



Modern Work transformation



Presenting at



NerdioCon

2025
PALM SPRINGS



Lior Bela

Director Business Growth - Microsoft



Matt Hache

Infrastructure Solutions Consultant - Pax8



Chris Plouffe

Senior Technical Trainer - Nerdio

Chris Plouffe

Senior Technical Trainer

- Started at Microsoft retail.
- Helped support the IEC in Redmond.
- Microsoft-funded Intune and W365 Workshops.
- I am a huge gamer/Star Wars nerd.
- I live in Seattle, Washington.



Two truths and a lie

Chris Plouffe

- I have changed tires in a NASCAR race.
- I have a 27-year-old daughter.
- I jumped out of aircrafts in the Army.



Agenda

What is Modern Work?

AD user management

Solution baselines

Enrollment strategies

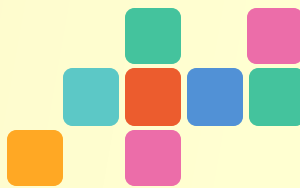
Intune

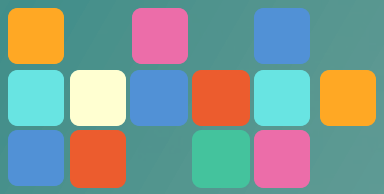
Group policy analytics

Policy baselines

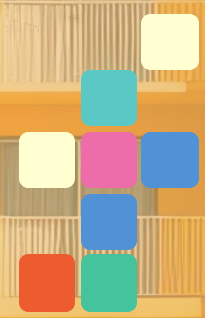
Security for Modern Work

Exchange Online management



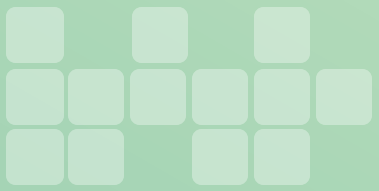


What is Modern Work?

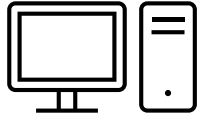


What is Modern Work?

Modern Work focuses on using technologies like **Microsoft 365** to **enhance** productivity, collaboration, and security for a **flexible** and **hybrid** workforce, enabling **seamless work from anywhere**.

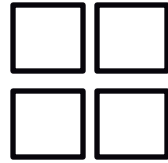


Why Modern Work matters for you



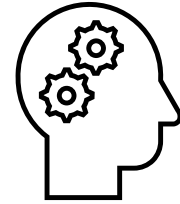
Virtual desktops

Not always wanted or needed



Distributed workforce

Existing tools don't offer
Modern Work management



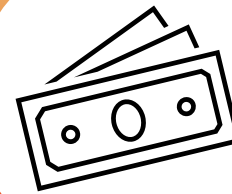
Diverse environments

Protecting access to customer
data and systems



Security is key

Managing Modern Work is vital
for a strong posture



Return on investment

MSPs miss out on full M365 value,
leaving money on the table

Windows 365

Also called CPC or “Cloud PC”

What is it?

- Under the hood, both AVD and Windows 365 leverage a similar set of Microsoft Cloud technologies.
- Technically, Windows 365 is built on top of existing AVD components but has a different transactional model.

Why use it?

- Easy management: all management through Intune.
- Ease of use: persistent desktops.
- Cost control: budget consistency & savings.
- Simplification: Microsoft manages infrastructure.

Windows 365

There are two versions

- Enterprise Cloud PCs are designed for organizations that have invested in Microsoft Intune and are using this powerful platform to manage their existing, physical Windows 10/11 desktops.
- Business Cloud PCs are designed for individual users and very small businesses who typically go to their local Best Buy when they need a new PC.

The main differences?

- Enterprise CPCs requires an Intune license for each
- Enterprise CPC require Entra or Hybrid joined (no Entra DS)
- Business CPCs does NOT require Intune license
- Business CPCs are natively Entra-joined w/no AD or Entra DS

In most cases MSPs use Enterprise*

What is Intune?



What is it?

- A set of technologies that securely manages identities, applications and devices (physical and virtual).

Why use it?

- Included in most M365 plans
- Augments RMM
- Helps to consolidate MSP tools

What are MSPs using Intune for?



Eliminating domain controllers

- Small businesses that have servers onsite may no longer need them.
- If you are no longer hosting any client/server applications, Intune can be a great replacement for a server.

Replacing Group Policy

- IT has been using GPO since the early 2000's.
- Intune has now surpassed most of what you can do using legacy GPOs with Intune Configuration Policies.

Implementing Zero Trust

- Enforce Zero Trust policies across your physical endpoint devices
- Set policies to never trust and always validate when accessing corporate data (conditional access policies).

Endpoint management

- Intune allows the MSP to offer RMM-like functionality out of the box.
- Manage desktops, laptops, Mac, Android, iOS devices in many ways, helping to augment existing tools.



The future of endpoint management

Lior Bela, Director, Microsoft Intune Growth



What we'll cover

Why here? Why now?
Why Microsoft?

Why cloud native?

The future





Lior Bela

Director Business Growth



Why here?

94% of SMBs consider cybersecurity critical to their business*

1 in 3 have already experienced a cyber attack.*

Top ranked challenges:

1

Confidential data
protection/managing work
data on personal devices

2

Phishing and
ransomware

3

Securing access for
remote workers

A single answer: Your solution, powered by Microsoft technology

*Source : aka.ms/SMBCybersecurityReport2024

Why now?

1

Artificial intelligence and machine learning:
Everyday, everywhere

2

Cybersecurity as strategic imperative

3

Remote work and hybrid models are
here to stay

4

Cloud computing and edge computing driving
agility and scalability



Jose Gomez Cueto
General Manager – Small and Medium Business
Microsoft, Redmond, Washington, United States



Why Microsoft?



Licenses for most

Microsoft 365 Business Premium

Microsoft 365 E3

Microsoft 365 E5

Microsoft 365 F1

Microsoft 365 F3

Enterprise Mobility + Security E3

Enterprise Mobility + Security E5



Truly cross-platform

macOS

- Automated Enrollment or BYOD
- Single sign-on
- Declarative device management (DDM)

Android

- Work profiles
- Remote actions
- Shared device mode (SDM)

iOS

- Zero-touch provisioning
- DDM, SDM



Partner-focused

License and Adoption Incentives

LevelUp Skilling Program

Digital marketing content on-demand

Community calls and forums

And much, much more

Why Microsoft + Nerdio?



Microsoft



nerdio

Why cloud native?



The end user



The company



The service provider

Why cloud native?



Zero trust security



Consolidated data for
analysis and insight



Building with agents
and Copilot

Why should you care?



Talent is expensive



IT is a 'commodity'
service

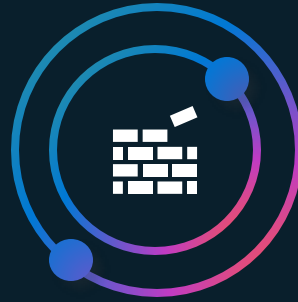


Margin is everything

What to do about it?



Get it all
in the cloud



Choose an integrated
stack



Build and package
unique value



Building with agents and Copilot



[As an MSP] you need to have new opportunities for all your employees, if we're doing the same every year, everybody's gone. If you still do the domain joined laptops, everybody's gone.

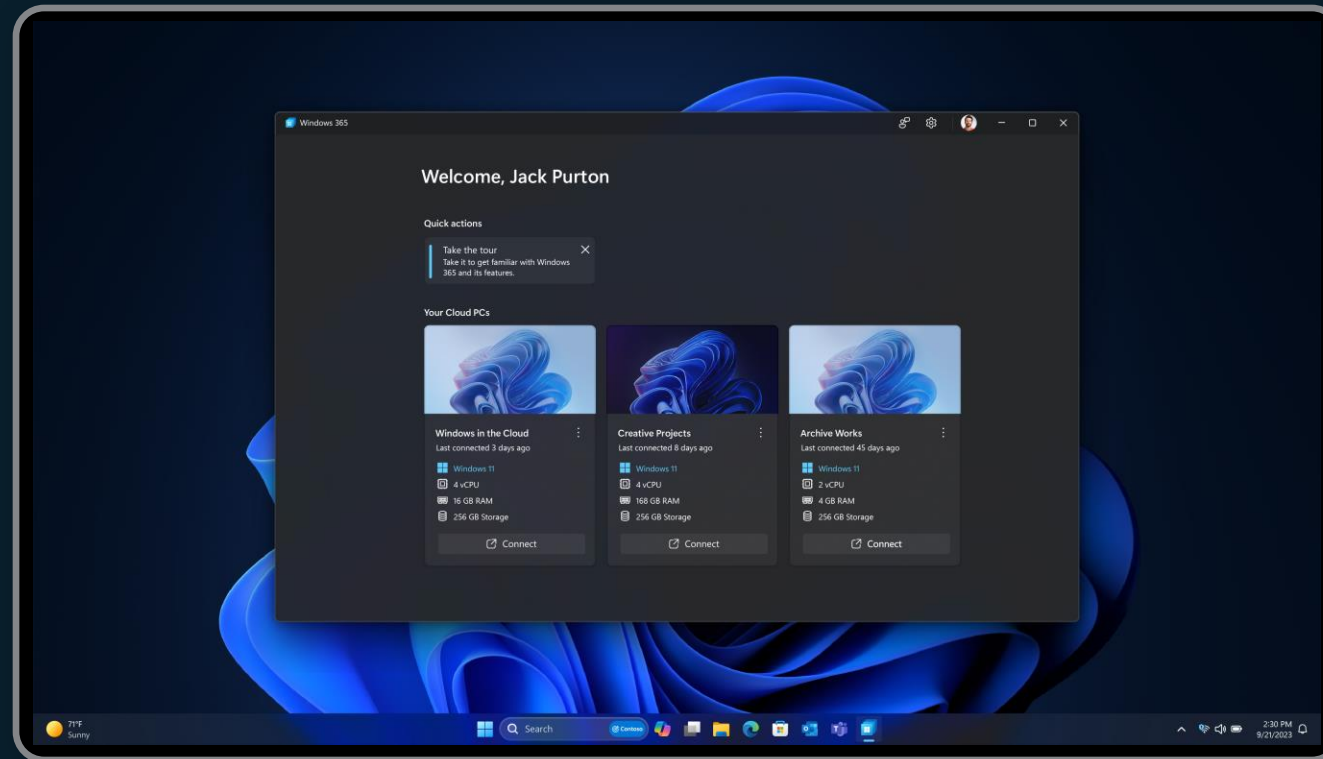
If you don't do Azure...if you don't do AI, everybody's gone.

Erik Loef

CTO & Owner PROXSYS*



Next-gen virtual devices





Next-gen virtual devices



We've added 350 end users to the solution which takes 20 minutes— a massive reduction from the four hours it took with our previous infrastructure.



Karin Niggli

Head of Workplace and Collaboration

Agents are the future

Agents vary in level of complexity and capabilities depending on your need

Simple



Retrieval

Retrieve information from grounding data, reason, summarize, and answer user questions.

Generally available



Task

Take actions when asked, automate workflows, and replace repetitive tasks for users.

Generally available



Autonomous

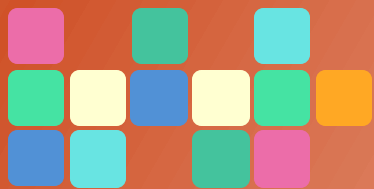
Operate independently, dynamically plan, orchestrate other agents, learn and escalate.

Preview

Advanced

Nerdio + Microsoft Intune Feedback Survey





How can Nerdio help?



Microsoft 365 & Modern Work

Modern Work (M365)



Entra ID & AD



**Intune &
endpoints**



Windows 365



Defender XDR



**Policies &
baselines**



**Microsoft 365
apps**



**Unified App
Management**



**OneDrive &
SharePoint**



**License
management**

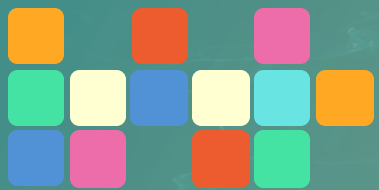


Nerdio Manager for MSP

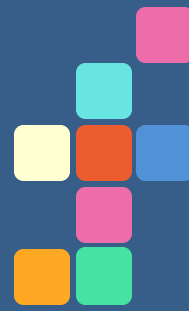
Modern Work capabilities

- Console Connect
- AD User Management
- SharePoint & OneDrive settings baselines
- Microsoft Defender for Endpoint
- Partner Center integration
- User onboarding/offboarding
- Intune management
- Entra ID settings baselines
- Risky & stale user reports
- Windows 365 management
- Templates for policy assignment to groups

- CIS Intune policies
- Vulnerability management
- Exchange Online settings baselines
- Microsoft Teams settings baselines
- Unified Application Management (UAM)
- Secure Score management
- Configuration drift management
- Microsoft Defender for Cloud
- Defender settings baselines
- Intune settings baselines
- Multi-tenant Microsoft management



AD user management



AD user management

Challenges



- Need a way to manage users across hybrid environments with on-premises Active Directory (AD) and Azure AD

Solution



- A unified, automated approach to hybrid AD and Azure AD user management

AD user management

Outcomes

- Reduce security risks.
- Simplify the management of hybrid user environments.
- Automate processes to speed up user management tasks.

The screenshot displays the Nerdio Manager for MSP-QA interface. On the left is a sidebar with navigation options: HOME, USERS (selected), GROUPS, DESKTOP IMAGES, AVD, INTUNE, POLICY MANAGEMENT..., APPLICATIONS, SERVERS, NETWORK, AZURE FILES, BACKUP, and RECOVERY SERVICE. The main panel shows the 'USERS' section with a search bar and a table of users. The table has columns for USER, MICROSOFT 365, DESKTOP/APP EXPERIENCE, GROUPS, ENTRA ID ROLES, and RISK STATE. Each user entry includes a 'Properties' button.

USER	MICROSOFT 365	DESKTOP/APP EXPERIENCE	GROUPS	ENTRA ID ROLES	RISK STATE
Sec19d917d7640e98b4b Sec19d917d7640e98b4b@nmm- -qa-man-act1.nerdio.net			All Users SG-248 SG-668-latest more...		
A-prdp-m365-none- test1 A-prdp-m365-none- test1@nmm-qa-man- act1.nerdio.net Last Sign In: Sep 22, 2023 05:43 AM			All Users SG-248 SG-668-latest more...		
AAA-M365- 1 AAA-M365- Test234567@nerdiofoxtrot.onm icrosoft.com			All Users SG-248 SG-668-latest more...		
aaaaaa1423 aaaaaa1423@nmm-qa-man- act1.nerdio.net			All Users SG-248 SG-668-latest more...		

AD user management

Notes



- There is no additional Nerdio cost to utilize AD user management, but Service Bus Relay Hybrid Connections do have an additional Azure cost

It depends on which App Services plan your Nerdio Manager installation utilizes.

Each domain controller connected to Nerdio Manager counts as a single connection.

App Service Plan	Hybrid Connection Limit
Basic (Nerdio Default)	5
Standard	25
Premium (v1-v3)	220
Isolated (v1-v2)	220

Lab 1

AD user management

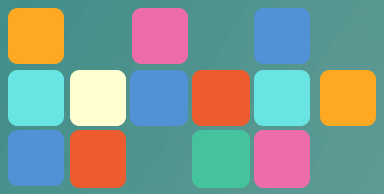
Walkthrough:

1 Create an AD user connection at the MSP level

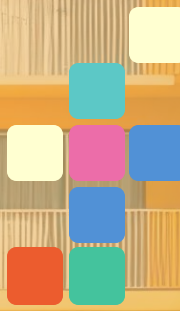
2 Install Hybrid Connection Manager (HCM)

3 Configure Hybrid Connection





Solution baselines



Tenant setting baselines

(Intune, Entra, Defender, OneDrive, SharePoint, Exchange Online, & Teams Online)

Challenges



- Management of identity and access across multiple clients is complex
- A way to ensure consistent security standards across all environments

Solution



- Standardized configurations across all client environments

Tenant Setting Baselines

(Intune, Entra, Defender, OneDrive, SharePoint, Exchange Online & Teams Online)

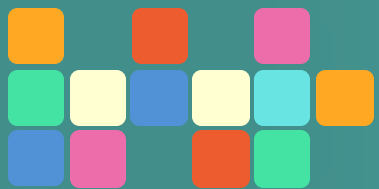
Outcomes

- Enforce consistent management across environments and simplify operations.
- Ensure configurations are evenly applied.
- Minimize misconfigurations.

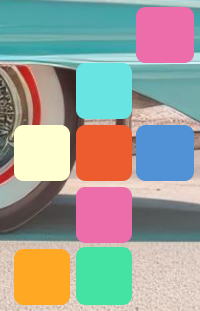
The screenshot displays the Nerdio Manager for MSP interface. The left sidebar contains a navigation menu with the following items: ACCOUNTS, NONCOMPLIANT ENDP..., PHYSICAL ENDPOINTS, NMM SCHEDULED TASKS, BACKUP DASHBOARD, AVD DASHBOARD, DEVICE DASHBOARD, WINDOWS UPDATES, GLOBAL IMAGES, APPLICATIONS, SCRIPTED ACTIONS, and CONSOLE CONNECT. The main content area is titled 'Solution baselines' and features a table of solution baselines. The table has columns for NAME, TYPE, CUSTOMER COMPLIANCE, ASSIGNMENTS, and LAST MODIFIED. The data rows are as follows:

NAME	TYPE	CUSTOMER COMPLIANCE	ASSIGNMENTS	LAST MODIFIED
Solution Baseline for Defender for Endpoint	DefenderForEndpoint (built-in)	100%	Nerdio Juliet (Report-only) Winhart Inc (Report-only)	Sep 3, 2024 02:03 PM
Solution Baseline for Defender for Office 365	DefenderForO365 (built-in)	100%	Nerdio Juliet (Report-only) Winhart Inc (Report-only)	Oct 15, 2024 08:39 PM
Solution Baseline for Entra ID	EntraId (built-in)	100%	Nerdio Juliet (Report-only) Winhart Inc (Enforced)	Oct 15, 2024 07:41 PM
Solution Baseline for Entra ID - CMMC Disabled	EntraId (cloned)	0%		Oct 28, 2024 02:22 PM
Solution Baseline for Intune	Intune (built-in)	100%	Nerdio Juliet (Enforced) Winhart Inc (Report-only)	Oct 30, 2024 11:26 AM

At the bottom of the table, it indicates '5 items'.



Configuration drift management



Configuration drift management

Challenges

- Inconsistent configurations create security gaps and non-compliance with standards.
- Tracking and correcting discrepancies manually is time-consuming and inefficient.

Solution

- The ability to monitor and correct discrepancies from defined configurations to maintain consistency across environments.

Configuration drift management

Outcomes

- Consistent configurations improve security and help meet compliance standards.
- Automation saves time and effort, fostering client confidence through reliable management.

ACCEPT DRIFT FOR BASELINE POLICY

BASELINE: ZTest-PRDP1

POLICY: test-app-config-prdp2

ACCOUNT: Nube Hart, Inc. (1)

Drift acceptance expires after

90 days ▼

Dec 24, 2024

Description

By customer request, see #73956 for details.

☐ Allow processing ⓘ

Cancel

Accept

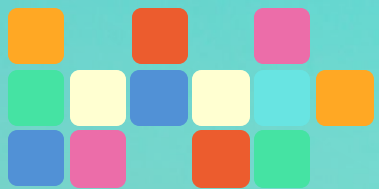
Lab 2

Solutions baselines

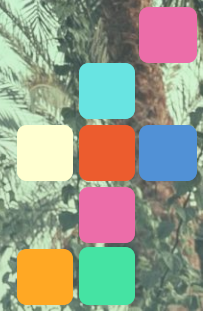
Walkthrough:

- 1 View/configure a few baselines
- 2 Assign accounts to a baseline
- 3 View status of baselines & drift



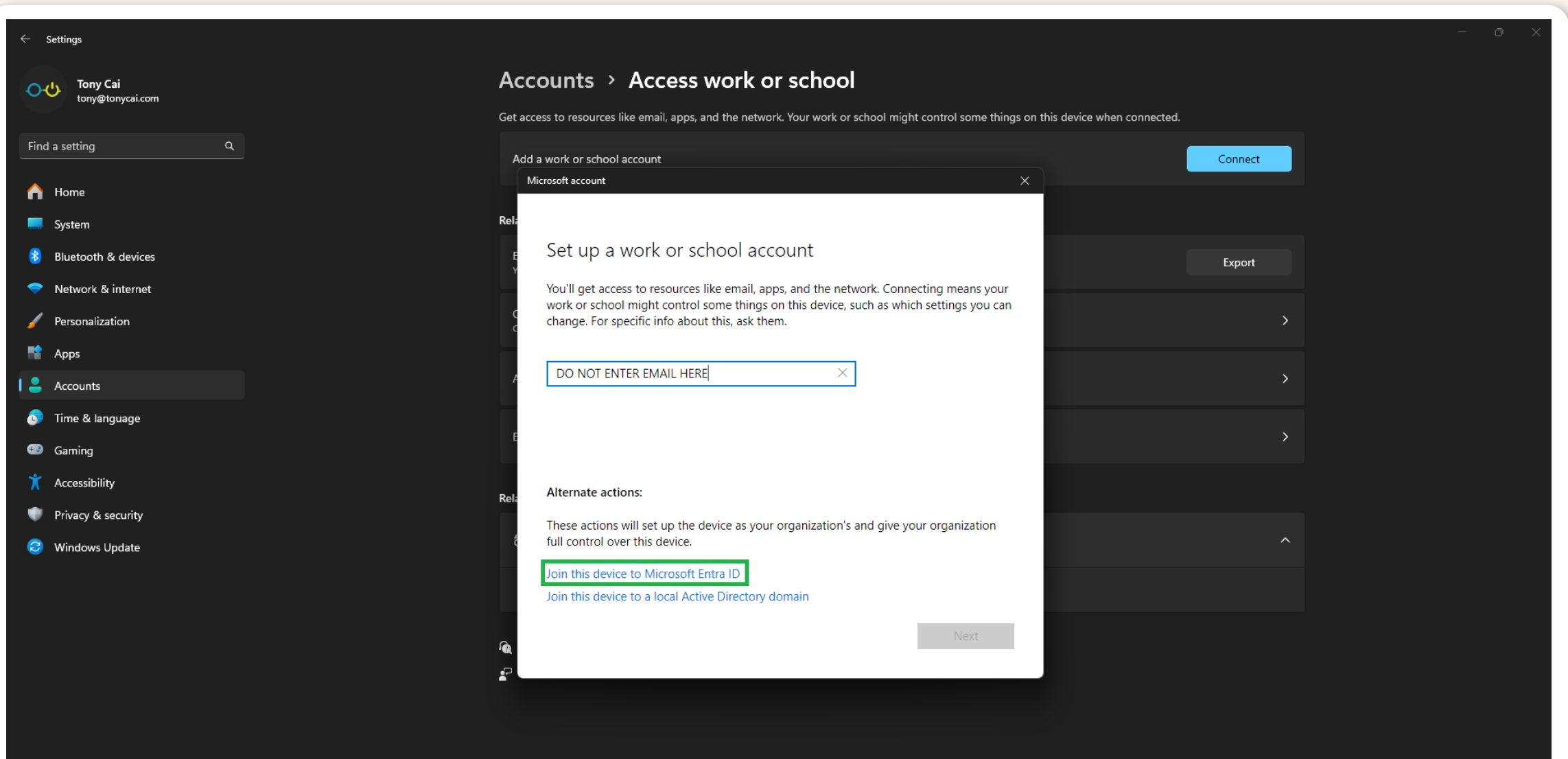


Device enrollment strategies



How to:

Enroll a Windows Device (via End User Enrollment)



How to:

Enroll a Windows Device (via USB or Network)

Windows Configuration Designer

File About

Start page

Windows ICD makes it easy to build and flash a Windows image, create provisioning packages, or set up devices to use within your organization. To get started, choose Create or open a Recent project.

Create

Provision desktop devices

Configure common settings for Windows desktop devices

Provision HoloLens devices

Configure common settings for HoloLens devices

Provision kiosk devices

Configure common settings for a device that will run a single app in kiosk mode

Provision Windows mobile devices

Configure common settings for Windows mobile devices

Provision Surface Hub devices

Configure common settings for Surface Hub devices

Advanced provisioning

Recent projects

Open

New project

Enter project details

Name:

Mass Deploy Intune

Project folder:


C:\Users\tony\OneDrive\Documents\Windows Imaging and Configuration Designer (WICD)\Mas

Browse...

Description:

Deploy Intune at Scale

Finish



Windows Configuration Designer

Microsoft Corporation

Open

4.2 ★

Average

77

Ratings

How to:

Enroll a Windows Device (via USB or Network)

Windows Configuration Designer

FileAbout

Start pageNerdio Mass Enrollment

Steps

Set up device

Set up network

Account Management

Add applications

Add certificates

Finish

Summary

Set up device

Share devices

Remove pre-installed software

Enter device name

Yes

Yes

Nerdio-SurfacePro-%SERIAL%

Network settings

Network SSID

Network type

Password

Corporate-Wifi

WPA2-Personal

Account Management

Bulk Token Expiry Date

Local admin user name

Local admin user password

"2024-08-18T21:22:06.830Z"

localadmin

Add applications

Add certificates

Protect your package

Protect the contents of your package by specifying a password. The password length must be 8-16 characters.

Yes

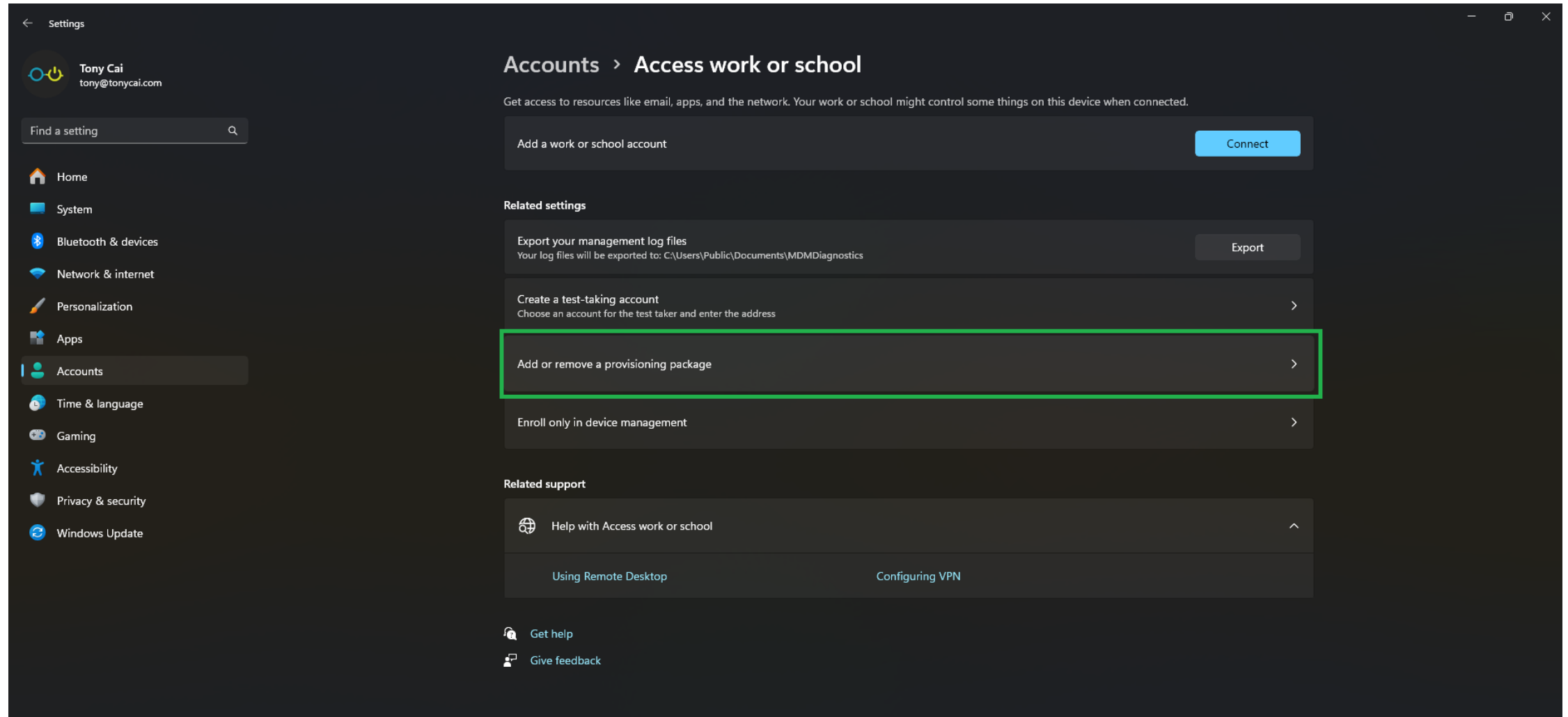
Password:

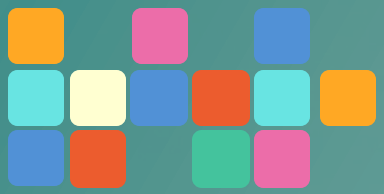
You are ready to create the package!

Create

How to:

Enroll a Windows Device (via USB or Network)

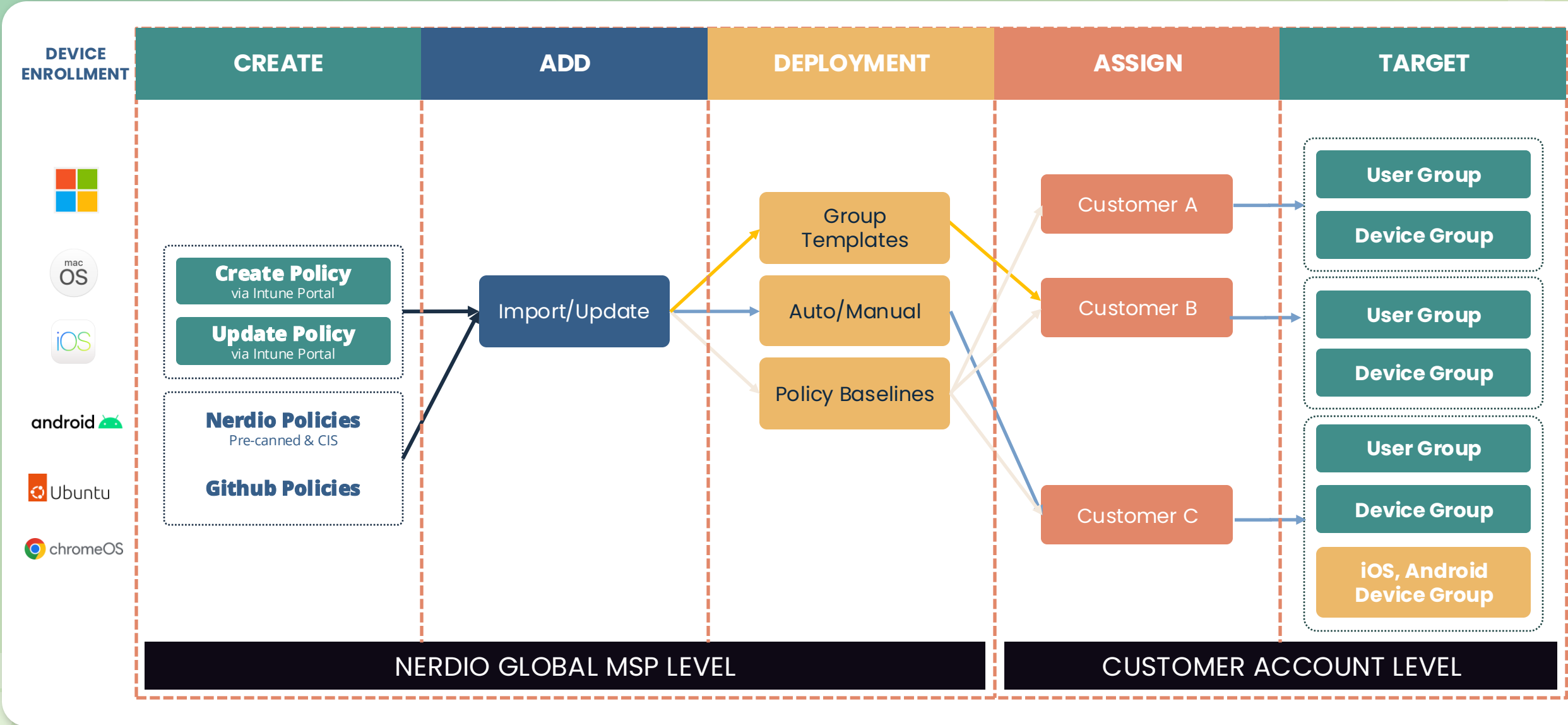




Intune policy management



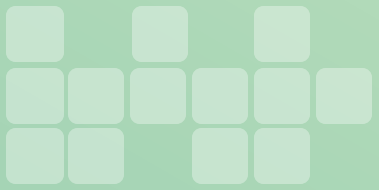
Intune policy creation/update flow



Microsoft Intune

Why use it?

- Extend your management beyond AVD.
- Create policies to automate common functions.
- Modify policies and track changes with the changelog.
- Quickly revert to previous policy versions.
- Identify resources that are non-compliant.
- Monitor and manage policy drift.



Variables in Nerdio for policies

Secure variables

- Created at the global / MSP level or the customer level.
- Stored in the key vault. Only available for scripted actions (NO Intune policies).
- Cannot be shared between accounts or levels.

Inherited variables

- Created at the global / MSP level.
- Are inherited by customer accounts.
- Allow you to centrally manage common scripts and Intune policies.
- Can be overridden at the customer account level.



Intune + Nerdio core features

Changelog

Track changes between versions with a centralized log.

Status

A simple visual indicator to identify accounts with non-compliant endpoint(s).

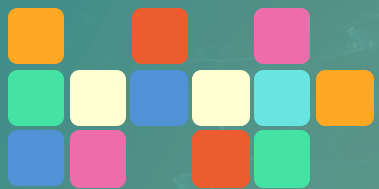
- Use in tandem with the account-level view to find the endpoint(s).

Versions

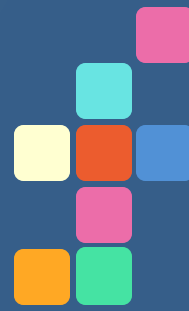
Policy versions can be rolled back in Nerdio.

- This feature is unavailable in native Intune.





Granular policy assignment & management



Granular policy assignment & management

Challenges



- Applying broad policies across client environments can lead to overprotection in some areas and under protection in others.

Solution



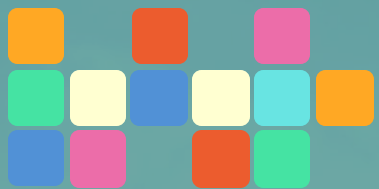
- The ability to apply specific settings to targeted users, groups, or devices

Granular policy assignment & management

Outcomes

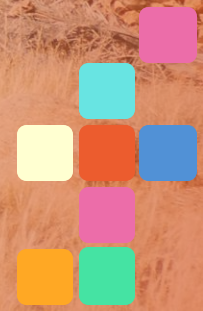
- Tailored policy management to meet specific client needs.
- More efficient operations through precise control over policies.

ASSIGNMENTS - NMM AUTO SUBSCRIBE FOR REMOTE DESKTOP & AVD			
CUSTOMER ACCOUNT	SYNC TYPE ⓘ	DIRECT ASSIGN	DEVICE FILTER
(7) Ganar Hart, Inc.	<input type="radio"/> Manual <input checked="" type="radio"/> Automatic	All Devices X X v	<input type="checkbox"/> Exclude Windows 10/11 Enterprise multi-session v
(1) Nube Hart, Inc.	<input type="radio"/> Manual <input checked="" type="radio"/> Automatic	All Devices X X v	<input type="checkbox"/> Exclude Windows 10/11 Enterprise multi-session v
2 Items			



★ *NerdioCon* ★
2025
PALM SPRINGS

Group templates



Group templates

Challenges



- Manually assigning policies to groups of users or devices can be time-consuming and prone to errors, especially in larger environments.

Solution



- Pre-built templates for group policy assignments.

Group templates

Outcomes



- Policy assignments become faster and more efficient.
- Policies are applied consistently and reliably.
- MSPs reduce their administrative workload.

CREATE GROUP TEMPLATE

General

Name Template

NAME Windows Corporate Devices

MEMBERSHIP TYPE Dynamic Device ▼

DYNAMIC RULE [New](#)

And/Or	Property	Operator
<input type="text" value=""/>	<input type="text" value="deviceO..."/>	<input type="text" value="Equals"/>
<input type="text" value="And"/>	<input type="text" value="deviceO..."/>	<input type="text" value="Starts ..."/>

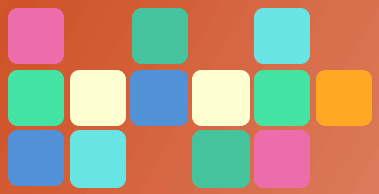
[Add expression](#)

Lab 3

Intune walkthrough

- 1 Creating policies
- 2 Importing policies to Nerdio
- 3 Editing policies in Nerdio
- 4 Assigning policies to accounts
- 5 Assigning policies to endpoints





Group Policy analytics



Group Policy analytics

Challenges

- Keeping up to date with current on-premises GPOs
- Understanding what cloud-based MDM providers support
- Manually configuring new GPOs into cloud (no visibility)

Solution

- Use Group Policy analytics to import or analyze existing on-premises GPOs

Group Policy analytics

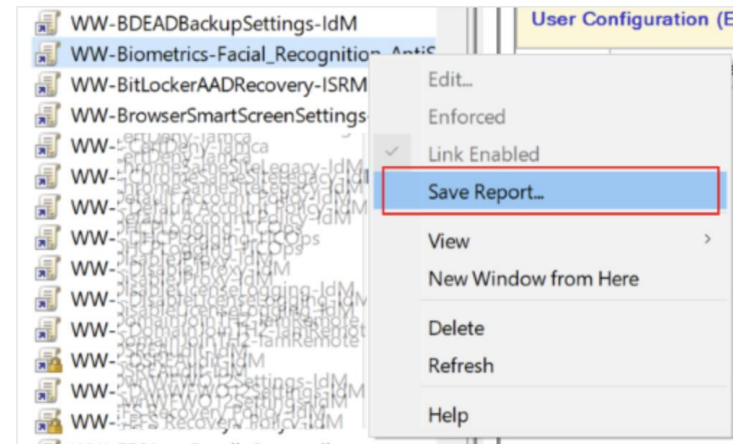
Outcomes

- Imports and analyzes on-premises GPOs
- Shows settings that Intune supports
- Shows deprecated settings

Export a GPO as an XML file

The following steps can be different on your server, depending on the GPMC version you're using. When you export the GPO, make sure you export as an XML file.

1. On your on-premises computer, open the **Group Policy Management** console (GPMC.msc).
2. In the management console, expand your **domain name**.
3. Expand **Group Policy Objects** to see all the available GPOs.
4. Right-click the GPO you want to migrate and choose **Save report**:



5. Select an easily accessible folder for your export. In **Save as type**, select **XML File**. In another step, you add this file to group policy analytics in Intune.

Make sure that the file is less than 4 MB and has a proper Unicode encoding. If the exported file is greater than 4 MB, then reduce the number of settings in the group policy object.

Group Policy analytics

Outcomes



- Imports and analyzes on-premises GPOs
- Shows settings that Intune supports
- Shows deprecated settings

- 1** Sign in to the Intune admin center as Intune admin or with a role that has “Security baselines” and “Device Configuration” permissions.
 - 2** Select **Import**, select your saved XML > **Next** (can select multiple)
 - 3** You can use **Scope tags**, by select an existing or using default
 - 4** Select **Next > Create**
-

After analysis runs, the GPO you imported lists some good info. MDM support: shows the percentage of group policy settings in the

GPO that have the same setting in Intune.

Yes: means there’s a matching setting available in Intune

No: means there isn’t a matching setting

Group Policy analytics

Outcomes



- Summary of GPO and policy statuses
- Shows the # of settings in your GPO that can be used in device configuration profile

- 1 In the Intune admin center, select **Reports > Device management > Group policy analytics**
- 2 In the **Summary** tab, a summary of the GPO and its policies are shown. Use this information to determine the status of the policies.
 - Ready for migration: policy has a matching setting
 - Not supported: policy doesn't have a matching setting
 - Deprecated: policy can apply to older versions or not used
- 3 Select **Reports** tab > **Group policy migration readiness**
 - You can use report to see the number of settings in your GPO that can be configured in a device configuration profile.
 - It also shows if the settings can be in a custom profile, aren't support or are deprecated.

Group Policy analytics

Outcomes

- It is best effort per Microsoft
- Some don't migrate exactly and could work better in other tools (Endpoint Security)
- Conflicting settings are detected early

1 In the Intune admin center, select **Devices > Manage devices > Group policy analytics**

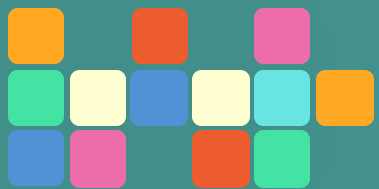
2 Next to the GPO you want in your Settings Catalog profile, select the **Migrate** checkbox. You can select one or many.

Migrate ↑↓	Group policy name ↑↓	Active Directory Ta... ↑↓	MDM Support ↑↓	Unknown Settings ↑↓	Targeted in AD ↑↓
<input checked="" type="checkbox"/>	SAS-SDW-Client-Baseline	SAS-SDW-Client-Baseline	⚠ 81%	View	No

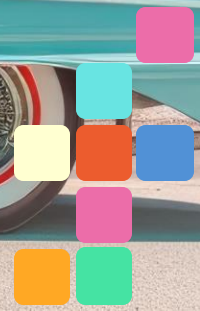
3 In the **Settings to migrate** tab, select **Migrate** column for the settings you want to include in your Settings Catalog profile. You can use the built-in features or select as needed.

4 In the **Configuration** tab, your settings and their values are shown.

5 Name your profile, add any **Scope tags, Assignments**, click **Next**.



Policy baselines



Policy baselines

What is a policy baseline?

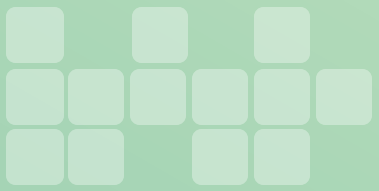
- A group of policies you can use to make initial deployment consistent across all your customer accounts.

Building your baseline

- Use Nerdio's pre-defined policies or your own custom policies.

Versions

- If multiple baselines are assigned, prioritize the order they apply.



Policy baselines

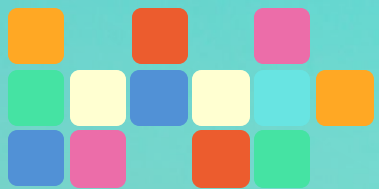
Enforced policy baselines

- Assigned to customer accounts.
- Synced and enforced if the sync type is set to auto.
- Enforced policies with a manual sync type can be published on an as-needed basis.

Report-only policy baselines

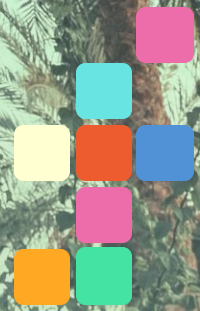
- Track configuration drift.
- Simplifies identifying customer endpoints that differ from the baseline status.
- Operate on an always-on, ongoing basis.





CIS-compliant templates

(Center for Internet Security)



Why did we partner with CIS?

- CIS is highly respected globally when it comes to defining security
- Funded by the U.S. Dept of Homeland Security and CISA to protect Federal, State, Tribal Territory interests
- CIS sets the rules (Benchmarks)
- Compliance frameworks align to Benchmarks
- Help our customers reduce attack surface and achieve compliance in an easy manner



Problems MSP admins encounter

- Told by leadership, they need to secure IT stack and meet X, Y, Z compliance.
- Not knowing where to begin, best practices that should be followed. ENTER CIS Benchmarks.
- CIS Benchmarks for Windows 11/Server OS has 1300+ pages of settings they need to sift through, determine which are appropriate, and then executing them takes a long time.
- Do it yourself approach leads to mistakes, hard to maintain, requires Ansible, Chef, IaC knowledge



CIS Baselines

Challenges

- Staying compliant is time-consuming.
- It can be difficult to apply security settings uniformly across clients.
- Limited resources make CIS policy management challenging.

Solution

- Use pre-configured templates that align with CIS standards and automatic updates that keep policies CIS-compliant.

CIS Baselines

Outcomes

- Pre-configured for easy CIS-compliant deployment.
- Ensure consistency and reduce manual effort with centralized control.
- Keep policies CIS-compliant with automatic updates.

Mappings ^

IG1 ▾

IG2 ▾

IG3 ▾

<input type="checkbox"/> Australian Signals Directorate's 'Essential Eight' See details	<input type="checkbox"/> Azure Security Benchmark v3 See details	<input type="checkbox"/> CISA Cross-Sector Cybersecurity Performance Goals See details
<input type="checkbox"/> CISA Cybersecurity Performance Goals See details	<input type="checkbox"/> CMMC v2.0 See details	<input type="checkbox"/> Criminal Justice Information Services (CJIS) Security Policy See details
<input type="checkbox"/> CSA Cloud Controls Matrix v4 See details	<input type="checkbox"/> Cyber Risk Institute (CRI) Profile v1.2 See details	<input type="checkbox"/> Federal Financial Institutions Examination Council (FFIEC-CAT) See details
<input type="checkbox"/> GSMA FS.31 Baseline Security Controls v2.0 See details	<input type="checkbox"/> Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals See details	<input type="checkbox"/> HIPAA See details
<input type="checkbox"/> ISACA COBIT 19 See details	<input type="checkbox"/> ISO/IEC 27001:2022 & 27002:2022 Information Security Controls See details	<input type="checkbox"/> MITRE Enterprise ATT&CK v8.2 See details
<input type="checkbox"/> New Zealand Information Security Manual v3.5 See details	<input type="checkbox"/> NIST CSF 1.0 See details	<input type="checkbox"/> NIST CSF 2.0 See details
<input type="checkbox"/> NIST SP 800-171 See details	<input type="checkbox"/> NIST SP 800-53 Revision 5 Low Baseline See details	<input type="checkbox"/> NIST SP 800-53 Revision 5 Moderate Baseline See details
<input type="checkbox"/> North American Electric Reliability Corporation-Critical Infrastructure Protection Standards (NERC-CIP Standards) See details	<input type="checkbox"/> NYDFS Part 500 See details	<input type="checkbox"/> PCI v3.2.1 See details
<input type="checkbox"/> PCI v4.0 See details	<input type="checkbox"/> SOC 2 See details	<input type="checkbox"/> TSA Security Directive Pipeline-2021-02 See details
<input type="checkbox"/> UK NCSC Cyber Assessment Framework See details	<input type="checkbox"/> UK NCSC Cyber Essentials v2.2 See details	

<https://www.cisecurity.org/controls/cis-controls-navigator>

Nerdio CIS policy packs

All this goodness is not only for AVD and Hardened Images. CIS Policy Baselines in Nerdio also allow you to harden any Windows 10/11 Endpoint using L1 policies deployed by Intune and PowerShell.

This is FREE and at no cost, official policies from CIS. On request, we can produce a CIS CAT report showing results.

Value:

1

Tremendous time saved from not needing to implement manually.

2

Support for L2 Windows, iOS, Android, Office coming soon

3

Faster user acceptance testing/security testing

4

Vanilla Windows is 24% compliant, CIS Policy Baselines gets you to 97%

5

Nerdio CIS policy baselines gets you to CMMC, HIPAA, PCI-DSS, FedRAMP + much faster. See CIS Controls Navigator.



v3.0.0 - 02-22-2024

[illegible][illegible][illegible]



Security Configuration Assessment Report for WindowsBuild

Target IP Address: 10.1.1.15

CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0

Level 1 (L1) - Corporate/Enterprise Environment (general use)
Thursday, April 18 2024 13:38:37
Assessment Duration: 1 minute, 45 seconds

Summary

Description	Tests					Scoring	
	Pass	Fail	Error	Not	Exc.	Score	Percent
1 Account Policies	3	7	0	0	1	3.0	30%
1.1 Password Policy	3	4	0	0	0	3.0	43%
1.2 Account Lockout Policy	0	3	0	0	1	0.0	0%
2 Local Policies	61	37	0	0	1	61.0	98%
2.1 Audit Policy	0	0	0	0	0	0.0	0%
2.2 User Rights Assignment	27	16	0	0	0	27.0	73%
2.3 Security Checklists	34	27	0	0	1	34.0	61%
2.3.1 Accounts	3	2	0	0	0	3.0	60%
2.3.2 Audit	1	1	0	0	0	1.0	50%
2.3.3 DCOM	0	0	0	0	0	0.0	0%
2.3.4 Devices	0	0	0	0	0	0.0	0%
2.3.5 Domain controller	0	0	0	0	0	0.0	0%
2.3.6 Domain member	6	0	0	0	0	6.0	100%
2.3.7 Interactive logon	2	5	0	0	0	2.0	29%
2.3.8 Microsoft network client	2	1	0	0	0	2.0	67%
2.3.9 Microsoft network server	2	3	0	0	0	2.0	40%
2.3.10 Network access	9	3	0	0	0	9.0	75%
2.3.11 Network security	2	9	0	0	1	2.0	10%
2.3.12 Recovery console	0	0	0	0	0	0.0	0%
2.3.13 Shutdown	0	0	0	0	0	0.0	0%
2.3.14 System cryptography	0	0	0	0	0	0.0	0%
2.3.15 System objects	2	0	0	0	0	2.0	100%
2.3.16 System settings	0	0	0	0	0	0.0	0%
2.3.17 User Account Control	5	3	0	0	0	5.0	62%
3 Event Log	0	0	0	0	0	0.0	0%
4 Restricted Groups	0	0	0	0	0	0.0	0%
5 System Services	10	10	0	0	0	10.0	50%
6 Registry	0	0	0	0	0	0.0	0%
7 File System	0	0	0	0	0	0.0	0%
8 Wired Network (IEEE 802.3) Policies	0	0	0	0	0	0.0	0%
9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)	0	23	0	0	0	0.0	23%
9.1 Domain Profile	0	7	0	0	0	0.0	7%
9.2 Private Profile	0	7	0	0	0	0.0	7%
9.3 Public Profile	0	9	0	0	0	0.0	9%
10 Network List Manager Policies	0	0	0	0	0	0.0	0%
11 Wireless Network (IEEE 802.11) Policies	0	0	0	0	0	0.0	0%
12 Public Key Policies	0	0	0	0	0	0.0	0%
13 Software Restriction Policies	0	0	0	0	0	0.0	0%
14 Network Access Protection NAP Client Configuration	0	0	0	0	0	0.0	0%
15 Application Control Policies	0	0	0	0	0	0.0	0%
16 IP Security Policies	0	0	0	0	0	0.0	0%
17 Advanced Audit Policy Configuration	9	14	0	0	0	9.0	27%
17.1 Account Logon	0	1	0	0	0	0.0	1%
17.2 Account Management	1	2	0	0	0	1.0	33%

Profiles

This benchmark contains 5 profiles. The **Level 1 (L1) - Corporate/Enterprise Environment (general use)** profile was used for this assessment.

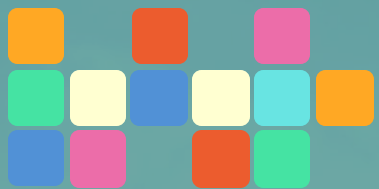
Title	Description
Level 1 (L1) - Corporate/Enterprise Environment (general use)	<p>Items in this profile intend to:</p> <ul style="list-style-type: none">• be the starting baseline for most organizations;• be practical and prudent;• provide a clear security benefit; and• not inhibit the utility of the technology beyond acceptable means. <p>Show Profile XML</p>
Level 1 (L1) + BitLocker (BL)	<p>This profile extends the "Level 1 (L1)" profile and includes BitLocker-related recommendations.</p> <p>Show Profile XML</p>
Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)	<p>This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the following characteristics:</p> <ul style="list-style-type: none">• are intended for environments or use cases where security is more critical than manageability and usability;• may negatively inhibit the utility or performance of the technology; and• limit the ability of remote management/access. <p>Note: Implementation of Level 2 requires that both Level 1 and Level 2 settings are applied.</p> <p>Show Profile XML</p>
Level 2 (L2) + BitLocker (BL)	<p>This profile extends the "Level 2 (L2)" profile and includes BitLocker-related recommendations.</p> <p>Show Profile XML</p>
BitLocker (BL) - optional add-on for when BitLocker is deployed	<p>This profile contains BitLocker-related recommendations, if your organization chooses to use it. It is intended to be an optional "add-on" to the Level 1 (L1) or Level 2 (L2) profiles.</p> <p>Show Profile XML</p>

Lab 4

Policy & CIS baselines

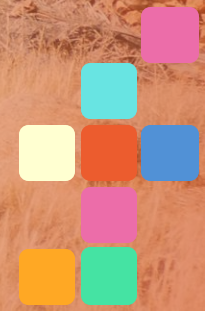
- 1 Creating policy baselines
- 2 Change priority of a baseline
- 3 Assign policies to a baseline
- 4 Go over CIS Benchmarks





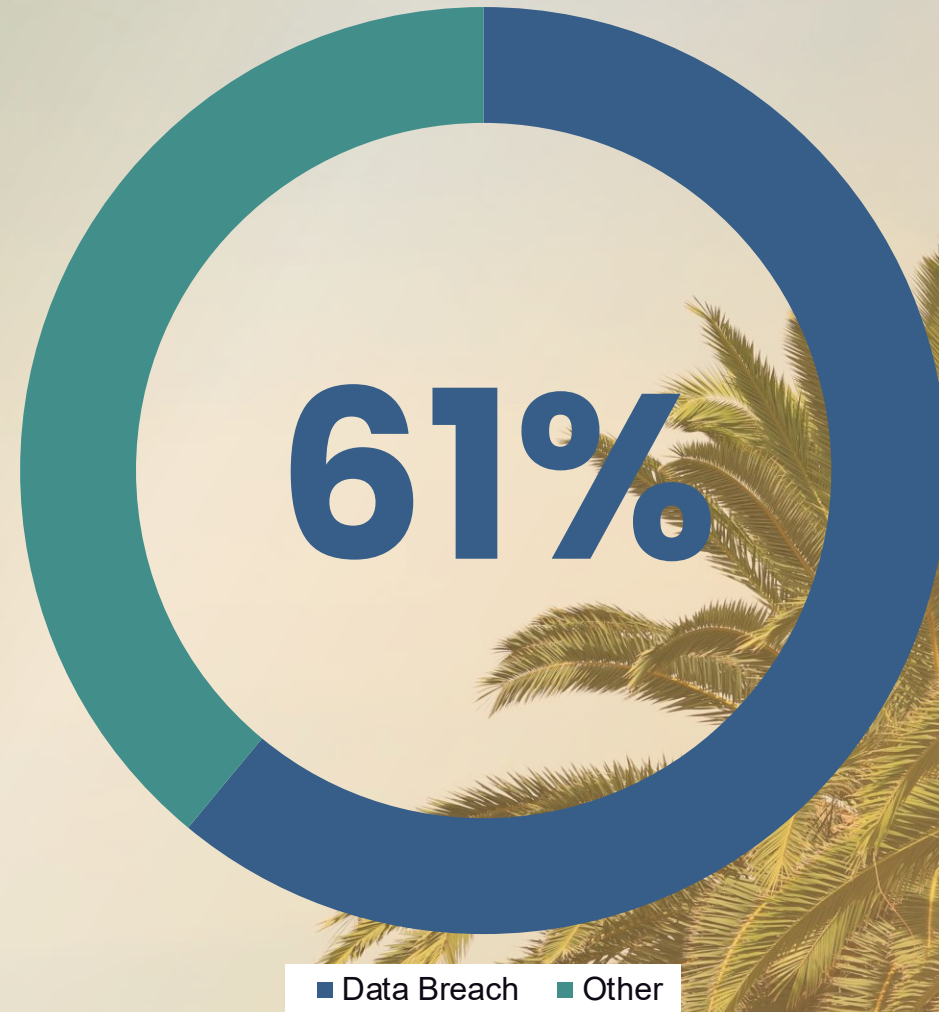
★ *NerdioCon* ★
2025
PALM SPRINGS

Security



Why security matters for MSPs

61% of SMBs have been hit by a successful cyberattack in the last year.



(BlackFog Cybersecurity Report, 2023)

The silent costs: Impacts beyond the bottom line



**Reputation
damage**



**Damage to
customer
relationships**



**Compliance & legal
penalties**

Security challenges MSPs face in managing Azure

Visibility gaps

Difficulty obtaining a unified view of security across clients, tenants, and environments.

Cost and resource strain

Balancing cost-effective resource usage while maintaining strict security measures.

Issues with backup / recovery process

Inconsistent Azure Backup policies create gaps in disaster recovery readiness.

Security pitfalls in the Modern Work landscape

1

Inconsistent
security policies

2

Data
exposure risks

3

Delayed threat
detection

4

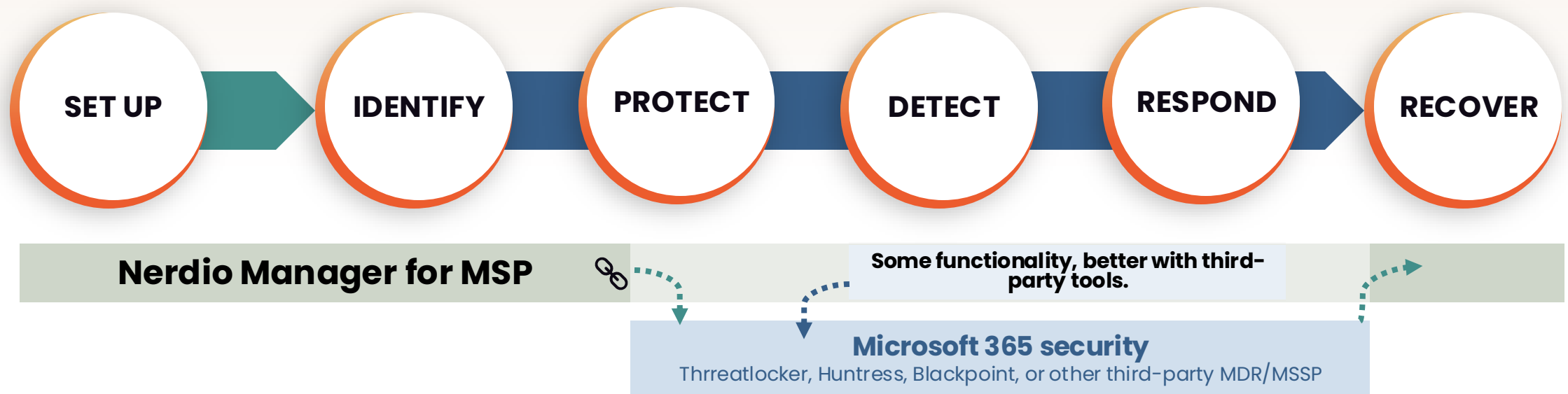
User management
challenges

Nerdio Modern Work: Closing security gaps

- 1 Secure access controls
- 2 Automated policy enforcement
- 3 Enhanced data protection
- 4 Proactive threat monitoring
- 5 Effortless user management



What is the NIST Cybersecurity Framework?



Nerdio Manager for MSP meets the NIST Cybersecurity Framework

Identify				
<ul style="list-style-type: none">• Audit logs• Risky & stale user reports• Defender vulnerability reporting• Device configuration compliance• Global views & dashboards• AVD utilization and performance• Tenant configuration compliance• Secure Score management				

Nerdio Manager for MSP meets the NIST Cybersecurity Framework

Identify	Protect			
<ul style="list-style-type: none">• Audit logs• Risky & stale user reports• Defender vulnerability reporting• Device configuration compliance• Global views & dashboards• AVD utilization and performance• Tenant configuration compliance• Secure Score management	<ul style="list-style-type: none">• Granular RBAC Model• CIS Hardened AVD images• CIS Intune Policies• Settings baselines• Conditional access• Policy management• Azure backup management• Golden image management• Global app catalog• Global policy management• Global Windows update rings			

Nerdio Manager for MSP meets the NIST Cybersecurity Framework

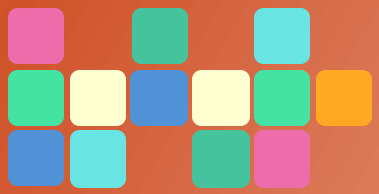
Identify	Protect	Detect		
<ul style="list-style-type: none">• Audit logs• Risky & stale user reports• Defender vulnerability reporting• Device configuration compliance• Global views & dashboards• AVD utilization and performance• Tenant configuration compliance• Secure Score management	<ul style="list-style-type: none">• Granular RBAC Model• CIS Hardened AVD images• CIS Intune Policies• Settings baselines• Conditional access• Policy management• Azure backup management• Golden image management• Global app catalog• Global policy management• Global Windows update rings	<ul style="list-style-type: none">• Defender for Endpoint functionality• Risky & stale user reporting		

Nerdio Manager for MSP meets the NIST Cybersecurity Framework

Identify	Protect	Detect	Respond	
<ul style="list-style-type: none">• Audit logs• Risky & stale user reports• Defender vulnerability reporting• Device configuration compliance• Global views & dashboards• AVD utilization and performance• Tenant configuration compliance• Secure Score management	<ul style="list-style-type: none">• Granular RBAC Model• CIS Hardened AVD images• CIS Intune Policies• Settings baselines• Conditional access• Policy management• Azure backup management• Golden image management• Global app catalog• Global policy management• Global Windows update rings	<ul style="list-style-type: none">• Defender for Endpoint functionality• Risky & stale user reporting	<ul style="list-style-type: none">• Console Connect	

Nerdio Manager for MSP meets the NIST Cybersecurity Framework

Identify	Protect	Detect	Respond	Recover
<ul style="list-style-type: none">• Audit logs• Risky & stale user reports• Defender vulnerability reporting• Device configuration compliance• Global views & dashboards• AVD utilization and performance• Tenant configuration compliance• Secure Score management	<ul style="list-style-type: none">• Granular RBAC Model• CIS Hardened AVD images• CIS Intune Policies• Settings baselines• Conditional access• Policy management• Azure backup management• Golden image management• Global app catalog• Global policy management• Global Windows update rings	<ul style="list-style-type: none">• Defender for Endpoint functionality• Risky & stale user reporting	<ul style="list-style-type: none">• Console Connect	<ul style="list-style-type: none">• Azure backup management & validation• Golden Image management & validation• CIS Hardened AVD Images• Recovery services for policies & baselines• AVD Auto-Heal• AI backup validation• AI image validation



Risky & stale user management



Risky & stale user reporting

Challenges

- Need a way to monitor and manage inactive or compromised user accounts.
- Limit the security risks that these users cause.

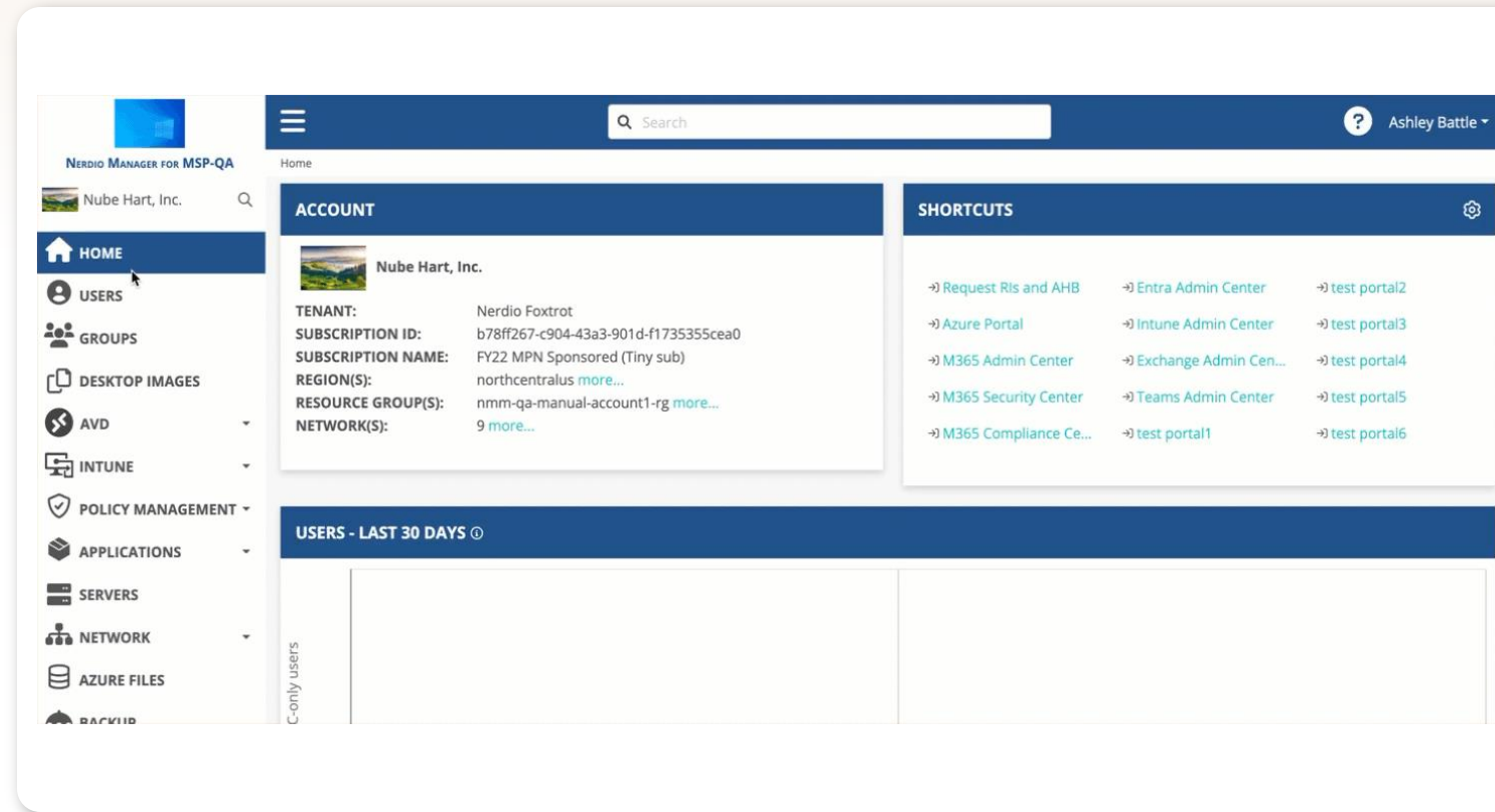
Solution

- Detailed reporting on user accounts that are flagged as risky or stale.

Risky & stale user reporting

Outcomes

- Reduce security risks.
- Ensure compliance with security protocols.
- Provide safer and more efficient client accounts.



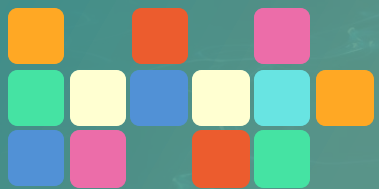
Lab 5

Risky & stale users

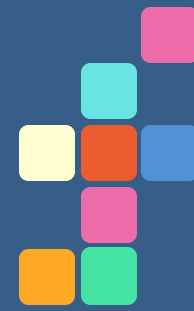
1

Walk through how to view and determine “risk state”...





Defender vulnerability dashboard



Defender vulnerability management

Challenges



- MSPs need visibility into vulnerabilities across client environments to proactively manage security risks.

Solution

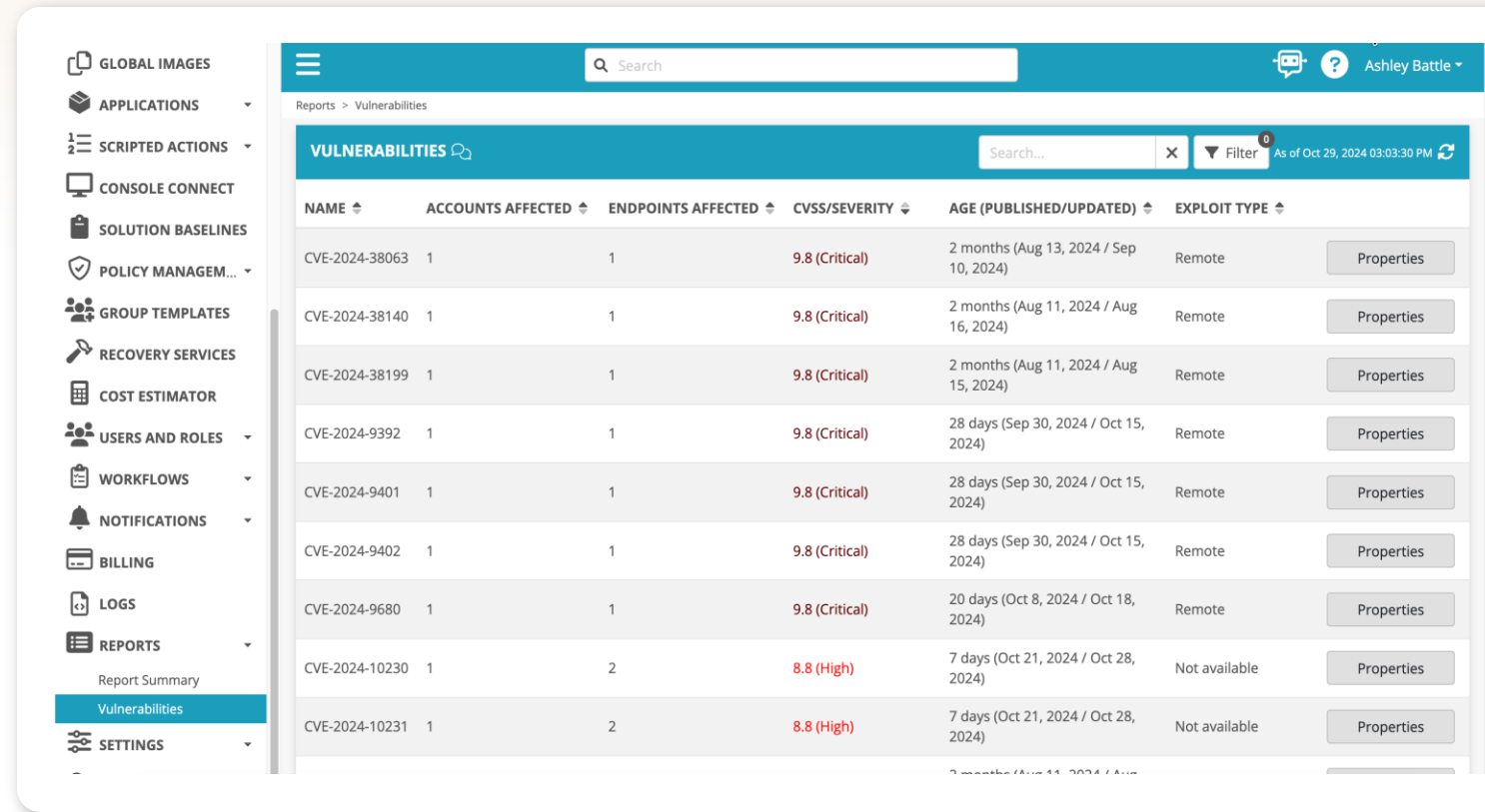


- Use a unified dashboard highlighting vulnerabilities.

Defender vulnerability management

Outcomes

- Gain a clear view of vulnerabilities across client environments.
- Enable faster resolution of security risks.
- Improve the security posture of client environments.



The screenshot displays the Defender Vulnerability Management console. On the left is a navigation sidebar with icons and labels for various sections: GLOBAL IMAGES, APPLICATIONS, SCRIPTED ACTIONS, CONSOLE CONNECT, SOLUTION BASELINES, POLICY MANAGEM..., GROUP TEMPLATES, RECOVERY SERVICES, COST ESTIMATOR, USERS AND ROLES, WORKFLOWS, NOTIFICATIONS, BILLING, LOGS, REPORTS (with sub-items Report Summary and Vulnerabilities), and SETTINGS. The main content area is titled 'Reports > Vulnerabilities' and features a search bar, a filter icon, and a refresh button. Below this is a table of vulnerabilities with columns for NAME, ACCOUNTS AFFECTED, ENDPOINTS AFFECTED, CVSS/SEVERITY, AGE (PUBLISHED/UPDATED), and EXPLOIT TYPE. Each row includes a 'Properties' button. The table lists several CVEs, mostly with a CVSS score of 9.8 (Critical) and an exploit type of 'Remote'. Two entries at the bottom have a CVSS score of 8.8 (High) and an exploit type of 'Not available'.

NAME	ACCOUNTS AFFECTED	ENDPOINTS AFFECTED	CVSS/SEVERITY	AGE (PUBLISHED/UPDATED)	EXPLOIT TYPE	Properties
CVE-2024-38063	1	1	9.8 (Critical)	2 months (Aug 13, 2024 / Sep 10, 2024)	Remote	Properties
CVE-2024-38140	1	1	9.8 (Critical)	2 months (Aug 11, 2024 / Aug 16, 2024)	Remote	Properties
CVE-2024-38199	1	1	9.8 (Critical)	2 months (Aug 11, 2024 / Aug 15, 2024)	Remote	Properties
CVE-2024-9392	1	1	9.8 (Critical)	28 days (Sep 30, 2024 / Oct 15, 2024)	Remote	Properties
CVE-2024-9401	1	1	9.8 (Critical)	28 days (Sep 30, 2024 / Oct 15, 2024)	Remote	Properties
CVE-2024-9402	1	1	9.8 (Critical)	28 days (Sep 30, 2024 / Oct 15, 2024)	Remote	Properties
CVE-2024-9680	1	1	9.8 (Critical)	20 days (Oct 8, 2024 / Oct 18, 2024)	Remote	Properties
CVE-2024-10230	1	2	8.8 (High)	7 days (Oct 21, 2024 / Oct 28, 2024)	Not available	Properties
CVE-2024-10231	1	2	8.8 (High)	7 days (Oct 21, 2024 / Oct 28, 2024)	Not available	Properties

Lab 6

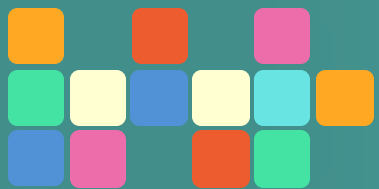
Vulnerability dashboard



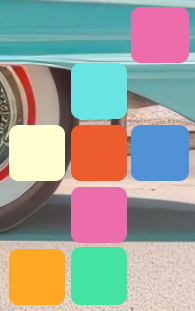
1

Walk through how to view the vulnerabilities report and see the details





Tenant monitoring



Tenant monitoring

Challenges



- Managing compliance across multiple tenants is challenging due to limited visibility and the need for manual audits, which increase the risk of errors and inconsistencies.

Solution

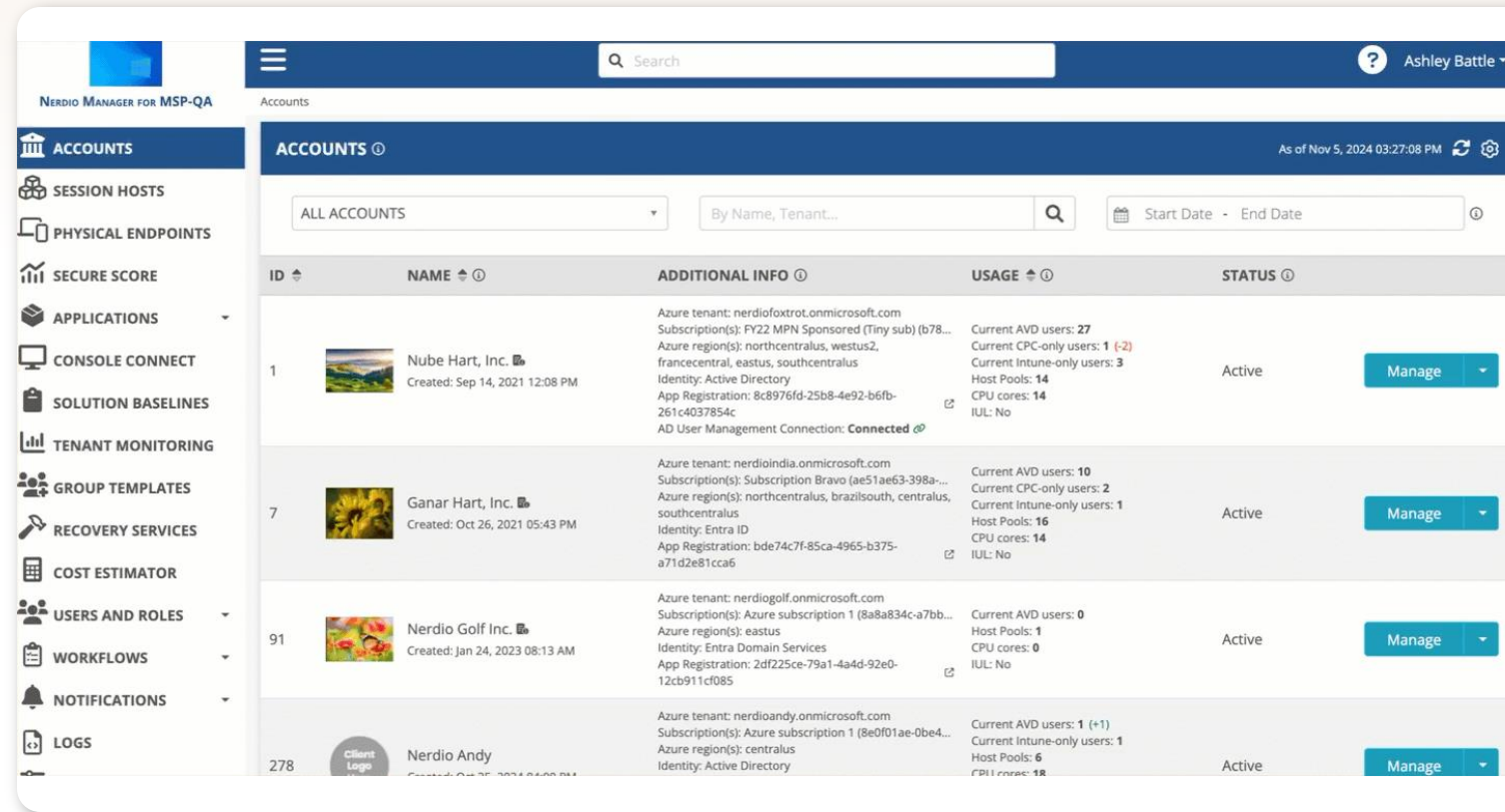


- A centralized tenant monitoring and reporting feature that allows MSPs to track, compare, and assess policy settings across customer tenants.

Tenant monitoring

Outcomes

- MSPs gain a clear, centralized view of policy compliance across all tenants.
- You can now identify and highlight policy deviations, enabling timely fixes and reducing risks.



The screenshot displays the 'Accounts' section of the Nerdio Manager for MSP-QA. The interface includes a sidebar with navigation options and a main content area with a table of accounts. The table columns are ID, NAME, ADDITIONAL INFO, USAGE, and STATUS. Each row represents a tenant account with associated details like Azure tenant, subscription, region, identity, and usage statistics (AVD users, CPC-only users, Intune-only users, Host Pools, CPU cores, IUL).

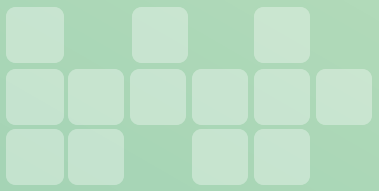
ID	NAME	ADDITIONAL INFO	USAGE	STATUS
1	Nube Hart, Inc.	Azure tenant: nerdiofoxtrout.onmicrosoft.com Subscription(s): FY22 MPN Sponsored (Tiny sub) (b78... Azure region(s): northcentralus, westus2, francecentral, eastus, southcentralus Identity: Active Directory App Registration: 8c8976fd-25b8-4e92-b6fb-261c4037854c AD User Management Connection: Connected	Current AVD users: 27 Current CPC-only users: 1 (-2) Current Intune-only users: 3 Host Pools: 14 CPU cores: 14 IUL: No	Active
7	Ganar Hart, Inc.	Azure tenant: nerdioindia.onmicrosoft.com Subscription(s): Subscription Bravo (ae51ae63-398a-... Azure region(s): northcentralus, brazilsouth, centralus, southcentralus Identity: Entra ID App Registration: bde74c7f-85ca-4965-b375-a71d2e81cca6	Current AVD users: 10 Current CPC-only users: 2 Current Intune-only users: 1 Host Pools: 16 CPU cores: 14 IUL: No	Active
91	Nerdio Golf Inc.	Azure tenant: nerdiogolf.onmicrosoft.com Subscription(s): Azure subscription 1 (8a8a834c-a7bb-... Azure region(s): eastus Identity: Entra Domain Services App Registration: 2df225ce-79a1-4a4d-92e0-12cb911cf085	Current AVD users: 0 Host Pools: 1 CPU cores: 0 IUL: No	Active
278	Nerdio Andy	Azure tenant: nerdioandy.onmicrosoft.com Subscription(s): Azure subscription 1 (8e0f01ae-0be4-... Azure region(s): centralus Identity: Active Directory	Current AVD users: 1 (+1) Current Intune-only users: 1 Host Pools: 6 CPU cores: 18	Active

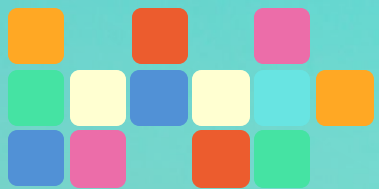
Lab 7

Tenant monitoring

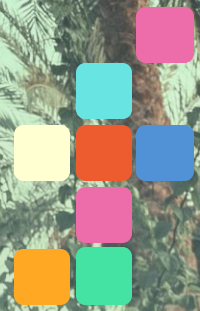
1 Walk through how to create a new Tenant Monitoring report

2 View the report





Secure Score management



Secure Score management

Challenges



- Managing Secure Scores for multiple clients is challenging due to limited visibility and significant manual effort, making it time-consuming to address security gaps.

Solution



- A centralized view to track and manage Secure Scores for all clients from a single interface.

Secure Score management

Outcomes

- Streamline security operations across multiple tenants
- Improve client security postures
- Reduce vulnerability risks

The screenshot displays the NERDIO Manager for MSP-QA interface. The left sidebar contains a navigation menu with the following items: ACCOUNTS, SESSION HOSTS, PHYSICAL ENDPOINTS, SECURE SCORE, APPLICATIONS, CONSOLE CONNECT, SOLUTION BASELINES, TENANT MONITORING, GROUP TEMPLATES, RECOVERY SERVICES, COST ESTIMATOR, USERS AND ROLES, and WORKFLOWS. The main content area is titled 'ACCOUNTS' and shows a table of accounts. The table has columns for ID, NAME, ADDITIONAL INFO, USAGE, and STATUS. Three accounts are listed: Nube Hart, Inc., Ganar Hart, Inc., and Nerdio Golf Inc. Each account row includes a 'Manage' button.

ID	NAME	ADDITIONAL INFO	USAGE	STATUS
1	Nube Hart, Inc. Created: Sep 14, 2021 12:08 PM	Azure tenant: neriiofoxtrout.onmicrosoft.com Subscription(s): FY22 MPN Sponsored (Tiny sub) (b78... Azure region(s): northcentralus, westus2, francecentral, eastus, southcentralus Identity: Active Directory App Registration: 8c8976fd-25b8-4e92-b6fb-261c4037854c AD User Management Connection: Connected	Current AVD users: 27 Current CPC-only users: 1 (-2) Current Intune-only users: 3 Host Pools: 14 CPU cores: 15 IUL: No	Active Manage
7	Ganar Hart, Inc. Created: Oct 26, 2021 05:43 PM	Azure tenant: neriioindia.onmicrosoft.com Subscription(s): Subscription Bravo (ae51ae63-398a-... Azure region(s): northcentralus, brazilsouth, centralus, southcentralus Identity: Entra ID App Registration: bde74c7f-85ca-4965-b375-a71d2e81cca6	Current AVD users: 10 Current CPC-only users: 2 Current Intune-only users: 1 Host Pools: 16 CPU cores: 14 IUL: No	Active Manage
91	Nerdio Golf Inc. Created: Jan 24, 2023 08:13 AM	Azure tenant: neriogolf.onmicrosoft.com Subscription(s): Azure subscription 1 (8a8a834c-a7bb-... Azure region(s): eastus Identity: Entra Domain Services App Registration: 2df225ce-79a1-4a4d-92e0-...	Current AVD users: 0 Host Pools: 1 CPU cores: 0 IUL: No	Active Manage

Lab 8

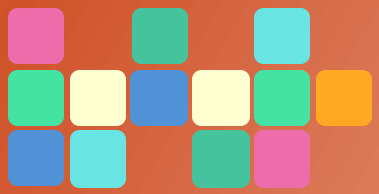
Secure Score management



1 Walk through how to enable Secure Score

2 View the reports





Exchange Online management



Exchange Online management

Challenges

- Frequent account switching for mailbox management is time-consuming and error-prone.
- Limited centralized control hinders consistent policy application.

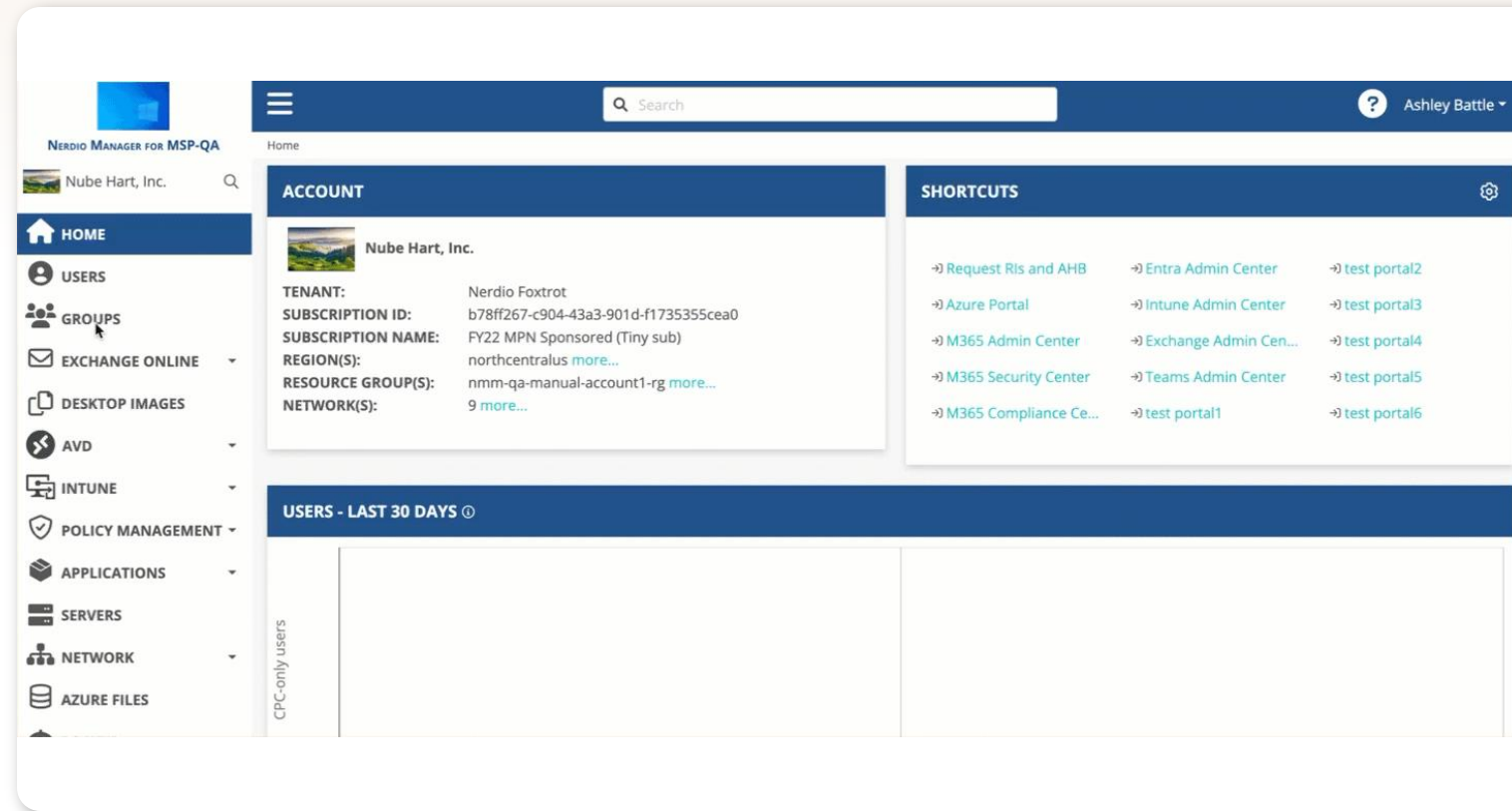
Solution

- A unified, cross-tenant view that allows MSPs to configure, monitor, and update mailboxes without needing multiple logins.

Exchange Online management

Outcomes

- Centralized mailbox management across clients for increased efficiency
- Consistent policy application across tenants
- Reduce admin time with fewer manual steps



Lab 9

Exchange Online management

- 1** Walk through how to enable Exchange Online management
- 2** Manage mailbox properties
- 3** Manage Exchange quarantine



Nerdio Manager for MSP

Newest updates: Version 5.8 (March 3)

- Console Connect: Can now be used on source VMs
- Group Templates: Can be used for license management
- Policy Management: Policies at account level show “managed” / drifted
- CIS Baselines: Can clone, remove, edit policies now
- Notifications: Email subject and bodies can be customized / variables
- Notifications: Can now notify for NMM upgrades available

- Windows 11 24H2 available / Server 2025 available
- AD User Management: Update OU UI with checkboxes
- Can now generate RDP file for individual hosts
- UAM: Shell apps can be deployed for Intune targets
- UAM: Shell apps can “uninstall and install” option for policies
- Cost Estimator: Can select payment terms for AHB

Where business goes big

Pre-sales support



- Dedicated channel account manager
- Dedicated solution consultants
- Infrastructure architects
- In-house cloud engineers

Post-sales support



- Launch kits
- In-house 24/7 technical support
- 80 Net Promoter Score for support
- Professional Services

Pax8 marketplace



- Quote, order, bill and provision
- Monthly, annual and usage-based billing (single invoice)
- Integrates with PSA tools

Cloud products



- MSP-centric vendors
- Optimized incentives and rebates
- Azure and Microsoft 365 Bootcamps
- API-enabled provisioning
- No quotas and no minimums

WHO WE ARE

A highly experienced team of Microsoft Infrastructure Solutions Consultants dedicated to helping partners create successful outcomes



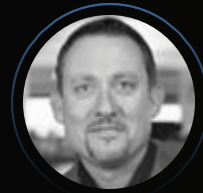
Stephen Slattery
Director of
Infrastructure Solutions



Blake Closner



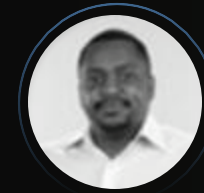
Matt Hache



Ryan Hughes



Collin Magnus



Travis Finley



Wes Johnson



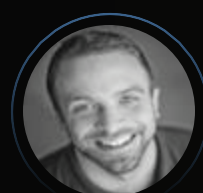
Carlton Martindale
Manager of
Infrastructure Solutions



Scott Fox



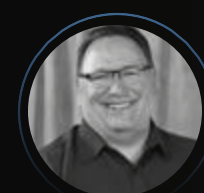
Nathan Rodriguez



Will Sebring



Steve Melnik



John Wrona

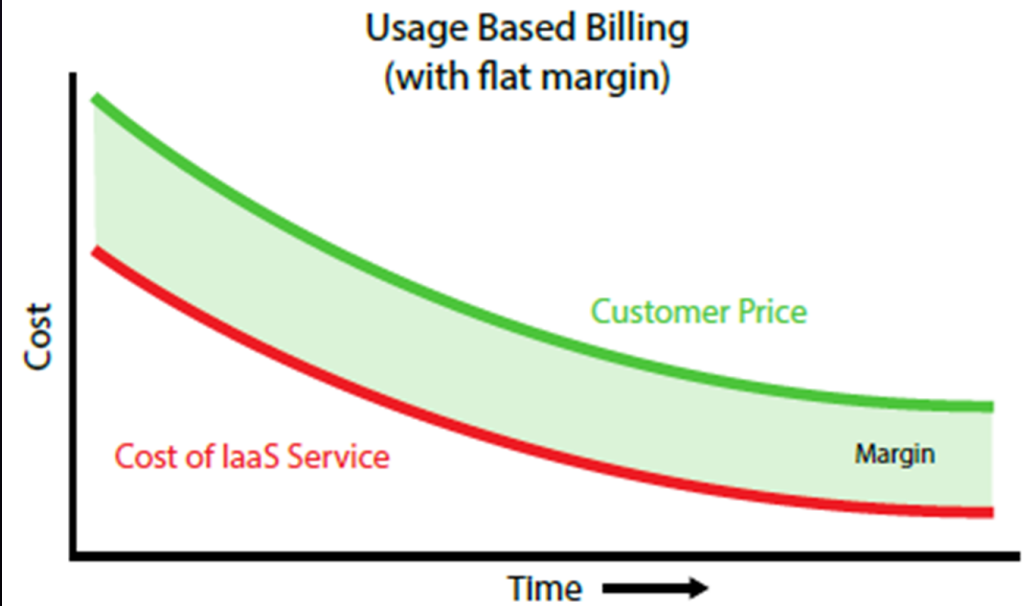
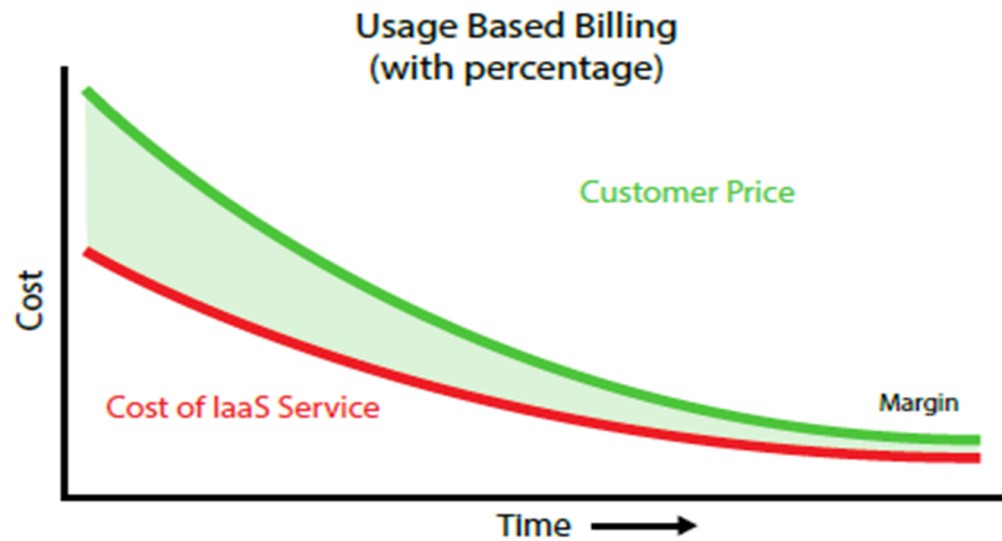
Unlocking the revenue potential



GTM pricing strategy

- Usage based = MSRP or markup on cost
- Percentage margin
- Set margin
- Fixed billing model

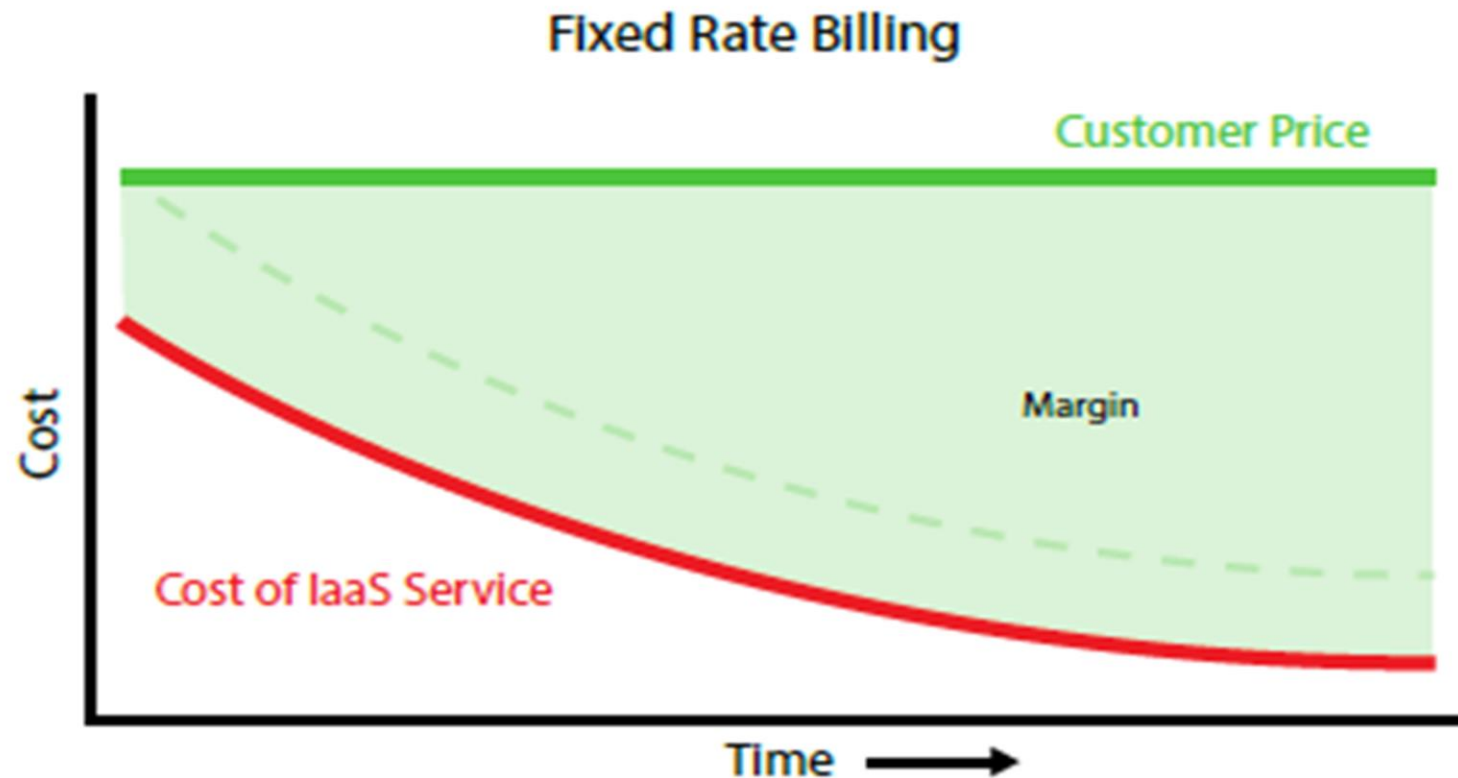
Unlocking the revenue potential



Unlocking the revenue potential

Bill in advance

Improve your
cashflow





How to do it: The game plan

Reproducible Steps



Collaborate with a partner who understands your current position



Assess your areas of financial waste

- Consider why you are using multiple tools that are already part of your package
-



Implement standardization, automation, and scaling

- Minimize your risks
 - Enhance client value
-



Invest in essential programs and tools

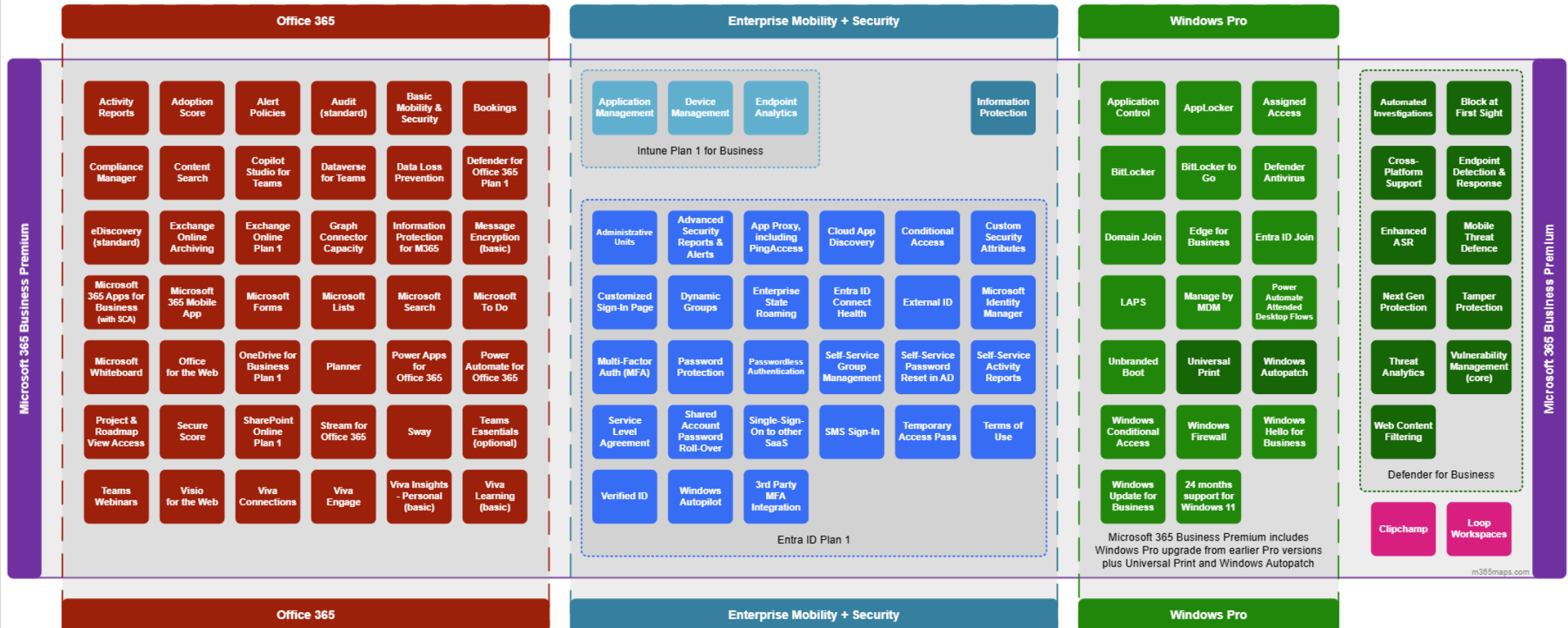


Enhance your MSP

Microsoft 365 Business Premium

January 2025

m365maps.com



*Slides from <https://m365maps.com/>

Defender for Business

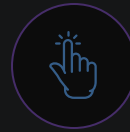
Elevated protection for the SMB

Designed for businesses with up to 300 employees



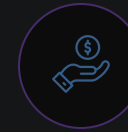
Enterprise-grade protection

Protect devices against ransomware and other cyberthreats with industry-leading Defender technologies like endpoint detection and response and threat and vulnerability management.



Easy to use

Wizard-based onboarding gets your environment prepared quickly. Out-of-the box policies and automated investigation and remediation help automatically protect against the latest threats, so you can focus on what's most important.



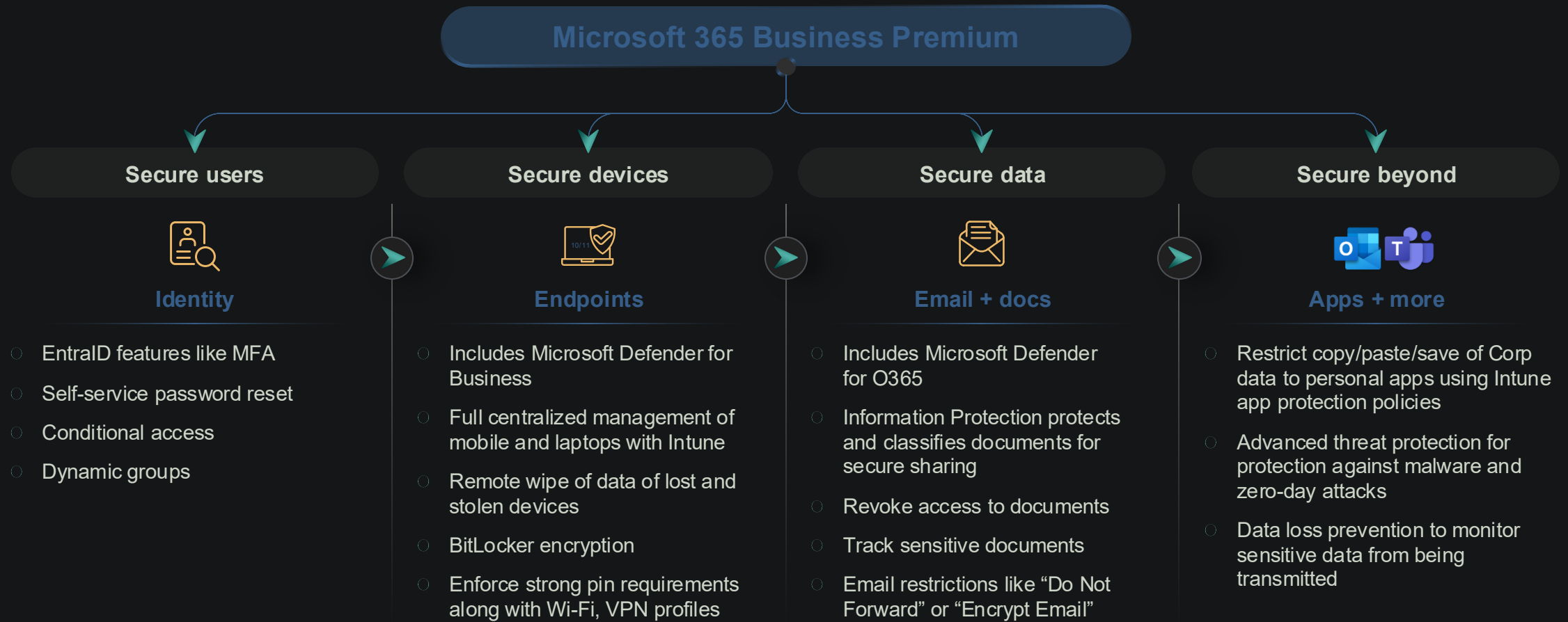
Cost-effective

Security that works without compromising budget. Available in two flexible plans as part of **Microsoft 365 Business Premium**, or as a standalone solution.

Security and compliance value for AI + SMB

Scenario for 300 users and under		Business Standard	Business Premium
Identity & Access Management	Login to Copilot for Microsoft 365 with a single identity	•	•
	Enforce MFA when accessing Microsoft 365 to use Copilot	Basic MFA	•
	Enable end-user password reset, change, and unlock when accessing Microsoft 365	Cloud only	•
	Implement Conditional Access policies based on identity, device, and location when accessing Microsoft 365 to use Copilot		•
	Enable near real-time access policies enforcement, evaluate critical events, and immediately revoke access to Microsoft 365		•
	Require employees or guests to accept terms of use policy before getting access		•
Endpoint Management	Push/deploy Microsoft 365 apps to devices and grant access to Copilot in those apps		•
	Manage Microsoft 365 app updates		•
	Restrict the use of Microsoft 365 apps and Teams – as well as Copilot in those apps – on personal devices		•
	Prevent saving files – including those generated by Copilot – to unprotected apps		•
	Wipe all work content – including content generated by Copilot – if a device is lost, stolen or compromised	•	•
	Revoke work access on noncompliant devices	Except Windows	•
Data security & compliance	Search for Copilot generated data by content, keyword search, apply legal hold, and export the search results; investigate incidents related to Copilot and respond to litigations	Content, keyword search, and export only	Standard
	Audit logs for Copilot interactions	Standard	Standard
	Apply a retention or deletion policy for Copilot interactions	•	•
	Data Loss Prevention policies to protect sensitive data, generated by Copilot and saved in Microsoft 365 locations, from exfiltration		Files & email
	Prohibit Copilot from summarizing or including data that users have no extract permissions in its response messages for the said users		•
	Exclude sensitive files that users have no view permission from being processed by Copilot for the said users	•	•

Security success steps with Microsoft 365



Call to Action

Work with your Pax8 Account Team to find out who your Infrastructure and Productivity Consultants are



Check out Nerdio Manager for MSP from the Pax8 Marketplace



Sign up for Per Tenant Pricing—a Pax8 Exclusive

Nerdio Manager for MSP: Modern Work per-customer pricing



A dark-themed pricing card for Nerdio Manager for MSP. In the top left corner is a cloud icon with 'pax8' inside. In the top right is a line-art icon of a multi-story building. A red diagonal banner with white text 'EXCLUSIVE DISCOUNT' is positioned across the top left. The text 'Starting at' is centered above a large blue '\$50'. To the right of '\$50' is the text 'per tenant'. Below this, 'Per month' is centered. At the bottom, a blue pill-shaped button contains the text 'Modern Work'.

Starting at

\$50

per tenant

Per month

Modern Work



Includes: All Modern Work features



License and manage ALL of your Microsoft Cloud customers



Introductory pricing—no contract required

Promo details



Goal

- Drive Pax8 partner adoption of premium Microsoft SKUs
- Drive Pax8 partner adoption of Nerdio for Modern Work

Free for 6 months!!

**Normal pricing is
\$50 per tenant**



Pax8 offer

- Offering Nerdio for MW per tenant free for 6 months with eligible upgrade or net new subscriptions of BP, E3, E5
- Partners must have at least 1 tenant to qualify, and they need to upgrade at least 10 users in each tenant
- Pax8 is the EXCLUSIVE provider of Nerdio for Modern Work



Eligibility

- Partner must upgrade Business Standard/Business Basic to Premium M365 MW solutions
- Minimum 10 user upgrades per tenant with at least 5 tenants per partner
- Submit proof of execution to Pax8 for verification and activation of their Nerdio for MW
- Onboard and join MW Security + Nerdio Masterclass

Test time!

- Scan the QR code to the right or open the short link in a browser.
- Complete the exam.
- Once you've passed the exam, bring a screenshot of your completed score to the registration desk to claim your certificate.

Good luck!

https://nerdio.co/Nerdio_PreCon_Modern_Work

