NerdioCon

2025

PALM SPRINGS

NerdioCon
2025
PALM SPRINGS

Securing AVD, windows 365, and intune endpoints with CIS + Nerdio. You’re welcome. 🎤

Sheldon Turner

Sr. Director Technical Strategy and Assessment

Tony Cai

Sr. Director, MSP Product

NerdioCon
2025
PALM SPRINGS

Who is CIS?

(The Center for Internet Security)

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 Security best practices

Preventative Cybersecurity Resources

CIS Benchmarks™

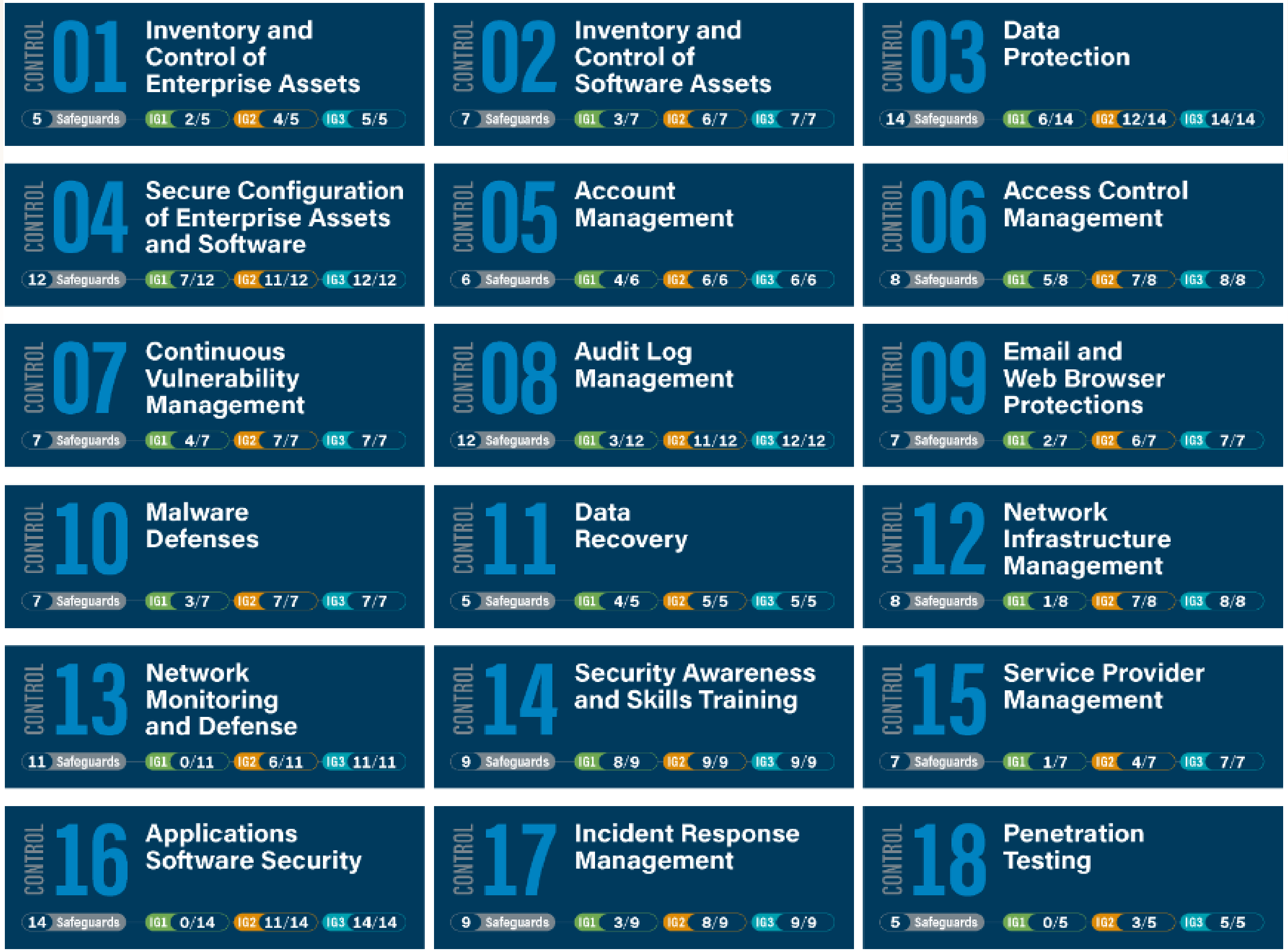
Consensus-developed secure configuration guidelines for hardening

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

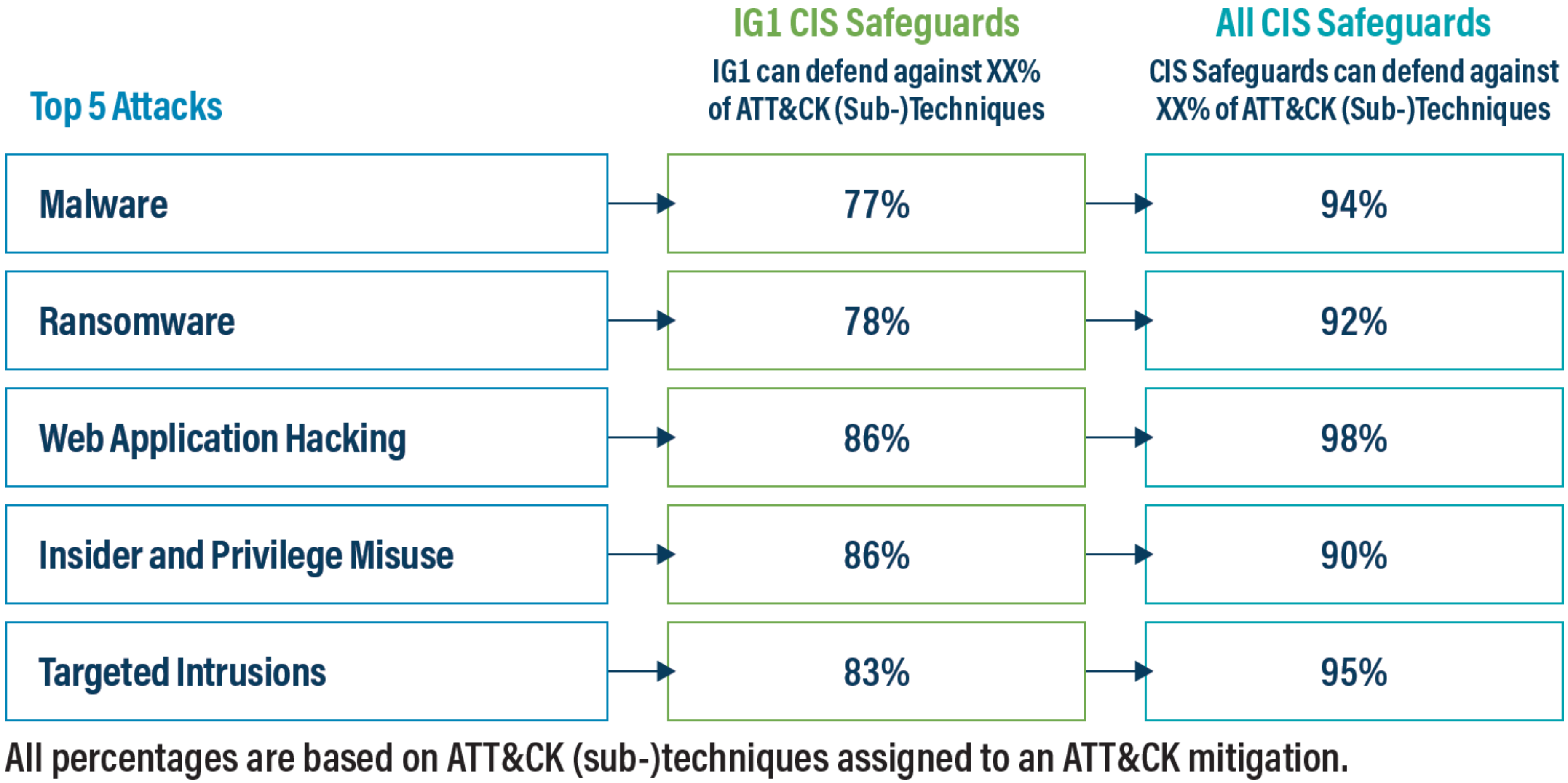
CIS Controls

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.

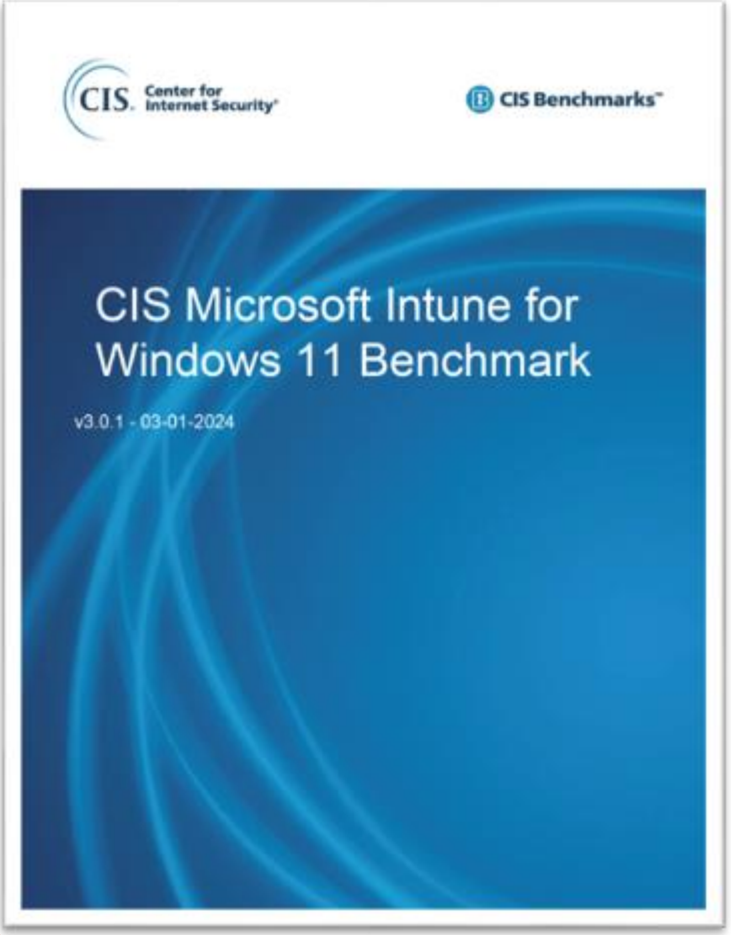
https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

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

Why did Nerdio and CIS partner?

- CIS is highly respected globally when it comes to defining security.
- Nerdio is an innovative organization that helps to build successful cloud practices with Microsoft.
- Compliance Frameworks align to Controls and Benchmarks.
- The partnership can help our customers reduce attack surface and achieve compliance in an easy manner.

Foundations for compliance

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

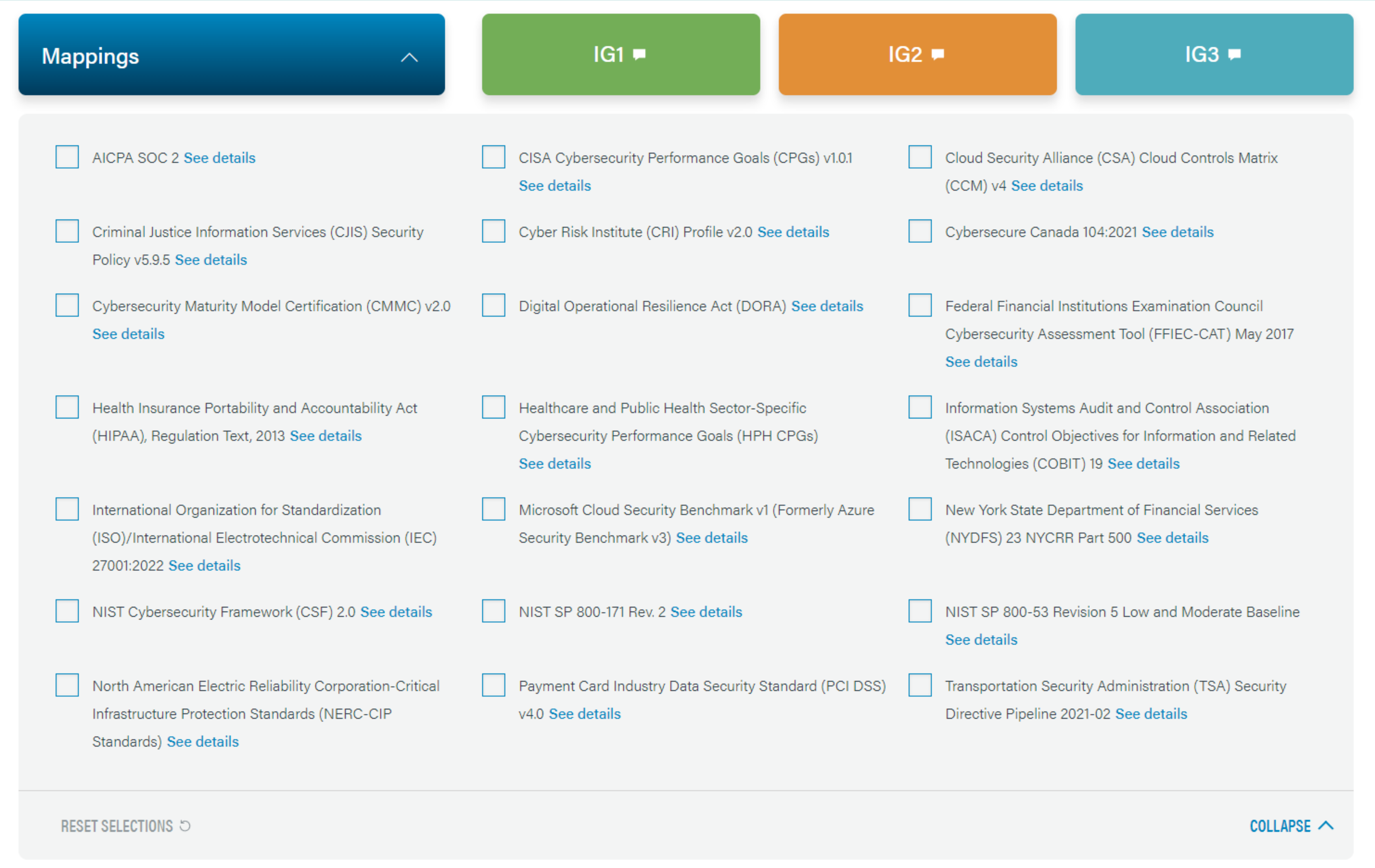
Frameworks Provided with CIS Controls Mapping

- 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 Controls Navigator v 8.1



- □ AICPA SOC 2 See details
- □ CISA Cybersecurity Performance Goals (CPGs) v1.0.1 See details
- □ Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v4 See details
- □ Criminal Justice Information Services (CJIS) Security Policy v5.9.5 See details
- □ Cyber Risk Institute (CRI) Profile v2.0 See details
- □ Cybersecure Canada 104:2021 See details
- □ Cybersecurity Maturity Model Certification (CMMC) v2.0 See details
- □ Digital Operational Resilience Act (DORA) See details
- □ Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC-CAT) May 2017 See details
- □ Health Insurance Portability and Accountability Act (HIPAA), Regulation Text, 2013 See details
- □ Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals (HPH CPGs) See details
- □ Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technologies (COBIT) 19 See details
- □ International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2022 See details
- □ Microsoft Cloud Security Benchmark v1 (Formerly Azure Security Benchmark v3) See details
- □ New York State Department of Financial Services (NYDFS) 23 NYCRR Part 500 See details
- □ NIST Cybersecurity Framework (CSF) 2.0 See details
- □ NIST SP 800-171 Rev. 2 See details
- □ NIST SP 800-53 Revision 5 Low and Moderate Baseline See details
- □ North American Electric Reliability Corporation-Critical Infrastructure Protection Standards (NERC-CIP Standards) See details
- □ Payment Card Industry Data Security Standard (PCI DSS) v4.0 See details
- □ Transportation Security Administration (TSA) Security Directive Pipeline 2021-02 See details

The shared responsibility model

How CIS resources help you meet those responsibilities

Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS	CIS Controls Cloud Companion Guide	CIS Foundations Benchmarks	CIS Hardened Images
Data classification and accountability	🟠	🟠	🟠	🟠	🟠	✓	✓	
Client and end-point protection	🟠	🟠	🟠	🟠🔵	🟠🔵	✓	✓	✓
Identity and access management	🟠	🟠	🟠🔵	🟠🔵	🟠🔵	✓	✓	✓
Application-level controls	🟠	🟠	🟠🔵	🟠🔵	🟠🔵	✓	✓	✓
Network controls	🟠	🟠🔵	🔵	🔵	🔵	✓	✓	✓
Host infrastructure	🟠	🟠🔵	🔵	🔵	🔵	✓		✓
Physical security	🟠	🔵	🔵	🔵	🔵			

🟠 Cloud Customer 🔵 Cloud Provider

Sources

1 Microsoft Azure, https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility.

2 Amazon Web Services, https://aws.amazon.com/compliance/shared-responsibility-model.

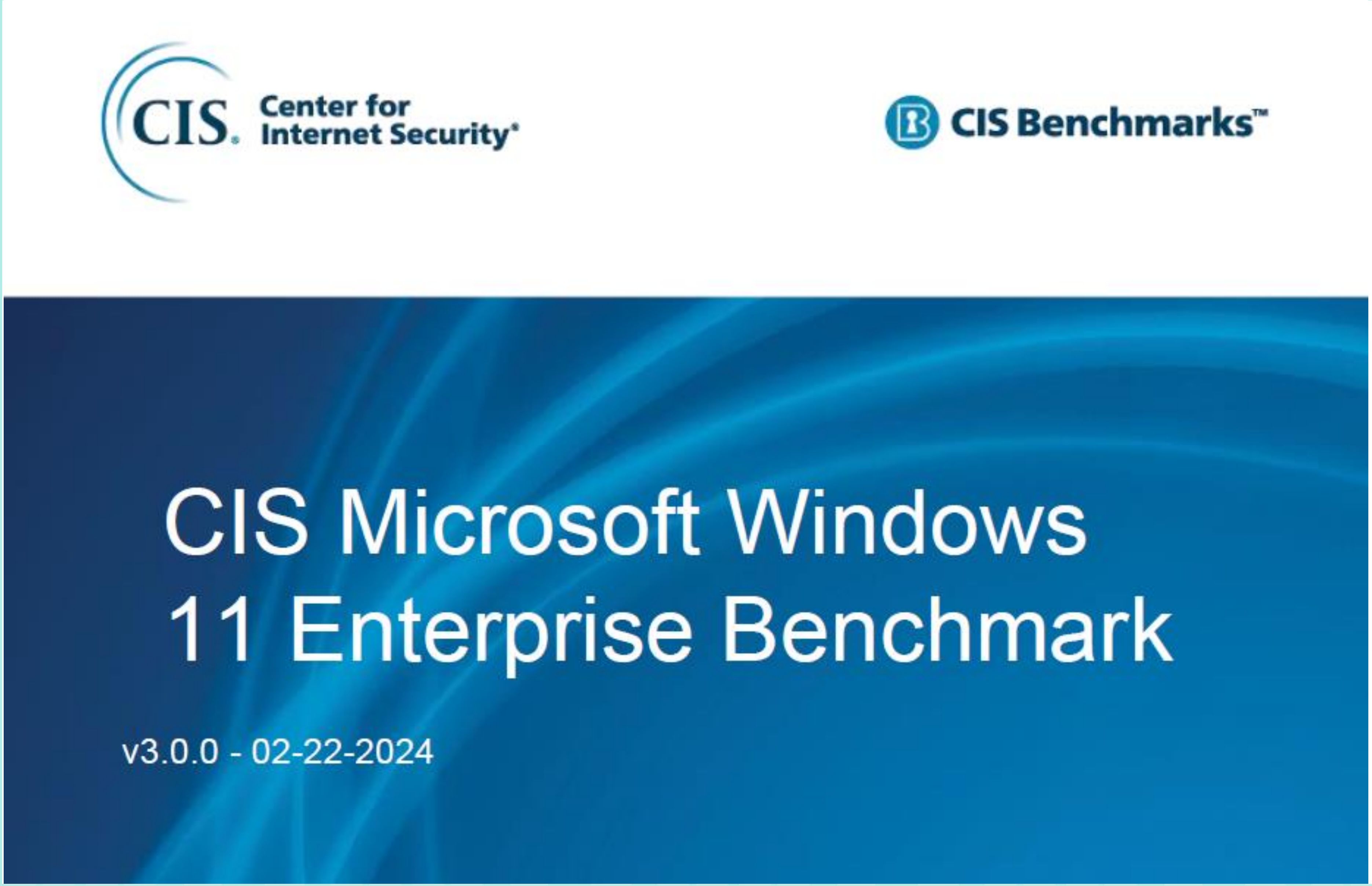
Problems IT Admins encounter

- 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 Ancible, Chef, IaC knowledge



CIS. Center for Internet Security®

CIS Benchmarks™

CIS Microsoft Windows 11 Enterprise Benchmark

v3.0.0 - 02-22-2024

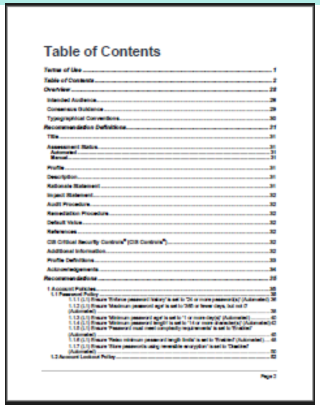
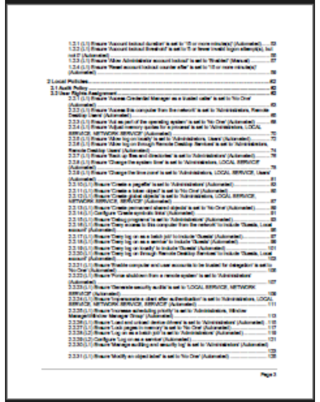
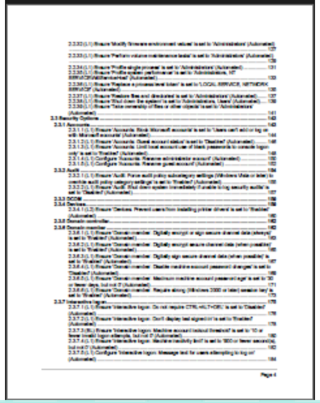
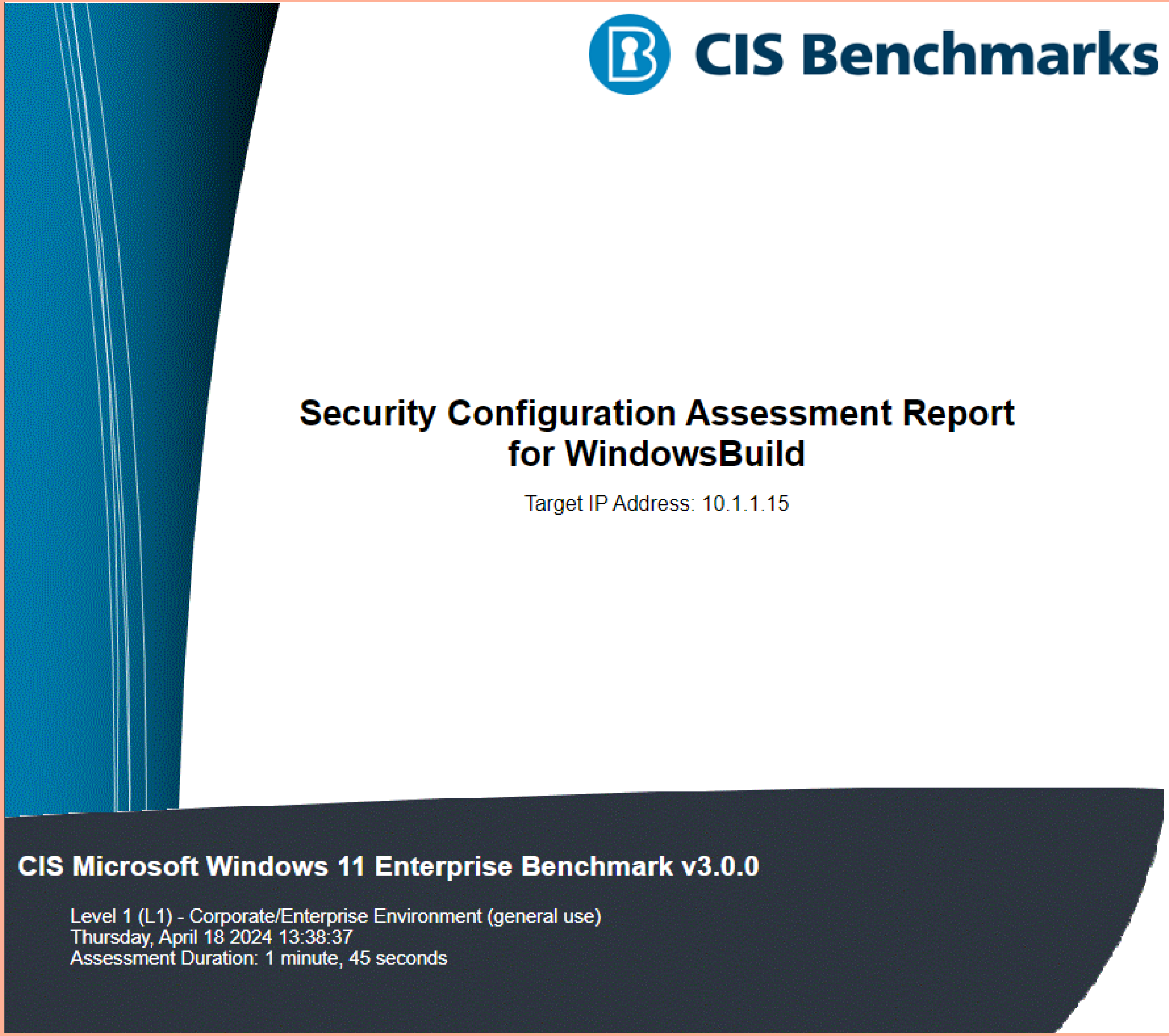


Table of Contents

Page 2







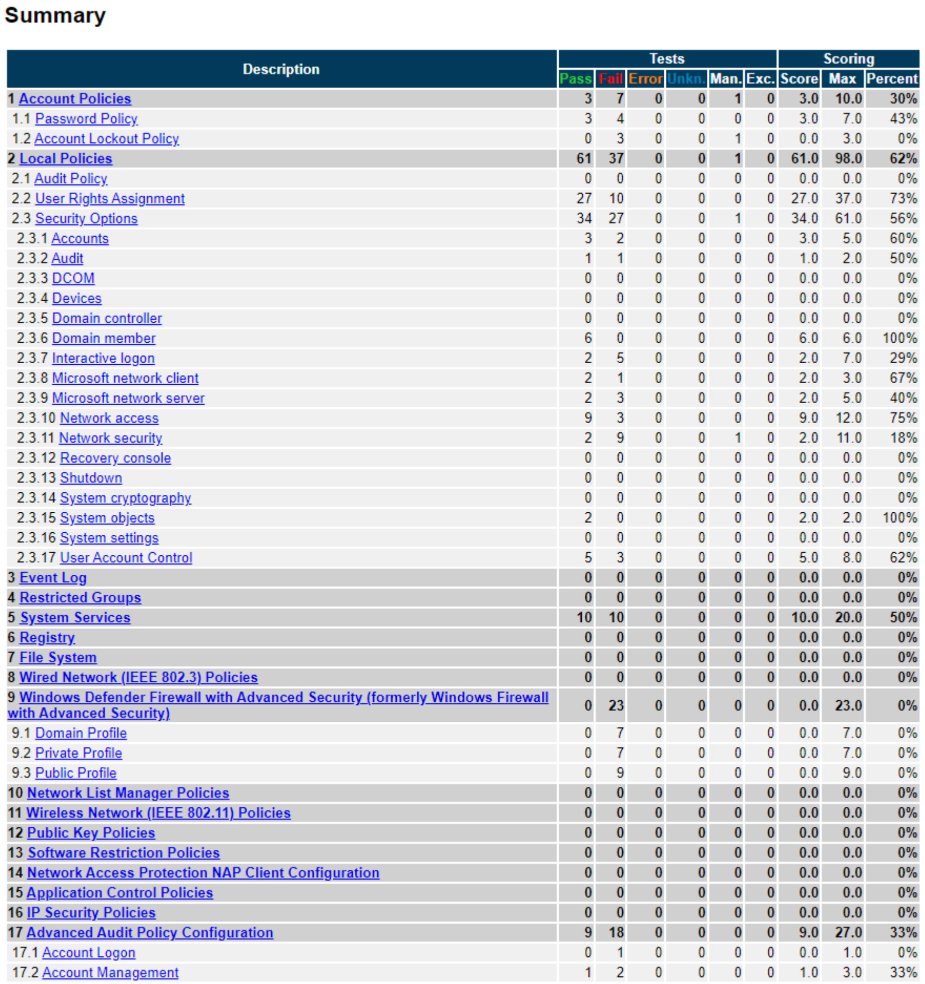
CIS Benchmarks

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	Unkn.	Man.	Exc.	Score	Max	Percent
1 Account Policies	**3**	**7**	**0**	**0**	**1**	**0**	**3.0**	**10.0**	**30%**
1.1 Password Policy	3	4	0	0	0	0	3.0	7.0	43%
1.2 Account Lockout Policy	0	3	0	0	1	0	0.0	3.0	0%
2 Local Policies	**61**	**37**	**0**	**0**	**1**	**0**	**61.0**	**98.0**	**62%**
2.1 Audit Policy	0	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	27	10	0	0	0	0	27.0	37.0	73%
2.3 Security Options	34	27	0	0	1	0	34.0	61.0	56%
2.3.1 Accounts	3	2	0	0	0	0	3.0	5.0	60%
2.3.2 Audit	1	1	0	0	0	0	1.0	2.0	50%
2.3.3 DCOM	0	0	0	0	0	0	0.0	0.0	0%
2.3.4 Devices	0	0	0	0	0	0	0.0	0.0	0%
2.3.5 Domain controller	0	0	0	0	0	0	0.0	0.0	0%
2.3.6 Domain member	6	0	0	0	0	0	6.0	6.0	100%
2.3.7 Interactive logon	2	5	0	0	0	0	2.0	7.0	29%
2.3.8 Microsoft network client	2	1	0	0	0	0	2.0	3.0	67%
2.3.9 Microsoft network server	2	3	0	0	0	0	2.0	5.0	40%
2.3.10 Network access	9	3	0	0	0	0	9.0	12.0	75%
2.3.11 Network security	2	9	0	0	1	0	2.0	11.0	18%
2.3.12 Recovery console	0	0	0	0	0	0	0.0	0.0	0%
2.3.13 Shutdown	0	0	0	0	0	0	0.0	0.0	0%
2.3.14 System cryptography	0	0	0	0	0	0	0.0	0.0	0%
2.3.15 System objects	2	0	0	0	0	0	2.0	2.0	100%
2.3.16 System settings	0	0	0	0	0	0	0.0	0.0	0%
2.3.17 User Account Control	5	3	0	0	0	0	5.0	8.0	62%
3 Event Log	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
4 Restricted Groups	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
5 System Services	**10**	**10**	**0**	**0**	**0**	**0**	**10.0**	**20.0**	**50%**
6 Registry	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
7 File System	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
8 Wired Network (IEEE 802.3) Policies	**0**	**0**	**0**	**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**	**0.0**	**23.0**	**0%**
9.1 Domain Profile	0	7	0	0	0	0	0.0	7.0	0%
9.2 Private Profile	0	7	0	0	0	0	0.0	7.0	0%
9.3 Public Profile	0	9	0	0	0	0	0.0	9.0	0%
10 Network List Manager Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
11 Wireless Network (IEEE 802.11) Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
12 Public Key Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
13 Software Restriction Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
14 Network Access Protection NAP Client Configuration	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
15 Application Control Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
16 IP Security Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
17 Advanced Audit Policy Configuration	**9**	**18**	**0**	**0**	**0**	**0**	**9.0**	**27.0**	**33%**
17.1 Account Logon	0	1	0	0	0	0	0.0	1.0	0%
17.2 Account Management	1	2	0	0	0	0	1.0	3.0	33%

CIS Benchmarks profiles

LEVEL 1

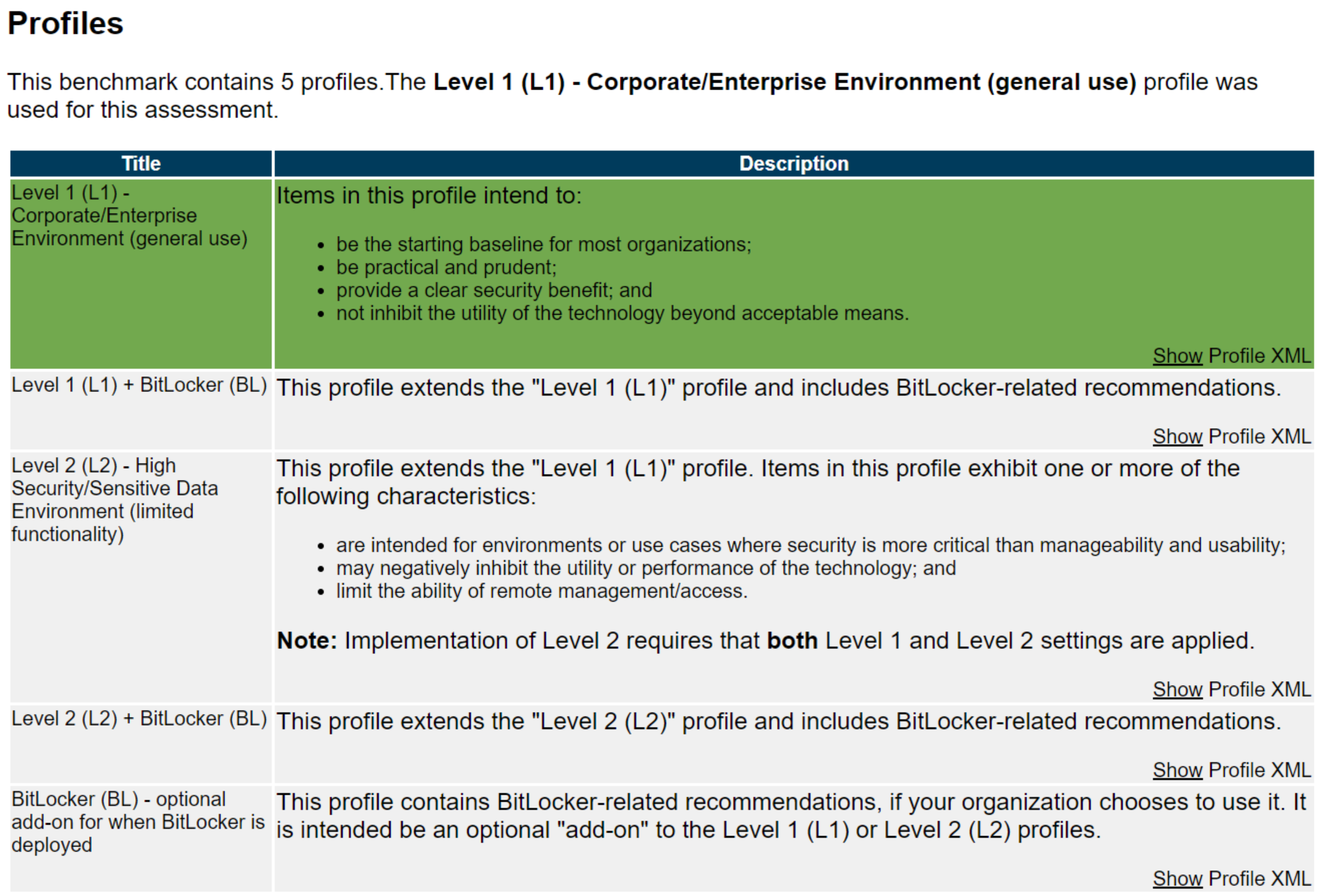
- Base recommendation, non-performance impacting
- General corporate/enterprise environment usage
- Ensures functionality remains unaffected

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



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)	Items in this profile intend to: • 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. Show Profile XML
Level 1 (L1) + BitLocker (BL)	This profile extends the "Level 1 (L1)" profile and includes BitLocker-related recommendations. Show Profile XML
Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)	This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the following characteristics: • 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. **Note:** Implementation of Level 2 requires that **both** Level 1 and Level 2 settings are applied. Show Profile XML
Level 2 (L2) + BitLocker (BL)	This profile extends the "Level 2 (L2)" profile and includes BitLocker-related recommendations. Show Profile XML
BitLocker (BL) - optional add-on for when BitLocker is deployed	This profile contains BitLocker-related recommendations, if your organization chooses to use it. It is intended be an optional "add-on" to the Level 1 (L1) or Level 2 (L2) profiles. Show Profile XML

NerdioCon

2025

PALM SPRINGS

nerdio

CIS Center for Internet Security®

Creating Confidence in the Connected World.™

We've made a Windows 11 Multi-session CIS Hardened Image for the world to use but what's the *NERDIO* advantage?

What’s the Nerdio special sauce?

🎇 When you use CIS Hardened Images with Nerdio, we can do "in-place patches" of CIS Benchmarks as they are released which means you don't have to go and redo you image every time there is a change in Benchmarks! 🎇

Value:

1. Tremendous time saved from not needing to rebuild images
2. Integrated to DevOps Pipeline for Image updates
3. Faster user acceptance testing/security testing
4. Re-image session hosts much quicker with latest updates
5. CIS HIs gets you to CMMC, HIPAA, PCI-DSS, FedRAMP +

CIS Hardened Image cost

	Old pricing	New pricing (April 2025)
Azure VM vCPU 1 Core	$0.0225	$0.010
Azure VM vCPU 2 Cores	$0.0225	$0.010
Azure VM vCPU 4 Cores	$0.0225	$0.020
Azure VM vCPU 8 Cores	$0.0225	$0.025
Azure VM vCPU 12 Cores	$0.0225	$0.030
Azure VM vCPU 16 Cores	$0.0225	$0.035
Azure VM vCPU 20 Cores	$0.0225	$0.045
Azure VM vCPU 32 Cores	$0.0225	$0.050
Azure VM vCPU 48 Cores	$0.0225	$0.055
Azure VM vCPU 64 Cores	$0.0225	$0.060

NerdioCon 2025 PALM SPRINGS

Demo of CIS Hardened Images

How to position CIS Hardened Images

- $0.01-$0.02 an hour-$4 a month per session host (auto-scaled for 50 hours) or $7-$16 a month if running (24/7), often time comes out to be less than $1/user

- During image setup, educate and spend time talking about the benefits of Hardened Images

- If the customer belongs in a compliance driven industry, ask if they need evidence of compliance. Each HI comes with CIS-CAT report that shows how close they are to CIS Benchmarks

- Assume they need this, because they should. No longer a nice to have. ~23% to 97% compliant

NerdioCon
2025
PALM SPRINGS

nerdio

CIS Center for Internet Security®
Creating Confidence in the Connected World.™

Not just Hardened Images! What about physical endpoints?

Nerdio CIS Policy Baselines for Intune

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—using FREE, 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 +

Nerdio's CIS partnership

Hardened Images

- ✓ For AVD Hosts/Images/Servers
- ✓ $.010 – $.025 per hour per VM additional cost ($7-$16/month or $2-$4/month if Autoscale ~50 hours)
- ✓ "Easiest" button
  - ✓ Deploy from marketplace
  - ✓ Billed through Azure
  - ✓ Instant CIS compliance

Intune Policy Baselines

- ✓ Endpoint hardening
  - ✓ Intune and Powershell delivered
- ✓ Nerdio exclusive in-product baselines
- ✓ Can take a "Vanilla" Windows deployment from 24% compliant to 97% compliant with just policies
- ✓ No extra cost in Nerdio Manager
- ✓ Official and Certified from CIS

Future releases

- ✓ Baselines for other OS(s)
  - ✓ MacOS for endpoint
  - ✓ iOS, iPadOS
  - ✓ Android
  - ✓ MS Office
- ✓ CIS-CAT integration
- ✓ CIS Benchmark updates

NerdioCon 2025 PALM SPRINGS

Let's collaborate

- **Partnering with CIS can help you:**
  - Strengthen your security offerings to protect clients and streamline compliance
  - Reduce risk and meet industry regulation
  - Secure cloud environments using Hardened Images and best practices
  - Stay ahead of cyberthreats, while delivering value to customers
- **You don't have to do it alone. Let's work together to secure the connected world.**
- **Contact us today to explore a CIS partnership.**

NerdioCon 2025 PALM SPRINGS

Q&A

NerdioCon
2025
PALM SPRINGS

Thank you