NerdioCon

2025

PALM SPRINGS

Intune endpoint management mastery

NerdioCon 2025

PALM SPRINGS

Kevin Sullivan

Principal Product Manager
Microsoft Intune

Sheldon Turner

Senior Director, Technical Strategy &
Assessment/ CIS

Rolando Jimenez

Technical Trainer / Nerdio

Rolando Jimenez

Technical Solutions Trainer

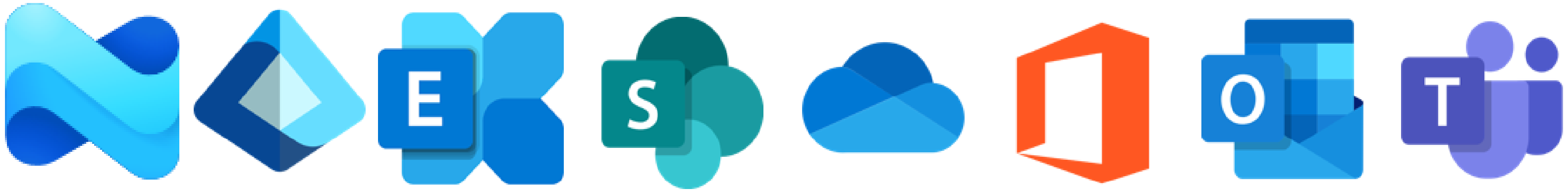
- Started at Microsoft retail
- Helped Support the IEC in Redmond
- Microsoft funded Intune and W365 workshops
- I am a huge gamer/Star Wars Nerd
- I live in Seattle, Washington

Two truths and a lie

- My dad is a National Boxing Champion
- I own a Humanoid Robot designed with the ability to read human emotions
- I have traveled to every state in the United States

Where are we? Where are we going?

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



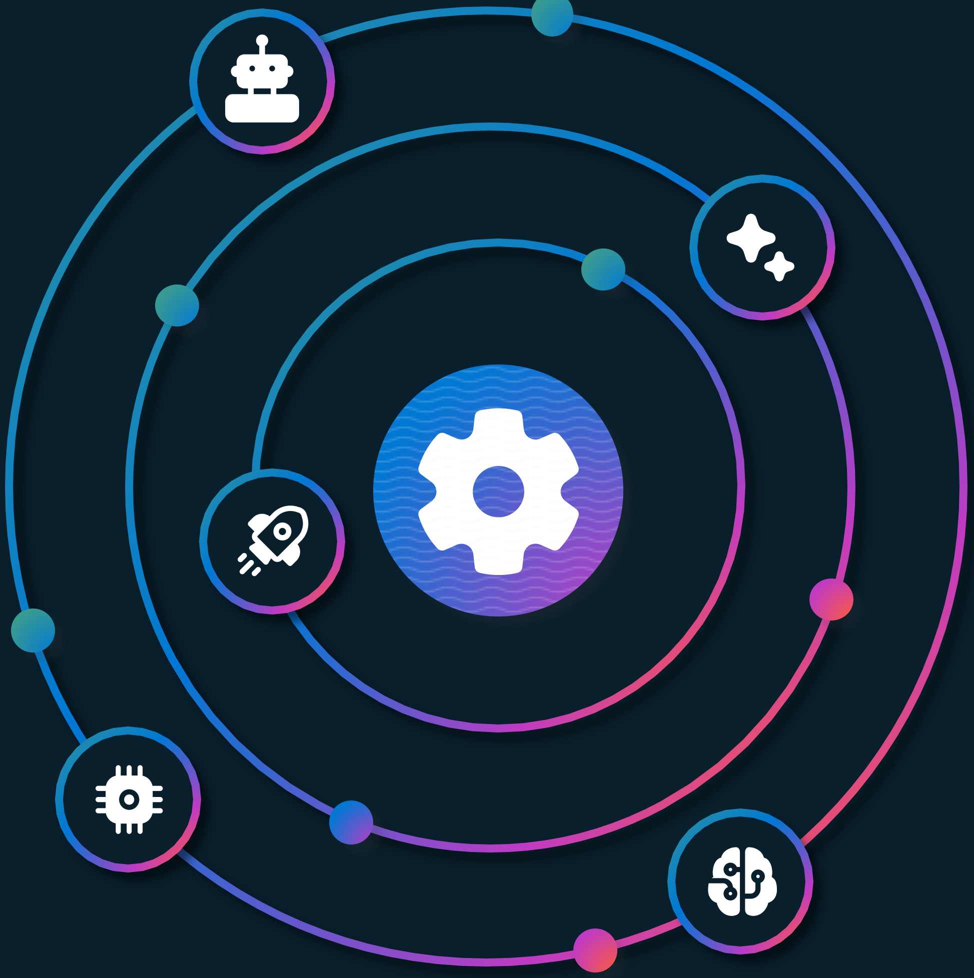
Microsoft

The future of endpoint management

Kevin Sullivan

What we'll cover

- Why here? Why now?
  Why Microsoft?
- Why cloud native?
- The future



Kevin Sullivan

Principal Product Manager

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

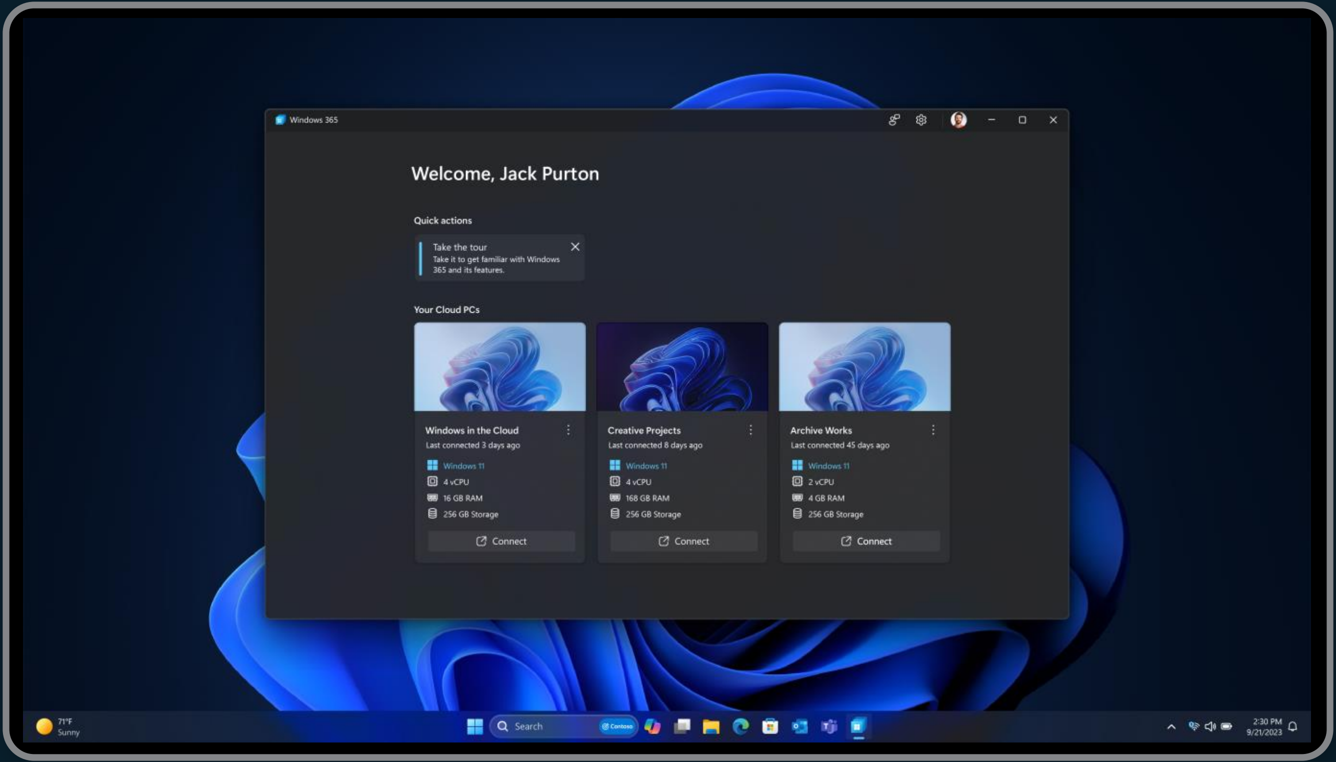
[As an MSP] you need to have new opportunities for all your employees, if we’re doing the same every year, everybody's gone. If you still do the domain joined laptops, everybody’s gone.

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

Erik Loef

CTO & Owner PROXSYS*

Next-gen virtual devices



Windows 365

Welcome, Jack Purton

Quick actions

Take the tour
Take it to get familiar with Windows 365 and its features.

Your Cloud PCs

Windows in the Cloud
Last connected 3 days ago
Windows 11
4 vCPU
16 GB RAM
256 GB Storage
Connect

Creative Projects
Last connected 8 days ago
Windows 11
4 vCPU
168 GB RAM
256 GB Storage
Connect

Archive Works
Last connected 45 days ago
Windows 11
2 vCPU
4 GB RAM
256 GB Storage
Connect

Next-gen virtual devices

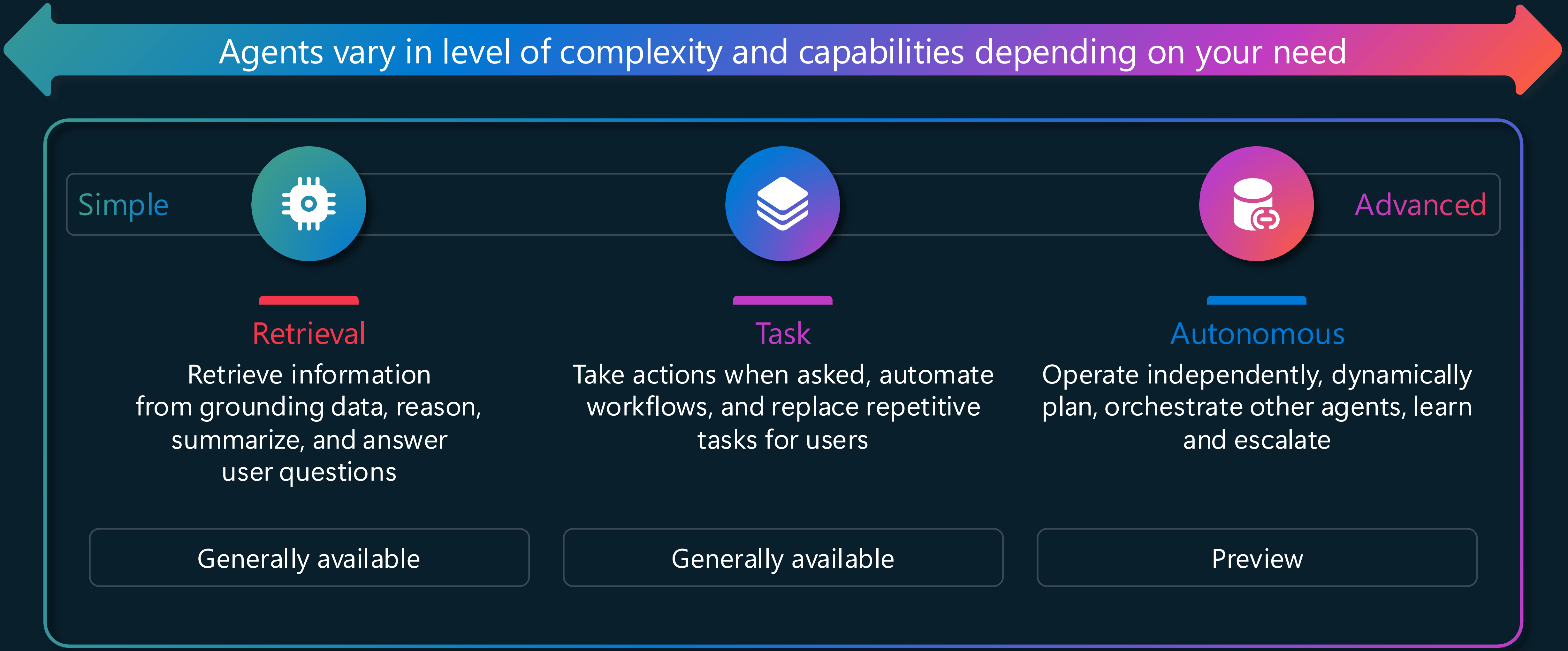
> We've added 350 end users to the solution which takes 20 minutes– a massive reduction from the four hours it took with our previous infrastructure.

BKW

Karin Niggli

Head of Workplace and Collaboration

Agents are the future



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

Simple

Advanced

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

Nerdio + Microsoft Intune Feedback Survey

Microsoft Intune

What is it?

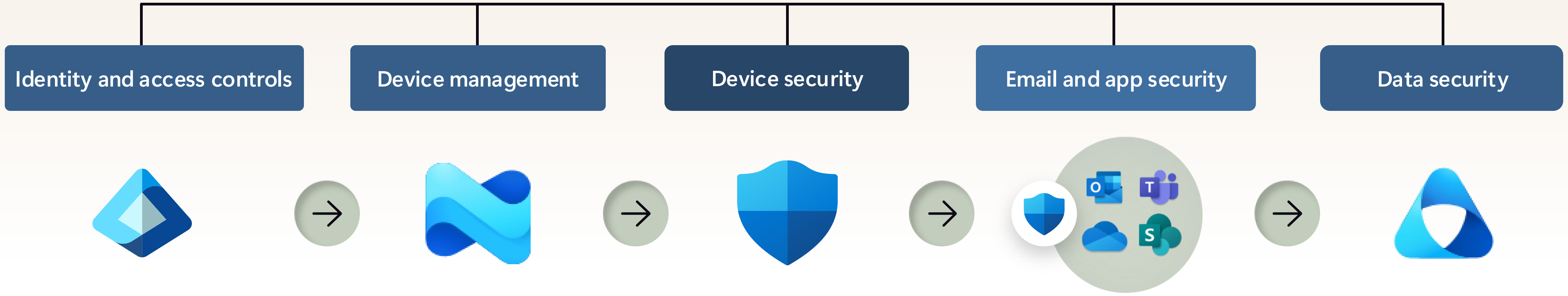
A set of technologies that securely manage identities, applications, and devices (physical and virtual).

Why use it?

- Included in M365 Business premium, E3+ plans.
- Augments RMM.
- Along with Entra, Defender, Purview, consolidates multiple MSP tools into a single solution.

Layered security

Microsoft 365 Business Premium



Identity and access controls

Device management

Device security

Email and app security

Data security

Microsoft Entra ID P1

Multifactor authentication to protect against password loss

Passwordless authentication

Self Service Password Reset

Conditional Access to provide access controls to work resources and applications

Cloud App Discovery to identify and discover “Shadow IT”

Microsoft Intune

Keep devices up-to-date with the latest OS

Protect devices from bad actors and misuse

Allow more secure access to sensitive data–even from personal devices

Remotely wipe data from lost and stolen devices

Pre-load access to Wi-Fi, VPN with certificate management

Microsoft Defender for Business

Ransomware protection with AI powered EDR with automatic attack disruption

Next gen-AV protection

Protection across Android, iOS, MacOS, Windows and Linux

Threat and vulnerability management

Monthly summary reports

Microsoft Defender for Office 365

AI powered LLM-based threat protection

Phishing and malware defense across email

Microsoft Teams, OneDrive and SharePoint

SafeLinks with time of click URL filtering

Safe attachments with real-time attachment scanning in sandbox

Microsoft Purview

Data Loss Prevention to protect sensitive data, such as credit card or social security numbers

Classify and label sensitive data

Apply protection, such as “Do Not Forward” or “Encrypt Email”

Audit, search, and legal hold

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

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).

Replacing Group Policy

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

Enabling work-from-anywhere

- Truly work from anywhere
- Intune enables secure remote work without a use of a VPN client of any kind
- Access corporate data from any compliant enrolled device
- Access applications without endpoint enrollment with Mobile Application Management (MAM)

Microsoft Intune + Nerdio = A match made in heaven

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

Live demo agenda

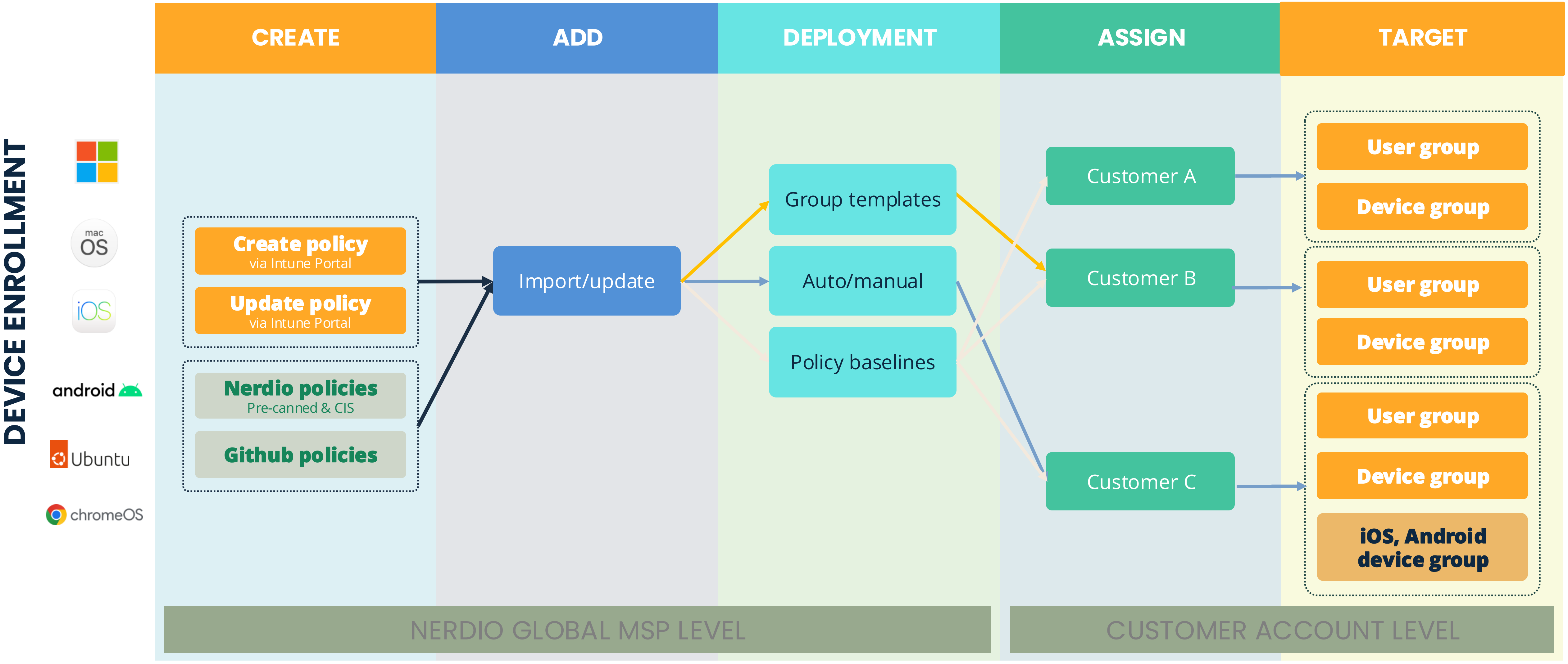
- Creating Intune polices
- Importing Intune polices into Nerdio
- Editing Intune polices in Nerdio
- Assigning polices to endpoints
- Configuring Conditional Access
- Solution Baselines and Modern Work
- BREAK TIME
- Mobile Application Management (MAM)
- Creating an MDM Compliance Policy in Intune
- Apple iOS Intune Enrollment Pre-Reqs
- Creating an App Protection Policy
- Creating an App Configuration
- BYOD Demo– Enrollment via Company Portal
- Intune and W365 overview
- Implementing CIS Intune Polices

What is an Intune policy?

Intune policies are a set of rules and configurations that help manage and secure devices, apps, and data in an organization.

- **Device management:**
  Set rules for device settings, security, and compliance
- **App management:**
  Control app installation, permissions, and updates
- **Data protection:**
  Company data stays secure and compliant
- **Automates with Nerdio:**
  Nerdio helps apply and manage Intune policies across multiple tenants quickly and efficiently

Intune policy creation/update flow



DEVICE ENROLLMENT

macOS

iOS

android

Ubuntu

chromeOS

CREATE

ADD

DEPLOYMENT

ASSIGN

TARGET

Create policy
via Intune Portal

Update policy
via Intune Portal

Nerdio policies
Pre-canned & CIS

Github policies

Import/update

Group templates

Auto/manual

Policy baselines

Customer A

Customer B

Customer C

User group

Device group

User group

Device group

User group

Device group

iOS, Android device group

NERDIO GLOBAL MSP LEVEL

CUSTOMER ACCOUNT LEVEL

Nerdio user hierarchy global / MSP level end users

MSP/global level users

This is the parent level in Nerdio.

- Items created here can be cascaded into the customer account level (one-to-many).
  - E.g., Images, Scripts, Applications

Users created here are given permissions to manage customer accounts in Nerdio.

- E.g., users created here can create account-level users

Customer account level users

This is the child level in Nerdio.

- Items are inherited from the MSP level.
- Items created here are account-specific (one-to-one).
  - E.g., Auto-Scale configurations, application deployment policies.

Users created here are the end users within the customer environment.

- E.g., Users created here can log into session hosts.

NerdioCon 2025 PALM SPRINGS

Demo Time

Configuring Conditional Access in Intune

Conditional Access:

- is like a security gate for your organization's apps and data. It ensures that only the right people, using the right devices, under the right conditions, can access your resources.

Demo

I will show how to set up conditional access and the configurations that can be applied.

Solution baselines are like a starter kit for setting up cloud environments

Nerdio Manager for MSP has pre-made templates with all the important settings and configurations needed to quickly and consistently build Intune or Windows 365 environments for clients

Using a solution baseline helps MSPs to:

- Save time—No need to set up everything from scratch.
- Stay consistent—Make sure every client setup looks and works the same.
- Avoid mistakes—Follow proven settings and best practices.

In short, a solution baseline is a quick and reliable way to set up cloud environments without reinventing the wheel every time.

Demo time

NerdioCon
2025
PALM SPRINGS

Breaktime 20

Mobile Application Management

(MAM)

Secure access

Ensure secure access to corporate applications and data on personal devices without full device enrollment.

Data protection

Implement policies to prevent data leakage, control copy/paste functions, and manage data sharing between applications.

Compliance management

Enforce compliance requirements to keep devices and data secure while providing a seamless user experience.

Compliance policies for MDM

Bring company and BYOD devices up to compliance before allowing corporate data access

Compliance policies we'll create today:

- OS Version Compliance
- Jailbreak/Root Detection
- Strong Passcode (minimum length + complexity)
- Auto-lock after inactivity
- Wipe on failed attempts

Apple iOS Intune Enrollment

Pre-requisites

Demo

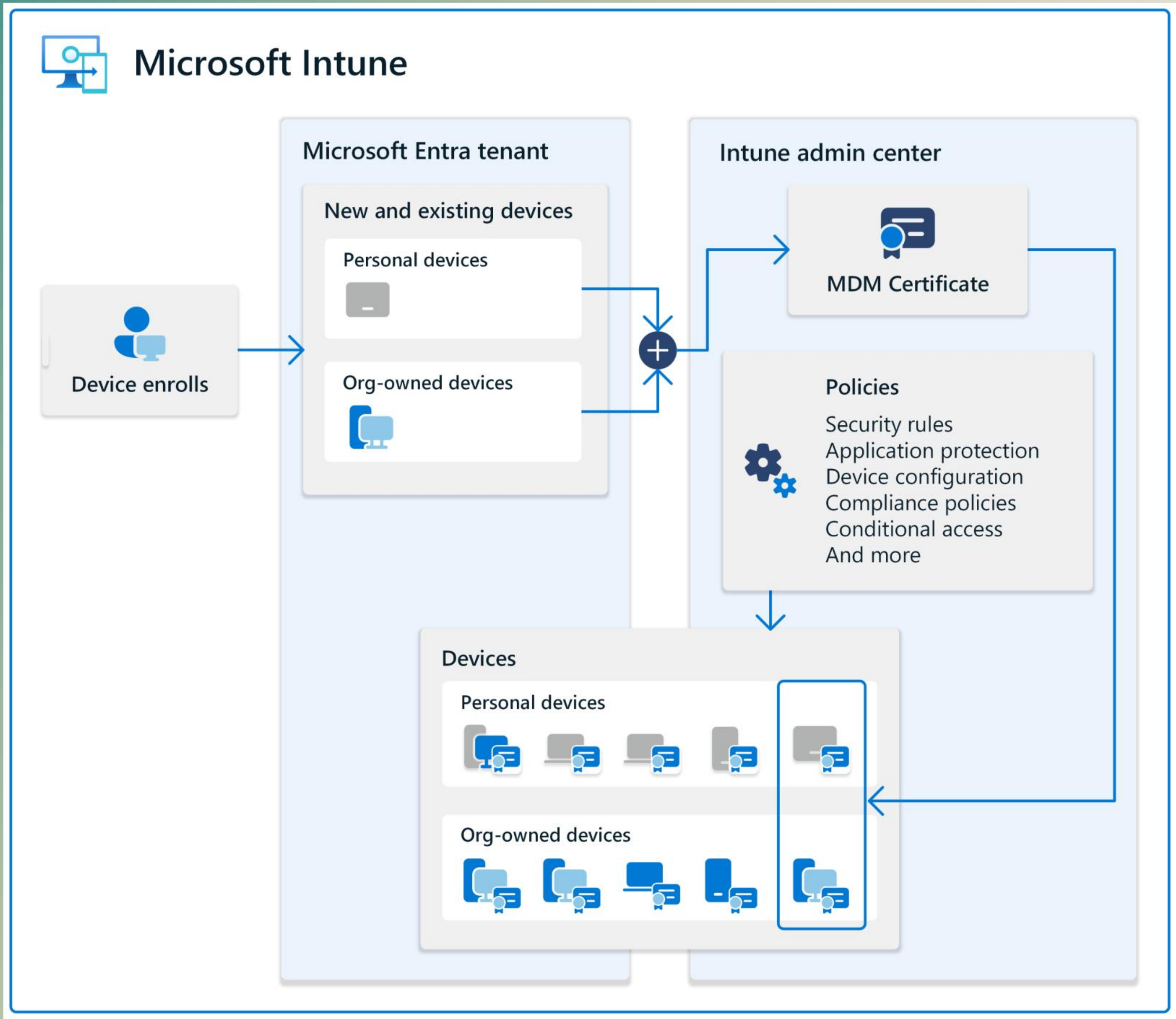
Grant Permissions: Agree to let Microsoft send user and device information to Apple.

1. Download CSR: Get the Certificate Signing Request (CSR) from Intune.

2. Create MDM Push Certificate: Use the Apple Push Certificates Portal to create the certificate with the downloaded CSR.

3. Upload and set up:
   - Enter Apple ID used to create the certificate.
   - Upload the MDM Push Certificate back to Intune.

Make sure to renew the certificate every year!!!


Microsoft Intune
Device enrolls
Microsoft Entra tenant
New and existing devices
Personal devices
Org-owned devices
Intune admin center
MDM Certificate
Policies
Security rules
Application protection
Device configuration
Compliance policies
Conditional access
And more
Devices
Personal devices
Org-owned devices

Creating App Protection & App Configuration policies

App Protection policy

1. Restrict copy/paste actions in the Microsoft Edge app.
2. Enforce data protection by allowing only managed app data transfers.

App Configuration policy

1. Managing data transfer between iOS apps in Intune.*

   **Only applies to iOS devices*

2. Reference Microsoft Intune iOS Data Transfer Guide.*

   **See the QR code*

BYOD device enrollment via Company Portal

1. Download the Company Portal app from the app store.
2. Log in with corporate credentials to start the enrollment process.
3. Follow the on-screen prompts to configure device settings.
4. Ensure our device complies with company security policies.
5. Complete the enrollment, then test the app protection and compliance policies.

NerdioCon 2025 PALM SPRINGS

Demo time

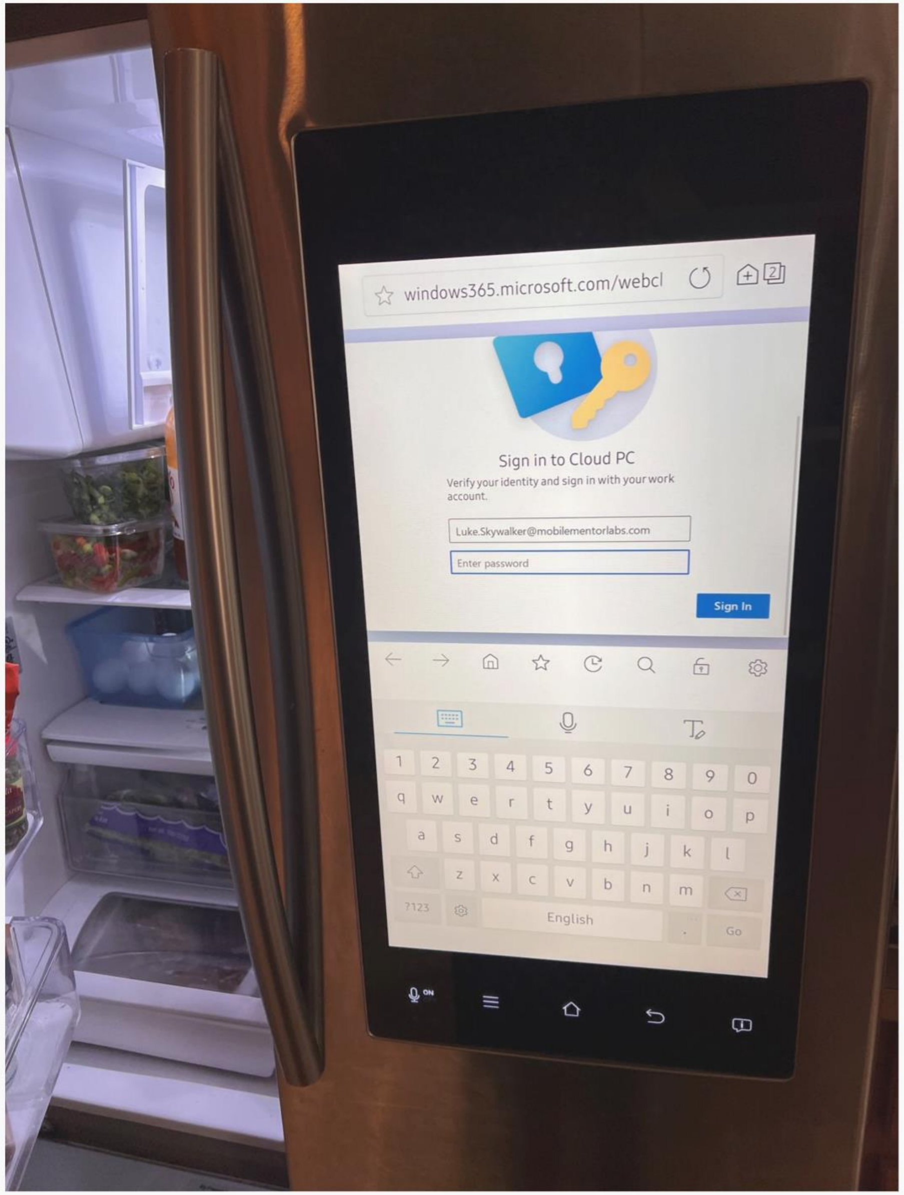
W365

What is W365?

- A Cloud PC: A full Windows experience streamed from the cloud.
- Accessible anywhere: Use on any device with an internet connection.
- IT managed: Secure, scalable, and managed via Intune.

Mission and vision

- **A Cloud PC** can be provisioned to any connected device…and when we say any connected device we mean it.
- This is my Samsung Smart Fridge running a cloud PC.
- And yes, it will run DOOM!



windows365.microsoft.com/webcl

Sign in to Cloud PC

Verify your identity and sign in with your work account.

Luke.Skywalker@mobilementorlabs.com

Enter password

CIS®

Center for Internet Security®

NerdioCon
2025
PALM SPRINGS

Strengthening security with Nerdio, Microsoft, and CIS

Mission and vision

Mission

Make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.

Vision

Leading the global community to secure our ever-changing connected world.

Creating Confidence in the Connected World™

About the Center for Internet Security (CIS)

Independent and trusted

Proven and effective

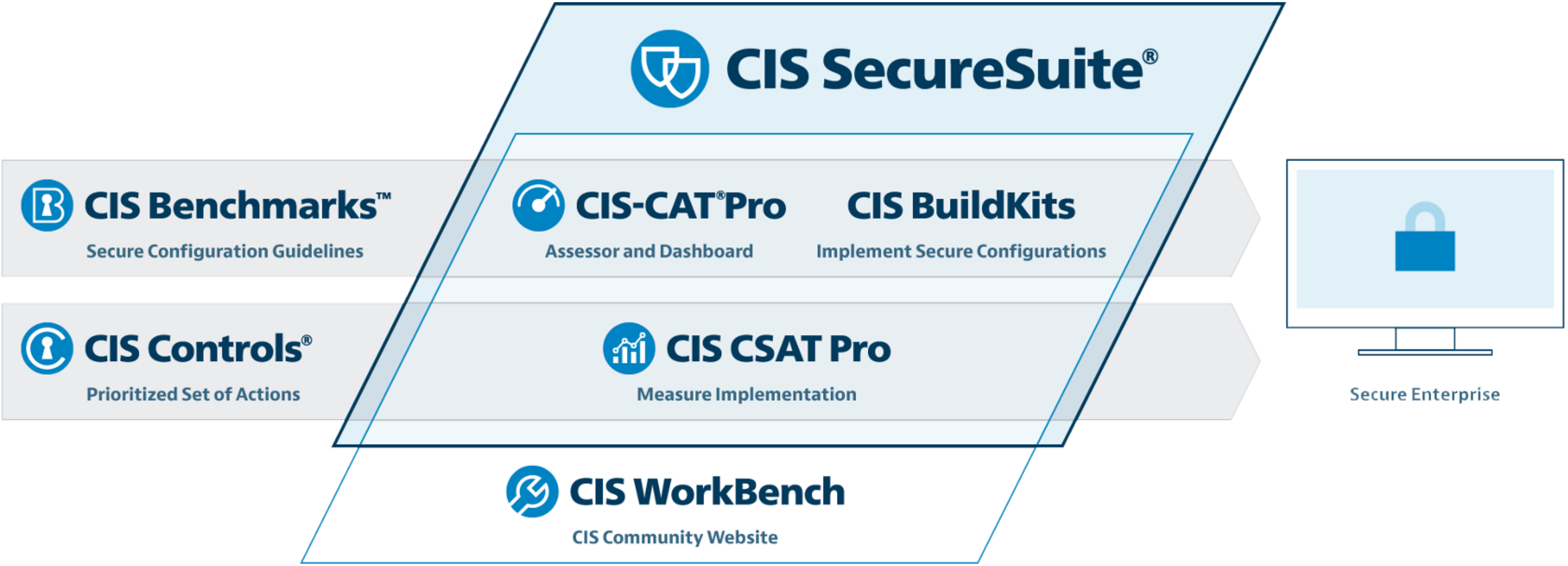
Collaboration

Operational expertise

Sustainable

CIS tools and resources

Integrated Cybersecurity resources



CIS SecureSuite®

CIS Benchmarks™
Secure Configuration Guidelines

CIS-CAT®Pro
Assessor and Dashboard

CIS BuildKits
Implement Secure Configurations

CIS Controls®
Prioritized Set of Actions

CIS CSAT Pro
Measure Implementation

Secure Enterprise

CIS WorkBench
CIS Community Website

Start Secure. Stay Secure.®

CIS Security best practices

Preventative cybersecurity resources

CIS Benchmarks™

Consensus-developed secure configuration guidelines for hardening

CIS Controls®

Prescriptive, prioritized, and simplified cybersecurity best practices

CIS Controls Version 8.1

18 Top-Level Best Practices Containing 153 Prioritized Safeguards

CONTROL		Safeguards	IG1	IG2	IG3
01	Inventory and Control of Enterprise Assets	5	2/5	4/5	5/5
02	Inventory and Control of Software Assets	7	3/7	6/7	7/7
03	Data Protection	14	6/14	12/14	14/14
04	Secure Configuration of Enterprise Assets and Software	12	7/12	11/12	12/12
05	Account Management	6	4/6	6/6	6/6
06	Access Control Management	8	5/8	7/8	8/8
07	Continuous Vulnerability Management	7	4/7	7/7	7/7
08	Audit Log Management	12	3/12	11/12	12/12
09	Email and Web Browser Protections	7	2/7	6/7	7/7
10	Malware Defenses	7	3/7	7/7	7/7
11	Data Recovery	5	4/5	5/5	5/5
12	Network Infrastructure Management	8	1/8	7/8	8/8
13	Network Monitoring and Defense	11	0/11	6/11	11/11
14	Security Awareness and Skills Training	9	8/9	9/9	9/9
15	Service Provider Management	7	1/7	4/7	7/7
16	Applications Software Security	14	0/14	11/14	14/14
17	Incident Response Management	9	3/9	8/9	9/9
18	Penetration Testing	5	0/5	3/5	5/5

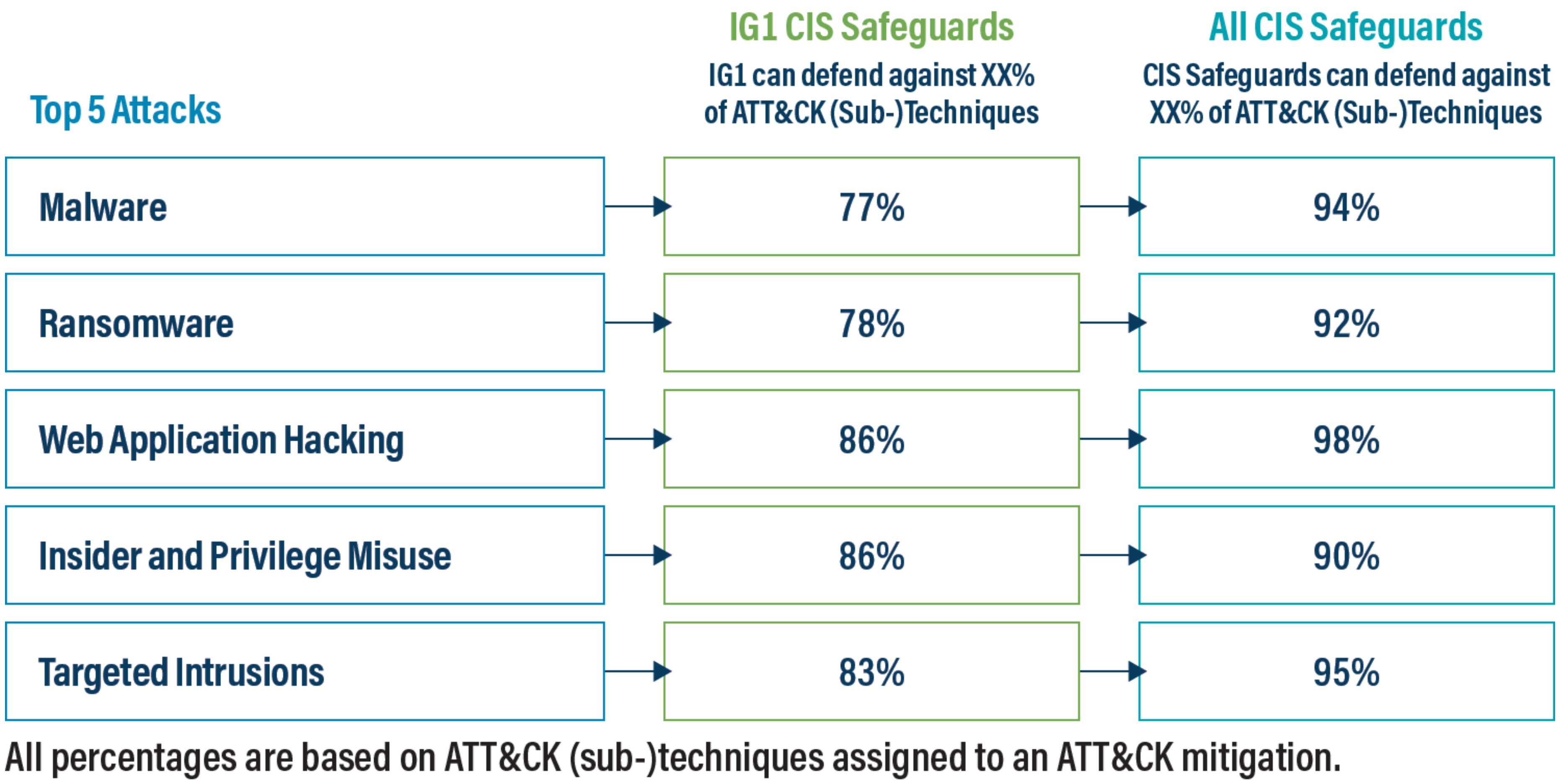
CIS Controls

ESSENTIAL CYBER HYGIENE
IG1
IG2
IG3

- IG1–Essential Cyber Hygiene
- IG2–Moderate resources and expertise
- IG3–Significant resources and expertise

Community Defense Model (CDM) v2.0

MITRE ATT&CK mitigation



Top 5 Attacks	IG1 CIS Safeguards IG1 can defend against XX% of ATT&CK (Sub-)Techniques	All CIS Safeguards CIS Safeguards can defend against XX% of ATT&CK (Sub-)Techniques
Malware	77%	94%
Ransomware	78%	92%
Web Application Hacking	86%	98%
Insider and Privilege Misuse	86%	90%
Targeted Intrusions	83%	95%

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

CDM 2.0 Attack Types & Data Sources

Attack types

1. Malware (moved up in rank vs. CDM v1.0)
2. Ransomware (moved up in rank)
3. Web Application Tracking (moved down in rank)
4. Insider and Privilege Misuse (moved down in rank
5. Targeted Intrusions (rank remained the same)

Data sources

- Verizon Data Breach Investigations Report (DBIR)
- IBM X-Force Threat Intelligence Index
- ENISA Threat Landscape–The Year in Review
- CrowdStrike Services Cyber Front Lines report
- Akamai The State of the Internet: A Year in Review

Foundations for compliance

CIS takes a collaborative approach to compliance by developing resources that work well with existing security frameworks.

Frameworks Provided with CIS Controls Mapping

- Australian Signals Directorate Essential Eight
- CISA Cybersecurity Performance Goals (CPGs)
- CMMC
- Criminal Justice Information Services (CJIS)
- CSA Cloud Controls Matrix v4
- Cyber Risk Institute (CRI) Profile v1.2
- FFIEC-CAT
- GSMA FS 31 Baseline Security Controls
- HIPAA
- ISACA COBIT 19
- ISO 27001:2022
- ISO/IEC 27002:2022
- Microsoft Cloud Security Benchmark
- MITRE ATT&CK v8.2
- NERC-CIP
- New Zealand Information Security Manual v3.5
- NIST CSF 1.0
- NIST CSF 2.0
- NIST SP 800-53 R5
- NIST SP 800-171
- PCI DSS
- NYS Department of Financial Services 23 NYCRR Part 500
- SOC 2
- TSA Security Defense Directive Pipeline
- UK Cyber Essentials
- UK National Cyber Security Centre (NCSC) Cyber Assessment v3.1

Industry Frameworks Referencing CIS Benchmarks

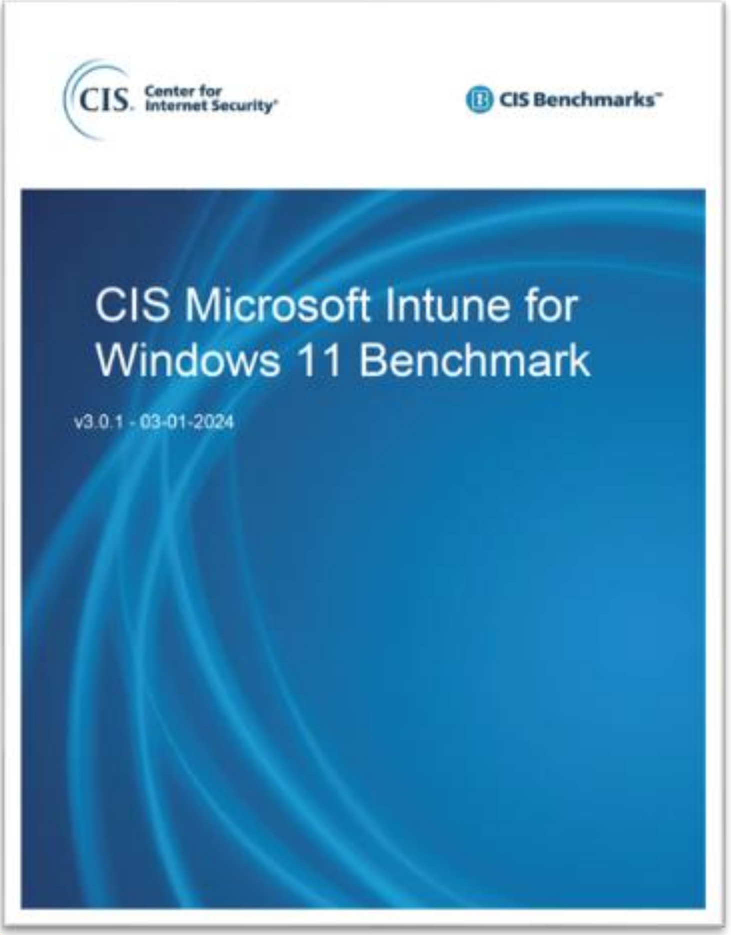
- DoD Cloud Computing SRG
- FedRAMP
- FFIEC
- FISMA
- PCI DSS

CIS Benchmarks

Consensus-developed secure configuration guidelines

- More than 100 CIS Benchmarks across 25+ vendor product families
- Recognized by industry frameworks
  - DoD Cloud Computing SRG, FISMA, FedRAMP, PCI DSS
- Community-developed
  - CIS members, subject matter experts, security community experts, technology vendors
- Prescriptive instruction
  - Step-by-step list to apply configurations
  - Rationale on “why” the configuration is recommended
  - Impact the configuration will make
- Mapped to CIS Controls

CIS Benchmarks™



CIS. Center for Internet Security®

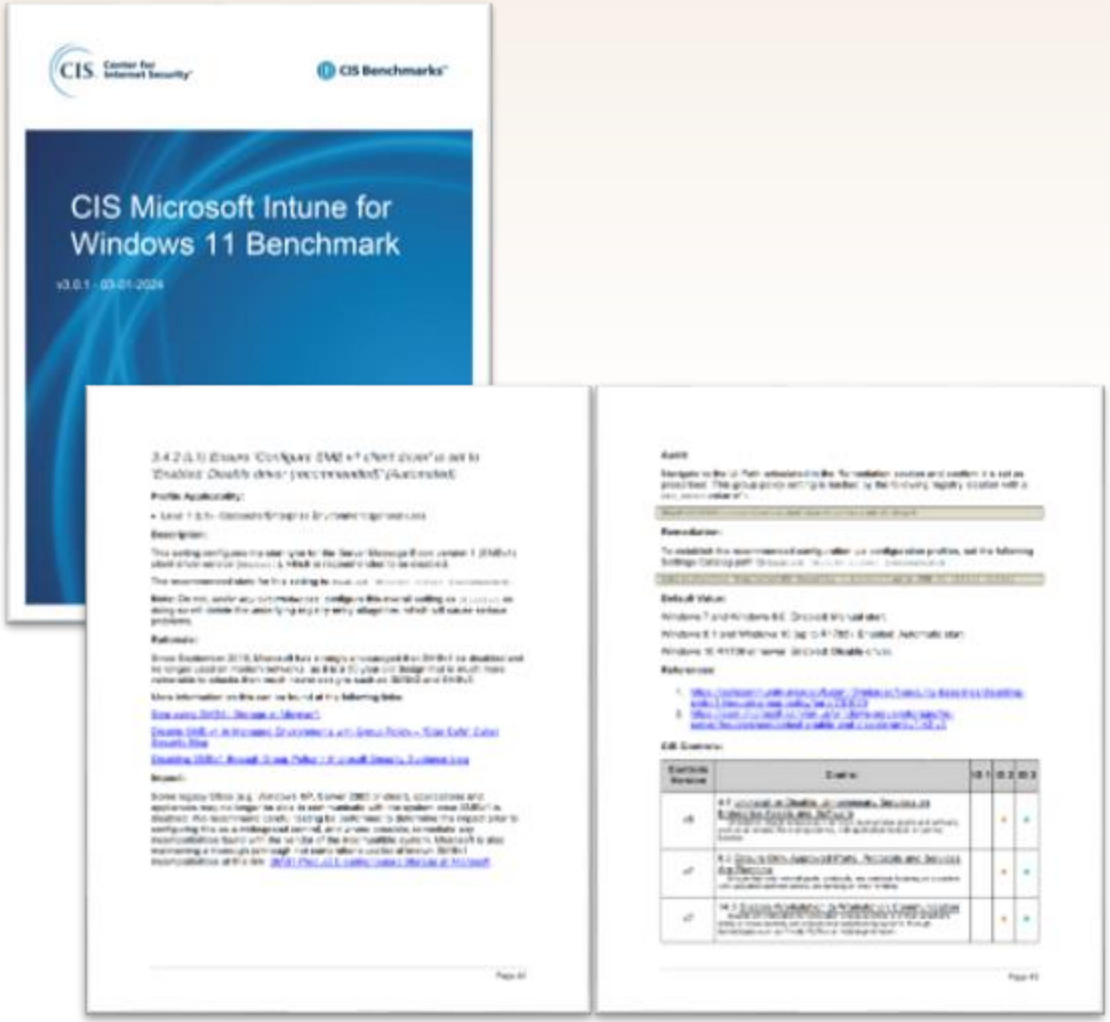
CIS Benchmarks™

CIS Microsoft Intune for Windows 11 Benchmark

v3.0.1 - 03-01-2024

Nerdio Manager CIS Baselines=CIS Benchmarks

- CIS Baselines in Nerdio Manager
  - Windows 10
  - Windows 11
- Single session VMs
- Multi-session VMs
- CIS Hardened Images
- Anatomy of a CIS Benchmark
  - **Description** provides understanding into related best practices
  - **Rationale** provides detail on the security value
  - **Audit** provides clear steps to assess implementation
  - **Remediation** provides clear steps to configure the setting
  - **References** to applicable vulnerabilities, documentation, implementation, etc.
  - CIS Controls Mappings included in all CIS Benchmarks
    - Demonstrate how the CIS Benchmark recommendation applies to the CIS Controls Safeguard



CIS Center for Internet Security

CIS Benchmarks

CIS Microsoft Intune for Windows 11 Benchmark

v3.0.1 - 03-01-2024

CIS Benchmarks profiles

LEVEL 1

- Base recommendation, non-performance impacting
- General corporate/enterprise environment usage
- Ensures functionality remains unaffected

LEVEL 2

- Extends Level 1 settings
- For high-security or sensitive data environments
- More strict security controls
- May impact useability

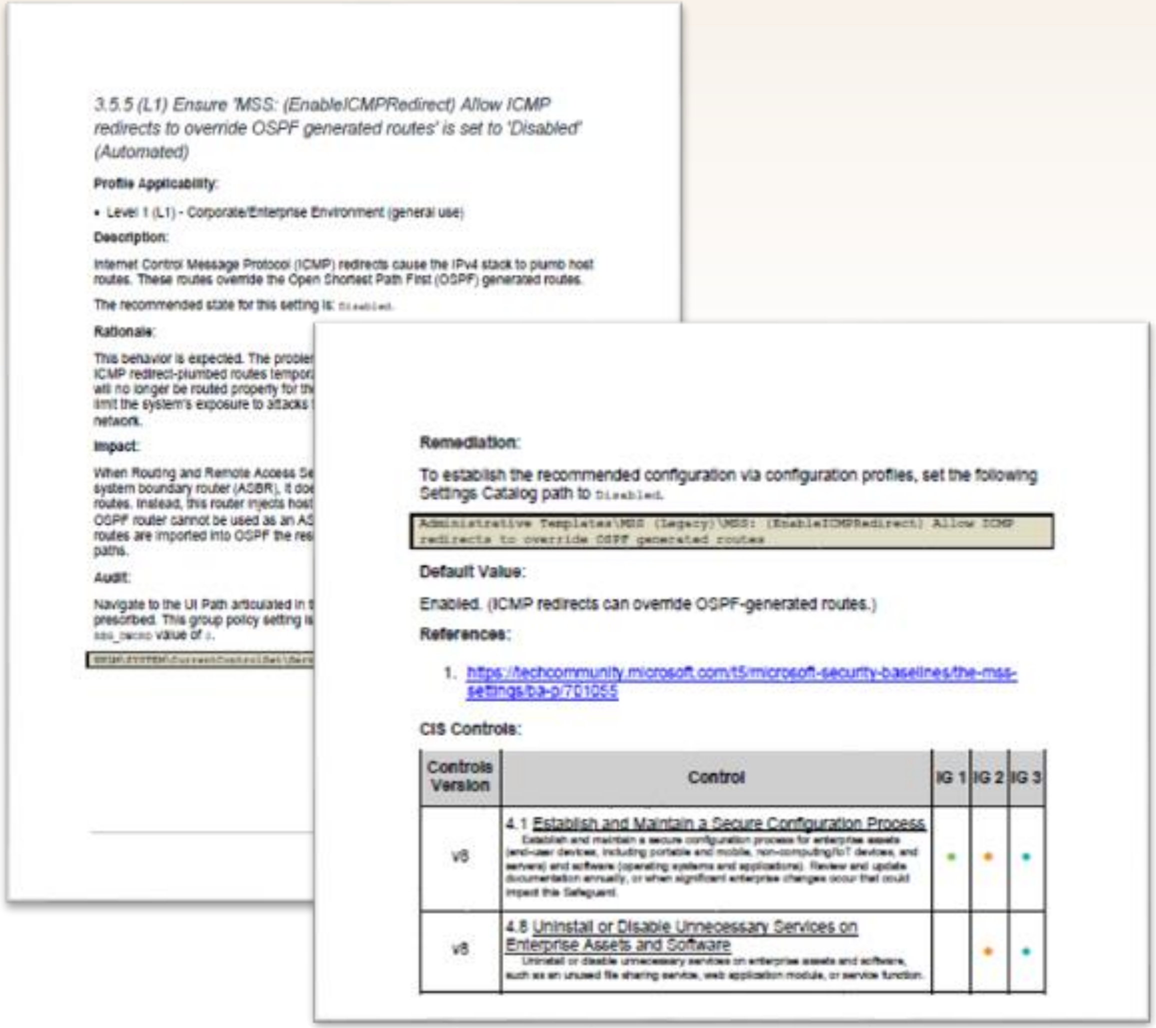
LEVEL 3

- Used primarily by government agencies, DOD agencies, highly regulated industries

Nerdio CIS Baselines in Nerdio Manager

Nerdio CIS Baselines

- Industry recognized security benchmarks for Windows, Azure, and Intune configurations
- Protection against common threats
- Detailed, actionable, security settings apps and devices per CIS Benchmarks
- Configured to align with best practices for security and compliance frameworks like NIST, HIPAA, ISO 27001, and GDPR
- Consistent configuration for deployment and management available through Nerdio Manager



3.5.5 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Internet Control Message Protocol (ICMP) redirects cause the IPv4 stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) generated routes.

The recommended state for this setting is: `Disabled`.

Rationale:

This behavior is expected. The probler
ICMP redirect-plumbed routes tempor
will no longer be routed properly for th
limit the system's exposure to attacks
network.

Impact:

When Routing and Remote Access Se
system boundary router (ASBR), it doe
routes. Instead, this router injects host
OSPF router cannot be used as an AS
routes are imported into OSPF the res
paths.

Audit:

Navigate to the UI Path articulated in t
prescribed. This group policy setting is
`[illegible]` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Servi
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Administrative Templates\MSS (Legacy)\MSS: (EnableICMPRedirect) Allow ICMP
redirects to override OSPF generated routes
```

Default Value:

Enabled. (ICMP redirects can override OSPF-generated routes.)

References:

1. https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

NerdioCon 2025 PALM SPRINGS

Implementing CIS Intune

DEMO

1. Select CIS Baselines: Choose CIS Policy Baselines from the dropdown, then pick Windows 10 or Windows 11.

2. Assign to customers: Apply the selected baseline to the relevant customer accounts.

Standardized environment– Why does it matter?

- MSPs, MSSPs, ISVs, VARs
- Reduces risk of misconfigurations
  - 74% of breaches include the human element
    - Either via Error, Privilege Misuse, Use of Stolen Credentials, or Social Engineering
      - Source: 2023 Verizon DBIR
  - Breaches caused by cloud misconfigurations:
    - Took 244 days to identify and contain
    - Cost an average of $3.98M
      - Source: 2024 IBM Security Cost of a Data Breach Report
- Predictable results
- Enhances trust

NerdioCon
2025
PALM SPRINGS

Test time!!

1. Scan the QR code to the right or open the short link in a browser.
2. Pass the exam.
3. 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_Intune_Mastery

NerdioCon 2025

PALM SPRINGS

Get in touch!

Rolando Jimenez

rjimenez@getnerdio.com

www.getnerdio.com

NOTICE TO ALL PUBLIC SECTOR OR STATE-OWNED ENTITY EMPLOYEES – Federal [including Military], State, Local and Public Education. This is a Microsoft partner event. Should items of value (e.g. food, promotional items) be disbursed to event participants, these items will be available at no charge to attendees. Please check with your ethics policies before accepting items of value.

nerdio

NerdioCon

2025

PALM SPRINGS

Thank you!

nerdio