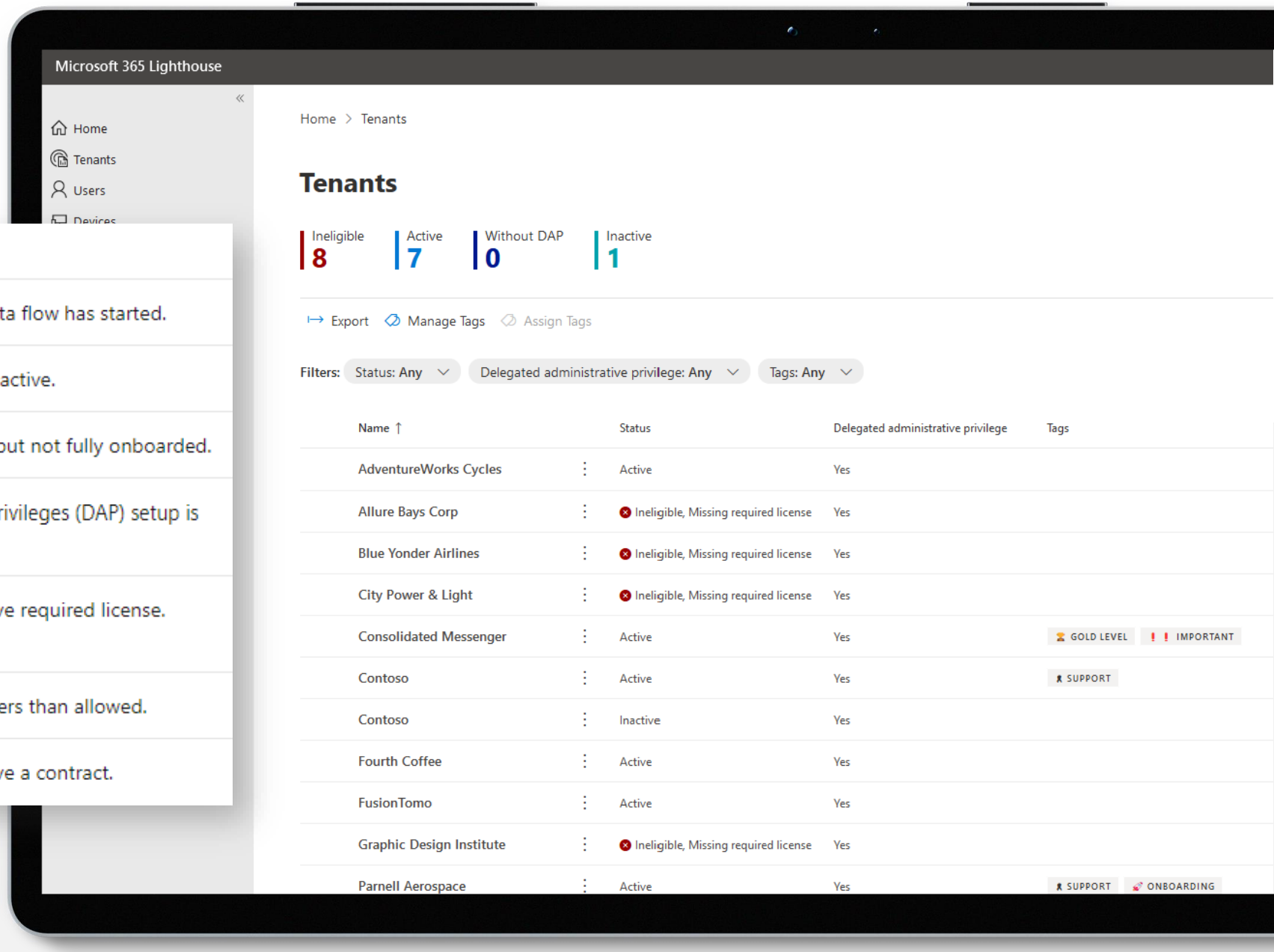
View risky users

Daily Security Health Check



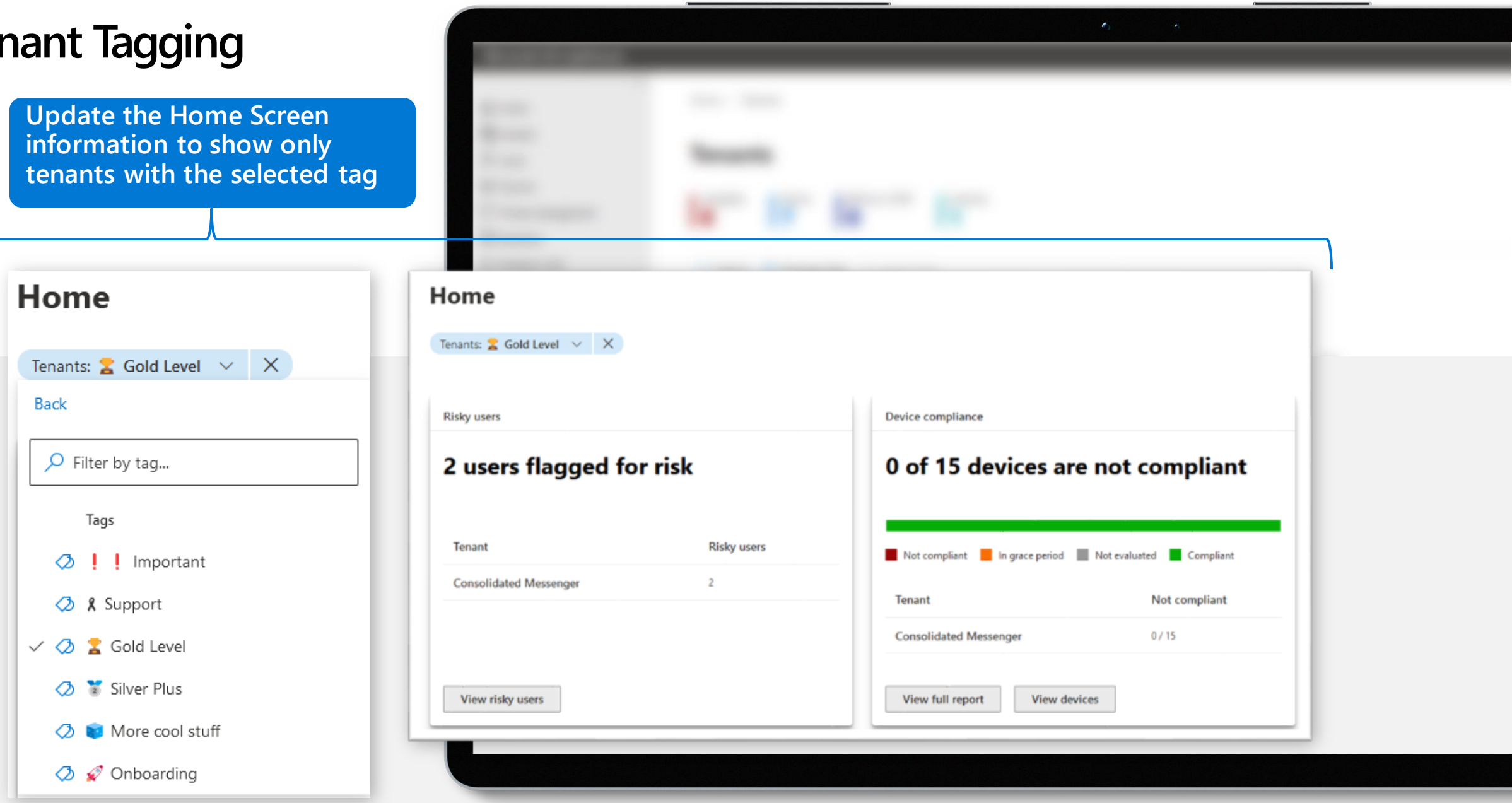
Tenant Status

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.

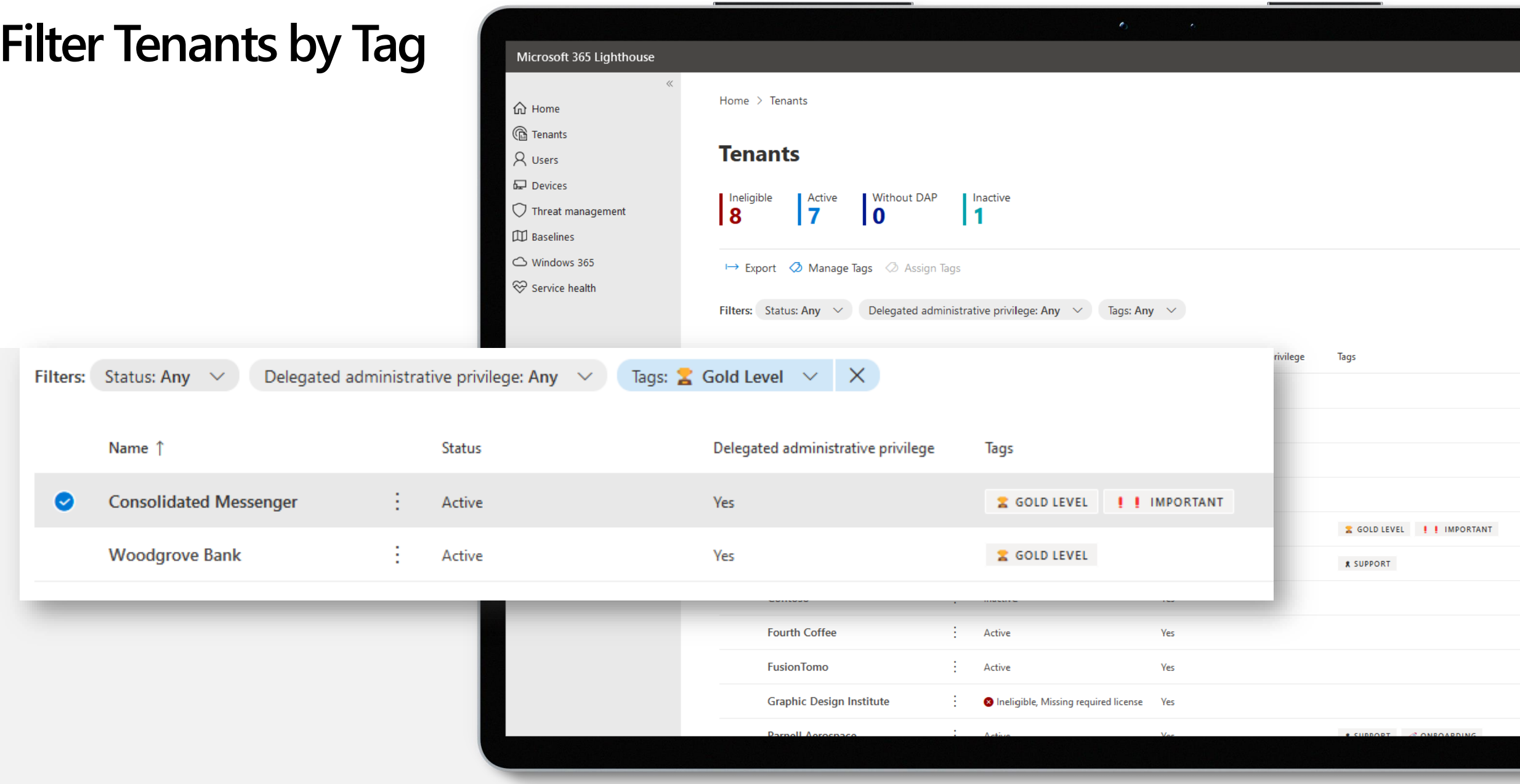


Tenant Tagging

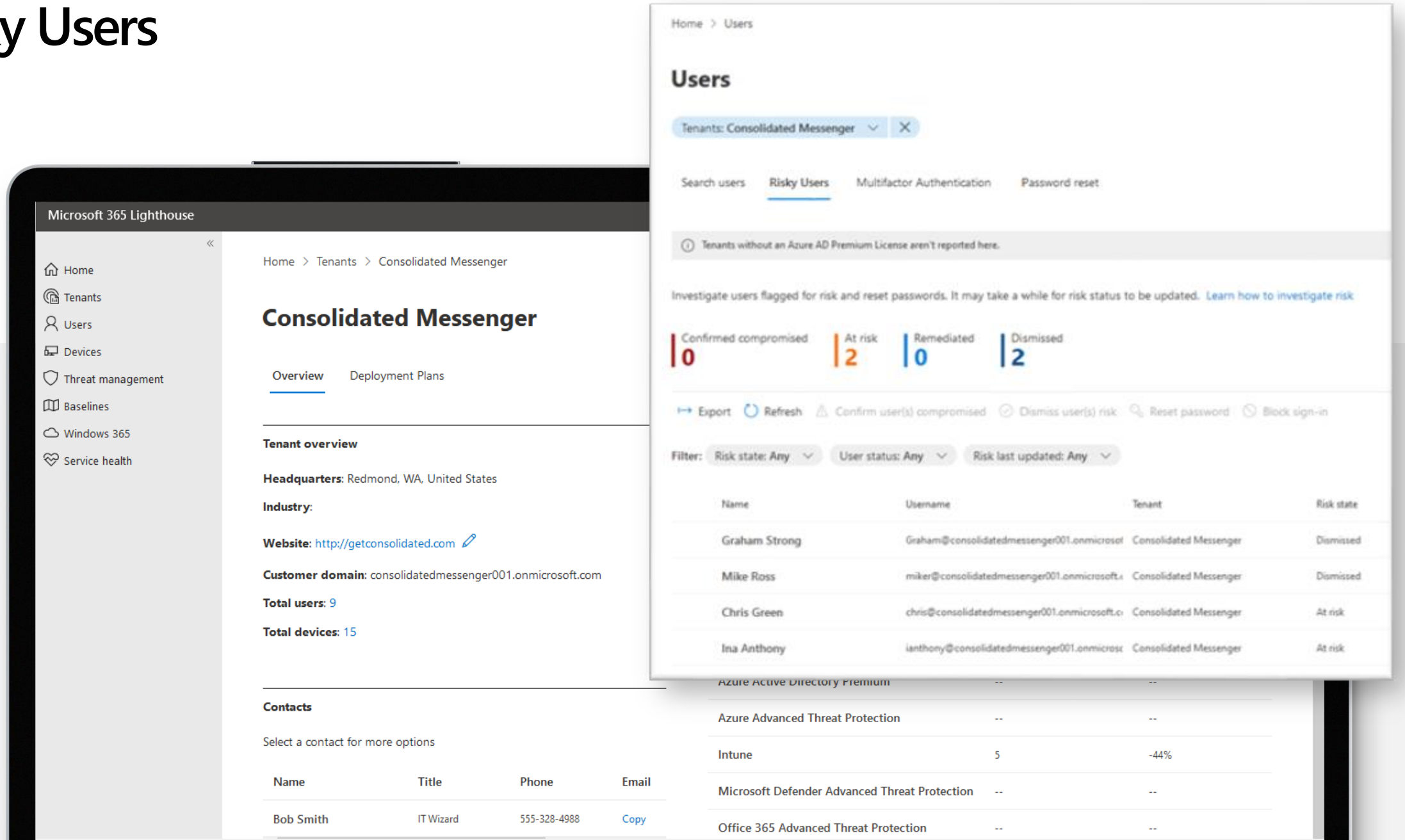
Update the Home Screen information to show only tenants with the selected tag



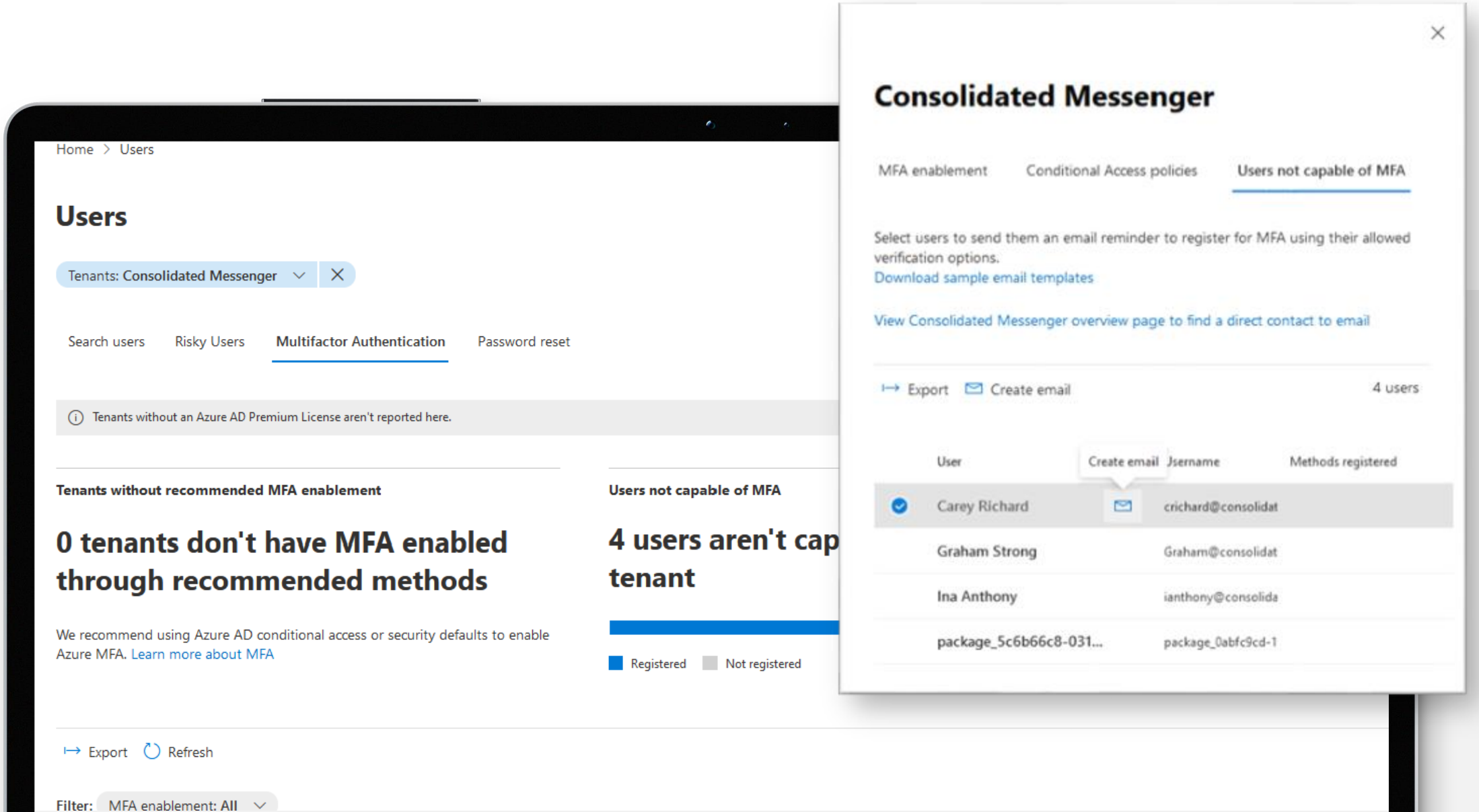
Filter Tenants by Tag



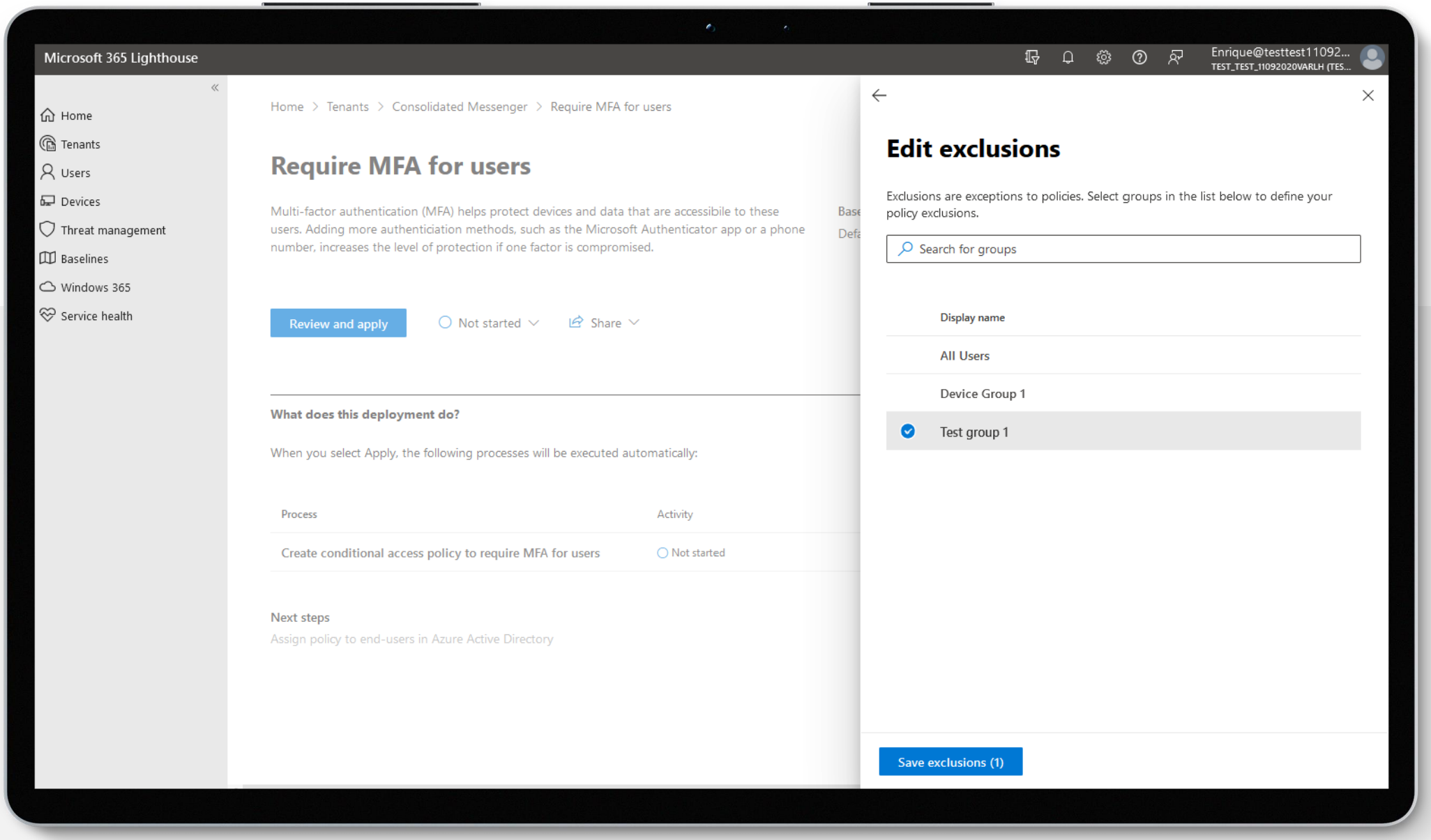
Risky Users


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
Consolidated Messenger
Dismissed
Mike Ross
Consolidated Messenger
Dismissed
Chris Green
Consolidated Messenger
At risk
Ina Anthony
Consolidated Messenger
At risk
Azure Active Directory Premium
Azure Advanced Threat Protection
Intune
5
-44%
Microsoft Defender Advanced Threat Protection
Office 365 Advanced Threat Protection

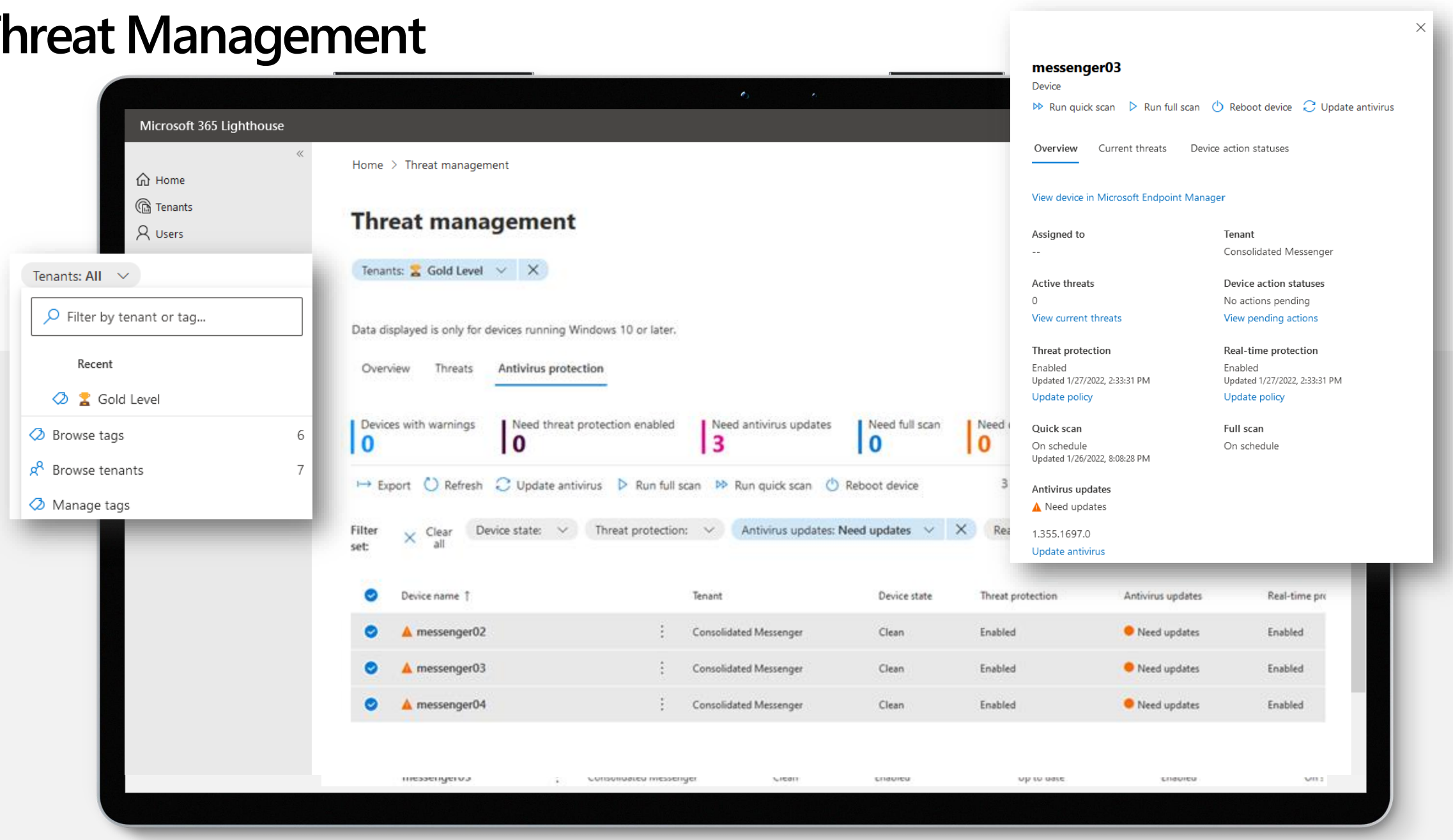
Multifactor Authentication



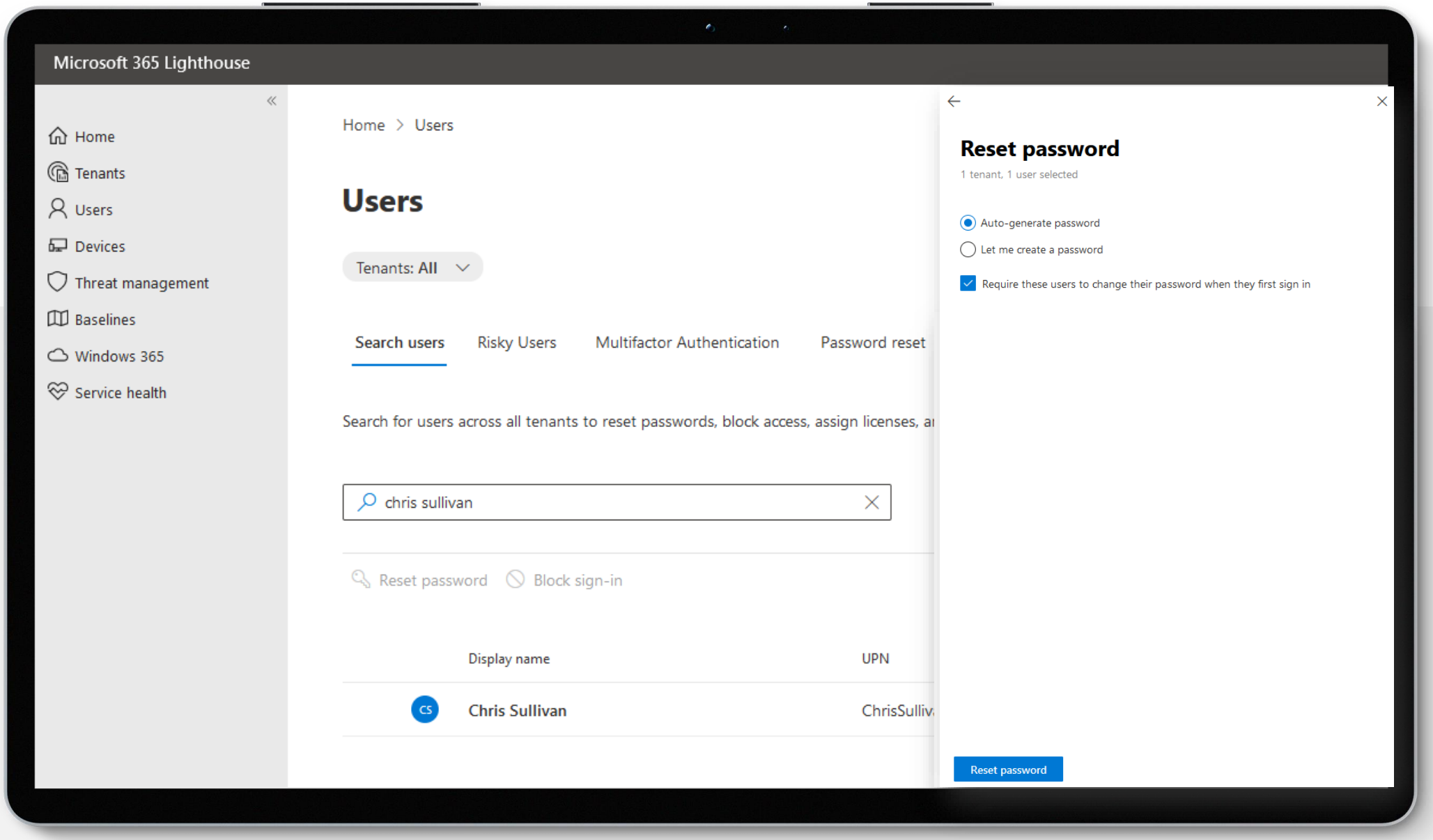
Manage MFA Exclusions



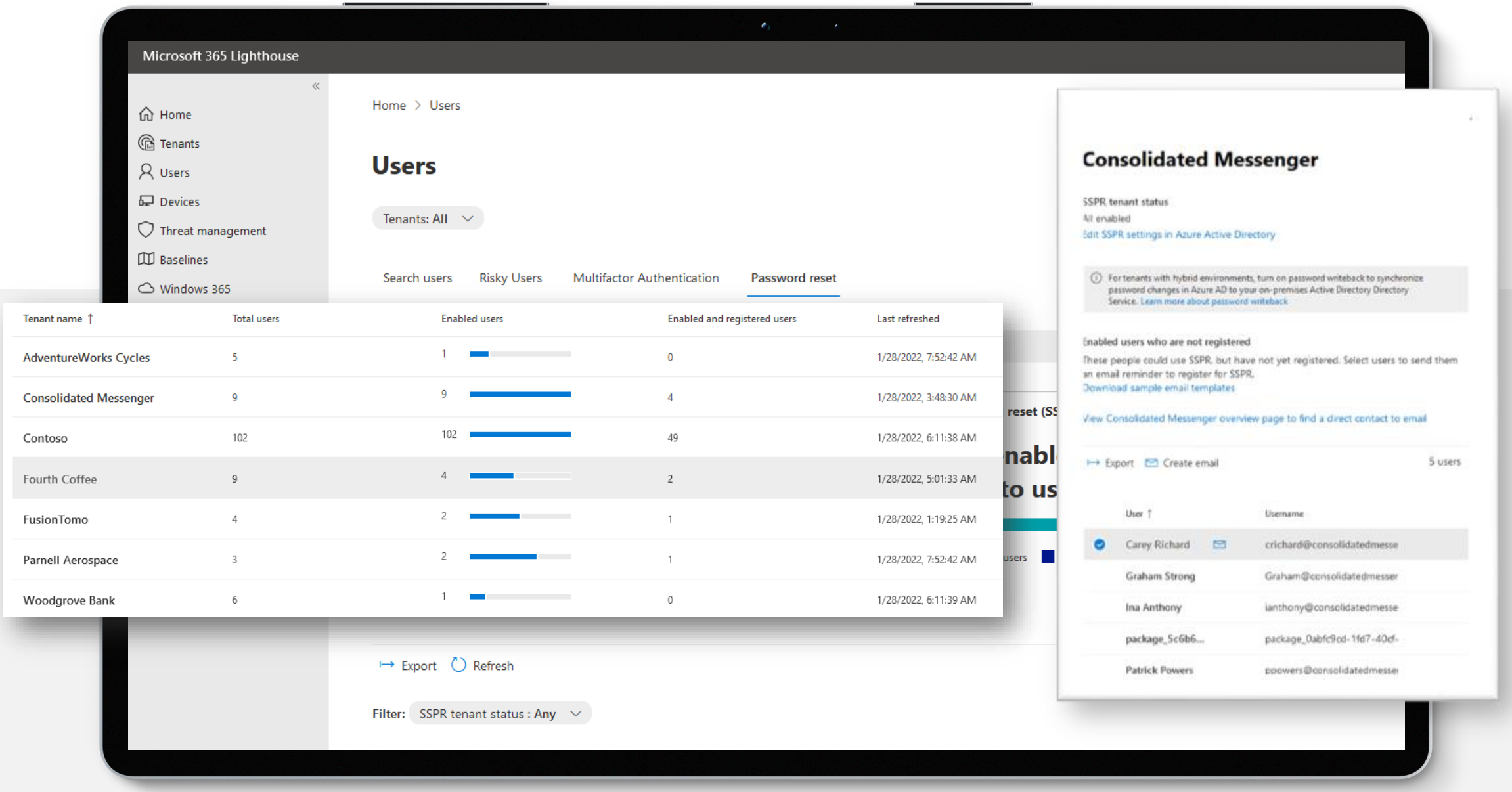
Threat Management



Password Reset

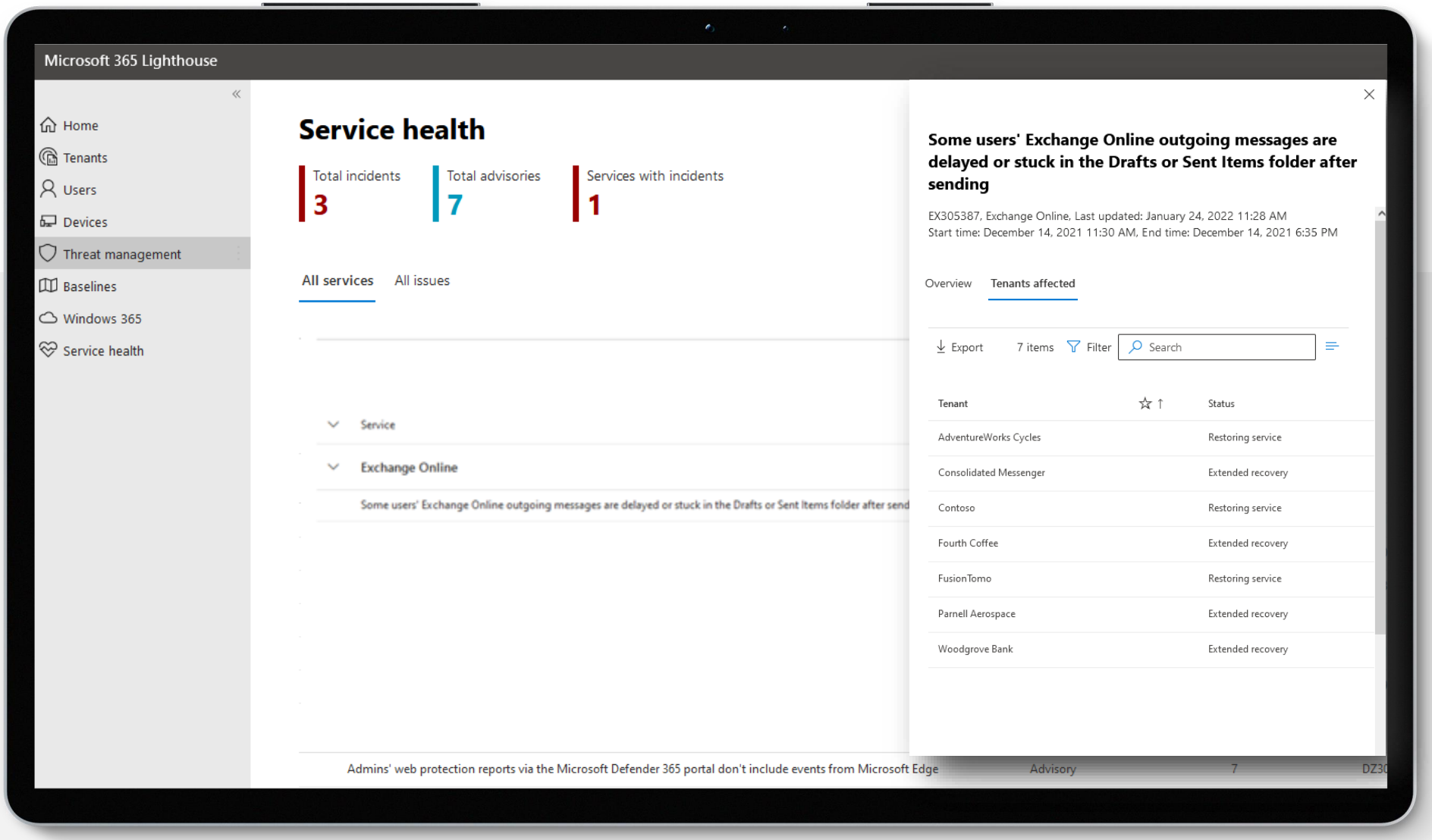


Self-Service Password Reset



Service Health & Status

[Check Microsoft 365 Service Health]



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.

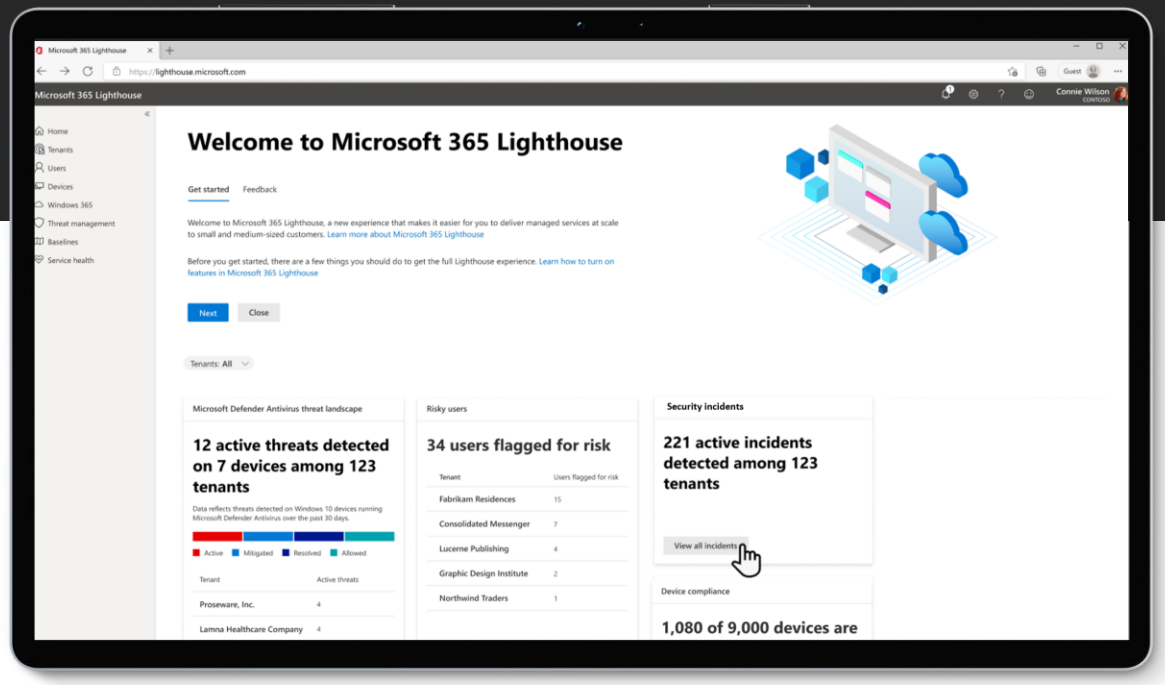


Image 1: Security incident summary on the Home dashboard

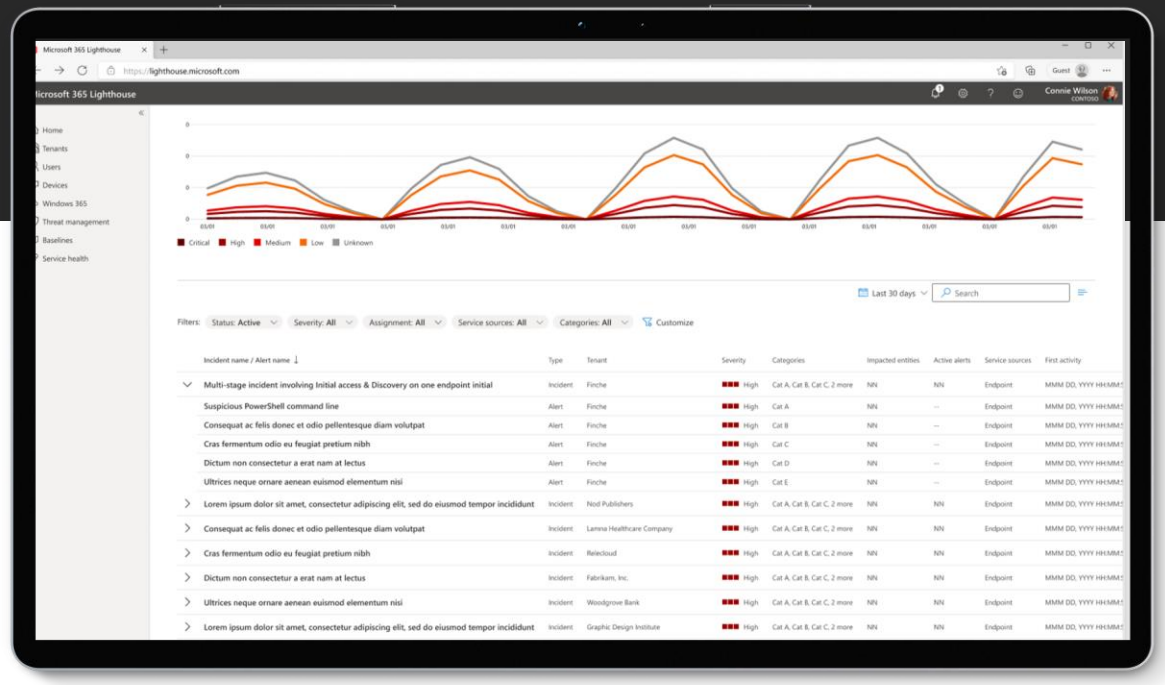


Image 2: Incident queue highlighting security incidents and alert details

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

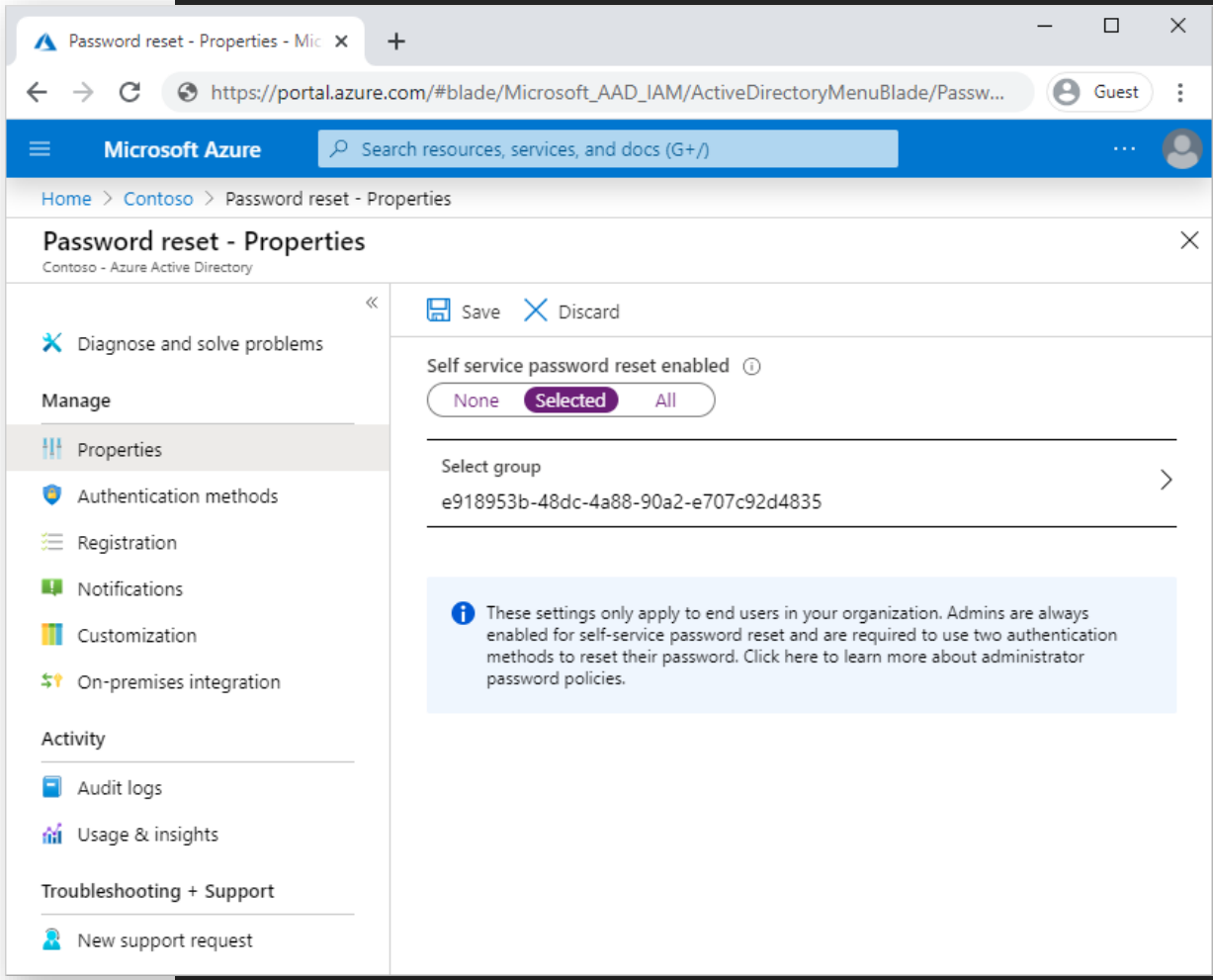
- Block Legacy Authentication
- Require MFA for admins
- Require MFA for all users
- Secure security info registration
- Block access by location (geo blocking)
- Require compliant devices

Self Service Password Reset

Enable Self Service Password Reset:

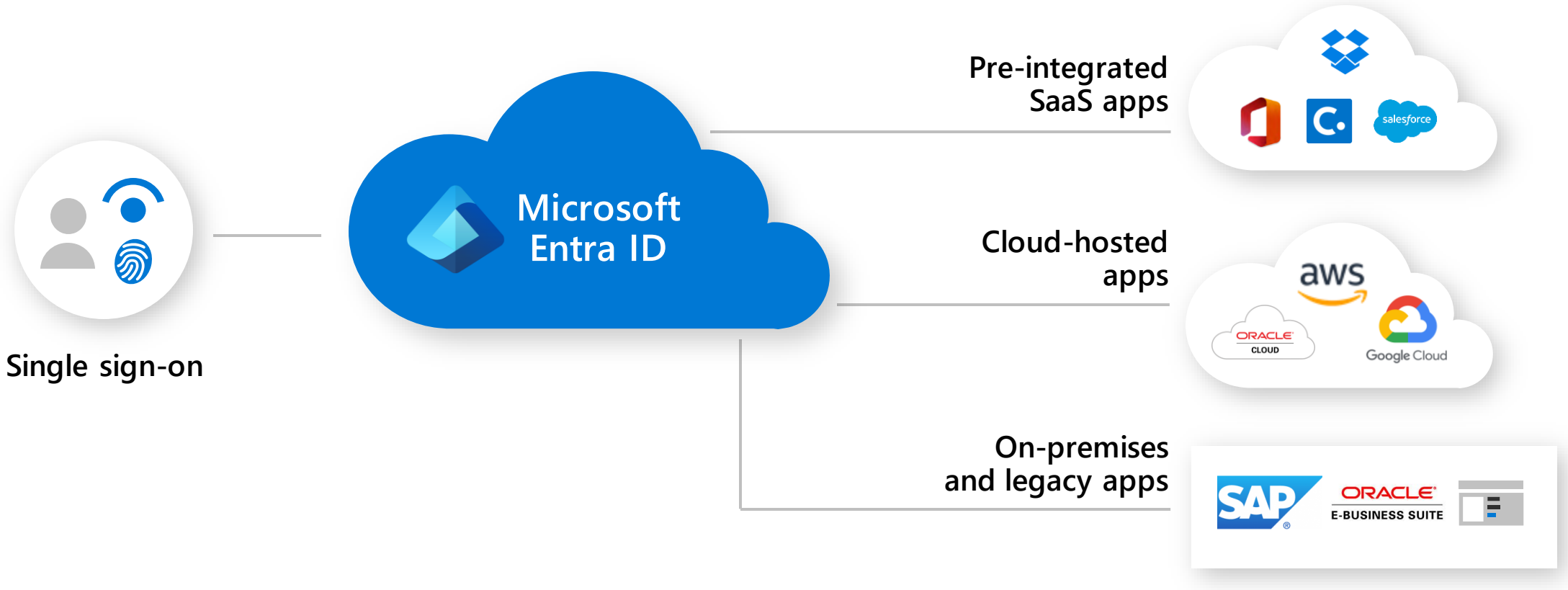
1. Sign into the Azure portal using an account with global administrator permissions.
2. Search for and select **Azure Active Directory**, then choose **Password reset** from the menu on the left-hand side.
3. From the Properties page, under the option Self service password reset enabled, choose **All**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

To learn more, see Enable Azure Active Directory self-service password reset - Microsoft Entra



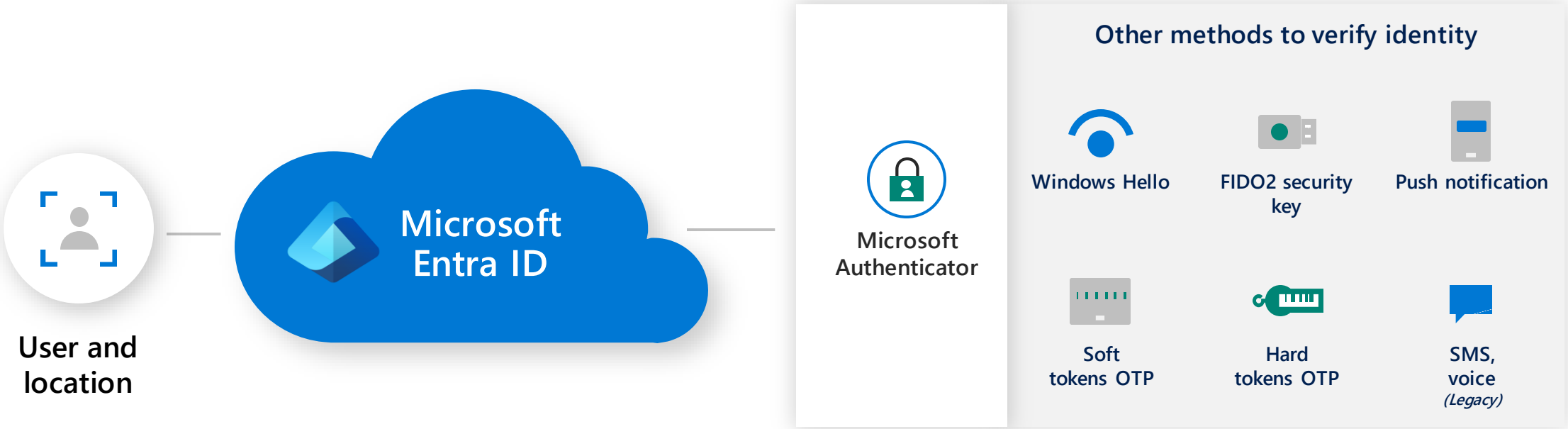
Securely access all apps using Single-Sign On

From cloud to on-premises apps



Enable MFA to keep remote employees protected

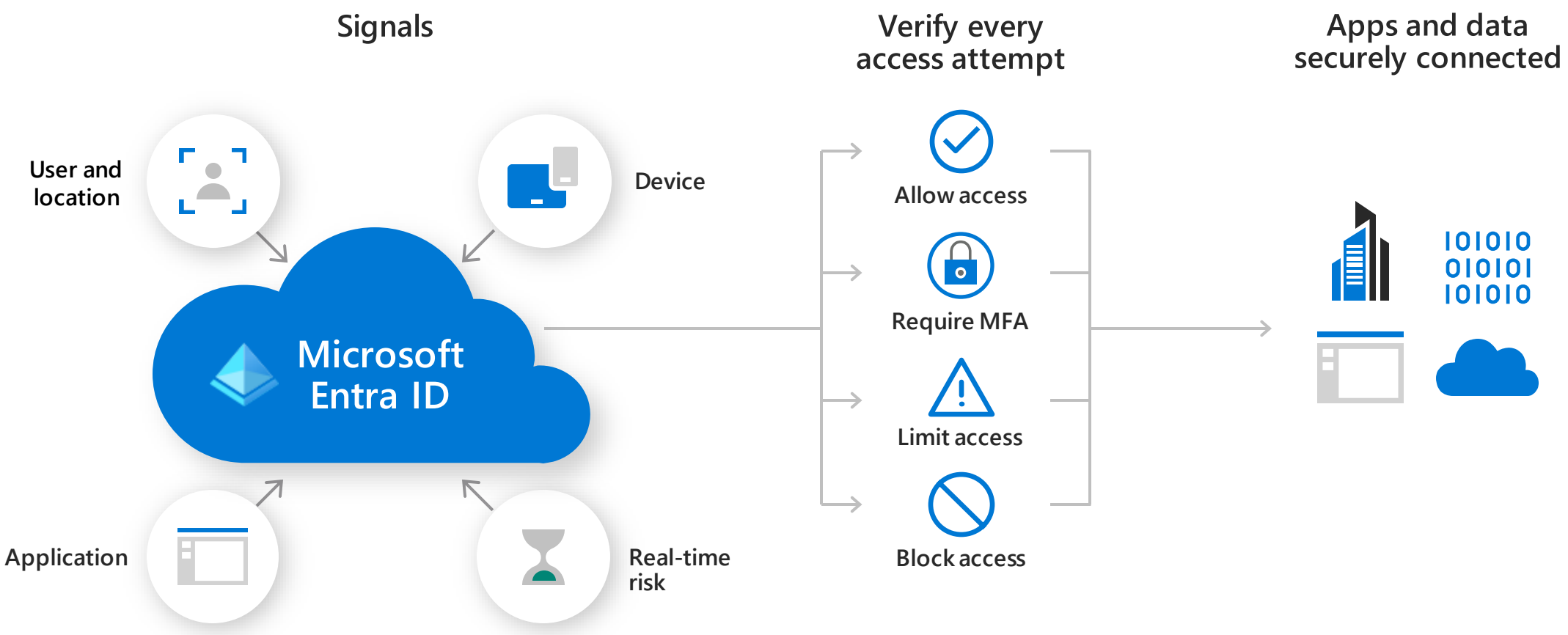
Verify user identities to establish trust



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

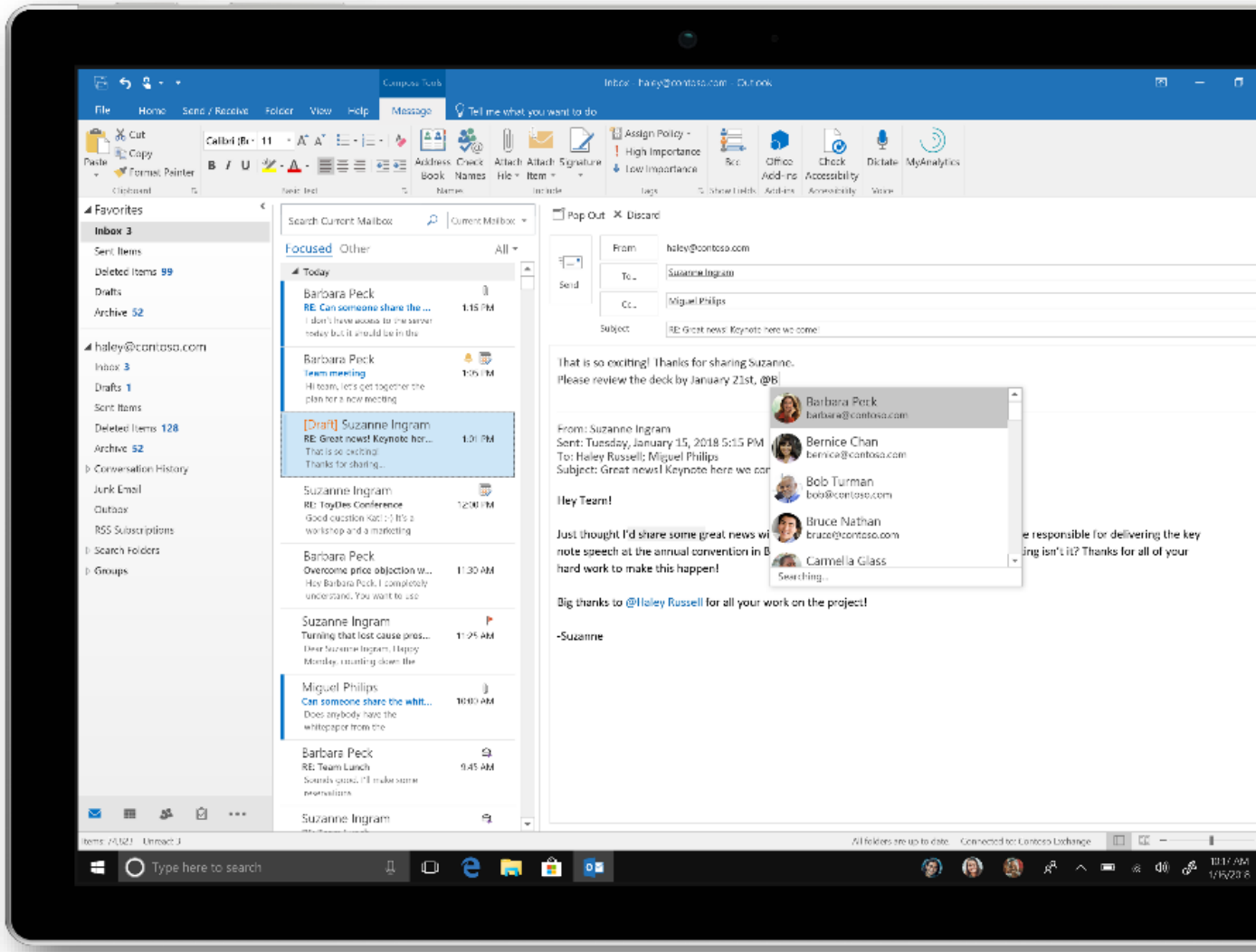
Set policies to **identify if email attachments are malicious**

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.

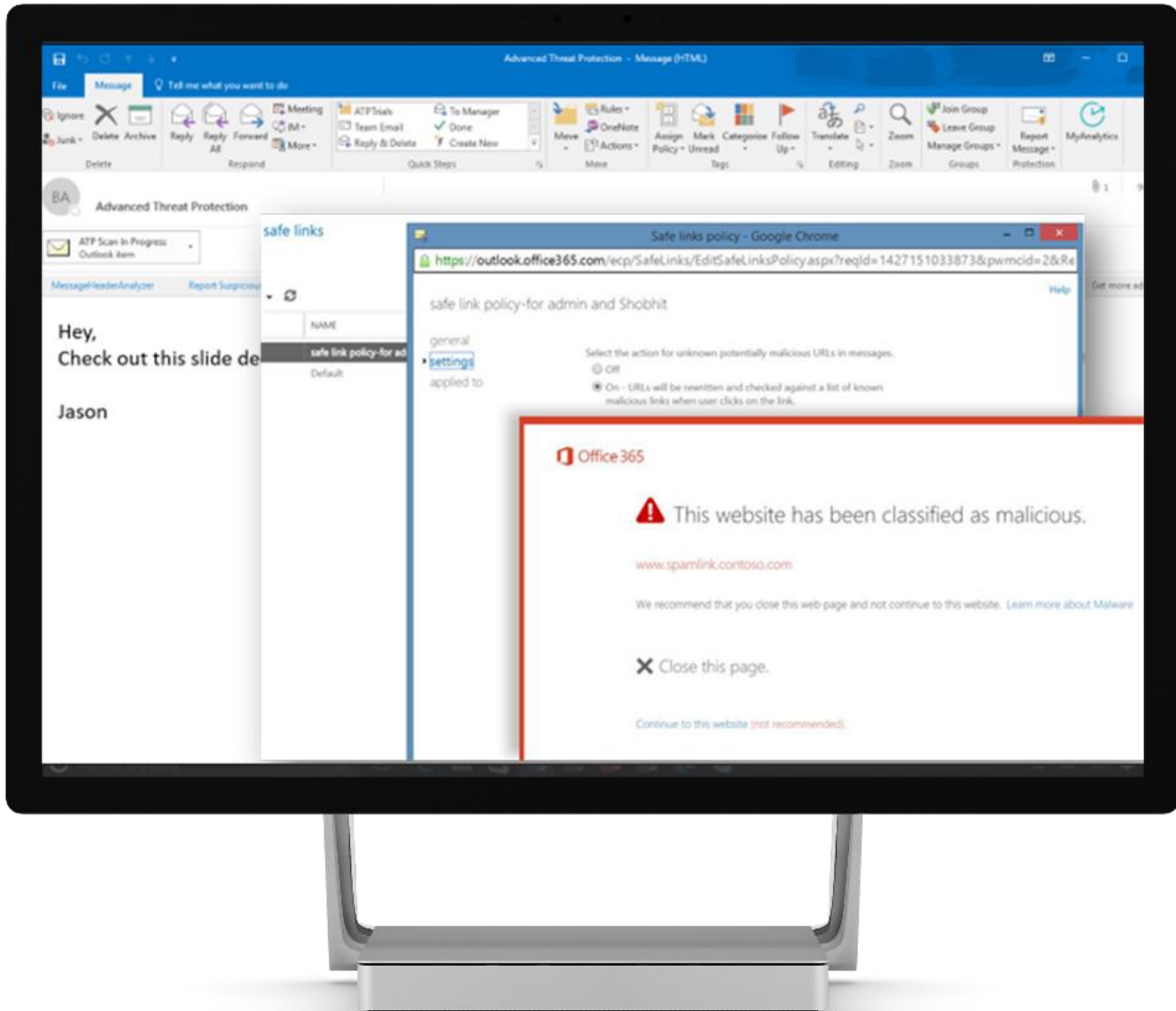


Safe Links & URL Detonation

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