PRODUCT TOUR

RoboShadow

Cyber Management Platform

National Cyber Security Centre *For Startups* Alumni

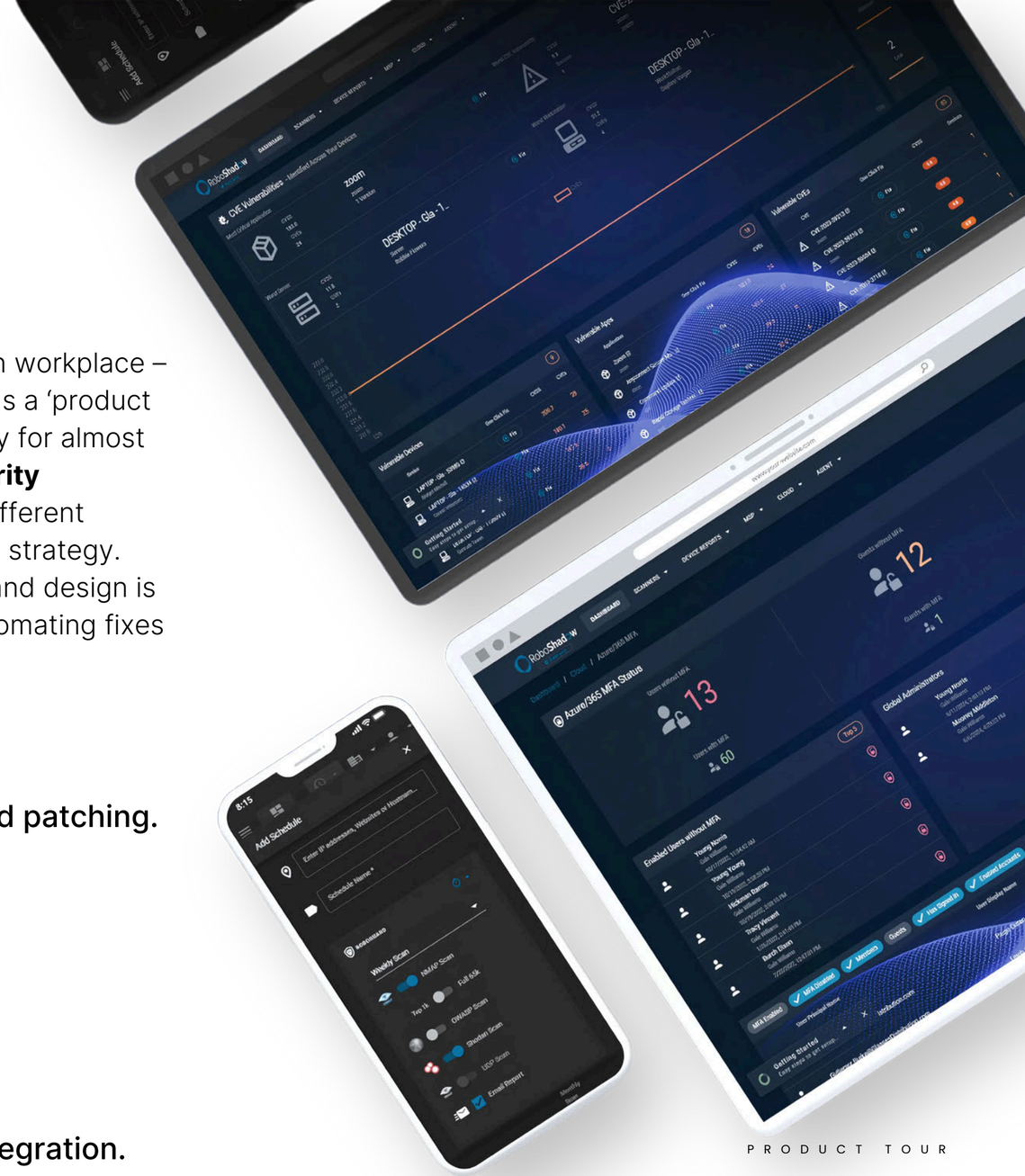


Demystify Cybersecurity For

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 this brochure as a 'product tour' to demonstrate just how RoboShadow helps to manage a modern cyber security capability for almost any organisation. We estimate that RoboShadow covers around **75% of corporate cyber security responsibilities.** 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. Our 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.



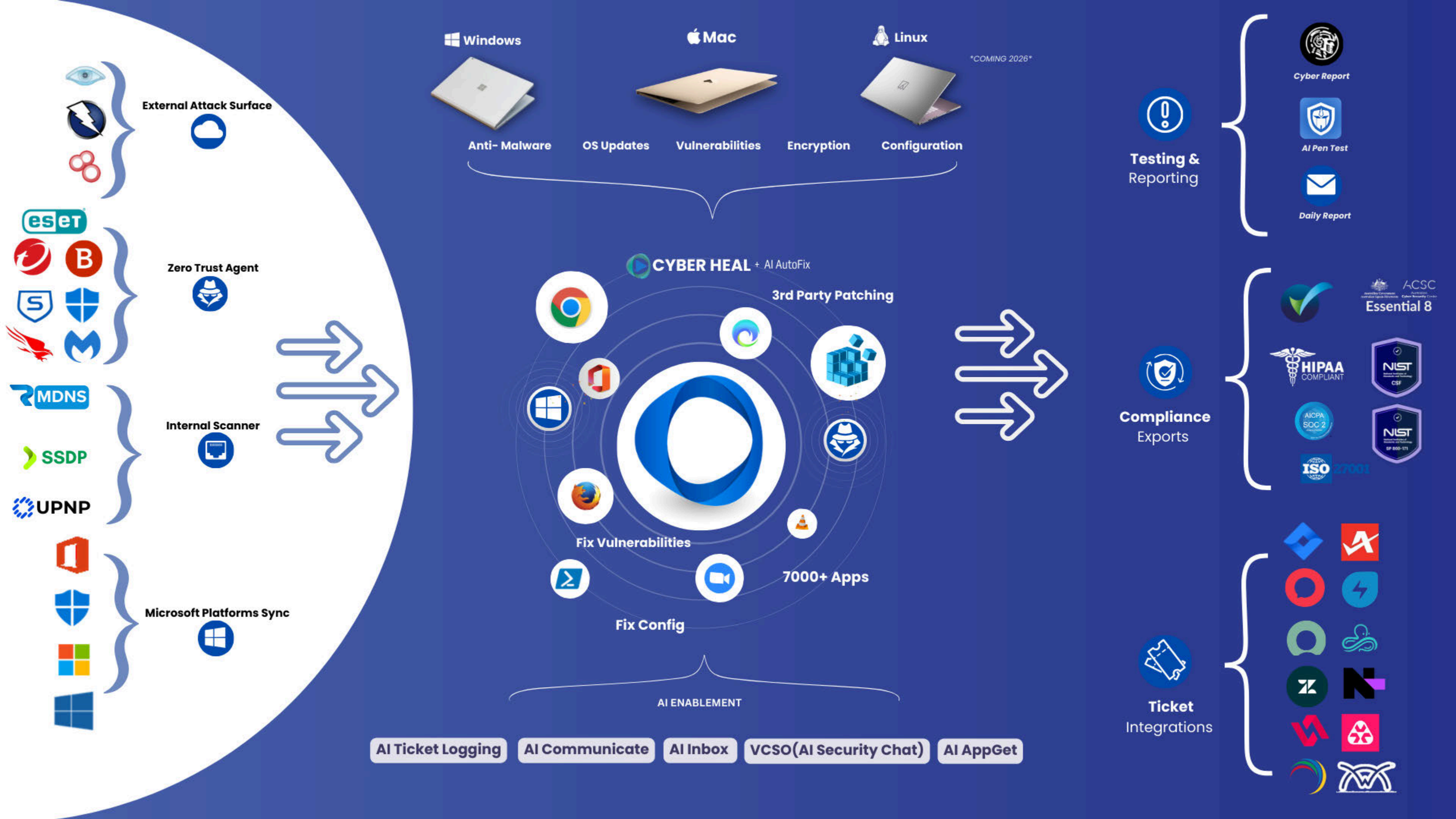
What RoboShadow Can Do in a Nutshell:

- 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.

PRODUCT TOUR

RoboShadow

Cyber Management Platform


Windows
Mac
Linux
COMING 2026
Anti- Malware
OS Updates
Vulnerabilities
Encryption
Configuration
External Attack Surface
Zero Trust Agent
Internal Scanner
Microsoft Platforms Sync
MDNS
SSDP
UPNP
CYBER HEAL + AI AutoFix
3rd Party Patching
Fix Vulnerabilities
7000+ Apps
Fix Config
AI ENABLEMENT
AI Ticket Logging
AI Communicate
AI Inbox
VCSO(AI Security Chat)
AI AppGet
Testing & Reporting
Cyber Report
AI Pen Test
Daily Report
Compliance Exports
ACSC Essential 8
HIPAA COMPLIANT
AICPA SOC 2
ISO 27001
Ticket Integrations

AI AutoFix (Cyber Heal) :

Auto Pilot Fixing Vulnerabilities



‘AI AutoFix’

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.

▶ 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.

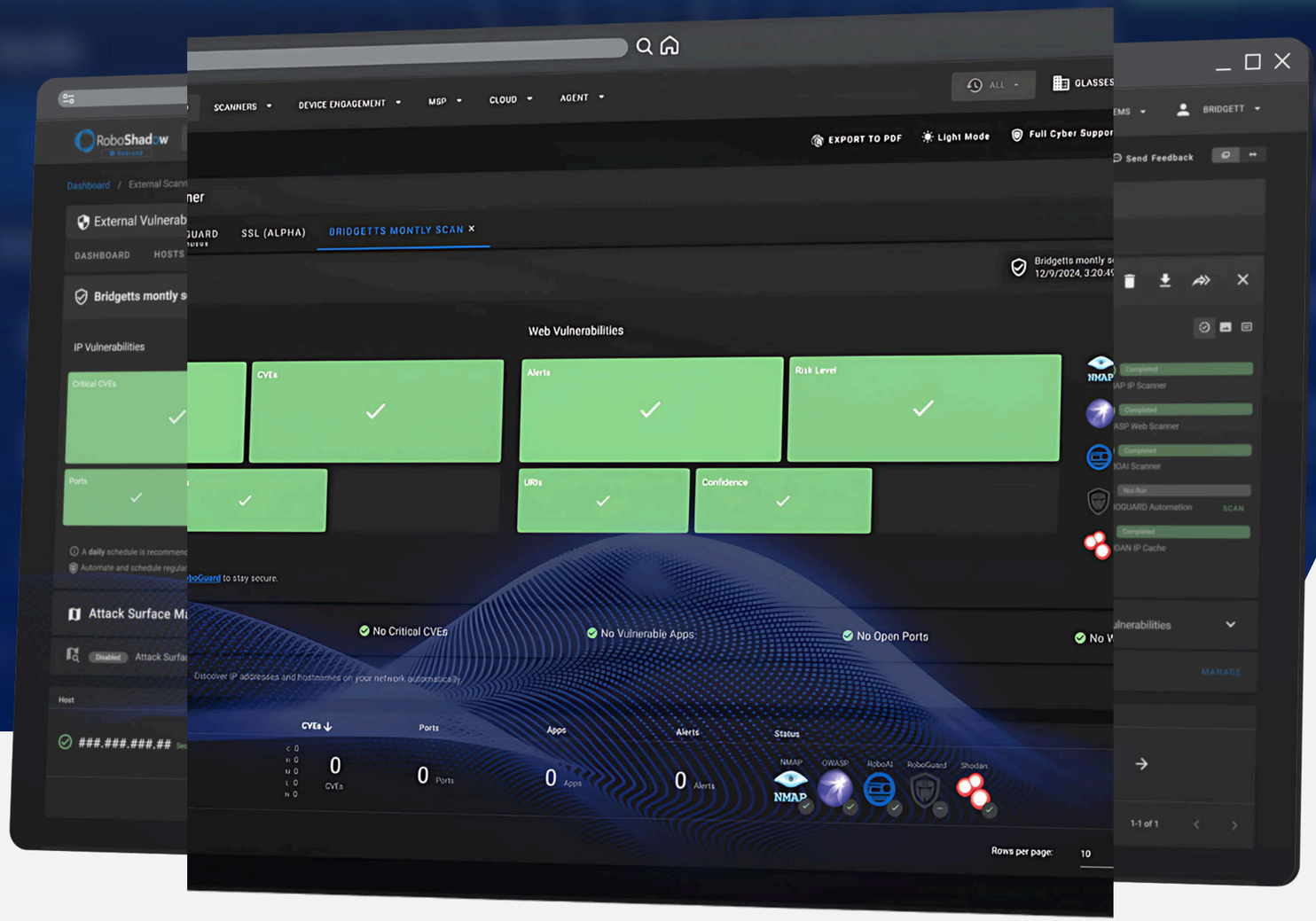
▶ Update **Firewall and Anti-Ransomware** settings.

▶ **Automate** all the Cyber Heal tasks in the background with AutoFix.

▶ Log any **AutoFix** fails into your Service Desk System / PSA for a follow-up.

External Scanner :

Manage the External Attack Surface



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.

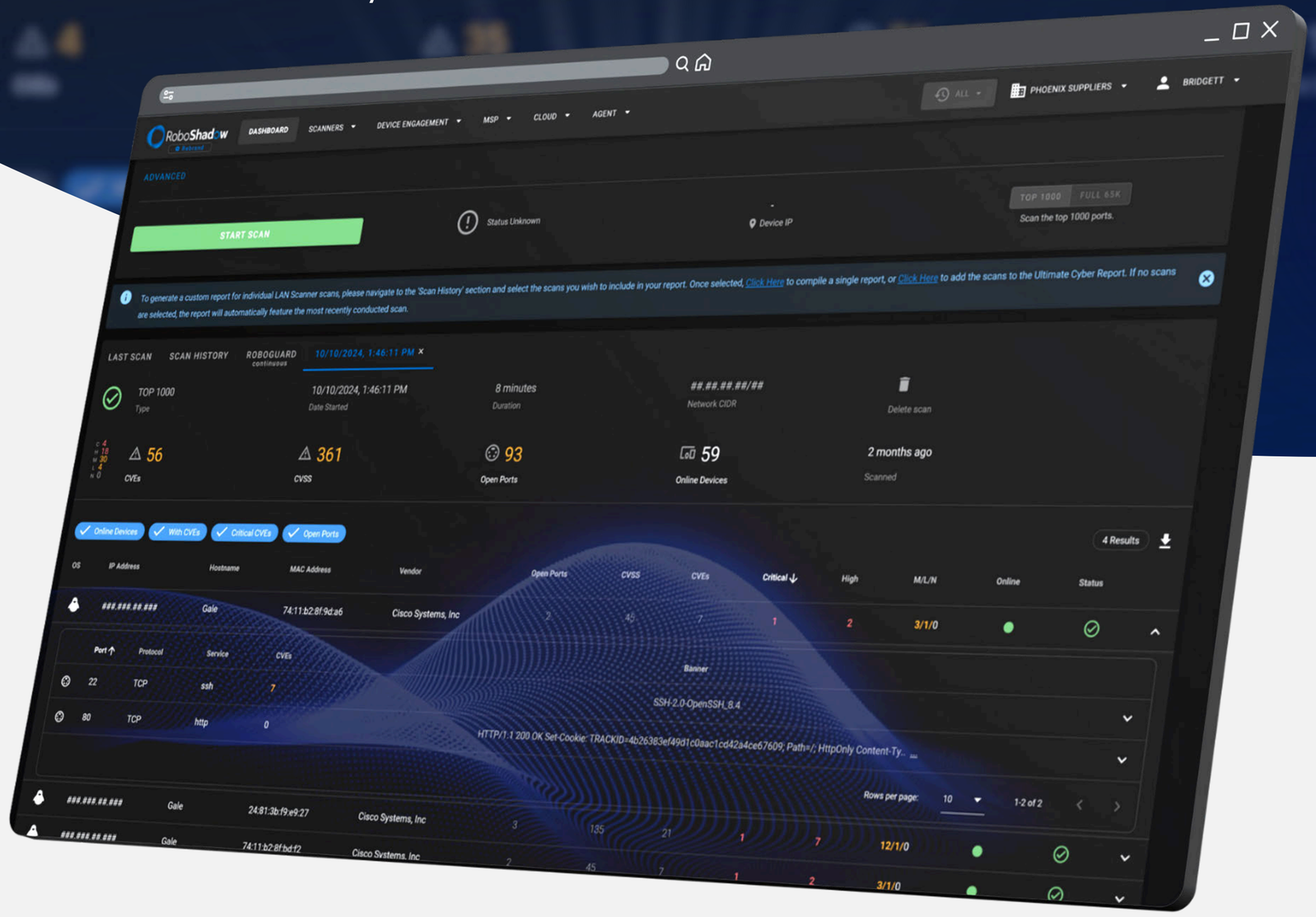
Our external attack surface scanner leverages the best of the open-source technology, and our proprietary RoboShadow technology to continuously cover the following scenarios:

- ▶ 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!



Scan Individual Devices

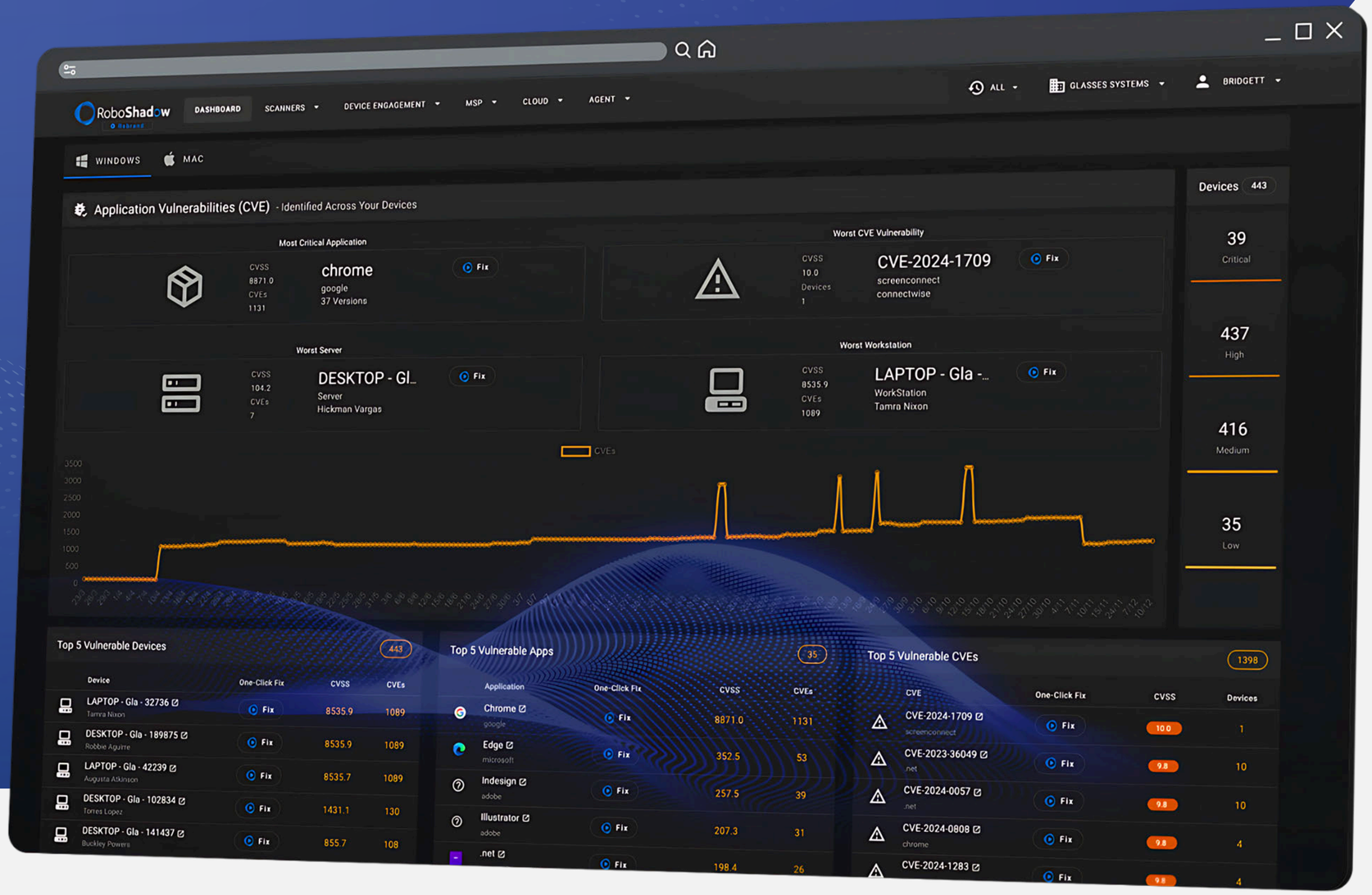
Once the bad guys have got into your network, often **via a vulnerable desktop or an unpatched firewall**, they will look for places to hide seeking cover somewhere more undetectable. Usually this involves establishing a **"reverse shell"** on a printer, scanner or another vulnerable IoT device, allowing 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



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



OS Update Patching 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.

OS Update Oversight continuously monitors Windows devices through the RoboShadow agent for missing security patches, critical updates, and roll-ups, presenting this information in a centralised dashboard that highlights which machines are falling behind and need attention.

When patching is required, AutoHeal can automatically deploy Windows security updates and identify devices that require a reboot to complete the process, enabling both automated remediation and manual oversight for business-critical servers.



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?
- Runs full patching windows via device groups
- Does the machine need to reboot to run updates?
- What driver updates are available to install?

Device Bitlocker Encryption:

Is Your Estate Correctly Encrypted?



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



PRODUCT TOUR

RoboShadow

Cyber Management Platform

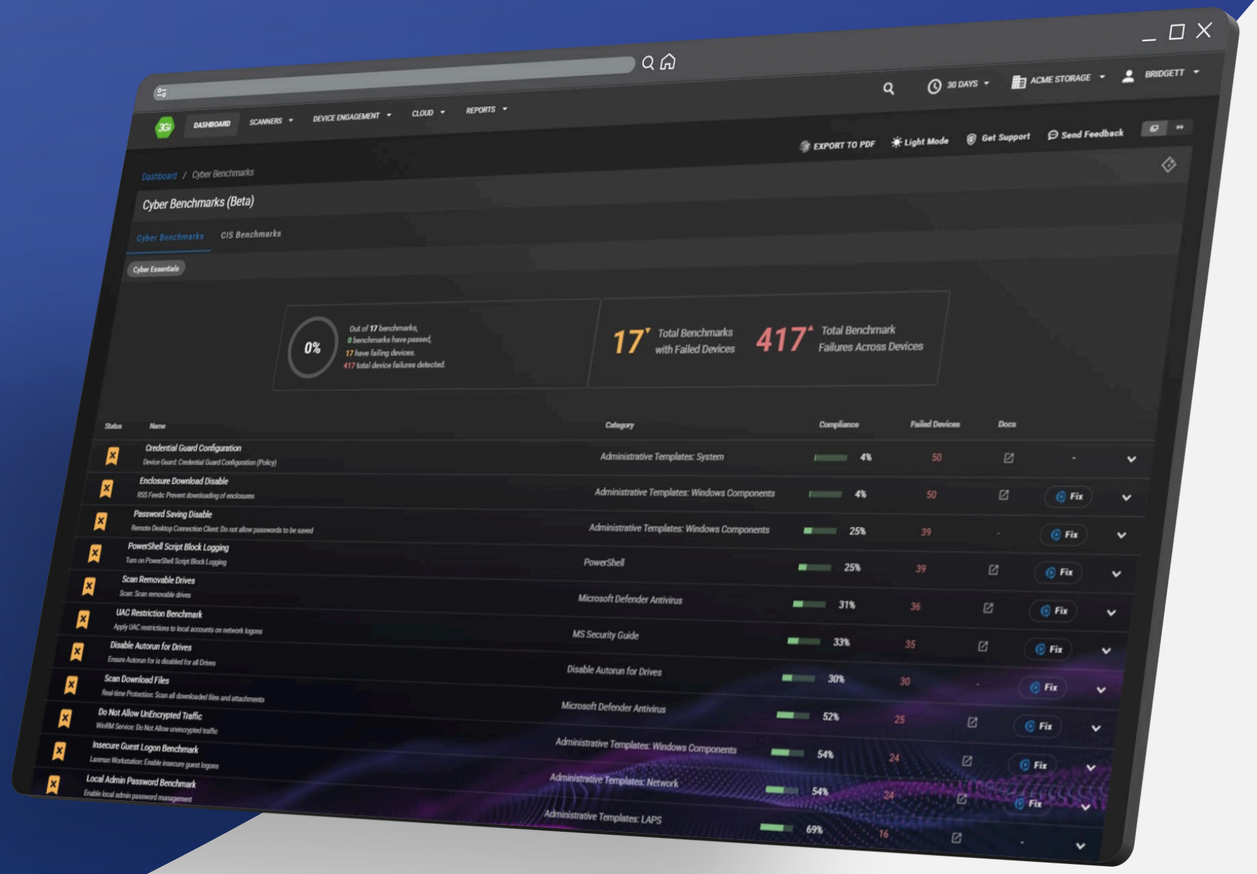
‘Automate Scans’

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



Configuration Hardening

Security configuration 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 then remediate using AI AutoFix any configuration vulnerabilities we have against the **universal cyber benchmarks** standard. We help you answer such questions 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?

365 CIS Benchmarks :



Microsoft 365

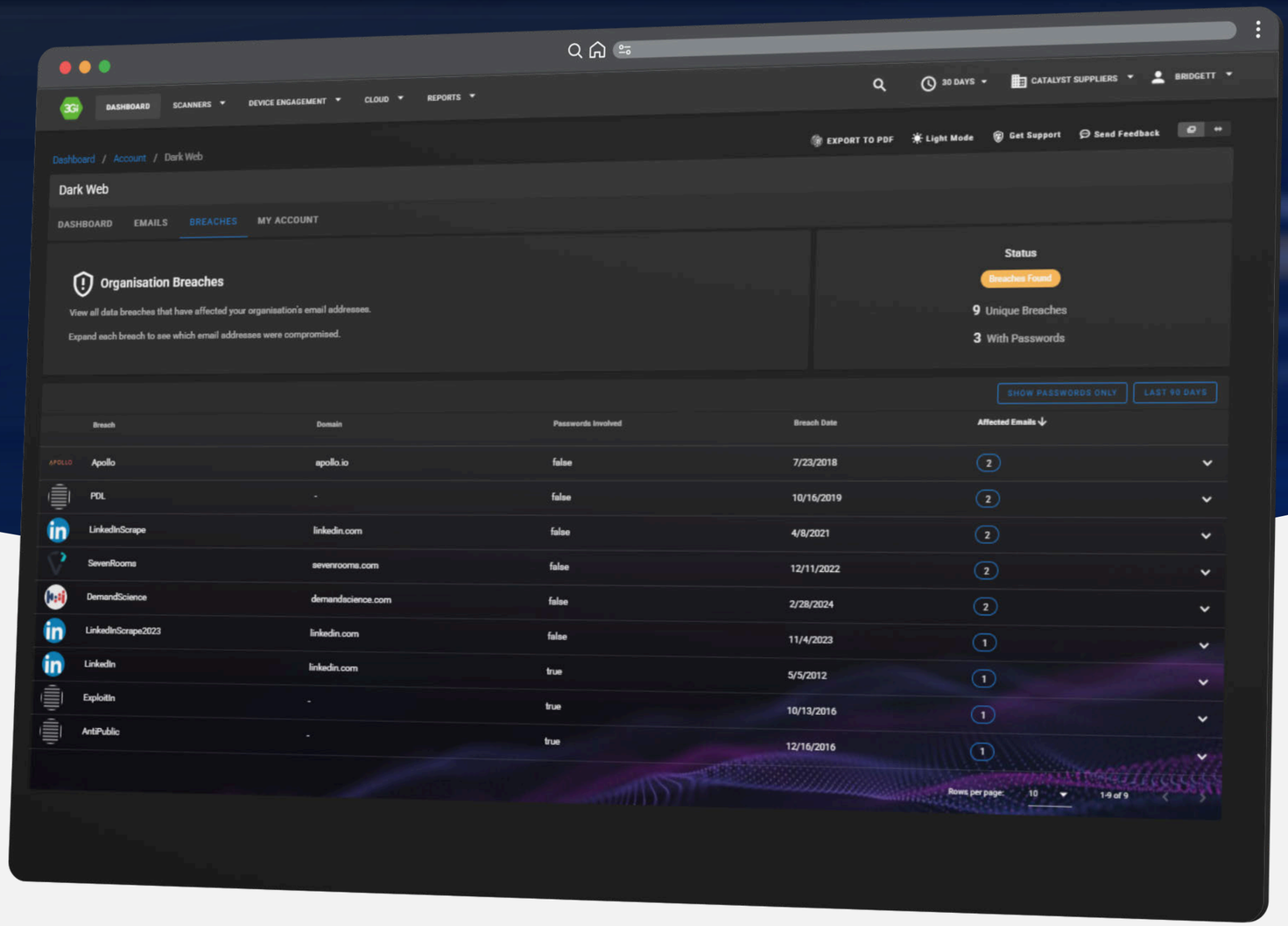
Measure Your 365 Security Against CIS Standards

In addition to the Cyber Benchmarks report, RoboShadow aligns your security posture with CIS Level 1 & 2 benchmarks the foundational security configurations recommended for all organizations. These industry standard controls provide essential hardening without impacting system functionality, ensuring your Windows environment meets baseline security requirements recognized globally by auditors, compliance frameworks, and security professionals.

- ▶ Are your **Microsoft 365 configurations aligned** with CIS Level 1 & 2 standards?
- ▶ Which controls are failing and increasing your **risk exposure**?
- ▶ Are critical security settings **consistently enforced** across your environment?

Dark Web Scanner :

Are your users credentials compromised?



Proactive Data Leak Detection

RoboShadow's Dark Web Monitoring continuously scans underground sources to detect if your organisation's credentials, domains, or sensitive data have been compromised and are being traded or exposed. It's part of RoboGuard's **continuous monitoring suite**, providing early warning of potential breaches before they escalate.

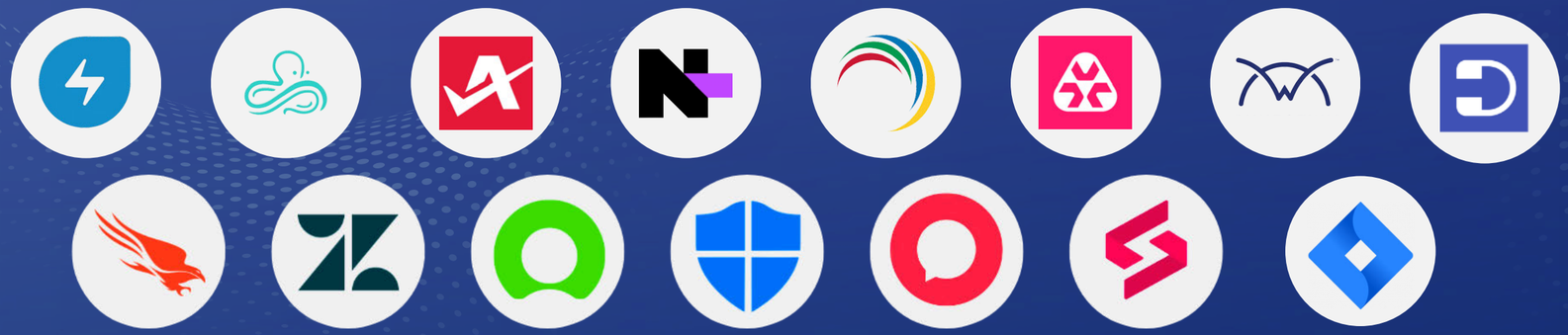
Key Features:

- **Credential breach alerts:** Detects if organisational email addresses or passwords appear in data dumps or dark web marketplaces
- **Proactive threat intelligence:** Identifies compromised assets before attackers weaponise them
- **Continuous surveillance:** Ongoing monitoring, not just one time scans, integrated with attack surface automation
- **Generate PSA tickets** from issues found in the Dark Web Scanner

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.



PRODUCT TOUR

RoboShadow

Cyber Management Platform

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



Microsoft 365

‘One click sync’

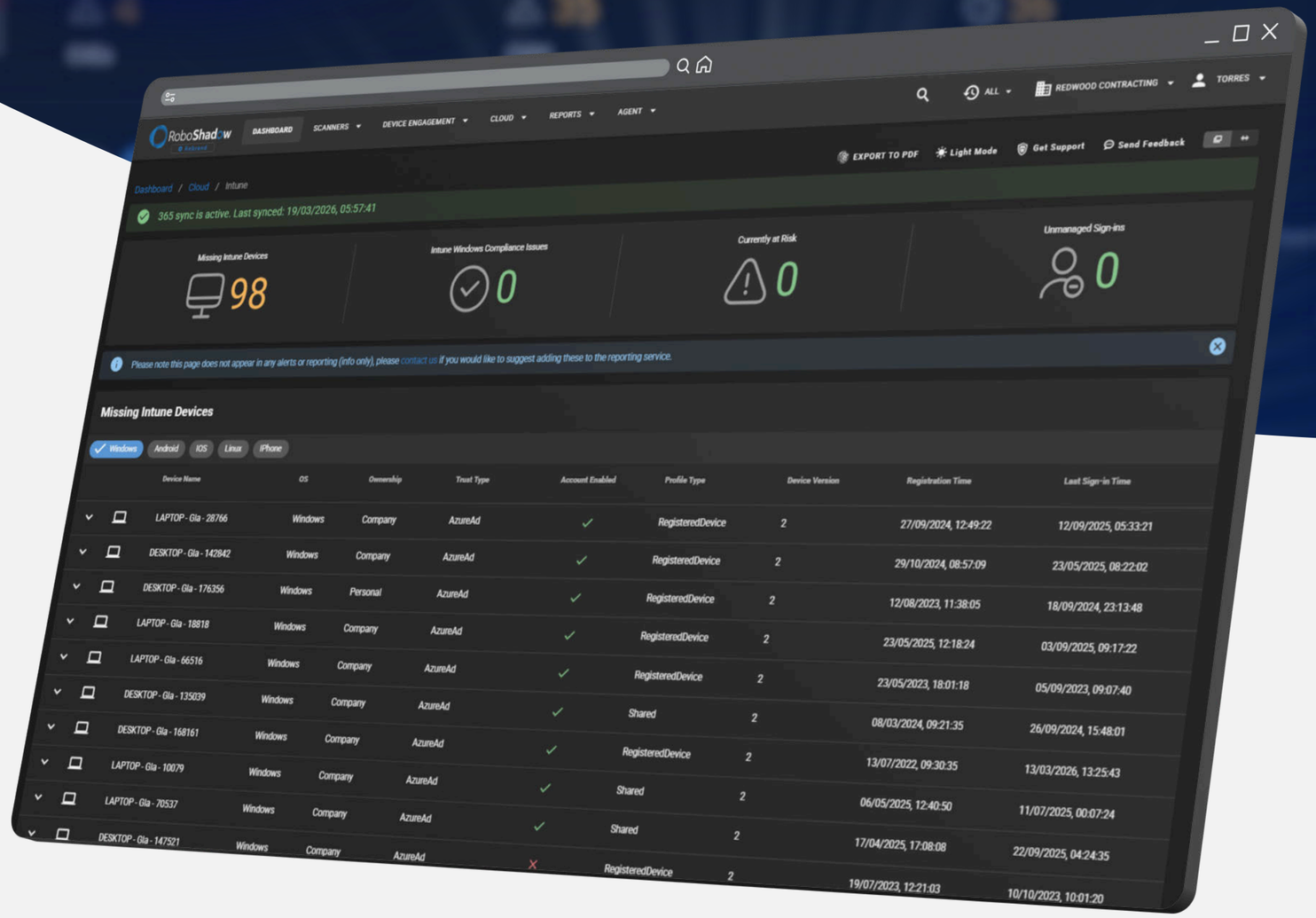
RoboShadow’ s one-click 365 sync enables you to **pull in Microsoft 365 MFA and authentication data** to help you stay on top of the most common way your organisation is likely to be hacked. Phishing exploits remain one of the most common way a network is breached and is now proliferate **by large AI 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 :

Deploy, Monitor and Secure



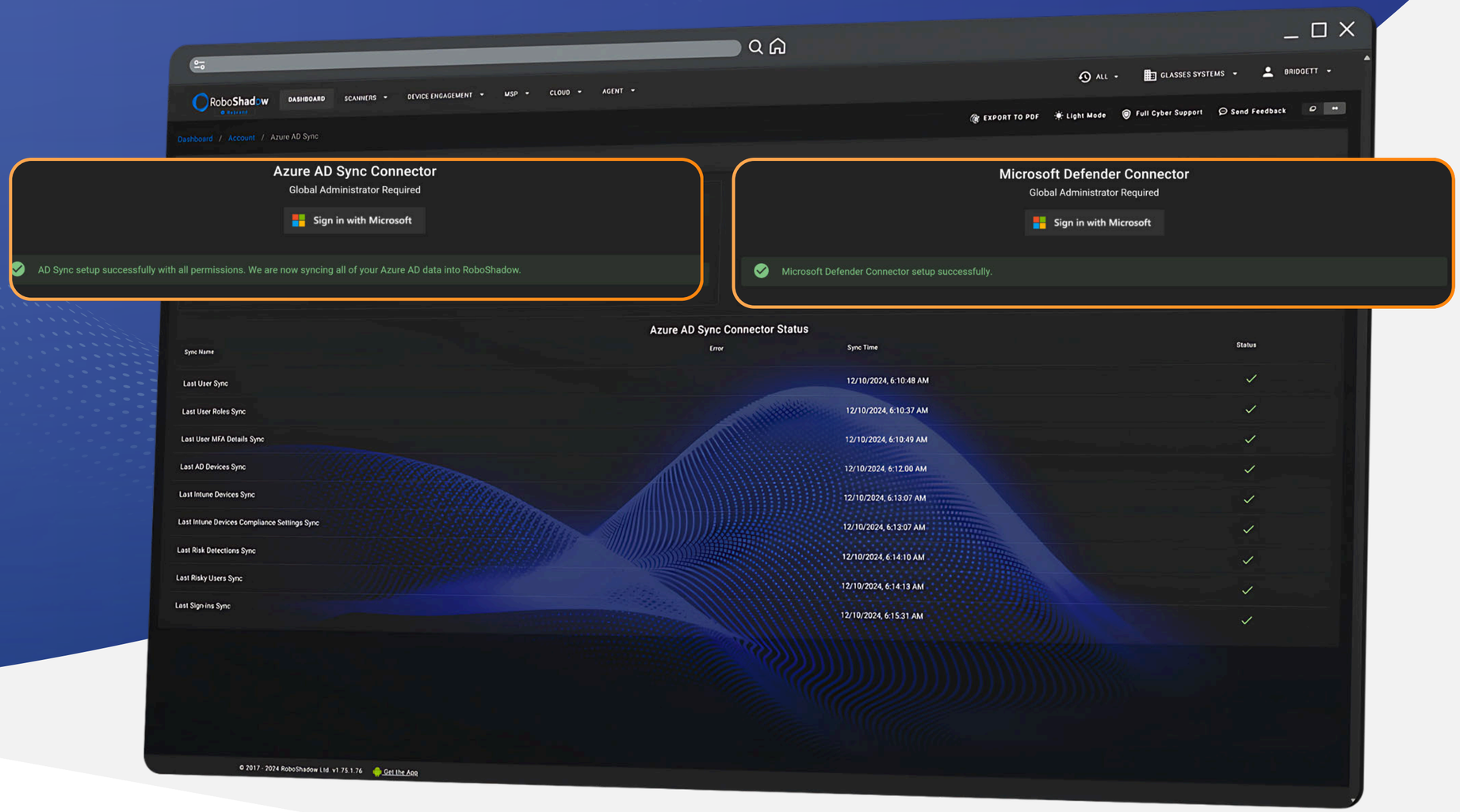
Deploy, Monitor, and Secure Your Estate via Intune

RoboShadow integrates directly with Microsoft Intune, enabling seamless deployment and continuous visibility across your managed devices. Gain real-time insight into device compliance, missing assets, and identity risks using enriched Intune data.

- ▶ One-click sync with Intune data for instant visibility across your estate
- ▶ Deploy RoboShadow agents via Intune across all managed devices
- ▶ Identify missing or unmanaged devices not enrolled in Intune
- ▶ Detect risky sign-ins and identity threats using Intune and Entra data

Windows Defender Sync :

Pull in Golden Vulnerability Data from Defender



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

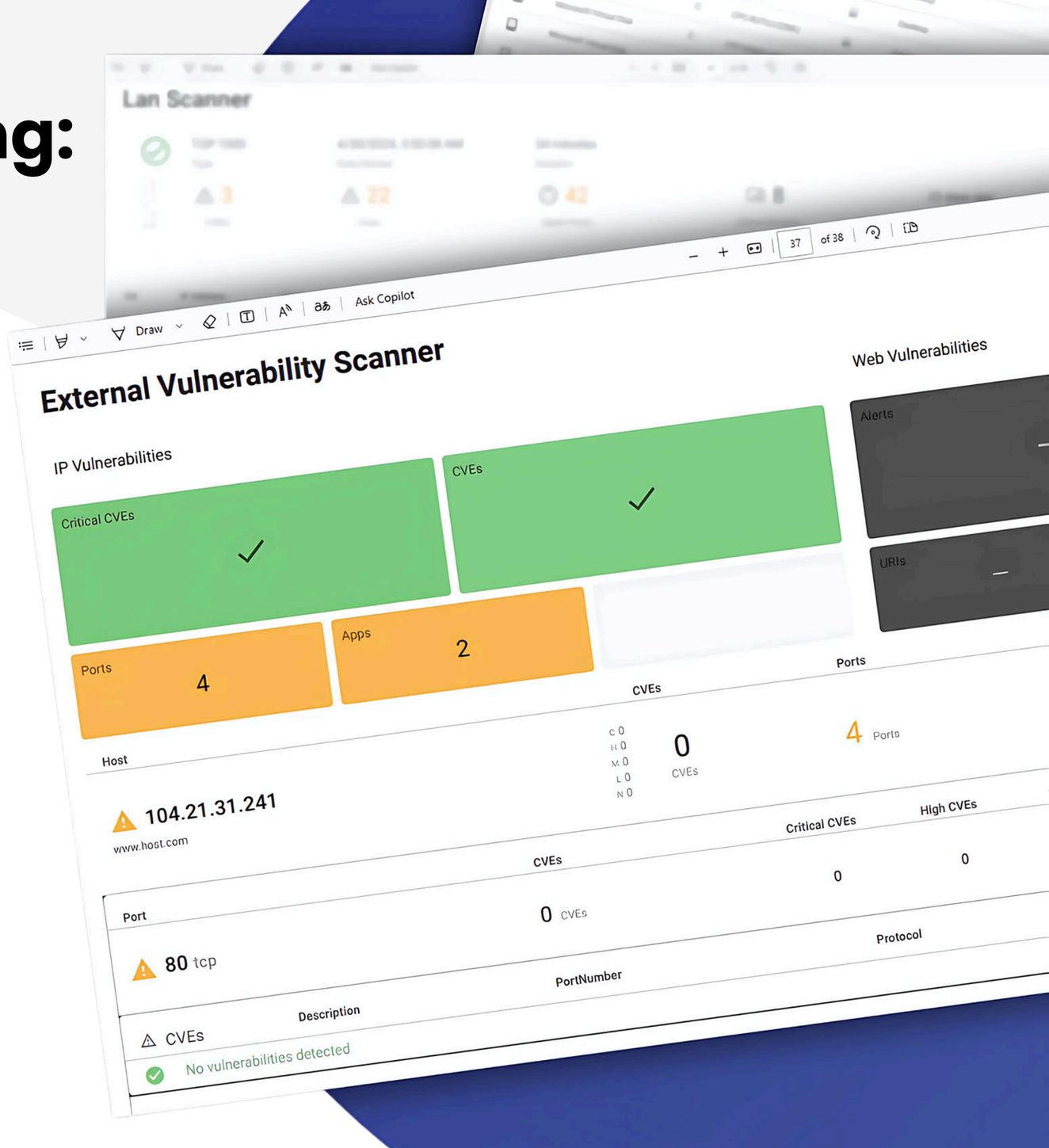
Getting reports which **give guidance instead of anxiety**, actionable intelligence and avoiding alert fatigue is the dream of all security-aware teams. RoboShadow delivers high level management overviews that offer a vast range of detailed **vulnerability level exposure and prioritisation** guidance. 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

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 National Institutes of Standards and Technology SP 800-171

NIST National Institutes of Standards and Technology CSF

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)*

AI ENABLEMENT

RoboShadow

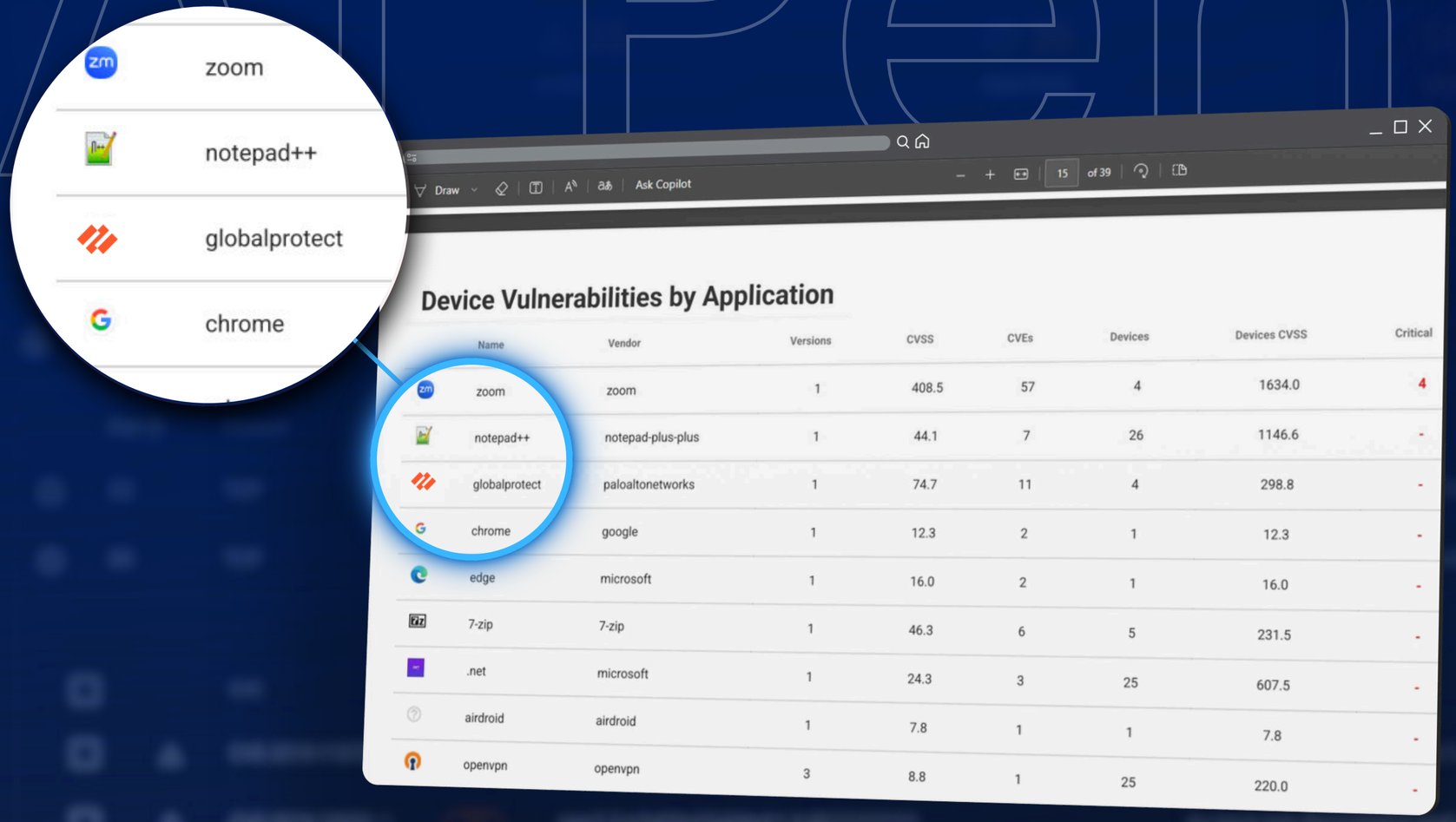
Cyber Management Platform

National Cyber Security Centre *For Startups* Alumni

AI ENABLEMENT

RoboShadow

National Cyber Security Centre *For Startups* Alumni



AI Pentest :

Using AI efficiency to make security connections

Our AI Pentest is now in live preview, which effectively allows **MSPs to use LLMs in place of penetration testers**. This means they can give their customers AI-driven penetration tests which look like a **$10,000+ penetration test** but can be run and exported using existing vulnerability dataset. It's already being used as a great way for MSPs to prospect.

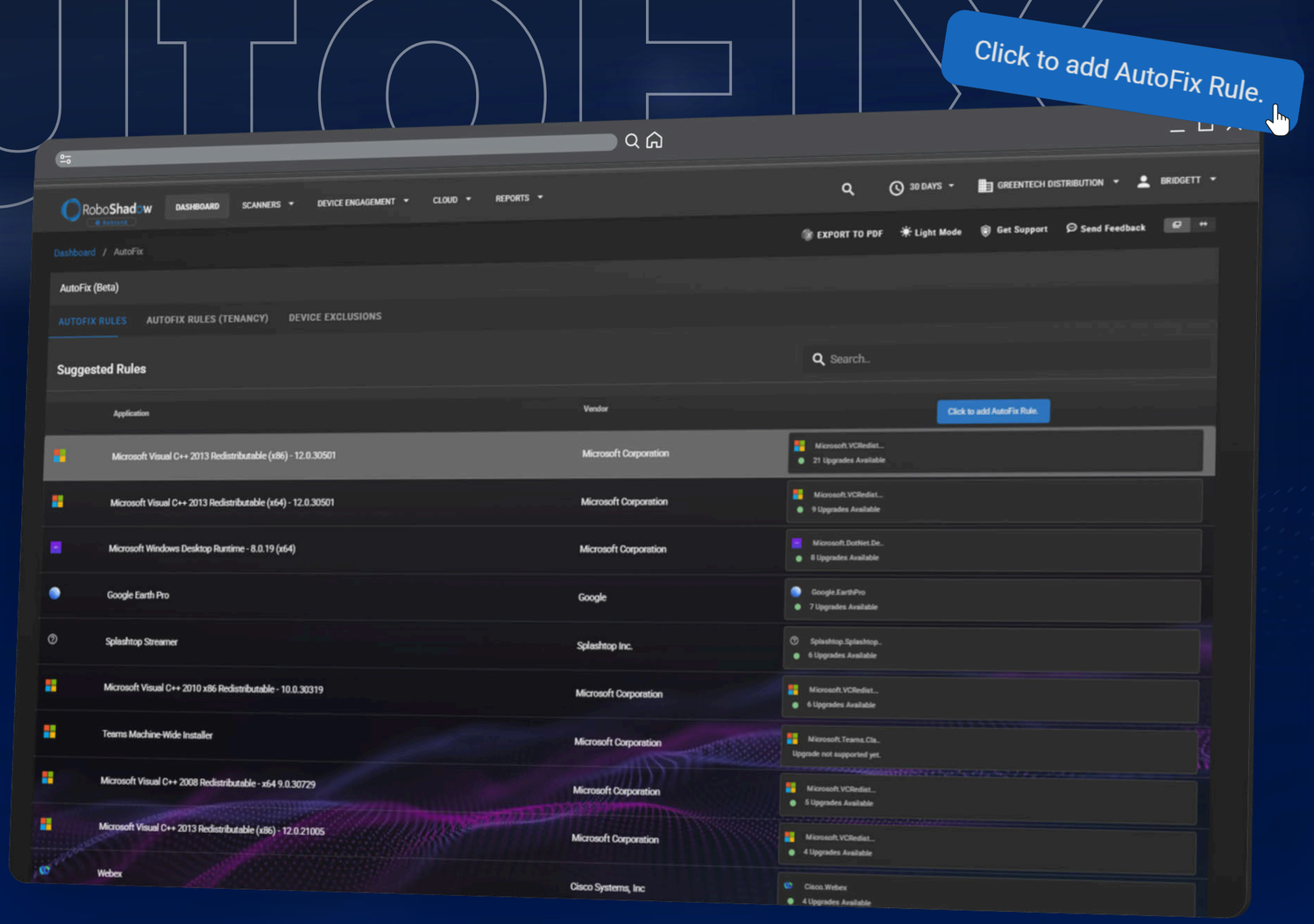
- AI will suggest the **scope of the exercise** from existing data context.
- The LLM will then provide overviews of **Findings, Suggestions, Best Practices,** and **Budget Requests.**
- All other document artifacts used in **litigation evidencing** will then be provided.

1 Scope — 2 Execution — 3 Findings — 4 Reporting

RoboShadow

National Cyber Security Centre *For Startups* Alumni

AI AutoFix



AI Autofix Rules :

Automated Vulnerability Remediation

Using our **Winget** integration, RoboShadow enables AutoFix rules to keep your **applications patched automatically**, reducing manual effort and minimising exposure to threats. AutoFix ensures vulnerabilities are addressed quickly and consistently, even across large estates.

AI AutoFix automatically remediates third-party application vulnerabilities, deploys Windows OS updates, and hardens security benchmarks (including CIS controls) handling 60-90% of remediation work while flagging items that require manual intervention.

AutoFix rules are configurable to:

- Schedule deployments at **set times**.
- Stagger rollouts (e.g., 5 devices on day one, 15 on day two)
- Exclude **sensitive systems** such as servers.
- **Apply policies** across multiple organisations for MSPs.
- Third-party application vulnerabilities, deploys Windows OS updates, and hardens security benchmarks

RoboShadow

National Cyber Security Centre *For Startups* Alumni

AI AppGet:

Agentic AutoFix Capability

The ability for autofix to find the install for applications using AI AI AppGet extends AutoFix by intelligently sourcing, validating, and deploying application patches beyond standard repositories like winget.

When patches are unavailable through traditional channels, AI AppGet actively hunts for trusted installers across the web, verifies their integrity, and prepares them for safe deployment.



- Automatically discovers application installers not available in winget
- Validates sources and files to ensure secure and trusted patching
- Enables AutoFix to remediate a broader range of applications
- Reduces manual effort in sourcing and packaging software updates

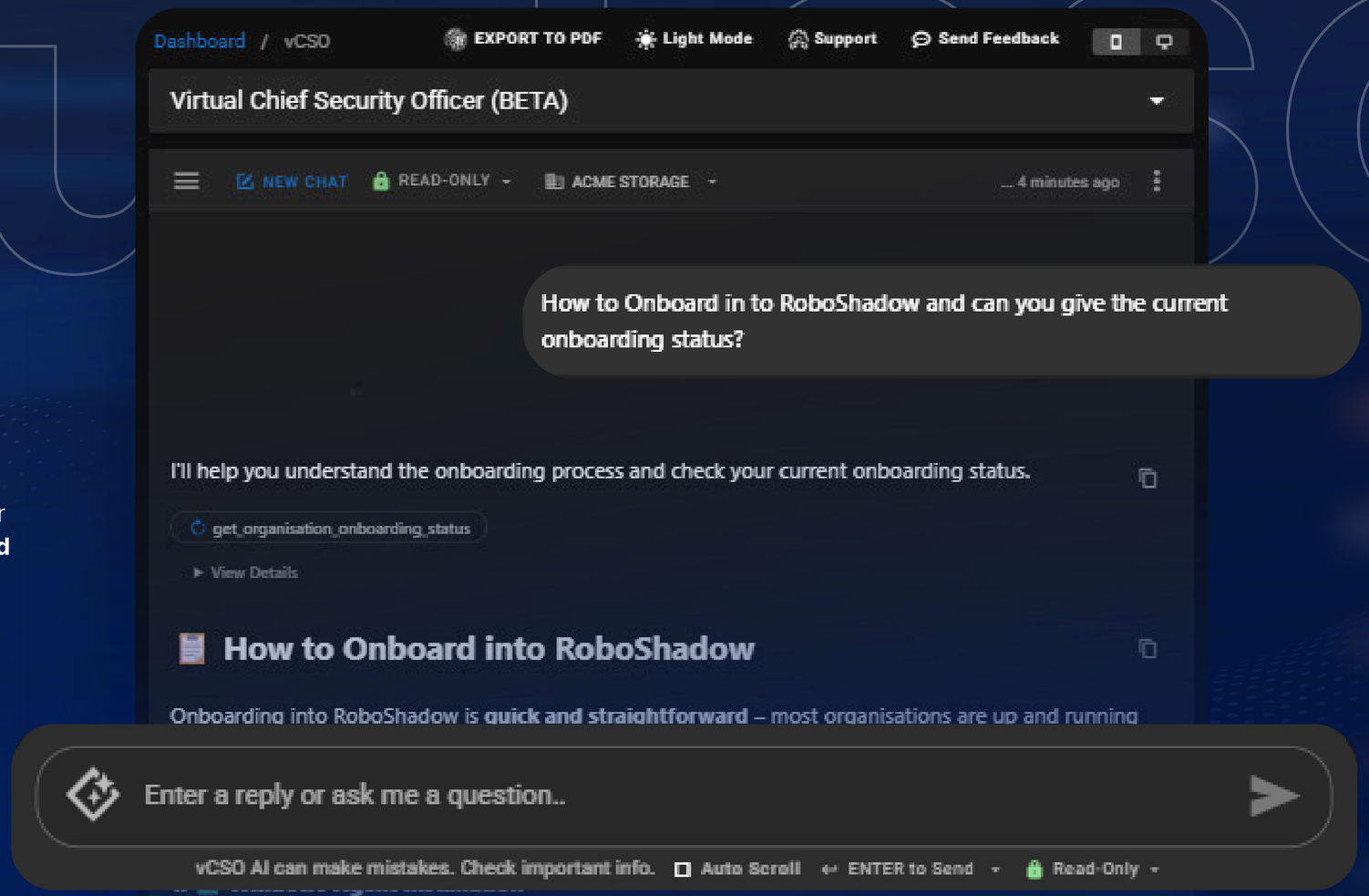
RoboShadow

National Cyber Security Centre *For Startups* Alumni

Virtual CSO :

Board-Level reporting

Using the same technology as our AI Pentest, our AI Agent will work with you when you log in and run you through where your security is at for that day: **highlighting movers, new items and wins.** Our virtual CSO will be configurable to **adjust the level of alerting and reporting**, ensuring the right amount of communication and work across all clients. This means noise reduction and a better return on time investment for MSPs.



The virtual CSO can answer questions and provide services such as:

- **Can you give me a quick cyber management summary for our board meeting later?**
- **Where do we need to get better to pass Soc2**
- **What are the organisation's largest threat**
- **What new threats have we detected since the last time we caught up?**
- **Are there any users that AutoFix is unable to remediate and we need to contact manually?**
- **Can you give me a quick cyber management summary for our board meeting later?**

RoboShadow

National Cyber Security Centre *For Startups* Alumni

Model Cont

Model Context Protocol :

Virtual Chief Security Officer

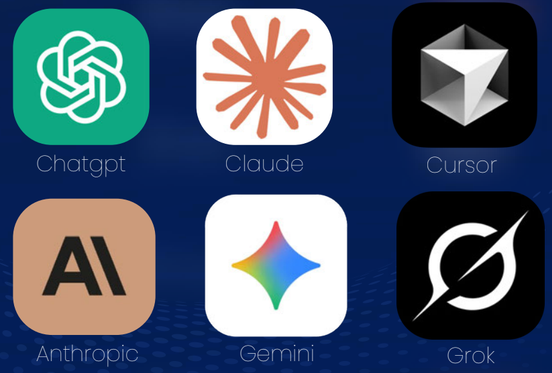
MCP connects to the data set to allow MSPs to use their own chatbot services, like **ChatGPT or Claude**, to work directly within the RoboShadow data set. This can also be **configured with a set of GPTs for MSPs & MIPs** to save time, understand data, or even request AutoFix jobs to remediate issues.

A combination of LLMs & Desktop AI Agents connected **directly into the Roboshadow platform** via our MCP gateway will allow RoboShadow users **a very rich experience** saving much needed time and effort ultimately reducing risk and increasing visibility across estates.

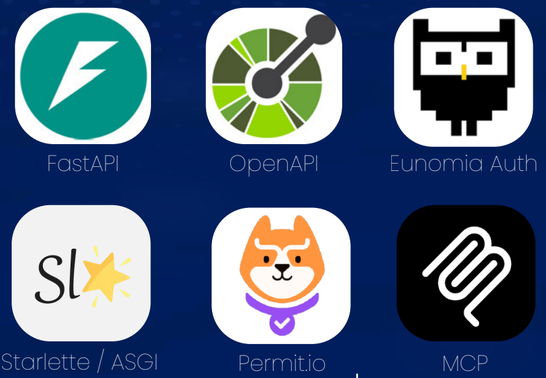
- Integrate cybersecurity data with **other AI agent platforms** and tools.
- Create your own daily reporting processes and **workflows using your preferred LLM.**
- Use **desktop LLM agents** to work directly in RoboShadow GUI to **automate cybersecurity tasks.**

Works with :

AI - related :



Not AI
(Frameworks, auth , specs, , etc) :

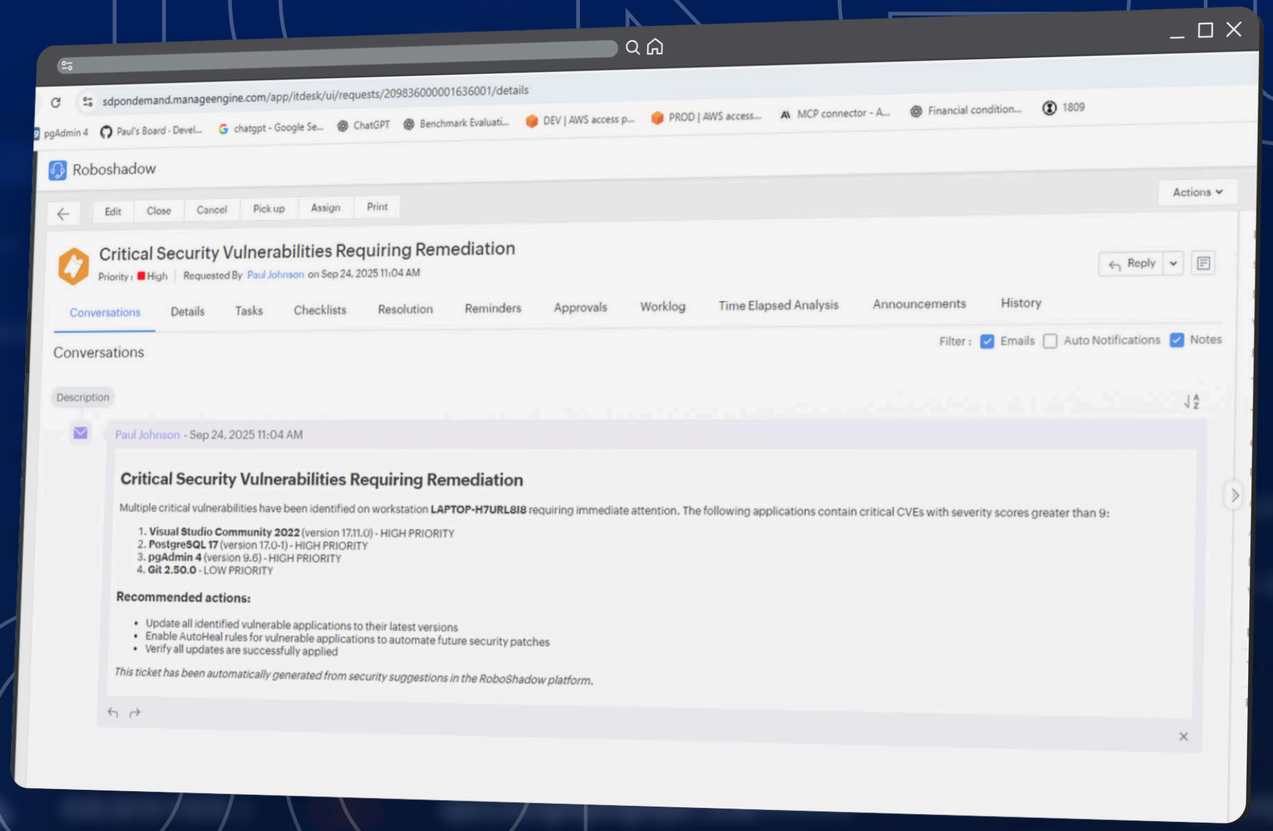


Integrations include : Anthropic API, AuthKit, ChatGPT, Claude Code, Claude Desktop, Cursor, Eunomia Auth, FastAPI, Gemini SDK, MCP.json, OpenAI API, OpenAPI, Permit.io, Starlette / ASGI

RoboShadow

National Cyber Security Centre *For Startups* Alumni

Ticketing



AI Ticket logging :

Compliance Made Simple with Auto Ticket Creation

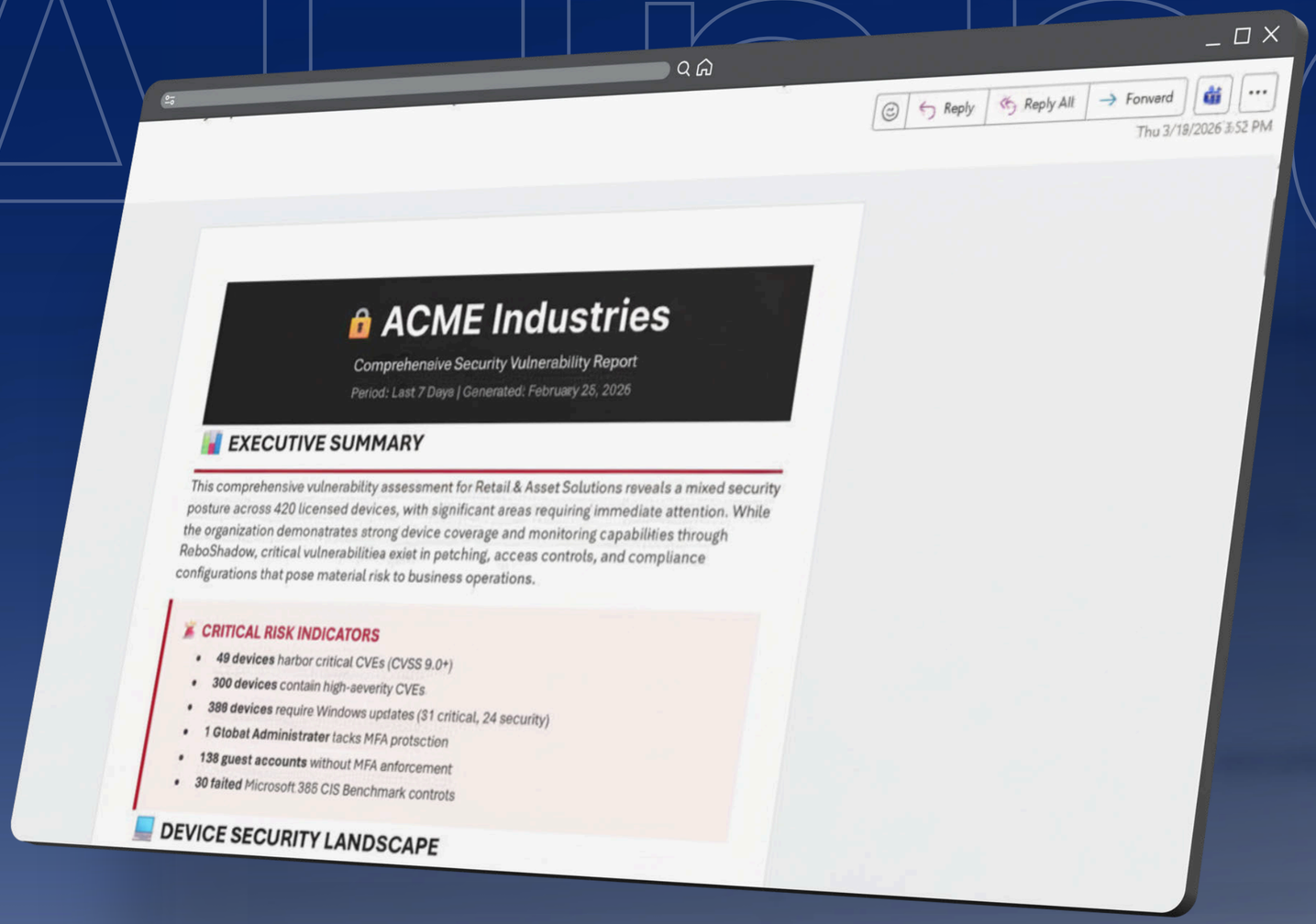
The AI Ticket Logging feature turns RoboShadow alerts into **automatic helpdesk tickets**. To help with compliance, RoboShadow continuously monitors vulnerabilities and, when issues exceed **a defined severity score**, it generates a ticket automatically. These tickets can then be tracked, escalated, and resolved within **your existing systems.**

With AI Ticket Logging you can:

- ➤ Automatically raise tickets for vulnerabilities over compliance thresholds
- ➤ Integrate seamlessly with most (if not all) major helpdesk and ticketing platforms
- ➤ Ensure every critical security issue is documented and assigned for resolution
- ➤ Provide a clear audit trail for compliance and reporting

RoboShadow

National Cyber Security Centre *For Startups* Alumni



AI Inbox :

Using AI to auto write & send Reports clients and internal team.

The AI Inbox turns RoboShadow data into clear, **actionable email reports**. Acting as your Virtual CSO, it listens to your prompts, analyses platform insights, and instantly delivers reports to you, your clients, or internal staff.

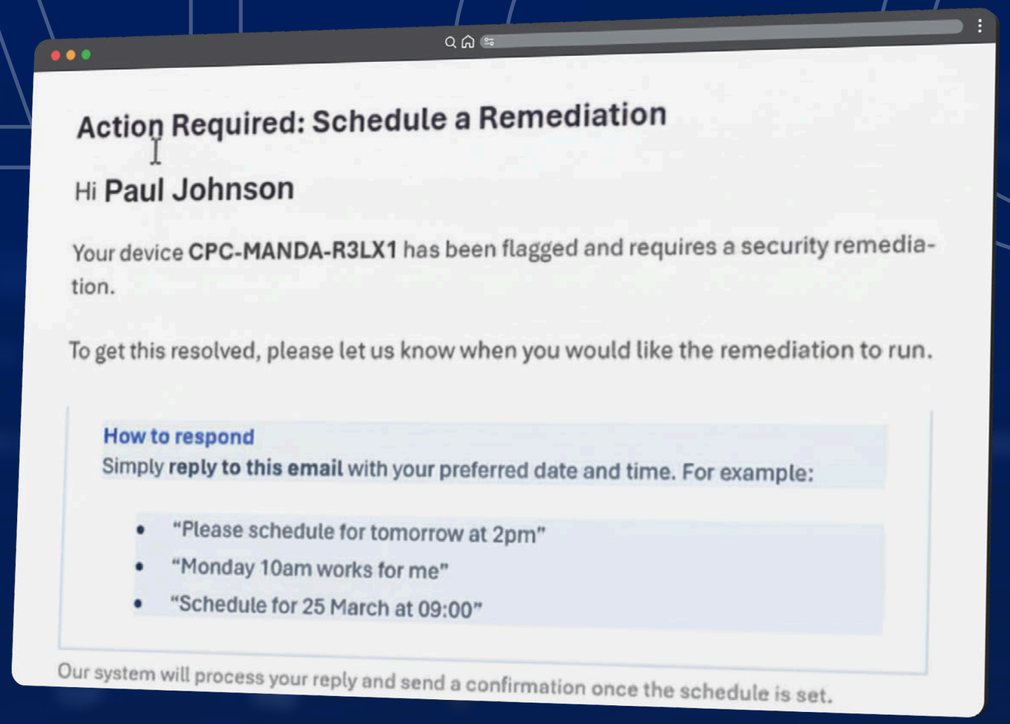
With AI Inbox you can:

- ➤ Generate board ready cyber summaries on demand
- ➤ Email remediation alerts when AutoFix cannot resolve issues
- ➤ Send tailored risk updates directly to clients or internal teams
- ➤ Store Prompts to run tasks and reports when you want

1 Scan — **2** Results — **3** Email — **4** Reporting

RoboShadow

National Cyber Security Centre *For Startups* Alumni



AI Communicate :

(AutoFix Feature)

AI Communicate is a feature within AutoFix that automatically reaches out to end users via email to arrange a convenient time for applying vulnerability patches, helping to streamline remediation whilst minimising disruption to users.

- Automatically reaches out to end users to schedule remediation at a convenient time.
- Uses natural language to handle replies and confirm scheduling without IT involvement.
- Reduces disruption by aligning remediationwith user availability.

RoboShadow

National Cyber Security Centre *For Startups* Alumni

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. Cybersecurity doesn't need to be overcomplicated, nor sold on fear, in fact winning the complexity game for cybersecurity is 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.

One of the biggest benefits from this is the ability to 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 cybersecurity less complex, less costly, and available to all.

Terry Lewis
CEO



National Cyber Security Centre
For Startups
Alumni