Synoptic Cyber

FEATURES

Simplify Compliance. Strengthen Security. Save Time.

Synoptic Cyber automates the RMF compliance journey from scans to fixes to documentation— So your team can focus on mission success, not manual process.

Synoptic Cyber

Why Choose Synoptic Cyber?

Built from real-world DoD experience, Synoptic Cyber ensures cybersecurity compliance is faster, simpler, and more reliable-across every connected device.

Save Time

Minutes instead of hours per system

Strengthen Compliance

Fewer errors, full audit trails

All-in-One Platform

Scan, fix, document in one tool

Mission-Ready Results

Trusted by DoD and government contractors

Synoptic Cyber

Automated STIG & SCAP Scanning

The Problem

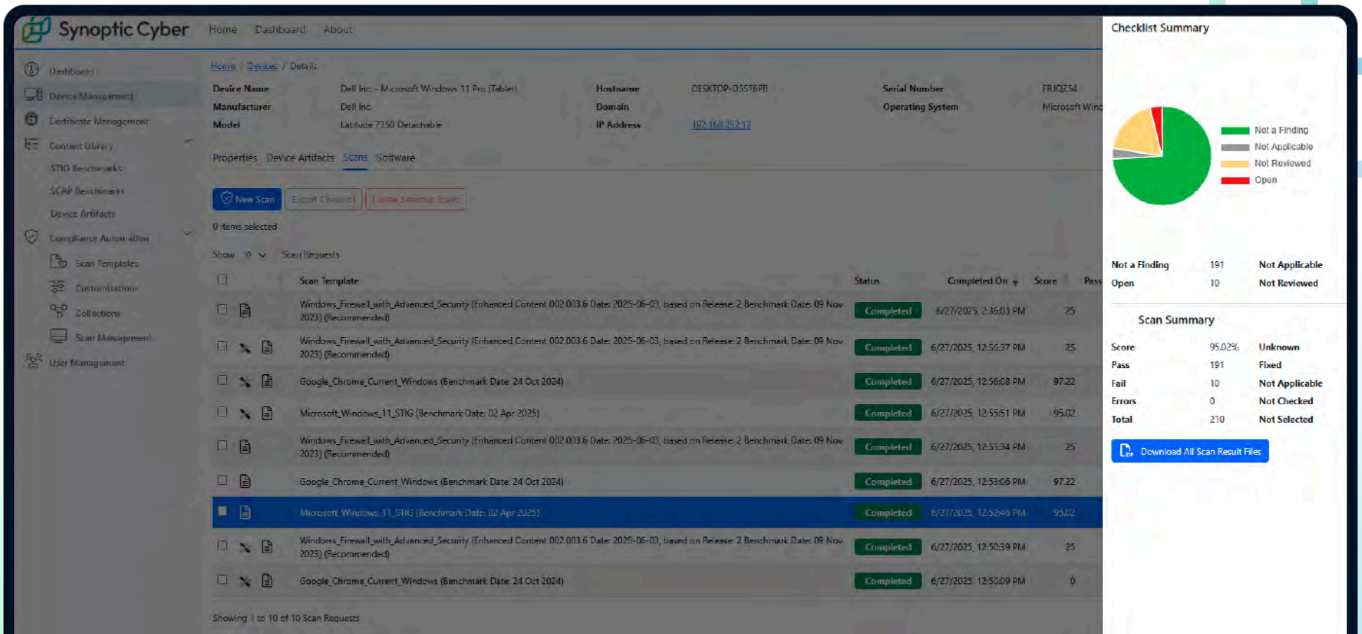
Manually scanning each system for vulnerbilities wastes critical time and increases the risk of missing key controls.

The Solution

Synoptic Cyber ingests both STIGs and SCAP benchmarks and ensures that 100% of the controls are verified to compliance.

Benefits

- ✓ Scan hundreds of devices in parallel
- ✓ Ensure up-to-date government compliance benchmarks
- ✓ Eliminate manual scanning errors
- ✓ Accelerate compliance reporting cycles



Home / Devices / Details

Device Name	Dell Inc. - Microsoft Windows 11 Pro (Tablet)	**Hostname**	DESKTOP-D5ST6PB	**Serial Number**	FRJQZ54
Manufacturer	Dell Inc.	**Domain**		**Operating System**	Microsoft Winc
Model	Latitude 7350 Detachable	**IP Address**	192.168.252.17		

0 items selected

Show 10 Scan Requests

☐		Scan Template	Status	Completed On	Score	Pass
☐		Windows_Firewall_with_Advanced_Security (Enhanced Content 002.003.6 Date: 2025-06-03, based on Release: 2 Benchmark Date: 09 Nov 2023) (Recommended)	Completed	6/27/2025, 2:36:03 PM	25	
☐		Windows_Firewall_with_Advanced_Security (Enhanced Content 002.003.6 Date: 2025-06-03, based on Release: 2 Benchmark Date: 09 Nov 2023) (Recommended)	Completed	6/27/2025, 12:56:37 PM	25	
☐		Google_Chrome_Current_Windows (Benchmark Date: 24 Oct 2024)	Completed	6/27/2025, 12:56:08 PM	97.22	
☐		Microsoft_Windows_11_STIG (Benchmark Date: 02 Apr 2025)	Completed	6/27/2025, 12:55:51 PM	95.02	
☐		Windows_Firewall_with_Advanced_Security (Enhanced Content 002.003.6 Date: 2025-06-03, based on Release: 2 Benchmark Date: 09 Nov 2023) (Recommended)	Completed	6/27/2025, 12:53:34 PM	25	
☐		Google_Chrome_Current_Windows (Benchmark Date: 24 Oct 2024)	Completed	6/27/2025, 12:53:06 PM	97.22	
■		Microsoft_Windows_11_STIG (Benchmark Date: 02 Apr 2025)	Completed	6/27/2025, 12:52:46 PM	95.02	
☐		Windows_Firewall_with_Advanced_Security (Enhanced Content 002.003.6 Date: 2025-06-03, based on Release: 2 Benchmark Date: 09 Nov 2023) (Recommended)	Completed	6/27/2025, 12:50:39 PM	25	
☐		Google_Chrome_Current_Windows (Benchmark Date: 24 Oct 2024)	Completed	6/27/2025, 12:50:09 PM	0	

Showing 1 to 10 of 10 Scan Requests

Checklist Summary

Not a Finding	191	**Not Applicable**
Open	10	**Not Reviewed**

Scan Summary

Score	95.02%	**Unknown**
Pass	191	**Fixed**
Fail	10	**Not Applicable**
Errors	0	**Not Checked**
Total	210	**Not Selected**

Synoptic Cyber

Automated (Fix Non-Compliant Items Instantly)

The Problem

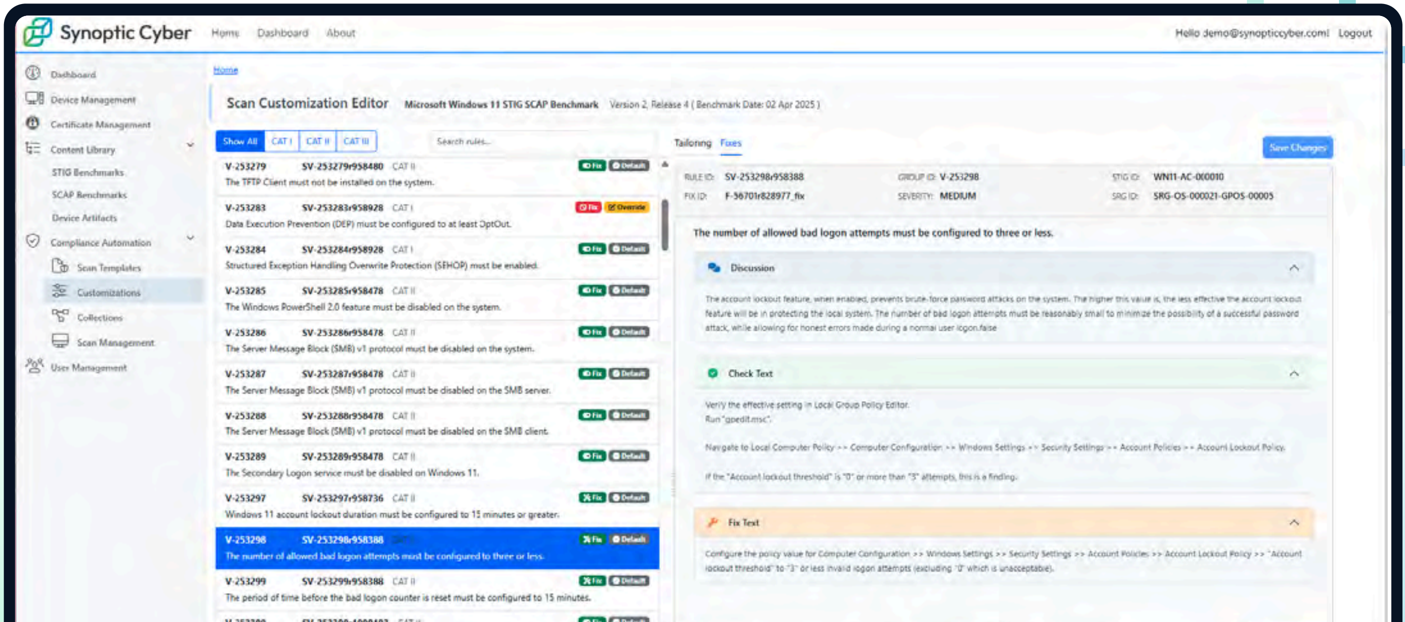
Fixing vulnerabilities manually is slow and inconsistent, especially across complex environments.

The Solution

Our system automatically remediates failed controls according to your approved benchmarks saving time and ensuring consistency.

Benefits

- ✓ Fix problems the moment they're detected
- ✓ Customize fixes control-by-control
- ✓ Keep full action logs for audits
- ✓ Reduce human error risk



Scan Customization Editor **Microsoft Windows 11 STIG SCAP Benchmark** Version 2, Release 4 (Benchmark Date: 02 Apr 2025)

V-253279 **SV-253279r958480** CAT II
The TFTP Client must not be installed on the system.

V-253283 **SV-253283r958928** CAT I
Data Execution Prevention (DEP) must be configured to at least OptOut.

V-253284 **SV-253284r958928** CAT I
Structured Exception Handling Overwrite Protection (SEHOP) must be enabled.

V-253285 **SV-253285r958478** CAT II
The Windows PowerShell 2.0 feature must be disabled on the system.

V-253286 **SV-253286r958478** CAT II
The Server Message Block (SMB) v1 protocol must be disabled on the system.

V-253287 **SV-253287r958478** CAT II
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.

V-253288 **SV-253288r958478** CAT II
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.

V-253289 **SV-253289r958478** CAT II
The Secondary Logon service must be disabled on Windows 11.

V-253297 **SV-253297r958736** CAT II
Windows 11 account lockout duration must be configured to 15 minutes or greater.

V-253298 **SV-253298r958388** CAT II
The number of allowed bad logon attempts must be configured to three or less.

V-253299 **SV-253299r958388** CAT II
The period of time before the bad logon counter is reset must be configured to 15 minutes.

RULE ID: SV-253298r958388 GROUP ID: V-253298 STIG ID: WN11-AC-000010
FIX ID: F-56701r828977_fix SEVERITY: MEDIUM SRG ID: SRG-OS-000021-GPOS-00005

The number of allowed bad logon attempts must be configured to three or less.

Discussion

The account lockout feature, when enabled, prevents brute-force password attacks on the system. The higher this value is, the less effective the account lockout feature will be in protecting the local system. The number of bad logon attempts must be reasonably small to minimize the possibility of a successful password attack, while allowing for honest errors made during a normal user logon.false

Check Text

Verify the effective setting in Local Group Policy Editor.
Run "gpedit.msc".

Navigate to Local Computer Policy >> Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy.

If the "Account lockout threshold" is "0" or more than "3" attempts, this is a finding.

Fix Text

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> "Account lockout threshold" to "3" or less invalid logon attempts (excluding "0" which is unacceptable).

Synoptic Cyber

Integrated STIG Editor

The Problem

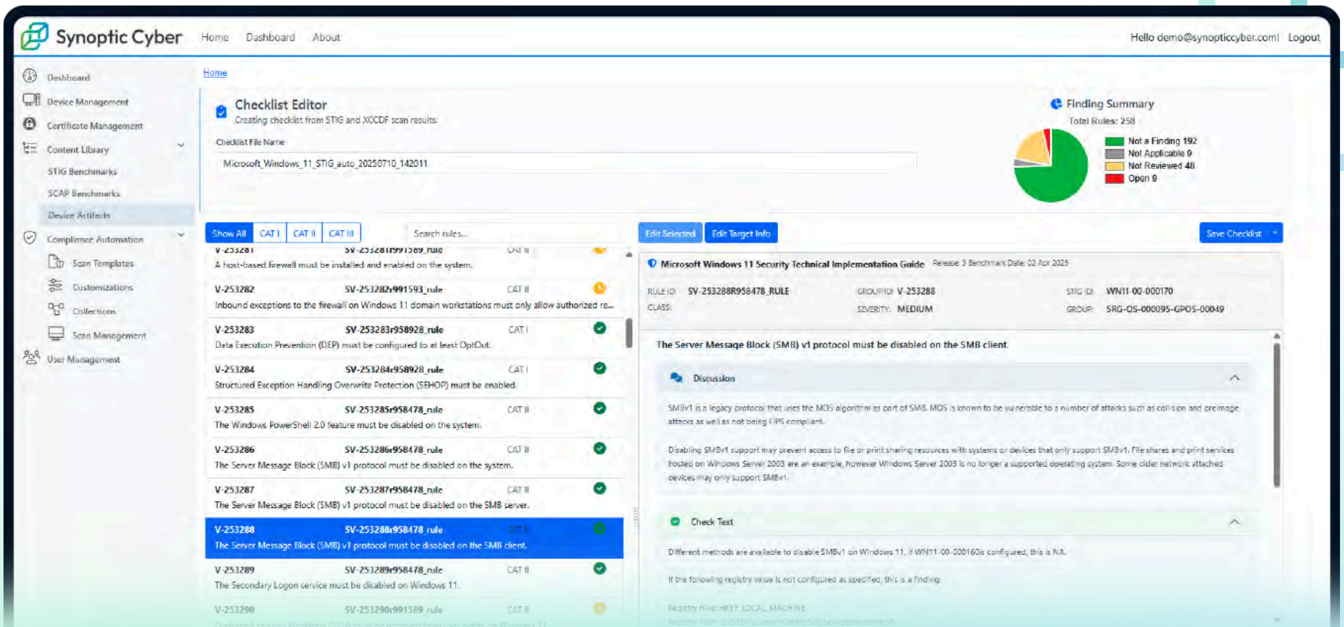
Manually editing and tracking STIGs creates version control chaos and audit challenges.

The Solution

Use Synoptic Cyber's built-in editor to review, adjust, and comment on STIGs within the platform- no extra tools needed.

Benefits

- ✓ Simplify STIG management
- ✓ Standardize documentation for audit teams
- ✓ Preserve full edit history automatically
- ✓ Speed up review cycles



Checklist Editor

Creating checklist from STIG and XCCDF scan results.

Checklist File Name: Microsoft_Windows_11_STIG_auto_20250710_142011

Finding Summary

Total Rules: 258

- 🟩 Not a Finding 192
- ▨ Not Applicable 9
- 🟨 Not Reviewed 48
- 🟥 Open 9

V-253281	SV-253281r991589_rule	CAT II	●
A host-based firewall must be installed and enabled on the system.			
V-253282	SV-253282r991593_rule	CAT II	●
Inbound exceptions to the firewall on Windows 11 domain workstations must only allow authorized re...			
V-253283	SV-253283r958928_rule	CAT I	✓
Data Execution Prevention (DEP) must be configured to at least OptOut.			
V-253284	SV-253284r958928_rule	CAT I	✓
Structured Exception Handling Overwrite Protection (SEHOP) must be enabled.			
V-253285	SV-253285r958478_rule	CAT II	✓
The Windows PowerShell 2.0 feature must be disabled on the system.			
V-253286	SV-253286r958478_rule	CAT II	✓
The Server Message Block (SMB) v1 protocol must be disabled on the system.			
V-253287	SV-253287r958478_rule	CAT II	✓
The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.			
V-253288	SV-253288r958478_rule	CAT II	✓
The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.			
V-253289	SV-253289r958478_rule	CAT II	✓
The Secondary Logon service must be disabled on Windows 11.			
V-253290	SV-253290r991589_rule	CAT II	●
Orphaned security identifiers (SIDs) must be removed from user rights on Windows 11.			

Microsoft Windows 11 Security Technical Implementation Guide Release: 3 Benchmark Date: 02 Apr 2025

RULE ID: SV-253288R958478_RULE
CLASS:
GROUP ID: V-253288
SEVERITY: MEDIUM
STIG ID: WN11-00-000170
GROUP: SRG-OS-000095-GPOS-00049

The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.

Discussion

SMBv1 is a legacy protocol that uses the MD5 algorithm as part of SMB. MD5 is known to be vulnerable to a number of attacks such as collision and preimage attacks as well as not being FIPS compliant.

Disabling SMBv1 support may prevent access to file or print sharing resources with systems or devices that only support SMBv1. File shares and print services hosted on Windows Server 2003 are an example, however Windows Server 2003 is no longer a supported operating system. Some older network attached devices may only support SMBv1.

Check Text

Different methods are available to disable SMBv1 on Windows 11, if WN11-00-000160is configured, this is NA.

If the following registry value is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SYSTEM\CurrentControlSet\Services\mrxsmb10\

Synoptic Cyber

Device Management Across Windows, Linux, Embedded Devices

The Problem

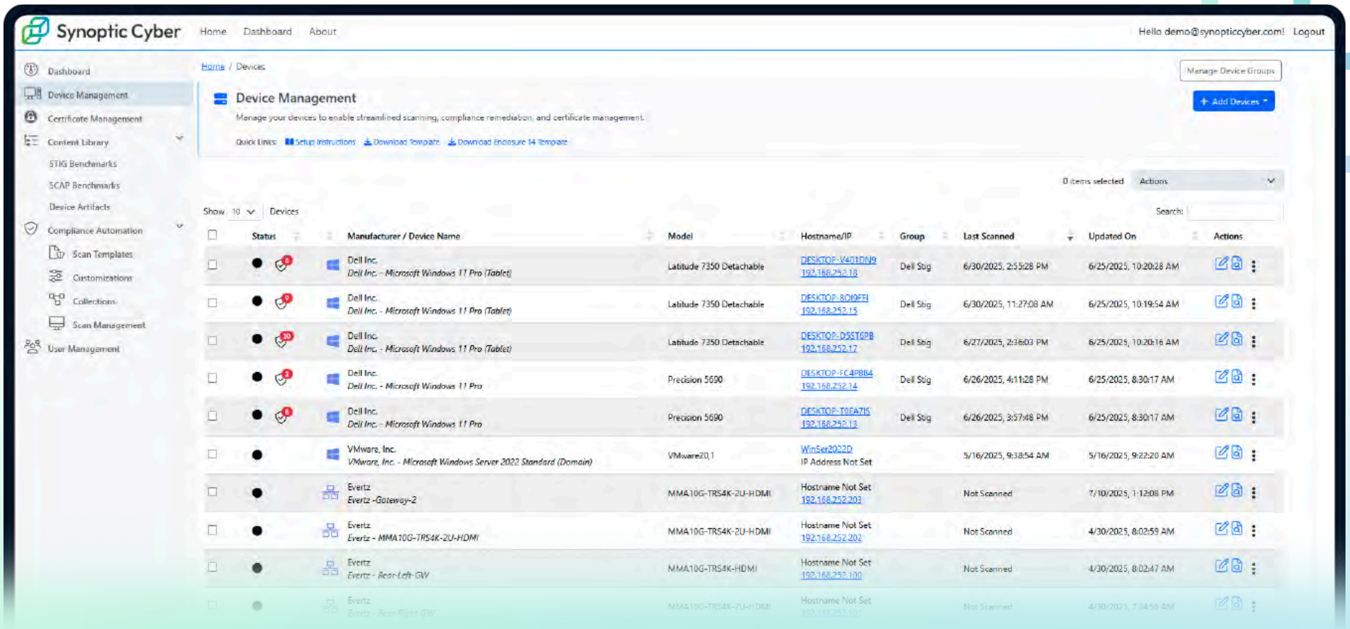
Different operating systems and device types require juggling multiple compliance tools.

The Solution

Synoptic Cyber managers scans and fixes across all supported platforms in one place, including Windows, Linux, software apps, and embedded devices.

Benefits

- ✓ Manage all systems with a single platform
- ✓ Centralize reporting across device types
- ✓ Scale compliance operations effortlessly
- ✓ Support niche devices with special configurations



Device Management

Manage your devices to enable streamlined scanning, compliance remediation, and certificate management.

□	Status	Manufacturer / Device Name	Model	Hostname/IP	Group	Last Scanned	Updated On	Actions
□	● 6	Dell Inc. *Dell Inc. - Microsoft Windows 11 Pro (Tablet)*	Latitude 7350 Detachable	DESKTOP-V401DN9 192.168.252.18	Dell Stig	6/30/2025, 2:55:28 PM	6/25/2025, 10:20:28 AM	⋮
□	● 9	Dell Inc. *Dell Inc. - Microsoft Windows 11 Pro (Tablet)*	Latitude 7350 Detachable	DESKTOP-8OI9FFI 192.168.252.15	Dell Stig	6/30/2025, 11:27:08 AM	6/25/2025, 10:19:54 AM	⋮
□	● 10	Dell Inc. *Dell Inc. - Microsoft Windows 11 Pro (Tablet)*	Latitude 7350 Detachable	DESKTOP-D5ST6PB 192.168.252.17	Dell Stig	6/27/2025, 2:36:03 PM	6/25/2025, 10:20:16 AM	⋮
□	● 2	Dell Inc. *Dell Inc. - Microsoft Windows 11 Pro*	Precision 5690	DESKTOP-FC4PBB4 192.168.252.14	Dell Stig	6/26/2025, 4:11:28 PM	6/25/2025, 8:30:17 AM	⋮
□	● 8	Dell Inc. *Dell Inc. - Microsoft Windows 11 Pro*	Precision 5690	DESKTOP-T0EA7IS 192.168.252.13	Dell Stig	6/26/2025, 3:57:48 PM	6/25/2025, 8:30:17 AM	⋮
□	●	VMware, Inc. *VMware, Inc. - Microsoft Windows Server 2022 Standard (Domain)*	VMware20,1	WinSer2022D IP Address Not Set		5/16/2025, 9:38:54 AM	5/16/2025, 9:22:20 AM	⋮
□	●	Evertz *Evertz -Gateway-2*	MMA10G-TRS4K-2U-HDMI	Hostname Not Set 192.168.252.203		Not Scanned	7/10/2025, 1:12:08 PM	⋮
□	●	Evertz *Evertz - MMA10G-TRS4K-2U-HDMI*	MMA10G-TRS4K-2U-HDMI	Hostname Not Set 192.168.252.202		Not Scanned	4/30/2025, 8:02:59 AM	⋮
□	●	Evertz *Evertz - Rear-Left-GW*	MMA10G-TRS4K-HDMI	Hostname Not Set 192.168.252.100		Not Scanned	4/30/2025, 8:02:47 AM	⋮
□	●	Evertz *Evertz - Rear-Right-GW*	MMA10G-TRS4K-2U-HDMI	Hostname Not Set 192.168.252.101		Not Scanned	4/30/2025, 7:24:56 AM	⋮

Synoptic Cyber

System Security Plan (SSP) & Artifact Generation

The Problem

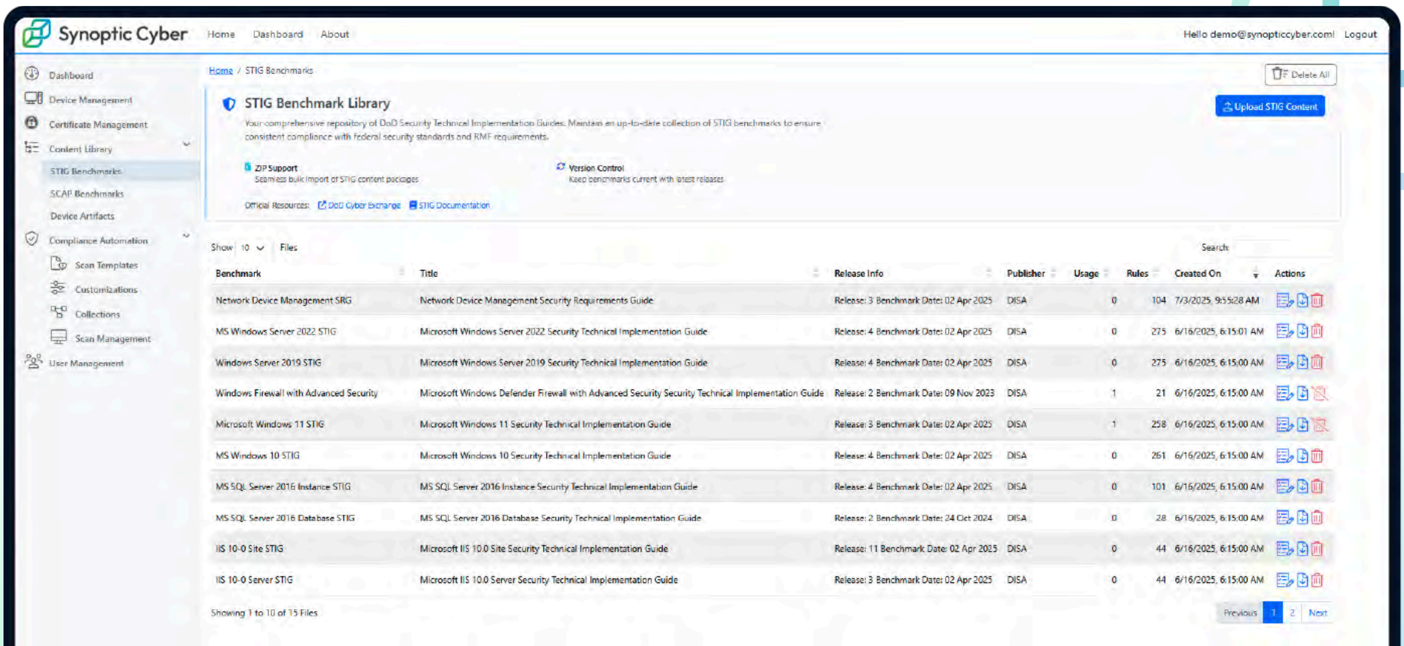
Manually compiling SSPs and compliance artifacts is tedious and risks missed components.

The Solution

Synoptic Cyber automatically compiles clean, audit-ready documentation - including Enclosure 14, PPSM, and all required artifacts.

Benefits

- ✓ Create audit-ready packages instantly
- ✓ Ensure no missing documentation
- ✓ Speed up pre-audit preparation
- ✓ Align with DoD RMF and NIST standards



Home / STIG Benchmarks

STIG Benchmark Library

Your comprehensive repository of DoD Security Technical Implementation Guides. Maintain an up-to-date collection of STIG benchmarks to ensure consistent compliance with federal security standards and RMF requirements.

ZIP Support
Seamless bulk import of STIG content packages

Version Control
Keep benchmarks current with latest releases

Official Resources: DoD Cyber Exchange STIG Documentation

Benchmark	Title	Release Info	Publisher	Usage	Rules	Created On	Actions
Network Device Management SRG	Network Device Management Security Requirements Guide	Release: 3 Benchmark Date: 02 Apr 2025	DISA	0	104	7/3/2025, 9:55:28 AM	
MS Windows Server 2022 STIG	Microsoft Windows Server 2022 Security Technical Implementation Guide	Release: 4 Benchmark Date: 02 Apr 2025	DISA	0	275	6/16/2025, 6:15:01 AM	
Windows Server 2019 STIG	Microsoft Windows Server 2019 Security Technical Implementation Guide	Release: 4 Benchmark Date: 02 Apr 2025	DISA	0	275	6/16/2025, 6:15:00 AM	
Windows Firewall with Advanced Security	Microsoft Windows Defender Firewall with Advanced Security Security Technical Implementation Guide	Release: 2 Benchmark Date: 09 Nov 2023	DISA	1	21	6/16/2025, 6:15:00 AM	
Microsoft Windows 11 STIG	Microsoft Windows 11 Security Technical Implementation Guide	Release: 3 Benchmark Date: 02 Apr 2025	DISA	1	258	6/16/2025, 6:15:00 AM	
MS Windows 10 STIG	Microsoft Windows 10 Security Technical Implementation Guide	Release: 4 Benchmark Date: 02 Apr 2025	DISA	0	261	6/16/2025, 6:15:00 AM	
MS SQL Server 2016 Instance STIG	MS SQL Server 2016 Instance Security Technical Implementation Guide	Release: 4 Benchmark Date: 02 Apr 2025	DISA	0	101	6/16/2025, 6:15:00 AM	
MS SQL Server 2016 Database STIG	MS SQL Server 2016 Database Security Technical Implementation Guide	Release: 2 Benchmark Date: 24 Oct 2024	DISA	0	28	6/16/2025, 6:15:00 AM	
IIS 10-0 Site STIG	Microsoft IIS 10.0 Site Security Technical Implementation Guide	Release: 11 Benchmark Date: 02 Apr 2025	DISA	0	44	6/16/2025, 6:15:00 AM	
IIS 10-0 Server STIG	Microsoft IIS 10.0 Server Security Technical Implementation Guide	Release: 3 Benchmark Date: 02 Apr 2025	DISA	0	44	6/16/2025, 6:15:00 AM	

Showing 1 to 10 of 15 Files

Synoptic Cyber

Certificate Management Tool (Add-On Feature)

The Problem

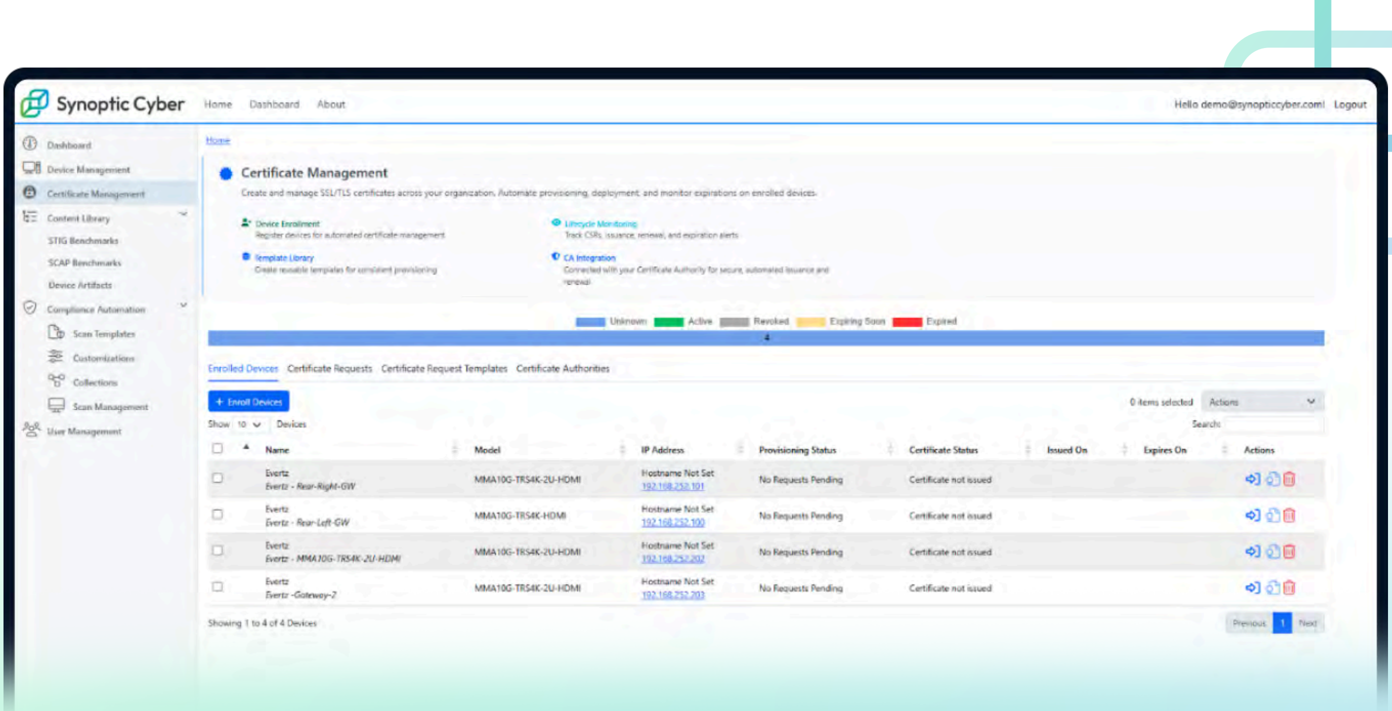
Applying local security certificates to embedded systems is tricky and time-consuming.

The Solution

Our Certificate Management tool integrates with on-premises certificate authorities and automates the generation and application of certificates to embedded systems.

Benefits

- ✓ Dramatically reduce time to apply certificates from days to minutes
- ✓ Eliminate manual certificate processes
- ✓ Full visibility over devices cert status
- ✓ Integrate to on premise certificate authorities



Certificate Management

Create and manage SSL/TLS certificates across your organization. Automate provisioning, deployment, and monitor expirations on enrolled devices.

Device Enrollment
Register devices for automated certificate management

Template Library
Create reusable templates for consistent provisioning

Lifecycle Monitoring
Track CSRs, issuance, renewal, and expiration alerts

CA Integration
Connected with your Certificate Authority for secure, automated issuance and renewal

Show 10 Devices

□	Name	Model	IP Address	Provisioning Status	Certificate Status	Issued On	Expires On	Actions
□	Evertz *Evertz - Rear-Right-GW*	MMA10G-TRS4K-2U-HDMI	Hostname Not Set 192.168.252.101	No Requests Pending	Certificate not issued			
□	Evertz *Evertz - Rear-Left-GW*	MMA10G-TRS4K-HDMI	Hostname Not Set 192.168.252.100	No Requests Pending	Certificate not issued			
□	Evertz *Evertz - MMA10G-TRS4K-2U-HDMI*	MMA10G-TRS4K-2U-HDMI	Hostname Not Set 192.168.252.202	No Requests Pending	Certificate not issued			
□	Evertz *Evertz -Gateway-2*	MMA10G-TRS4K-2U-HDMI	Hostname Not Set 192.168.252.203	No Requests Pending	Certificate not issued			

Showing 1 to 4 of 4 Devices

Synoptic Cyber

Contact for Government Inquiries

Matt Krstulja

Government Contracting Contact

www.synopticcyber.com

EMAIL
info@synopticcyber.com

PHONE
720-303-9028

OFFICE
**11786 Shaffer Pl S-203,
Littleton, CO 80127**