PRODUCT TOUR

RoboShadow

Cyber Management Platform

National Cyber Security Centre
For Startups
Alumni

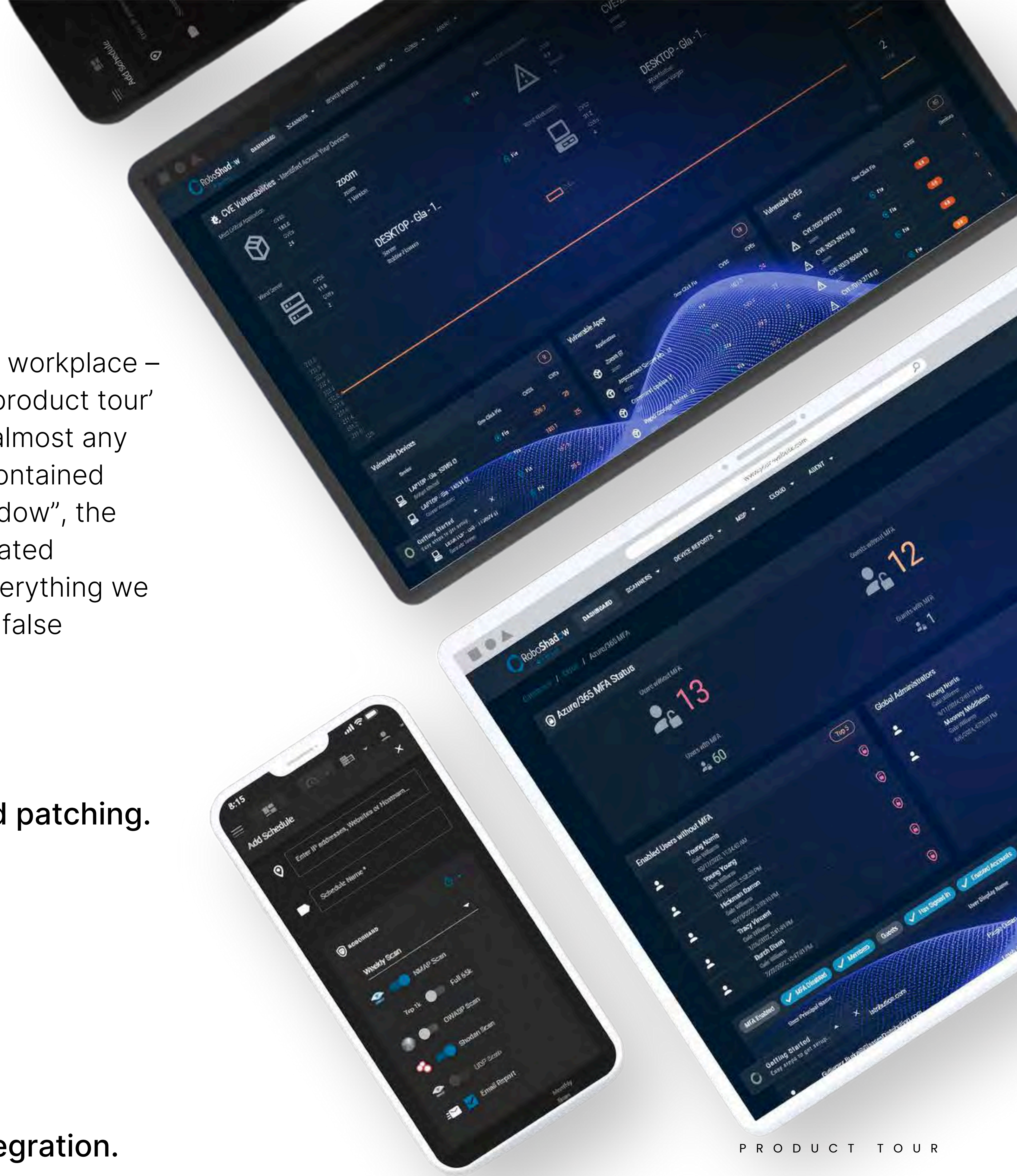
Demystify Cybersecurity For **SMBs, MSPs and The Enterprise**

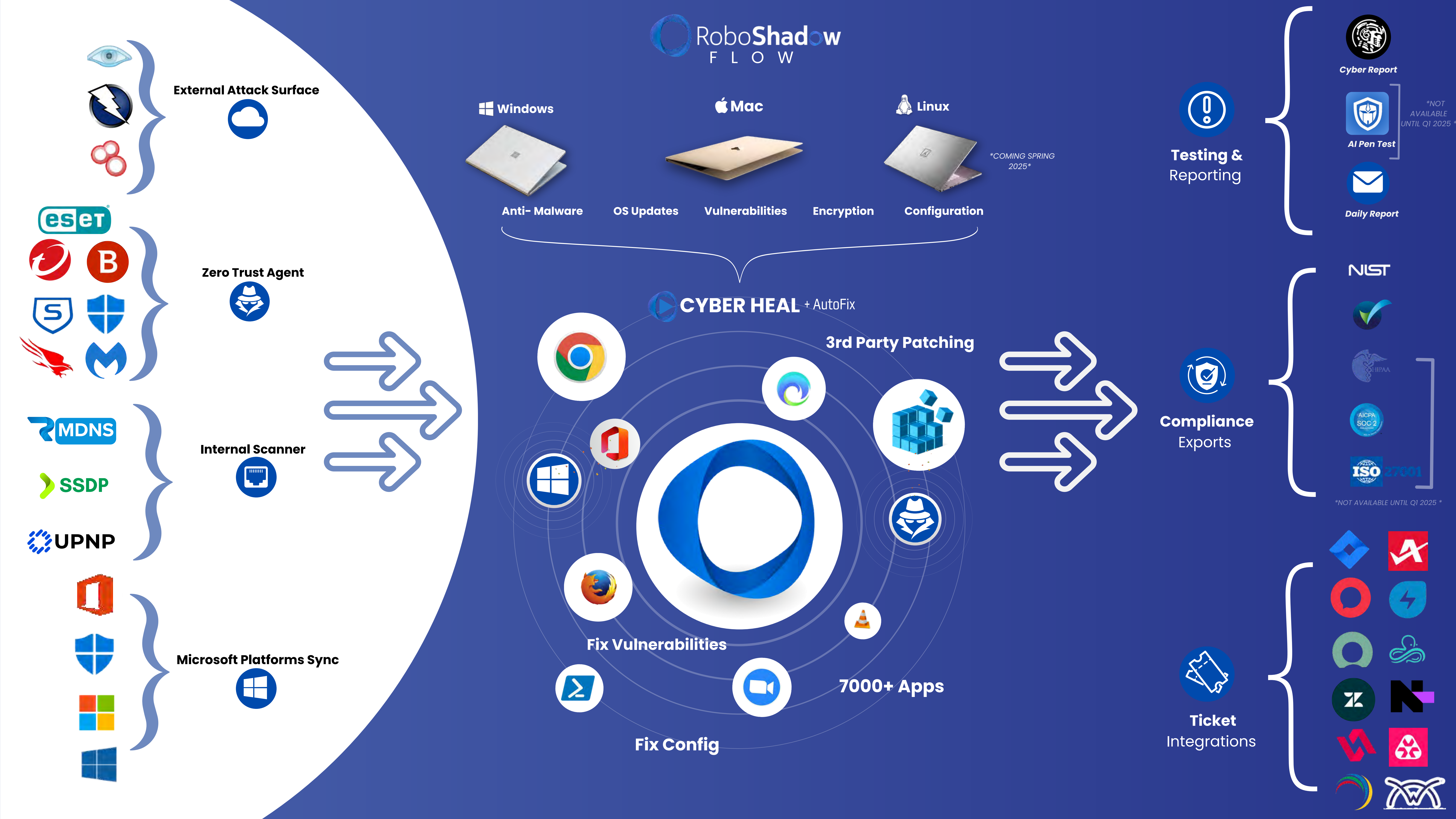
What Cyber Responsibilities Does RoboShadow Cover?

The following overview aims to provide a quick guide to managing cyber security in the modern workplace – **not just for technical people**, but business leaders as well. This is presented in the guise of a ‘product tour’ to demonstrate just how RoboShadow helps to manage a modern cyber security capability for almost any organisation. We estimate that around **75% of corporate cyber security responsibilities** are contained within the RoboShadow platform. Whilst we do not claim that “all you will ever need is RoboShadow”, the 180 different integrations across Antivirus, PSA, and Cloud Authentication delivers a truly integrated security strategy. Many users report that RoboShadow is **“a massive time saver platform”** - everything we build, and design is around saving the administration time, reducing the communication sprawl, false positives, automating fixes and automating the healing processes.

What RoboShadow Can Do in a Nutshell:

- Save real-world remediation time by using our Cyber Heal autopilot for fixing and patching.
- Mitigate threats from the new GPT-style AI attacks used by bad guys.
- Integrate with your existing security ecosystem toolsets.
- Minimise alert fatigue and noise created by Cyber Security counters.
- Receive actionable alerts and accountability with Service Desk System / PSA integration.





RoboShadow FLOW

External Attack Surface

Zero Trust Agent

Internal Scanner

Microsoft Platforms Sync

Windows

Mac

Linux

COMING SPRING 2025

Anti- Malware

OS Updates

Vulnerabilities

Encryption

Configuration

CYBER HEAL + AutoFix

3rd Party Patching

Fix Vulnerabilities

7000+ Apps

Fix Config

Cyber Report

AI Pen Test

*NOT AVAILABLE UNTIL Q1 2025 *

Daily Report

Testing & Reporting

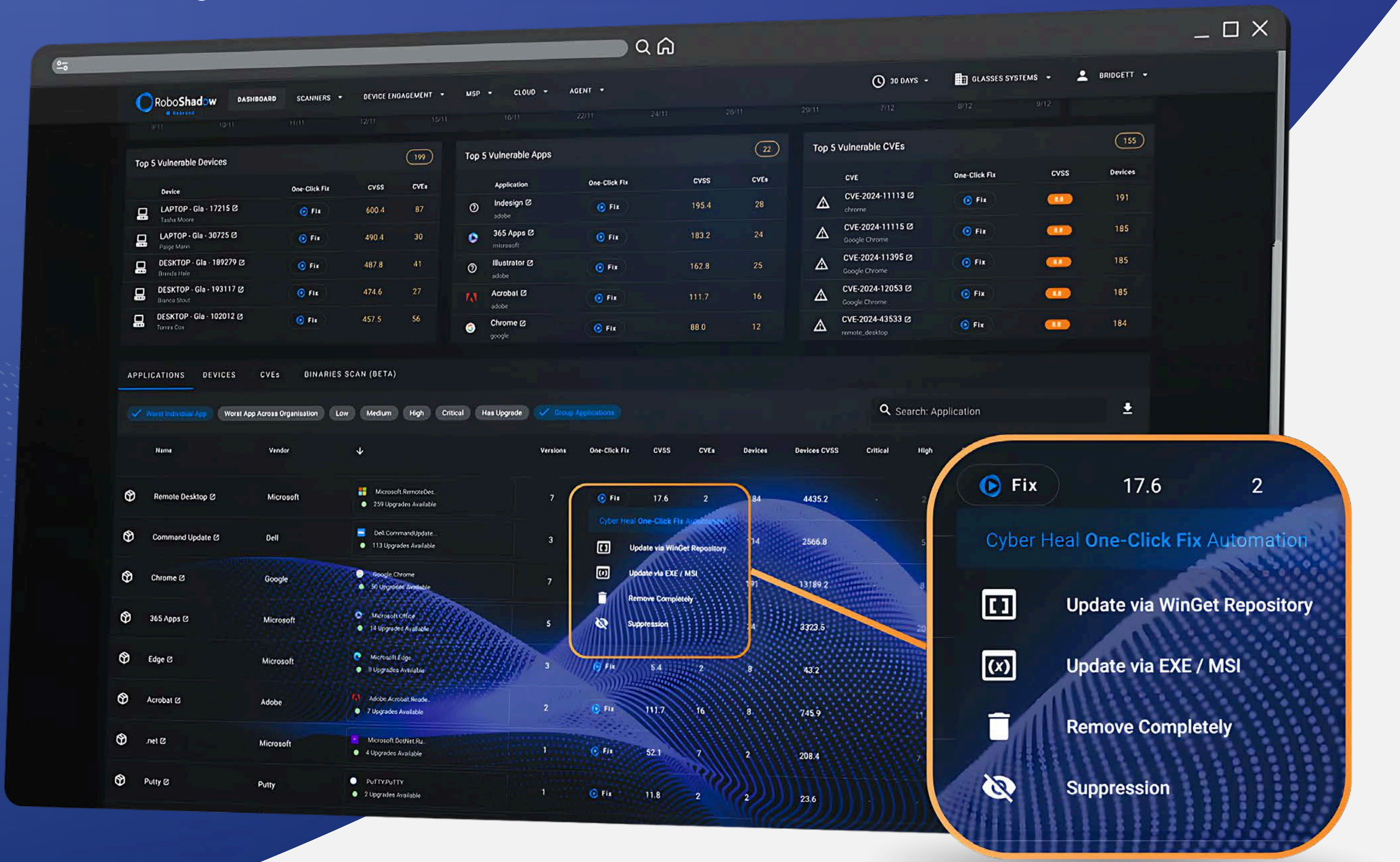
Compliance Exports

*NOT AVAILABLE UNTIL Q1 2025 *

Ticket Integrations

Cyber Heal:

Auto Pilot Fixing Vulnerabilities



RoboShadow
DASHBOARD · SCANNERS ▾ · DEVICE ENGAGEMENT ▾ · MSP ▾ · CLOUD ▾ · AGENT ▾
30 DAYS ▾ · GLASSES SYSTEMS ▾ · BRIDGETT ▾

Top 5 Vulnerable Devices (199)

Device	One-Click Fix	CVSS	CVEs
LAPTOP - Gla - 17215 Tasha Moore	Fix	600.4	87
LAPTOP - Gla - 30725 Paige Mann	Fix	490.4	30
DESKTOP - Gla - 189279 Brenda Hale	Fix	487.8	41
DESKTOP - Gla - 193117 Bianca Stout	Fix	474.6	27
DESKTOP - Gla - 102012 Torres Cox	Fix	457.5	56

Top 5 Vulnerable Apps (22)

Application	One-Click Fix	CVSS	CVEs
Indesign adobe	Fix	195.4	28
365 Apps microsoft	Fix	183.2	24
Illustrator adobe	Fix	162.8	25
Acrobat adobe	Fix	111.7	16
Chrome google	Fix	88.0	12

Top 5 Vulnerable CVEs (155)

CVE	One-Click Fix	CVSS	Devices
CVE-2024-11113 chrome	Fix	[illegible]	191
CVE-2024-11115 Google Chrome	Fix	[illegible]	185
CVE-2024-11395 Google Chrome	Fix	[illegible]	185
CVE-2024-12053 Google Chrome	Fix	[illegible]	185
CVE-2024-43533 remote_desktop	Fix	[illegible]	184

APPLICATIONS · DEVICES · CVEs · BINARIES SCAN (BETA)

✓ Worst Individual App · Worst App Across Organisation · Low · Medium · High · Critical · Has Upgrade · ✓ Group Applications

Search: Application

Name	Vendor	↓	Versions	One-Click Fix	CVSS	CVEs	Devices	Devices CVSS	Critical	High
Remote Desktop	Microsoft	Microsoft.RemoteDes... 259 Upgrades Available	7	Fix	17.6	2	184	4435.2	-	2
Command Update	Dell	Dell.CommandUpdate... 113 Upgrades Available	3	[illegible]	[illegible]	[illegible]	[illegible]	2566.8	[illegible]	5
Chrome	Google	Google.Chrome 50 Upgrades Available	7	[illegible]	[illegible]	[illegible]	[illegible]	13189.2	-	8
365 Apps	Microsoft	Microsoft.Office 14 Upgrades Available	5	[illegible]	[illegible]	[illegible]	[illegible]	3323.5	[illegible]	20
Edge	Microsoft	Microsoft.Edge 8 Upgrades Available	3	Fix	5.4	2	8	43.2	[illegible]	[illegible]
Acrobat	Adobe	Adobe.Acrobat.Reade... 7 Upgrades Available	2	Fix	111.7	16	8	745.9	[illegible]	11
.net	Microsoft	Microsoft.DotNet.Ru... 4 Upgrades Available	1	Fix	52.1	7	2	208.4	[illegible]	7
Putty	Putty	PuTTY.PuTTY 2 Upgrades Available	1	Fix	11.8	2	2	23.6	[illegible]	[illegible]

Fix
17.6
2
Cyber Heal One-Click Fix Automation
Update via WinGet Repository
Update via EXE / MSI
Remove Completely
Suppression

'One Click Fix'

Fix

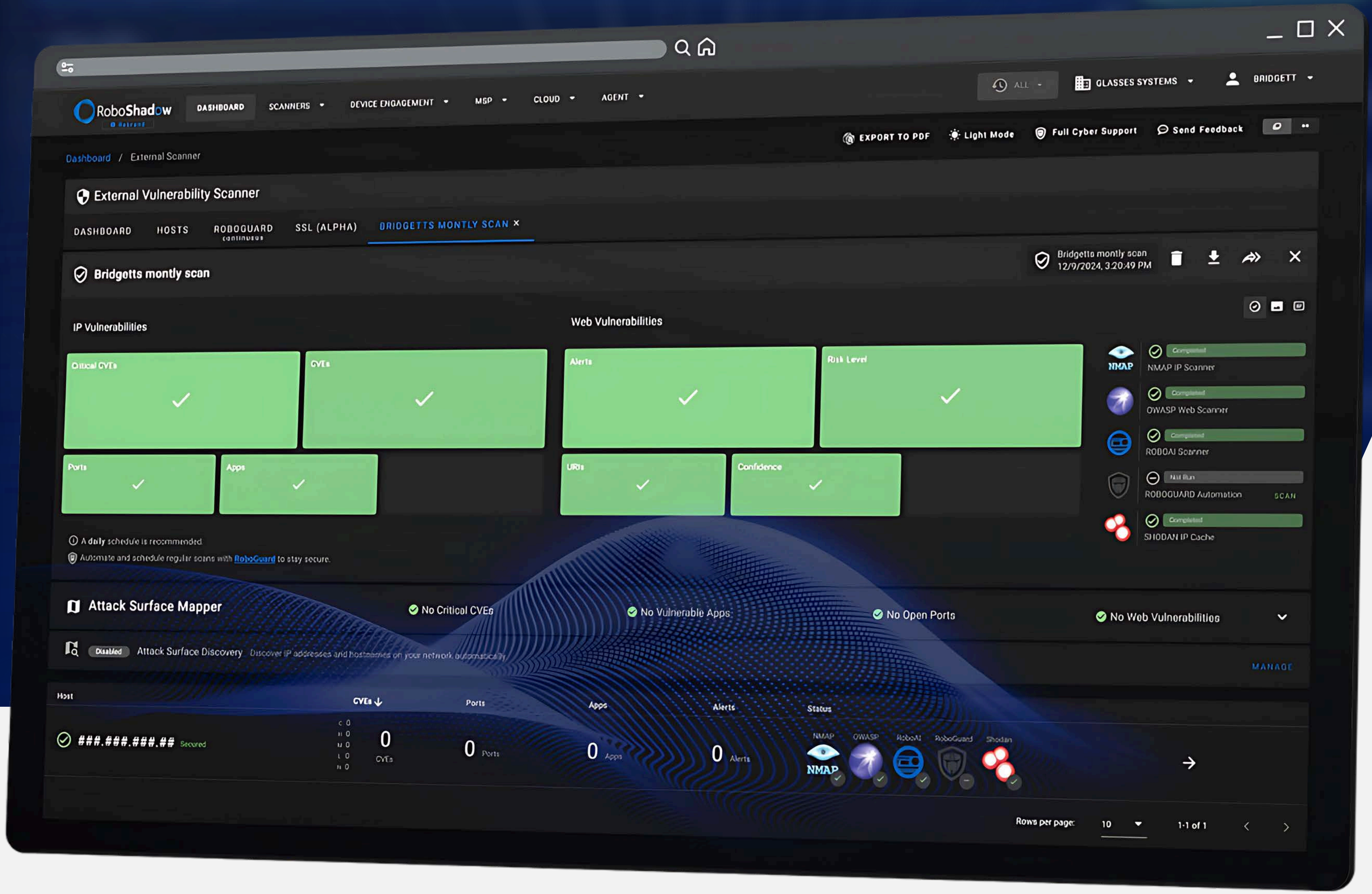
Technology changes rapidly, and staying on top of vulnerabilities is time-consuming. **AI-enabled hacking** has removed "security via obscurity," with most breaches caused by a lack of patching or oversight. Organisations must demonstrate daily identification and remediation to maintain security in the modern world.

Using our Cyber Heal technology, our **AutoPilot process** remediates issues across the estate in the background using a variety of techniques:

- ▶ **Update over 7000+** Applications from Microsoft Winget Repository.
- ▶ Rapidly uninstall unwanted or unsecure applications.
- ▶ Manually update less popular titles using your own **MSIs / EXEs**.
- ▶ Change **Cyber Benchmark** configuration to meet compliance standards.
- ▶ Update **Firewall and Anti-Ransomware** settings.
- ▶ **Automate** all the Cyber Heal tasks in the background with Autopilot.
- ▶ Log any Autopilot fails into your **Service Desk System / PSA** for a follow-up.

External Scanner :

Manage the External Attack Surface



External Vulnerability Scanner

Bridgotts montly scan

Bridgetts montly scan 12/9/2024, 3:20:49 PM

IP Vulnerabilities

Critical CVEs	CVEs
✓	✓

Ports	Apps
✓	✓

Web Vulnerabilities

Alerts	Risk Level
✓	✓

URIs	Confidence
✓	✓

Status	Scanner
Completed	NMAP IP Scanner
Completed	OWASP Web Scanner
Completed	ROBOAI Scanner
Not Run	ROBOGUARD Automation SCAN
Completed	SHODAN IP Cache

A daily schedule is recommended.

Automate and schedule regular scans with RoboGuard to stay secure.

Attack Surface Mapper

✓ No Critical CVEs ✓ No Vulnerable Apps ✓ No Open Ports ✓ No Web Vulnerabilities

Disabled Attack Surface Discovery Discover IP addresses and hostnames on your network automatically

Host	CVEs ↓	Ports	Apps	Alerts	Status
✓ ###.###.###.## Secured	C 0 H 0 M 0 L 0 N 0 0 CVEs	0 Ports	0 Apps	0 Alerts	NMAP ✓ OWASP ✓ RoboAI ✓ RoboGuard – Shodan ✓

Scan IPs , Websites & Hostnames

A core responsibility for any organisation is to continuously scan your external IP addresses that face the raw internet, ensuring that you're not exposing your technology to the world's bad guys. **No longer are these 'shady figures with hoods'** manually trying to find weaknesses, the challenge these days is more about battling against large-scale bot-backed AI hacking operations supported by global crime gangs or nation states.

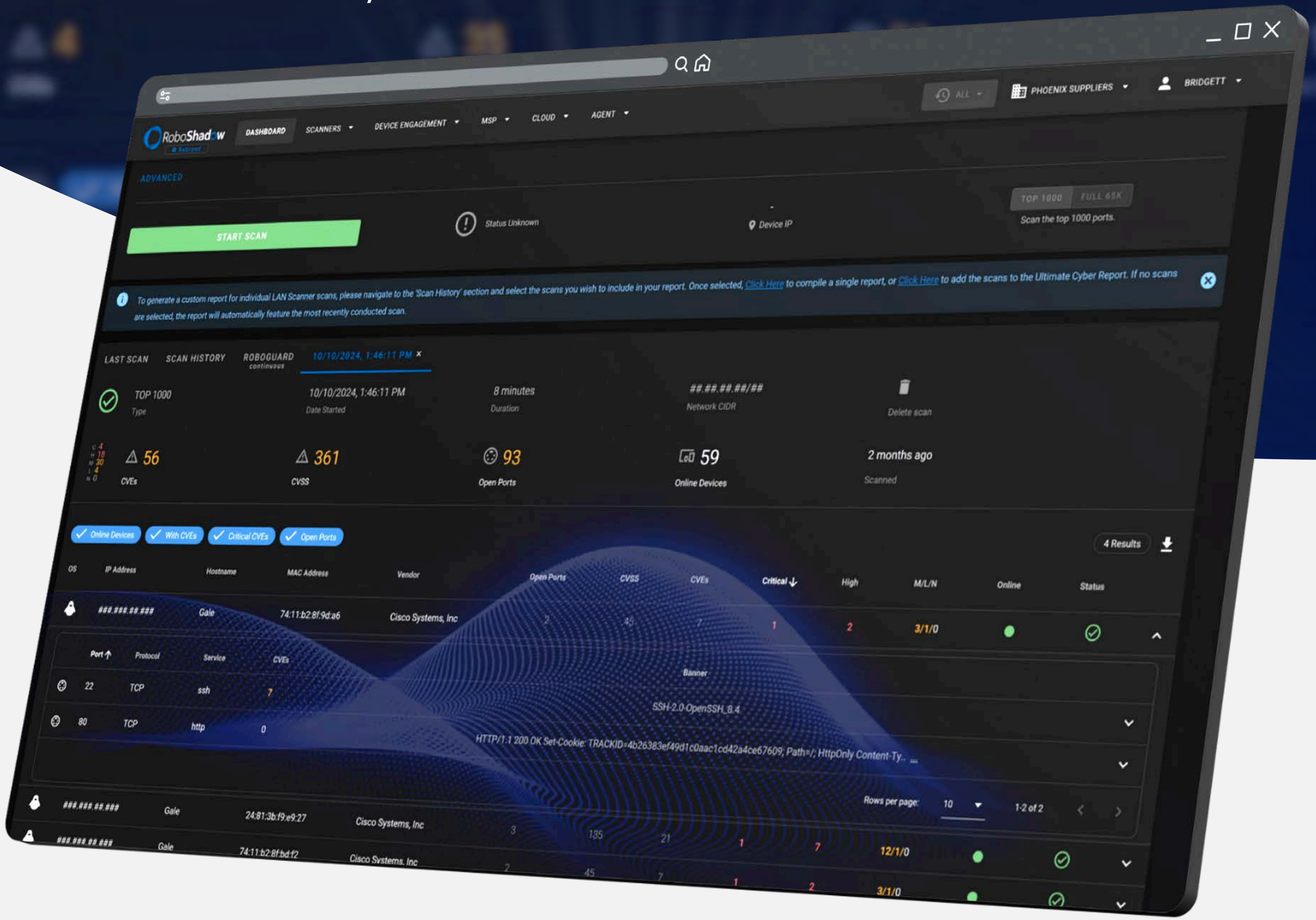
Our external attack surface scanner leverages the best of the open-source technology, and our proprietary RoboShadow technology to continuously cover the following scenarios:

- Are your office IP addresses locked down?
- Are your websites and SaaS applications vulnerability managed?
- Are your data centre and/or cloud environments secure from vulnerabilities?
- Are your home offices locked down and protected?
- Are your SSL certificates updated and enabled?

As soon as RoboShadow detects any new weaknesses during scans we raise the alarm for you, via email or through your service desk or PSA ticketing system as part of the RoboGuard service.

LAN Scanner:

See Where the Bad Guys Hide Inside!



Status Unknown

Device IP

Scan the top 1000 ports.

To generate a custom report for individual LAN Scanner scans, please navigate to the 'Scan History' section and select the scans you wish to include in your report. Once selected, Click Here to compile a single report, or Click Here to add the scans to the Ultimate Cyber Report. If no scans are selected, the report will automatically feature the most recently conducted scan.

TOP 1000 Type	10/10/2024, 1:46:11 PM Date Started	8 minutes Duration	##.##.##.##/## Network CIDR	Delete scan
56 CVEs	361 CVSS	93 Open Ports	59 Online Devices	2 months ago Scanned

C 4, H 18, M 30, L 4, N 0

OS	IP Address	Hostname	MAC Address	Vendor	Open Ports	CVSS	CVEs	Critical	High	M/L/N	Online	Status
	###.###.##.###	Gale	74:11:b2:8f:9d:a6	Cisco Systems, Inc	2	45	7	1	2	3/1/0	●	✓
	###.###.##.###	Gale	24:81:3b:f9:e9:27	Cisco Systems, Inc	3	135	21	1	7	12/1/0	●	✓
	###.###.##.###	Gale	74:11:b2:8f:bd:f2	Cisco Systems, Inc	2	45	7	1	2	3/1/0	●	✓

Port	Protocol	Service	CVEs	Banner
22	TCP	ssh	7	SSH-2.0-OpenSSH_8.4
80	TCP	http	0	HTTP/1.1 200 OK Set-Cookie: TRACKID=4b26383ef49d1c0aac1cd42a4ce67609; Path=/; HttpOnly Content-Ty...

Scan Individual Devices

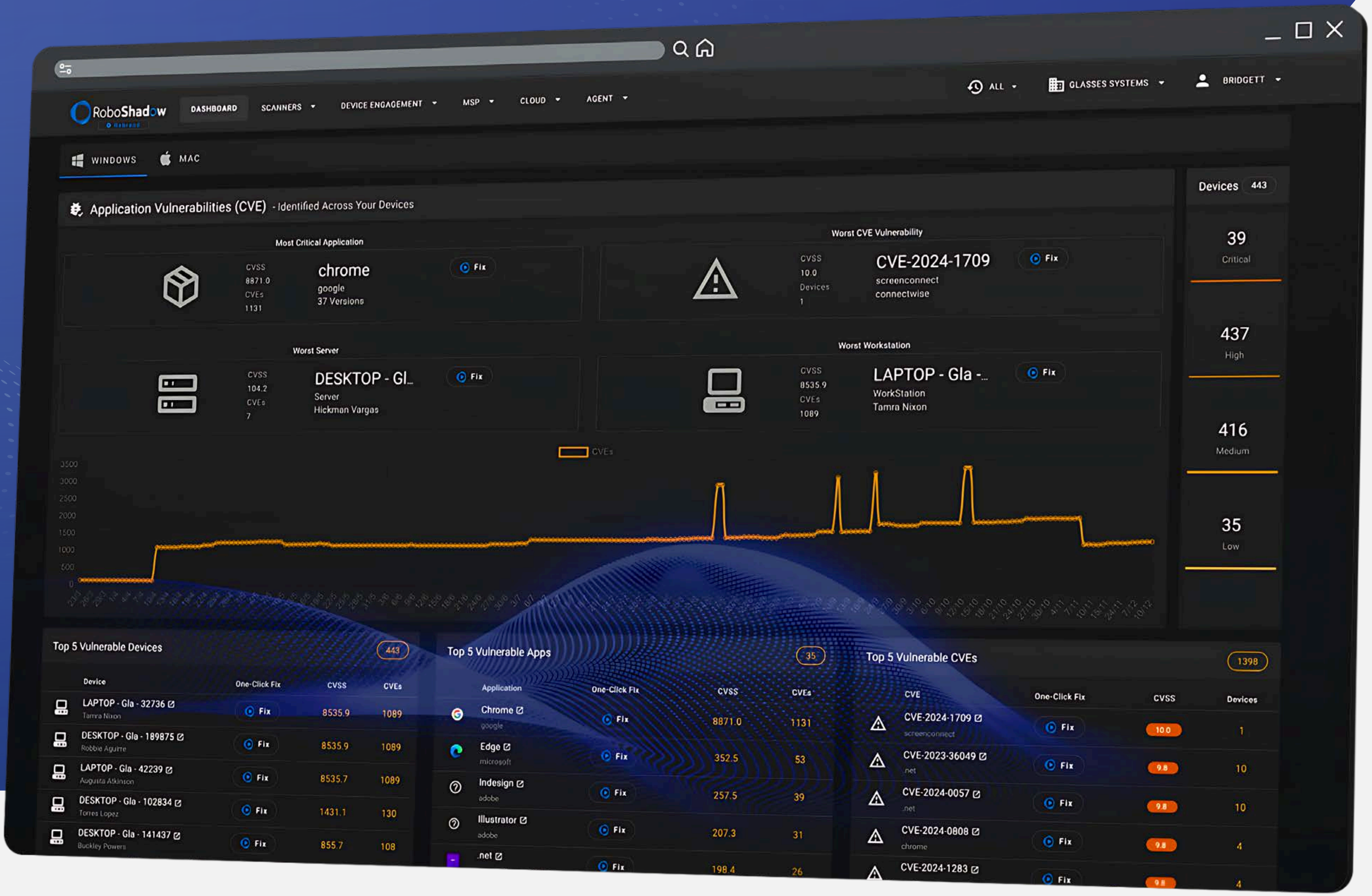
Once the bad guys have got into your network, often **via a vulnerable desktop or an unpatched firewall**, they will look for places to hide seeking cover somewhere more undetectable. Usually this involves establishing a **"reverse shell"** on a printer, scanner or another vulnerable IoT device, allowing them to launch attacks over a longer period. This used to be a manual effort, but now bots and **AI get quietly placed internally somewhere and remain hidden on your network**, ready to "call home" if they manage to exploit a weakness.

The RoboShadow LAN Scanner performs a **device discovery scan on your local network**, followed by a full vulnerability assessment across the whole network subnet. The LAN Scanner shows you what devices internally are vulnerable, and reveals where the bad guys could hide if they get in. The scanner helps you understand and managed your internal attack surface, and covers the following scenarios:

- What **vulnerable IoT Devices** could a hacker hide in?
- Are your networks open (flat), or are they properly segregated?
- Which network equipment has **exploitable vulnerabilities**?

Device Vulnerabilities:

Achieve Zero Trust Status for Your Device Estate



Application Vulnerabilities (CVE) - Identified Across Your Devices

Most Critical Application

CVSS 8871.0
CVEs 1131
chrome
google
37 Versions
Fix

Worst CVE Vulnerability

CVSS 10.0
Devices 1
CVE-2024-1709
screenconnect
connectwise
Fix

Worst Server

CVSS 104.2
CVEs 7
DESKTOP - Gl...
Server
Hickman Vargas
Fix

Worst Workstation

CVSS 8535.9
CVEs 1089
LAPTOP - Gla -...
WorkStation
Tamra Nixon
Fix

Devices 443

39	Critical
437	High
416	Medium
35	Low

Top 5 Vulnerable Devices 443

Device	One-Click Fix	CVSS	CVEs
LAPTOP - Gla - 32736 Tamra Nixon	Fix	8535.9	1089
DESKTOP - Gla - 189875 Robbie Aguirre	Fix	8535.9	1089
LAPTOP - Gla - 42239 Augusta Atkinson	Fix	8535.7	1089
DESKTOP - Gla - 102834 Torres Lopez	Fix	1431.1	130
DESKTOP - Gla - 141437 Buckley Powers	Fix	855.7	108

Top 5 Vulnerable Apps 35

Application	One-Click Fix	CVSS	CVEs
Chrome google	Fix	8871.0	1131
Edge microsoft	Fix	352.5	53
Indesign adobe	Fix	257.5	39
Illustrator adobe	Fix	207.3	31
.net	Fix	198.4	26

Top 5 Vulnerable CVEs 1398

CVE	One-Click Fix	CVSS	Devices
CVE-2024-1709 screenconnect	Fix	10.0	1
CVE-2023-36049 .net	Fix	9.8	10
CVE-2024-0057 .net	Fix	9.8	10
CVE-2024-0808 chrome	Fix	9.8	4
CVE-2024-1283	Fix	9.8	4

Zero Trust Status

The following **five pillars** are essential to pass penetration tests and compliance standards, but more importantly, make it extremely difficult for your workforce to make silly mistakes and compromise security:

1. Does the device have known vulnerabilities?
2. Are laptops and notebooks encrypted?
3. Is antivirus software up-to-date and enabled?
4. Is the operating system updated?
5. Are the 3rd party applications updated?

Getting your devices to a **zero trust** state is the game we are all playing. The challenge of **"How do we lock the IT estate down, but not supress the creativity and agility of the work force?"** is a question every security conscious leader faces daily. Whether your estate is configured with "zero trust" principles (i.e. assuming everything is potentially malicious) is often the deciding factor on whether you will fail an internal penetration test, or worse: get hacked by someone in your workforce clicking on or opening something malicious.

Antivirus Management :

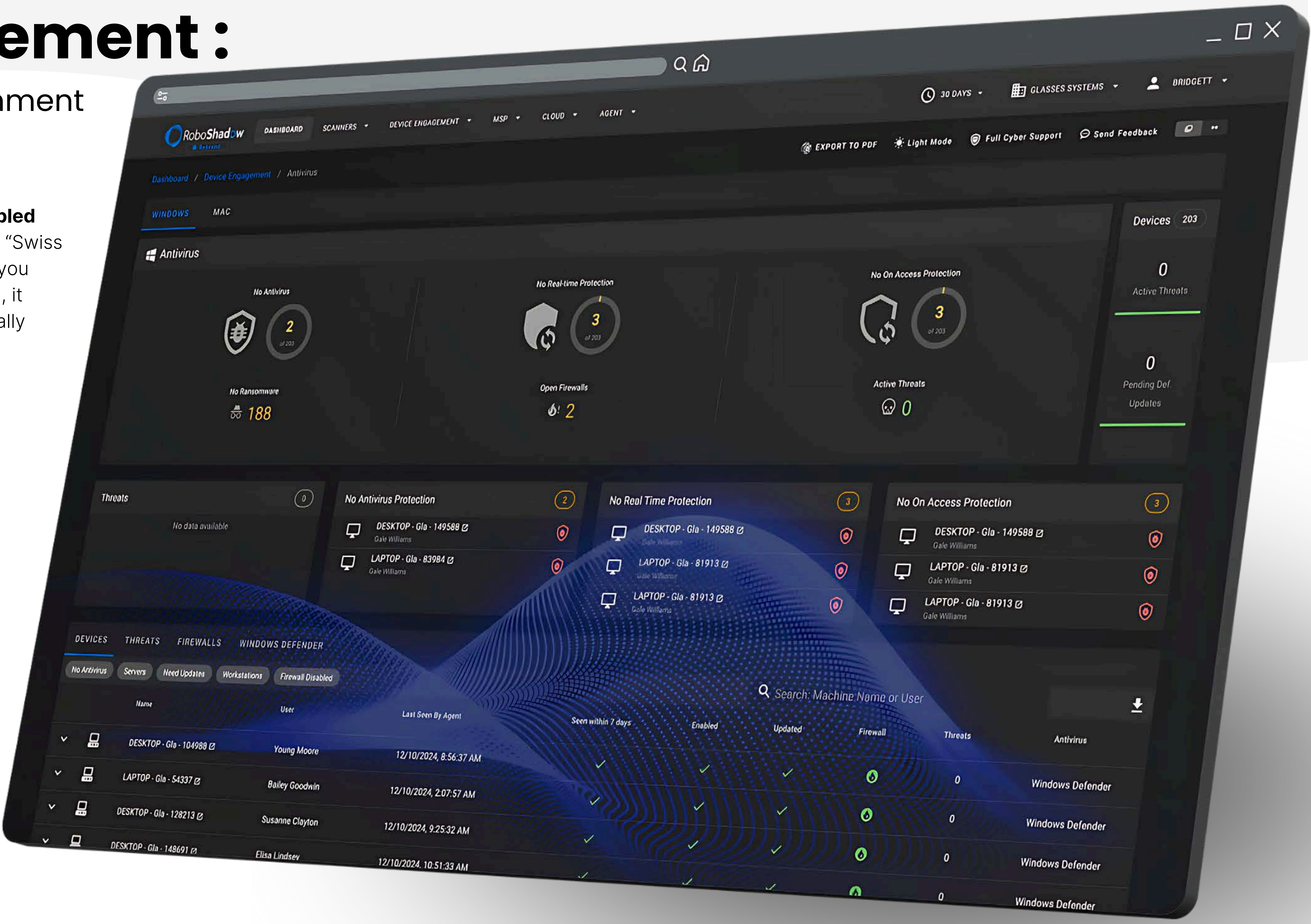
Centrally Monitor All Your AV Environment

Many organisations have a mixture of 3rd Party AV or built in Defender. To pass minimum standards during an internal penetration test, **you will need to know that your AV is enabled** and being updated. AV is often the last line of defence in the “Swiss cheese” security model - where a vulnerable app may make you susceptible to a phishing attack. If your AV is on and working, it might just catch the threat. Many teams do not always centrally manage the AV coverage, and its these often-overlooked oversights which lead to an internal device attack.

RoboShadow **integrates with just about every AV on the planet** and allows you to centrally manage the core fundamentals to check if it’s turned on, and if it’s updated:

- ▶ Is the AV enabled?
- ▶ Is the AV updated?
- ▶ Are there **any actionable alerts**?

+ 20 More



Threats 0

No data available

No Antivirus Protection 2

- DESKTOP - Gla - 149588 — Gale Williams
- LAPTOP - Gla - 83984 — Gale Williams

No Real Time Protection 3

- DESKTOP - Gla - 149588 — Gale Williams
- LAPTOP - Gla - 81913 — Gale Williams
- LAPTOP - Gla - 81913 — Gale Williams

No On Access Protection 3

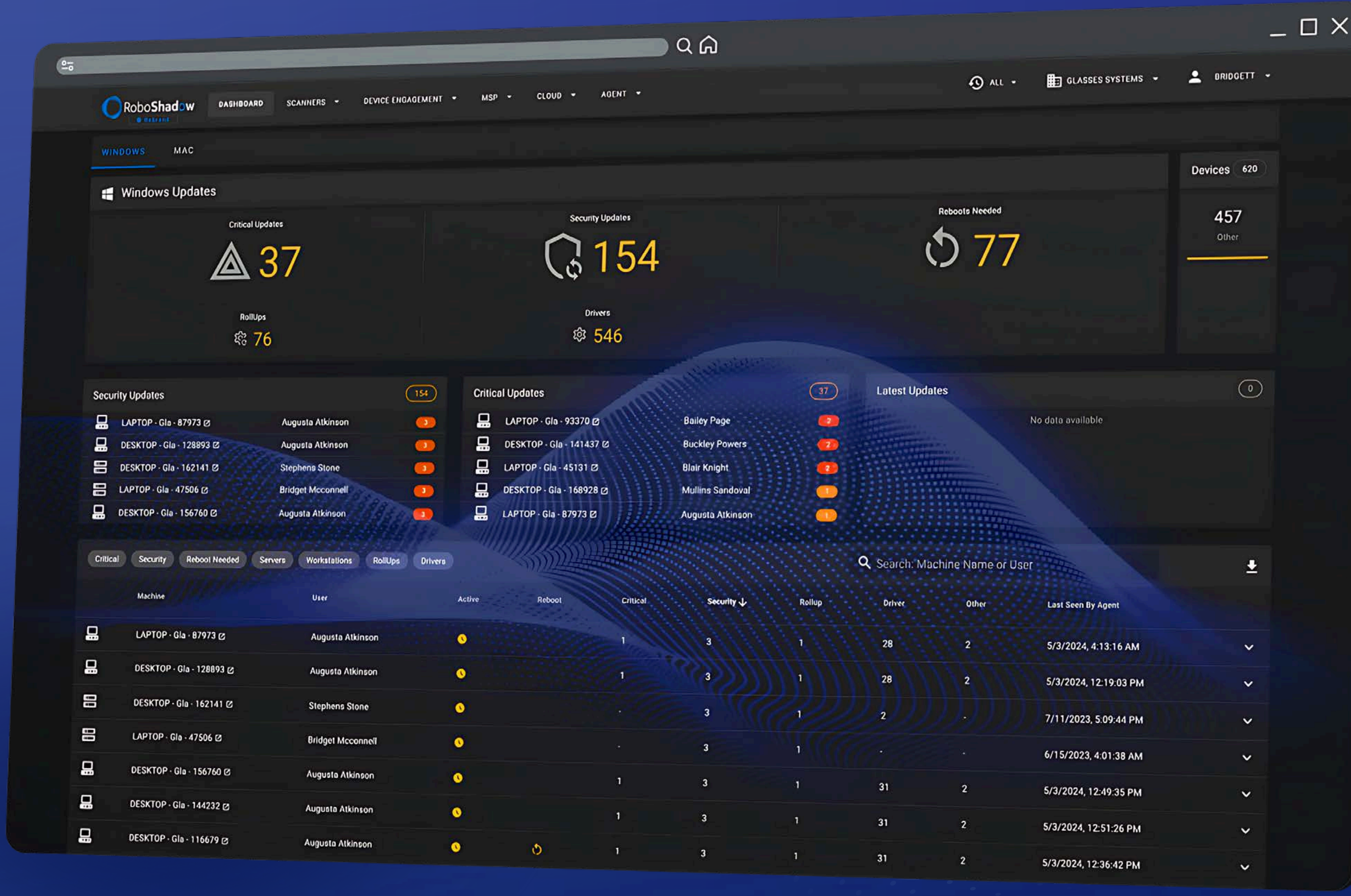
- DESKTOP - Gla - 149588 — Gale Williams
- LAPTOP - Gla - 81913 — Gale Williams
- LAPTOP - Gla - 81913 — Gale Williams

Name	User	Last Seen By Agent	Seen within 7 days	Enabled	Updated	Firewall	Threats	Antivirus
DESKTOP - Gla - 104988	Young Moore	12/10/2024, 8:56:37 AM	✓	✓	✓	●	0	Windows Defender
LAPTOP - Gla - 54337	Bailey Goodwin	12/10/2024, 2:07:57 AM	✓	✓	✓	●	0	Windows Defender
DESKTOP - Gla - 128213	Susanne Clayton	12/10/2024, 9:25:32 AM	✓	✓	✓	●	0	Windows Defender
DESKTOP - Gla - 148691	Elisa Lindsey	12/10/2024, 10:51:33 AM	✓	✓	✓	●	0	Windows Defender

OS Update Oversight :

Ensure Operating Systems Stay Updated

Keeping on top of Operating System updates is still vital. Desktops and laptops tend to manage updates themselves automatically, while server estates still require careful management. OS update **“fire drills”** are quite common. Microsoft, for example, will often give little notice to a Zero-Day fix, leaving IT teams scrambling around to patch a 10-score vulnerability via an OS update.



Windows Updates

Critical Updates 37

Security Updates 154

Reboots Needed 77

RollUps 76

Drivers 546

Devices 620

457 Other

Security Updates 154

LAPTOP - Gla - 87973	Augusta Atkinson	3
DESKTOP - Gla - 128893	Augusta Atkinson	3
DESKTOP - Gla - 162141	Stephens Stone	3
LAPTOP - Gla - 47506	Bridget Mcconnell	3
DESKTOP - Gla - 156760	Augusta Atkinson	3

Critical Updates 37

LAPTOP - Gla - 93370	Bailey Page	2
DESKTOP - Gla - 141437	Buckley Powers	2
LAPTOP - Gla - 45131	Blair Knight	2
DESKTOP - Gla - 168928	Mullins Sandoval	1
LAPTOP - Gla - 87973	Augusta Atkinson	1

Latest Updates 0

No data available

Machine	User	Active	Reboot	Critical	Security ↓	Rollup	Driver	Other	Last Seen By Agent
LAPTOP - Gla - 87973	Augusta Atkinson	●		1	3	1	28	2	5/3/2024, 4:13:16 AM
DESKTOP - Gla - 128893	Augusta Atkinson	●		1	3	1	28	2	5/3/2024, 12:19:03 PM
DESKTOP - Gla - 162141	Stephens Stone	●		-	3	1	2	-	7/11/2023, 5:09:44 PM
LAPTOP - Gla - 47506	Bridget Mcconnell	●		-	3	1	-	-	6/15/2023, 4:01:38 AM
DESKTOP - Gla - 156760	Augusta Atkinson	●		1	3	1	31	2	5/3/2024, 12:49:35 PM
DESKTOP - Gla - 144232	Augusta Atkinson	●		1	3	1	31	2	5/3/2024, 12:51:26 PM
DESKTOP - Gla - 116679	Augusta Atkinson	●	↻	1	3	1	31	2	5/3/2024, 12:36:42 PM

PRODUCT TOUR

RoboShadow

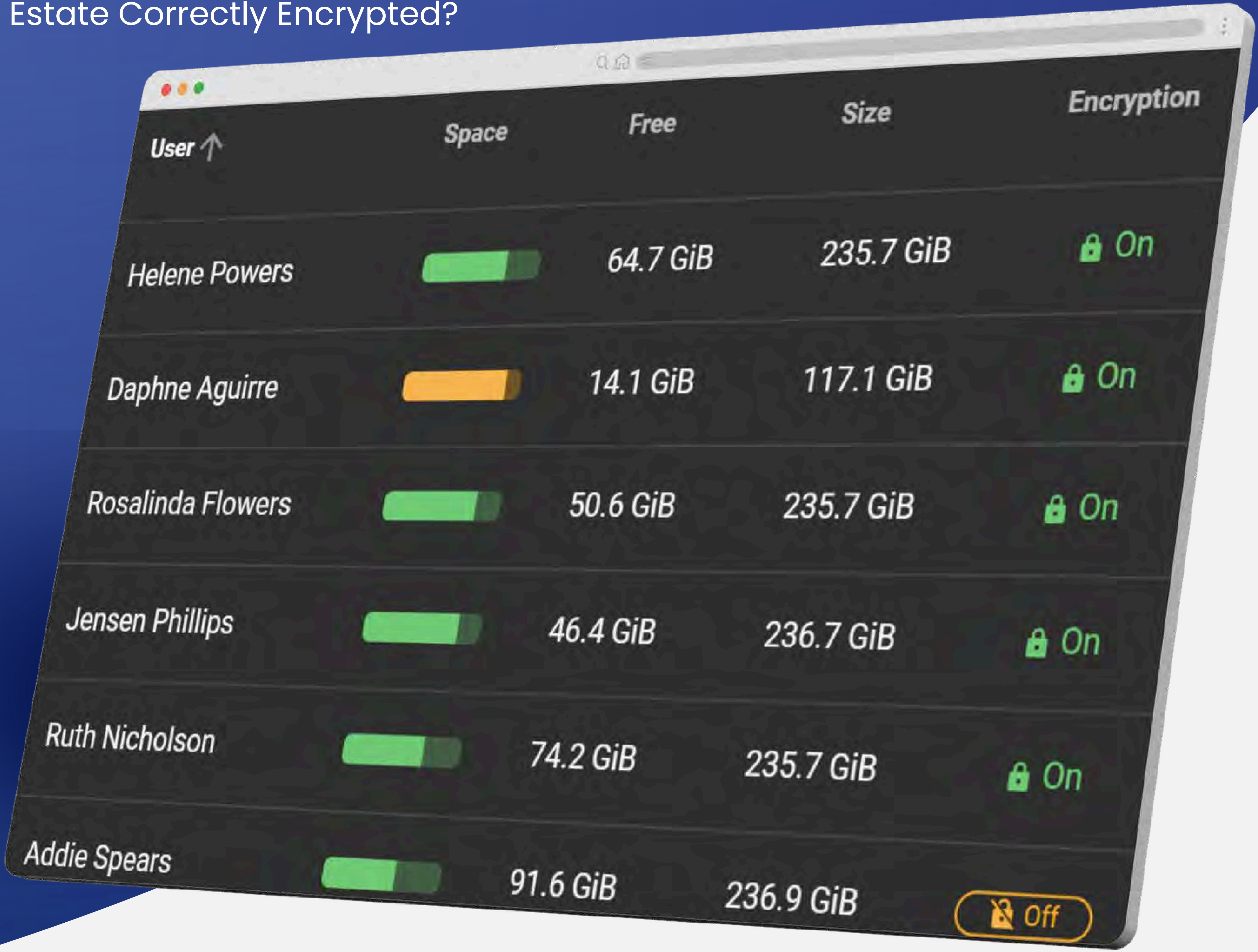
Cyber Management Platform

RoboShadow provides oversight across **the whole OS update ecosystem**, ensuring your compliance requirements and maintain robust security. Key questions include:

- What OS critical and security updates need to be applied?
- Does the machine need to reboot to run updates?
- What driver updates are available to install?

Device Encryption :

Is Your Estate Correctly Encrypted?



User ↑	Space	Free	Size	Encryption
Helene Powers	🟩	64.7 GiB	235.7 GiB	🔒 On
Daphne Aguirre	🟨	14.1 GiB	117.1 GiB	🔒 On
Rosalinda Flowers	🟩	50.6 GiB	235.7 GiB	🔒 On
Jensen Phillips	🟩	46.4 GiB	236.7 GiB	🔒 On
Ruth Nicholson	🟩	74.2 GiB	235.7 GiB	🔒 On
Addie Spears	🟩	91.6 GiB	236.9 GiB	Off

Bitlocker Status

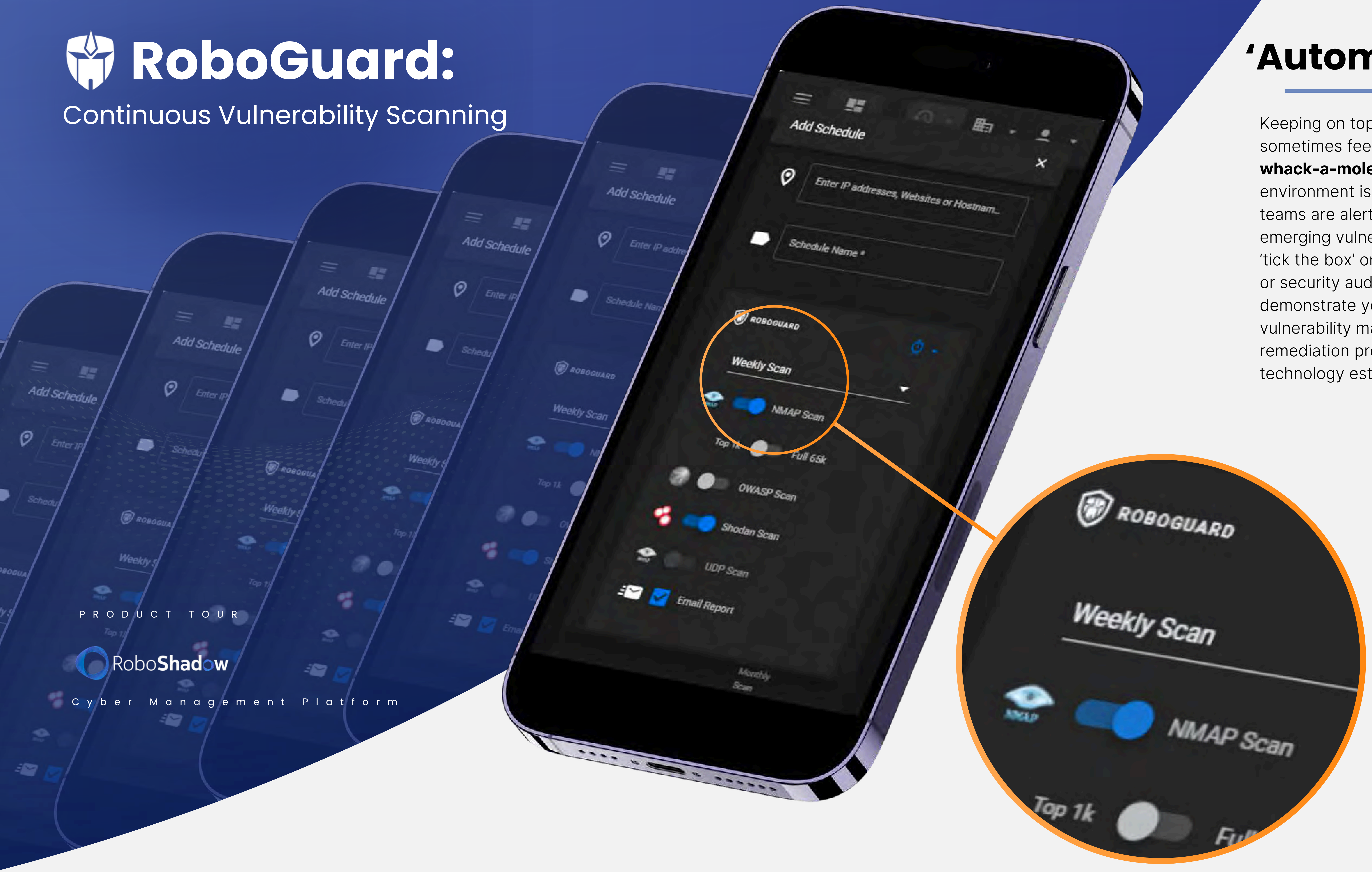
Losing a device on a train that contains customer data can be very scary, especially if the device is not encrypted. **You may have to report to your local data commissioner** or even worse: your customer base, to let them know of a potential breach. Device encryption these days is a ubiquitous requirement, but there are **1001 reasons why encryption fails to be implemented** as part of a user or server deployment.

RoboShadow covers your duty to your **customers, regulators, investors, and staff** by ensuring you have device encryption enabled where you need it, including:

- Which laptops are not encrypted (most important)?
- What folder shares are open on the network?
- Which USB Keys are plugged-in and un-encrypted?

RoboGuard:

Continuous Vulnerability Scanning



Add Schedule

Enter IP addresses, Websites or Hostnam...

Schedule Name *

ROBOGUARD

Weekly Scan

● NMAP Scan

Top 1k ○ Full 65k

○ OWASP Scan

● Shodan Scan

○ UDP Scan

☑ Email Report

Monthly Scan

PRODUCT TOUR

RoboShadow

Cyber Management Platform

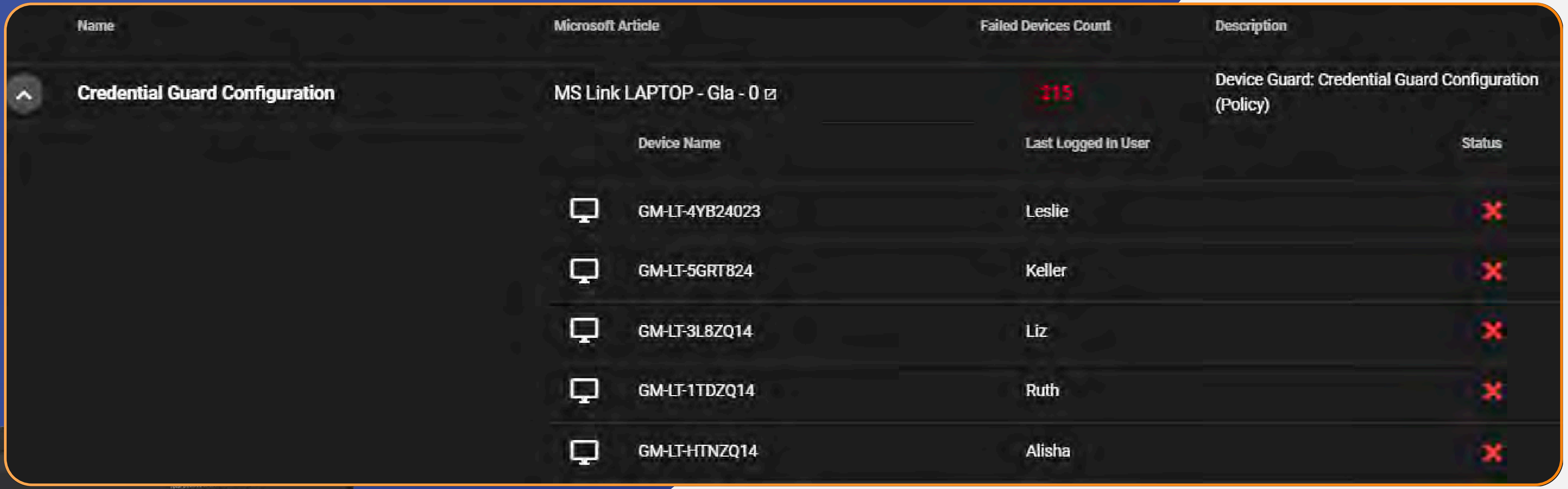
‘Automate Scans’

Keeping on top of your Cyber posture can sometimes feel a bit like a game of **cyber whack-a-mole.** With RoboGuard, your environment is continuously scanned and teams are alerted in real time of newly emerging vulnerabilities. RoboGuard will ‘tick the box’ on any compliance framework or security audit, requiring you to demonstrate you have a continuous vulnerability management, reporting, and remediation process in place across your technology estate:

- Continuously scan Internal & External Networks alongside your Devices.
- Real-time alerts via email or automated tickets log in your PSA or service desk for vulnerabilities found.
- Daily Digest Reports of new items detected across the attack surface.

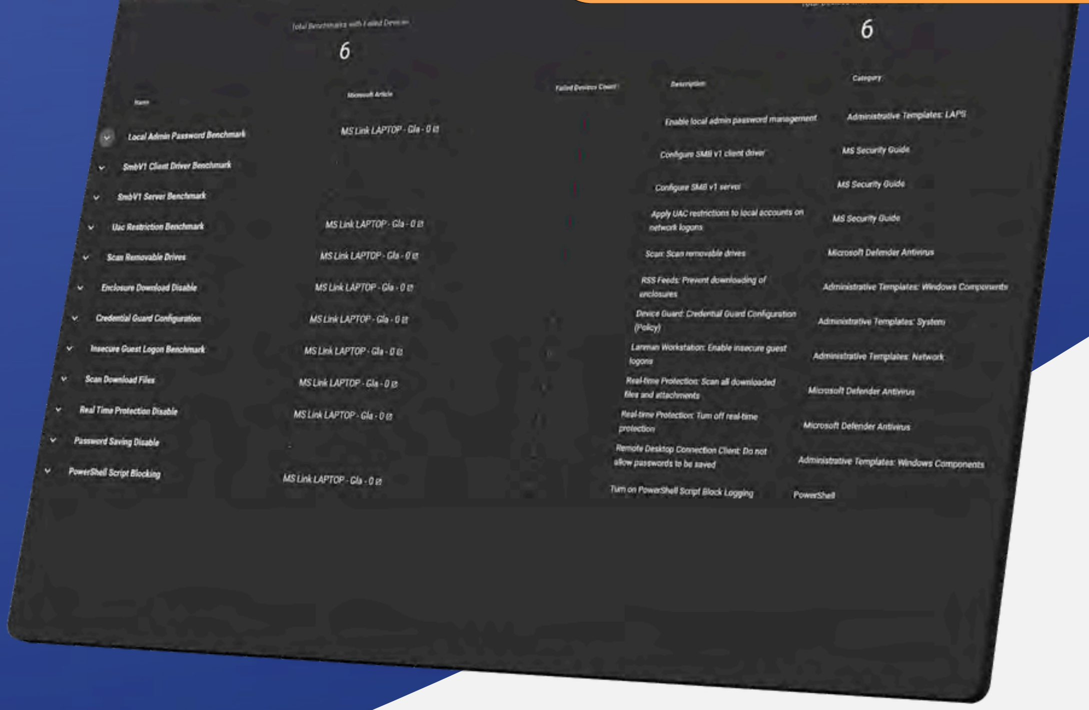
Cyber Benchmarks :

Centrally Keep Tabs on Your Security Benchmarks



Name	Microsoft Article	Failed Devices Count	Description
Credential Guard Configuration	MS Link LAPTOP - Gla - 0 ⧉	215	Device Guard: Credential Guard Configuration (Policy)

Device Name	Last Logged In User	Status
GM-LT-4YB24023	Leslie	✗
GM-LT-5GRT824	Keller	✗
GM-LT-3L8ZQ14	Liz	✗
GM-LT-1TDZQ14	Ruth	✗
GM-LT-HTNZQ14	Alisha	✗



Cyber Benchmarks (Beta)

Total Benchmarks with Failed Devices 6

6

Name	Microsoft Article	Failed Devices Count	Description	Category
Local Admin Password Benchmark	MS Link LAPTOP - Gla - 0 ⧉		Enable local admin password management	Administrative Templates: LAPS
SmbV1 Client Driver Benchmark			Configure SMB v1 client driver	MS Security Guide
SmbV1 Server Benchmark			Configure SMB v1 server	MS Security Guide
Uac Restriction Benchmark	MS Link LAPTOP - Gla - 0 ⧉		Apply UAC restrictions to local accounts on network logons	MS Security Guide
Scan Removable Drives	MS Link LAPTOP - Gla - 0 ⧉		Scan: Scan removable drives	Microsoft Defender Antivirus
Enclosure Download Disable	MS Link LAPTOP - Gla - 0 ⧉		RSS Feeds: Prevent downloading of enclosures	Administrative Templates: Windows Components
Credential Guard Configuration	MS Link LAPTOP - Gla - 0 ⧉		Device Guard: Credential Guard Configuration (Policy)	Administrative Templates: System
Insecure Guest Logon Benchmark	MS Link LAPTOP - Gla - 0 ⧉		Lanman Workstation: Enable insecure guest logons	Administrative Templates: Network
Scan Download Files	MS Link LAPTOP - Gla - 0 ⧉		Real-time Protection: Scan all downloaded files and attachments	Microsoft Defender Antivirus
Real Time Protection Disable	MS Link LAPTOP - Gla - 0 ⧉		Real-time Protection: Turn off real-time protection	Microsoft Defender Antivirus
Password Saving Disable			Remote Desktop Connection Client: Do not allow passwords to be saved	Administrative Templates: Windows Components
PowerShell Script Blocking	MS Link LAPTOP - Gla - 0 ⧉		Turn on PowerShell Script Block Logging	PowerShell

Hardening

Security configuration, or “hardening” as it is called, can be a semi-daunting aspect to manage. However, outside of known vulnerability exploits, exposing a **weakness caused by poor configuration** are the next major threats you must cover.

RoboShadow helps you identify and fix security baseline benchmarks and configurations to keep your estate secure, covering questions such as:

- Are core items locked down e.g., SMB1, TLS Settings etc?
- Do you have rogue local administrator accounts in your estate?
- Do you have the correct password settings and management processes in place

PSA / Ticket Integration:

Actionable Insights Through Ticketing

Staying on top of cyber issues can be challenging. You need enough information to stay safe, but not so much that you are drowning in alerts and become numb. The trick is to **agree a standard for remediation** (for example, **focusing on vulnerabilities with a 7+ severity score**) and manage issues at an application level across the estate to minimise noise. All of this can be achieved via RoboShadow which can integrate with any Service Desk or PSA system on the planet.

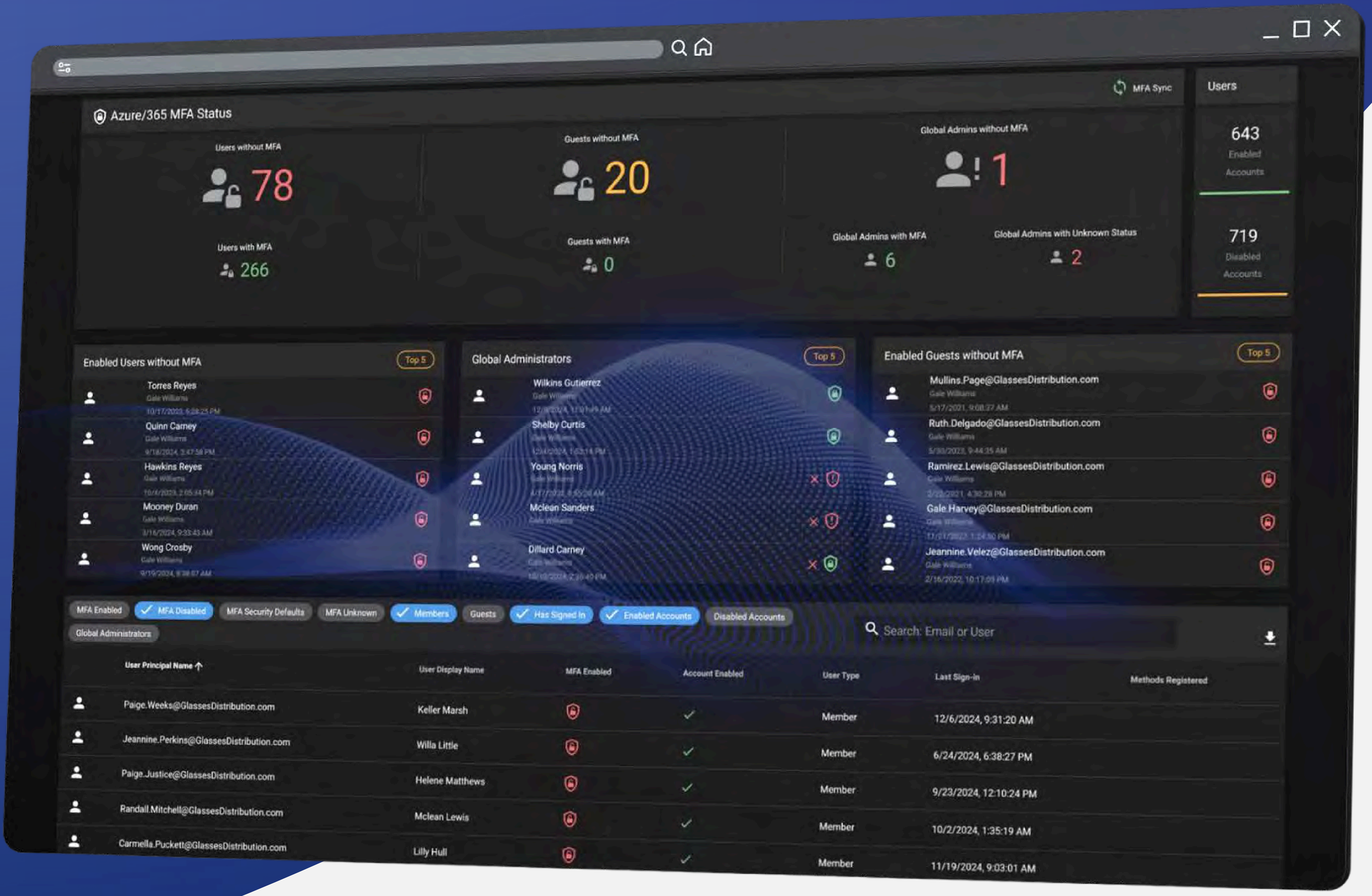
Cyber Efficiency

We integrate with every PSA and ticketing system to:

- ▶ Alert you of any new vulnerabilities **directly** into your Service Desk or PSA system.
- ▶ **Reduce noise** by ensuring only relevant alerts are sent into your ticketing system.
- ▶ Provide **actionable insights** and track accountability over actions and updates through tickets.

365 MFA Sync :

Keep on top of Multi Factor Authentication



Azure/365 MFA Status

MFA Sync

Users without MFA 78

Users with MFA 266

Guests without MFA 20

Guests with MFA 0

Global Admins without MFA 1

Global Admins with MFA 6

Global Admins with Unknown Status 2

Users

643 Enabled Accounts

719 Disabled Accounts

Enabled Users without MFA — Top 5

- Torres Reyes, Gale Williams, 10/17/2023, 6:28:25 PM
- Quinn Carney, Gale Williams, 9/18/2024, 3:47:58 PM
- Hawkins Reyes, Gale Williams, 10/4/2023, 2:05:34 PM
- Mooney Duran, Gale Williams, 3/16/2024, 9:33:43 AM
- Wong Crosby, Gale Williams, 9/19/2024, 8:38:07 AM

Global Administrators — Top 5

- Wilkins Gutierrez, Gale Williams, 12/9/2024, 11:19:49 AM
- Shelby Curtis, Gale Williams, 12/4/2024, 1:52:14 PM
- Young Norris, Gale Williams, 4/17/2023, 8:55:26 AM
- Mclean Sanders, Gale Williams
- Dillard Carney, Gale Williams, 10/10/2024, 2:30:40 PM

Enabled Guests without MFA — Top 5

- Mullins.Page@GlassesDistribution.com, Gale Williams, 5/17/2021, 9:08:27 AM
- Ruth.Delgado@GlassesDistribution.com, Gale Williams, 5/30/2023, 9:44:35 AM
- Ramirez.Lewis@GlassesDistribution.com, Gale Williams, 2/22/2021, 4:30:28 PM
- Gale.Harvey@GlassesDistribution.com, Gale Williams, 11/21/2022, 1:24:30 PM
- Jeannine.Velez@GlassesDistribution.com, Gale Williams, 2/16/2022, 10:17:09 PM

MFA Enabled | ✓ MFA Disabled | MFA Security Defaults | MFA Unknown | ✓ Members | Guests | ✓ Has Signed In | ✓ Enabled Accounts | Disabled Accounts | Global Administrators

Search: Email or User

User Principal Name ↑	User Display Name	MFA Enabled	Account Enabled	User Type	Last Sign-in	Methods Registered
Paige.Weeks@GlassesDistribution.com	Keller Marsh		✓	Member	12/6/2024, 9:31:20 AM	
Jeannine.Perkins@GlassesDistribution.com	Willa Little		✓	Member	6/24/2024, 6:38:27 PM	
Paige.Justice@GlassesDistribution.com	Helene Matthews		✓	Member	9/23/2024, 12:10:24 PM	
Randall.Mitchell@GlassesDistribution.com	Mclean Lewis		✓	Member	10/2/2024, 1:35:19 AM	
Carmella.Puckett@GlassesDistribution.com	Lilly Hull		✓	Member	11/19/2024, 9:03:01 AM	

Microsoft 365

‘One click sync’

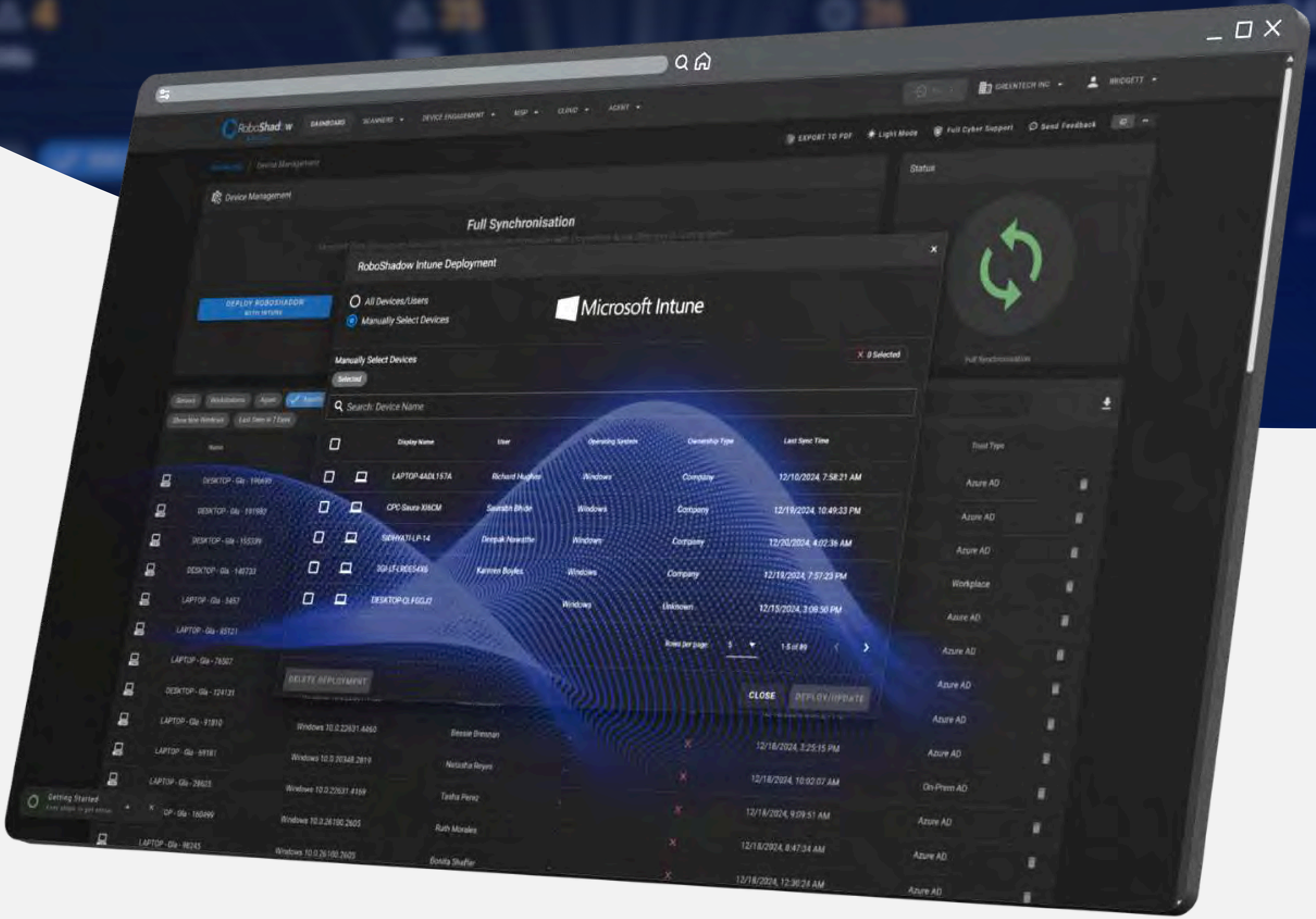
RoboShadow’ s one-click 365 sync enables you to **pull in Microsoft 365 MFA and authentication data** to help you stay on top of the most common way your organisation is likely to be hacked. Phishing exploits remain one of the most common way a network is breached and is now proliferate **by large AI farms**. Many organisations think “Well hang on, we have MFA in place!?” but the truth is that there are lots of workarounds - including exception policies and config mishaps - which leads fragmented MFA compliance across the estate.

RoboShadow helps you maintain a consistent and effective MFA strategy by addressing the following scenarios:

- Which accounts do not have MFA enabled?
- What redundant accounts can be disabled?
- How are Global Admins being managed in 365?
- What “outside guests” have access to your 365 universe?

Intune Integration :

Roll Out via Intune in One Click



Full Synchronisation

RoboShadow Intune Deployment

○ All Devices/Users
● Manually Select Devices

Microsoft Intune

Manually Select Devices

Selected

0 Selected

Search: Device Name

□		Display Name	User	Operating System	Ownership Type	Last Sync Time
□	💻	LAPTOP-4ADL157A	Richard Hughes	Windows	Company	12/10/2024, 7:58:21 AM
□	💻	CPC-Saura-XI6CM	Saurabh Bhide	Windows	Company	12/19/2024, 10:49:33 PM
□	💻	SIDHYATI-LP-14	Deepak Nawathe	Windows	Company	12/20/2024, 4:02:36 AM
□	💻	SGI-LT-LR0E54X6	Kamren Boyles	Windows	Company	12/19/2024, 7:57:23 PM
□	💻	DESKTOP-CLFGGJ2		Windows	Unknown	12/15/2024, 3:09:50 PM

Rows per page: 5 ▾ 1-5 of 89 ‹ ›

DELETE DEPLOYMENT

CLOSE DEPLOY/UPDATE

Microsoft Integrated

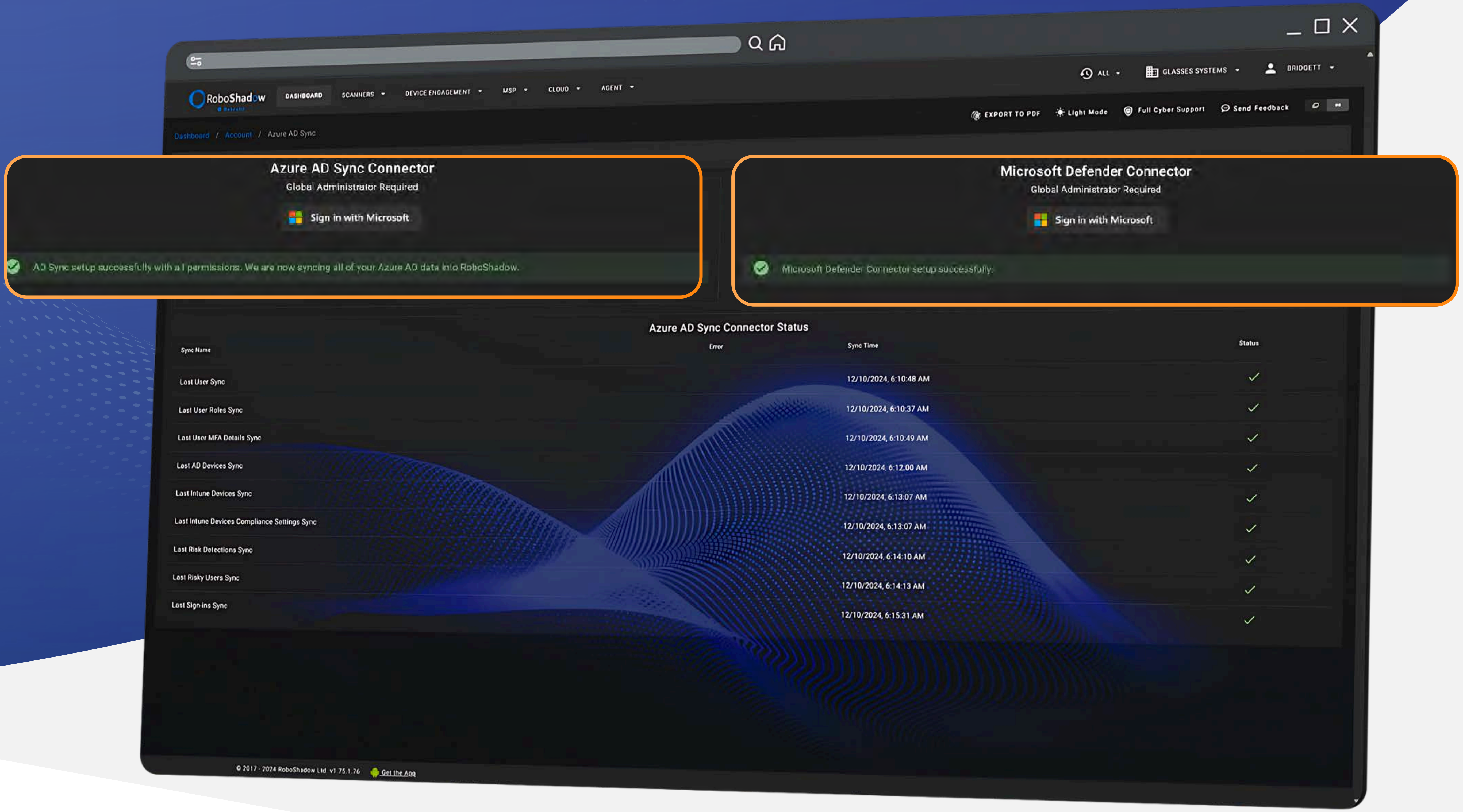
With Intune, you can easily roll out the RoboShadow agent and keep your estate protected through RoboShadow’ s RoboGuard and Cyber Heal Autopilot: all via a one-click Intune process. RoboShadow also ingests Intune data to alert you to devices not managed in Intune, as well as tracking risky sign in data coming from Intune.

It is easy to fully roll out RoboShadow to your complete estate using Intune to:

- One-Click-Sync with Intune data.
- One-Click roll out the RoboShadow Agent via Intune on all your devices.
- Receive Intune coverage reports and analyse risk sign-in data.

Windows Defender Sync :

Pull in Golden Vulnerability Data from Defender



Azure AD Sync Connector

Global Administrator Required

AD Sync setup successfully with all permissions. We are now syncing all of your Azure AD data into RoboShadow.

Microsoft Defender Connector

Global Administrator Required

Microsoft Defender Connector setup successfully.

Azure AD Sync Connector Status

Sync Name	Error	Sync Time	Status
Last User Sync		12/10/2024, 6:10:48 AM	✓
Last User Roles Sync		12/10/2024, 6:10:37 AM	✓
Last User MFA Details Sync		12/10/2024, 6:10:49 AM	✓
Last AD Devices Sync		12/10/2024, 6:12:00 AM	✓
Last Intune Devices Sync		12/10/2024, 6:13:07 AM	✓
Last Intune Devices Compliance Settings Sync		12/10/2024, 6:13:07 AM	✓
Last Risk Detections Sync		12/10/2024, 6:14:10 AM	✓
Last Risky Users Sync		12/10/2024, 6:14:13 AM	✓
Last Sign ins Sync		12/10/2024, 6:15:31 AM	✓

© 2017 - 2024 RoboShadow Ltd v1 75.1.76

Defender Sync

If you have a Business Premium Subscription in Microsoft 365, then you already have access to a major source of vulnerability data in Windows Defender as part of the package. However, managing this data and making it actionable is hard. Using RoboShadow, you can pull in your Windows Defender data and turn it into actionable insights by creating simple reports, AI Pen tests, or simply automatically creating tickets into your PSA and ticketing systems helping you manage and stay on top of the vulnerabilities.

RoboShadow completely enhances the Microsoft 365 and Defender device vulnerability strategy by:

- Centrally managing device vulnerabilities from Defender and Microsoft 365.
- Logging PSA or service desk Tickets based on your Microsoft Defender data.
- Making real use of your investment into 365 Business Premium, by including Tier-1 Defender vulnerability data.

Advanced Cyber Reporting:

Getting neat Cyber Security reports

Getting reports which **give guidance instead of anxiety**, actionable intelligence and avoiding alert fatigue is the dream of all security-aware teams. RoboShadow delivers high level management overviews that offer a vast range of detailed **vulnerability level exposure and prioritisation** guidance. Getting hold of the accurate, meaningful, and fair cybersecurity data is a challenge that everyone is trying to solve

At RoboShadow we have solved this through our reporting engine, allowing you to answer the following reporting scenarios:

- Do you have a **board-level management** summary?
- Do you have **device-level vulnerability** reporting?
- Do you have **clear prioritisation and remediation guidance**?

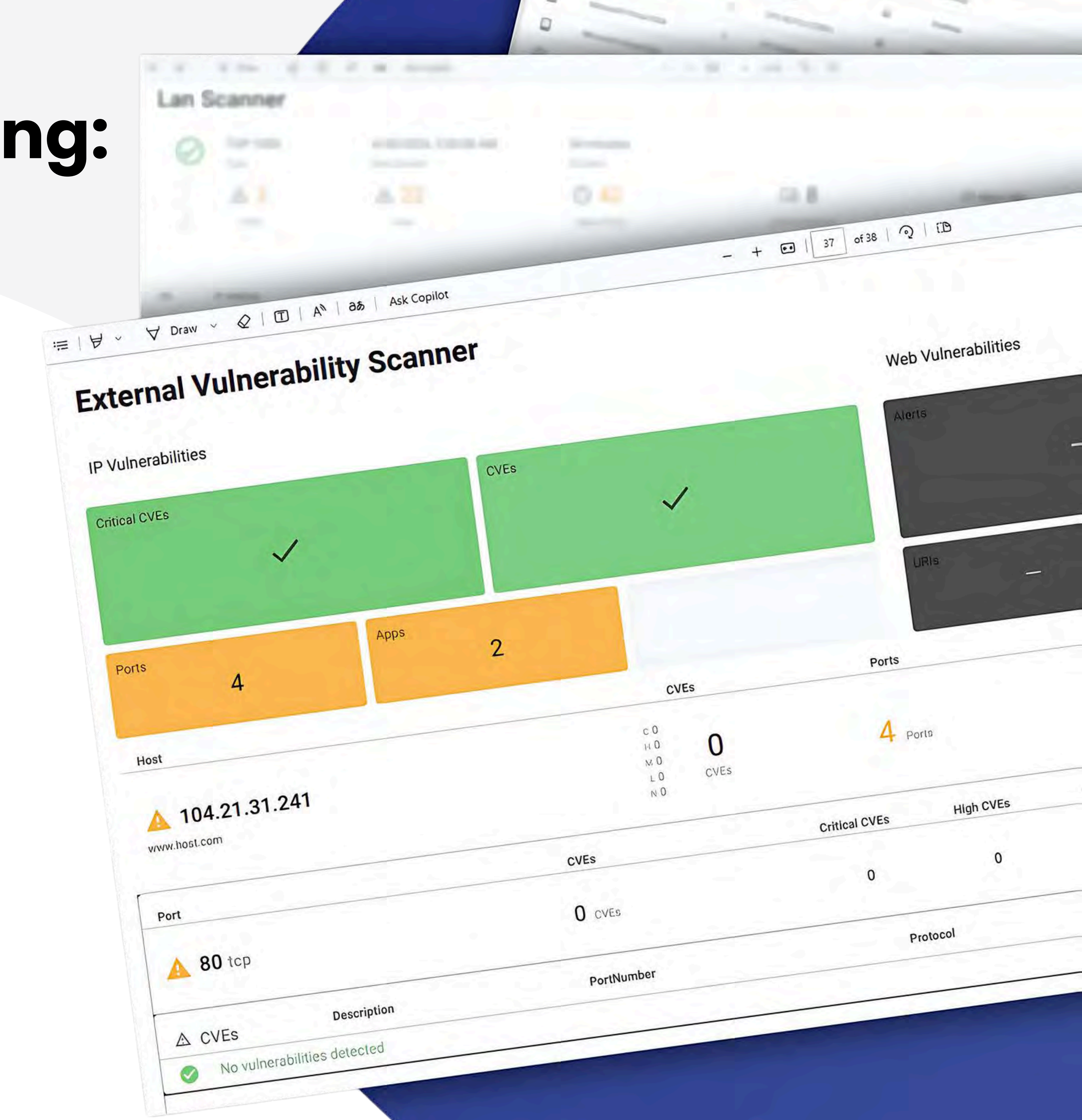
Cyber Report ***Daily Report*** ***AI Pen Test***

**NOT AVAILABLE UNTIL Q1 2025 **

PRODUCT TOUR

RoboShadow

Cyber Management Platform



External Vulnerability Scanner

IP Vulnerabilities

Critical CVEs ✓

CVEs ✓

Ports 4

Apps 2

Web Vulnerabilities

Alerts —

URIs —

Host	CVEs	Ports
104.21.31.241 www.host.com	C 0 H 0 M 0 L 0 N 0 0 CVEs	4 Ports

	CVEs	Critical CVEs	High CVEs
		0	0

Port		CVEs
80 tcp		0 CVEs

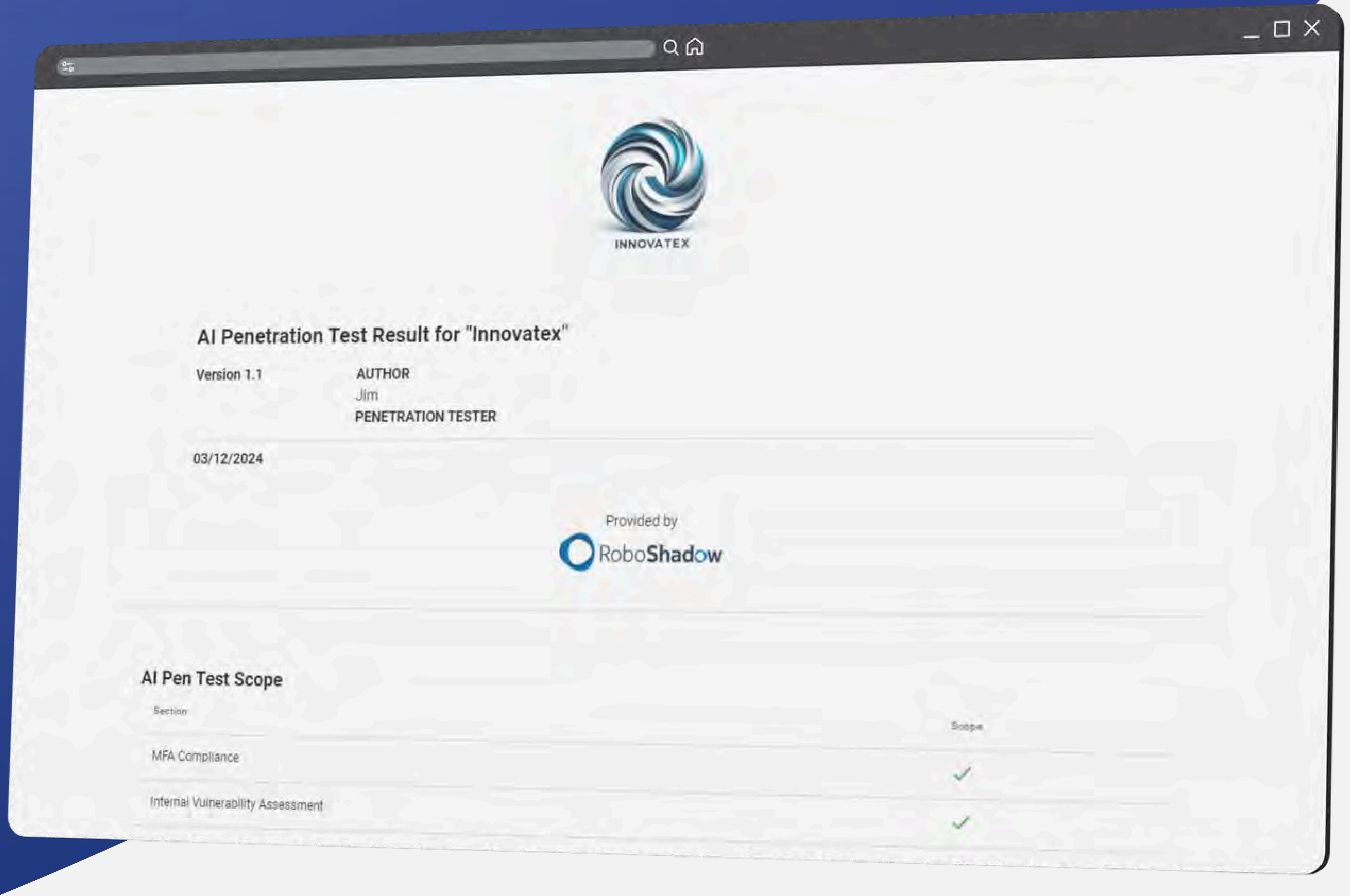
	Description	PortNumber	Protocol

CVEs

No vulnerabilities detected

AI Pen Test :

"In the Middle" of a Vulnerability Assessment and a Penetration Test



INNOVATEX

AI Penetration Test Result for "Innovatex"

Version 1.1

AUTHOR
Jim
PENETRATION TESTER

03/12/2024

Provided by
RoboShadow

AI Pen Test Scope

Section	Scope
MFA Compliance	✓
Internal Vulnerability Assessment	✓

Is it a bird? is it a plane? No, its an AI Pentest.

Often a vulnerability assessment is not enough for every compliance situation, but a full penetration test can be too expensive and **"out of reach"** for many organisations. RoboShadow' s AI Pentest uses trained LLMs to give you a penetration test feel to your vulnerability reporting. The AI overlay gives you the all-important scope, management overview, and strategy suggestions, much like a full penetration test process will do..

Key items you need included in a penetration test, which are covered as part of the RoboShadow AI Pentest include:

- The scope and toolset used to conduct the assessment.
- A management overview and overall scoring.
- Vulnerability and **exploit information** discovered during the test.
- Actionable next steps and **strategy suggestions**

Compliance Exports :

How do you prove your cyber posture to the world ?

CYBER ESSENTIALS

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations ™

ISO 27001

HIPAA

NIST

Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security Centre

Essential 8

Showing Proof to Your Clients , Regulators & Investors

Around the world, we all have different ways of proving our cyber security posture. For many businesses, using a **good governance framework** is a great way of proving to your customers, regulators, and investors how seriously you take your cyber governance.

RoboShadow has a compliance engine built within the platform, allowing you to export evidence data for a whole host of cyber governance frameworks including but not limited to:

- *Cyber Essentials (UK)*
- *Essential 8 (Australia)*
- *NIST (US)*
- *SOC 2 (Worldwide)*
- *ISO 27001 (Worldwide)*
- *HIPPA (US)*

**NOT AVAILABLE UNTIL Q1 2025 **

Notes from our CEO :

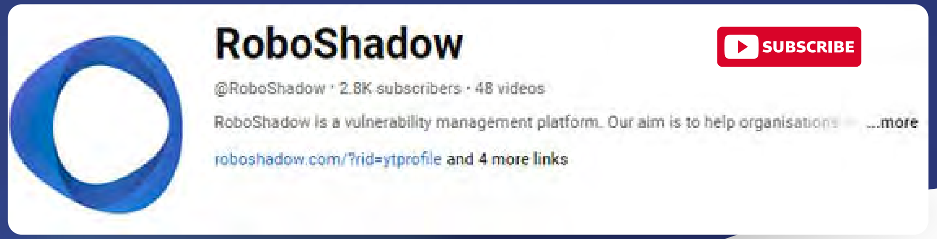
Our commitment to technology

When we set out to build RoboShadow, our mission was to **disrupt an industry that is full of overpriced incumbents** often relying on fear to sell their solutions. Cyber security doesn't need to be overcomplicated, nor sold on fear. In fact, winning the complexity game for cyber security is done through having solid product management and getting your hands dirty with lots of very messy, ungoverned data.

The real trick for us has been addressing the cost, trying to make the vulnerability data efficient and therefore cheaper to manage has been somewhat of a challenge. The net result is that we sit on top of a completely integrated microservices platform on AWS. This state of the art, completely serverless platform, allows us to effectively commoditise the cybersecurity data, allowing us to distribute it to users a lot more cost effectively. This has been a learning curve for us like no other. However, there has been one glorious benefit that both the engineering team and the users enjoy alike. We release changes almost daily in a very contemporary continuous delivery model. Our engineering pedigree was forged in the world of investment banking, and the team and I really enjoy the challenge of trying to make cyber security less complex, less costly, and available to all.

Terry Lewis

Terry Lewis
CEO


RoboShadow

@RoboShadow · 2.8K subscribers · 48 videos

RoboShadow is a vulnerability management platform. Our aim is to help organisations ...more

roboshadow.com/?rid=ytprofile and 4 more links

National Cyber
Security Centre
For Startups
Alumni