MAY 2026

inside zhero

Manual to Magical

Zhero's Trailblazing Automation

The Human Firewall

From Users to Defenders

Smart Cyber Defence

Data Risk Mitigation for SMEs

Message from Izak

Thank you for joining us in this May edition of Inside Zhero. There's a lot to get your teeth into, including celebrating our N-able Automation Trailblazer award.

We also check out the benefits of end-user risk mitigation and how XDR and MDR go beyond being a magic bullet for SMEs

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "Manual to Magical" celebrates yet another Zhero achievement in the realm of AI and automation.

97% of UK organisations consider cybersecurity automation to be business-critical.

"I've seen automation help businesses become faster, more efficient, and much more resilient. I believe the real value of automation is giving people time to focus on innovation, customer experience, and strategic growth instead of repetitive manual tasks. Automation reduces errors, improves consistency, and helps SMEs compete more effectively. Embrace automation today and guarantee long-term success."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

50% discount **cyberzhero542**

MANUAL TO MAGICAL

The N-able Automation Trailblazer Award is a prestigious honour presented at the N-able Empower partner conference, recognising MSPs that demonstrate exceptional innovation in automation, AI-driven security, and IT management. Zhero won this year's award at N-able Empower 2026 in Fort Lauderdale, Florida. With Wesley Harris, Zhero's Head of Development, and Louis Oosthuizen, our SOC Team Lead, accepting the award, it recognised Zhero for its proactive approach to AI-driven automation using N-central, shifting from reactive, manual work to "building proactive, automation-first environments". Louis and Wesley were specifically honoured for their roles in using automation to boost performance and security. The Automation Trailblazer Award highlights partners who are "trailblazing stateside" and abroad, pushing the boundaries of automation technology to deliver faster, smarter, and more secure IT solutions. It is part of N-able's broader mission to honour partners who turn manual work into magic using AI and automation to enhance efficiency.

"We were honoured to accept the award for automation trailblazer. It proves that we are doing something unique in the world of automation that not many MSPs are doing."

Wesley Harris,
Zhero Head of Development

Driving Business Growth

Powered by N-central, automation is streamlining everything from patch management and asset control to self-healing systems, helping organisations reduce risk, improve performance and save valuable time. This means IT teams can focus on strategic initiatives, security and business growth rather than repetitive operational tasks. With N-able and Zhero continuing to advance AI-driven security and IT management, the future is moving towards faster decision-making, stronger protection and more intelligent operations.

"You guys are doing things no one else in the space is."

Jason Murphy,
N-able

" The level of automation we build will only increase the disruption brought to MSPs with business models like ours."

Louis Oosthuizen,
Zhero SOC Team Lead

THE HUMAN FIREWALL

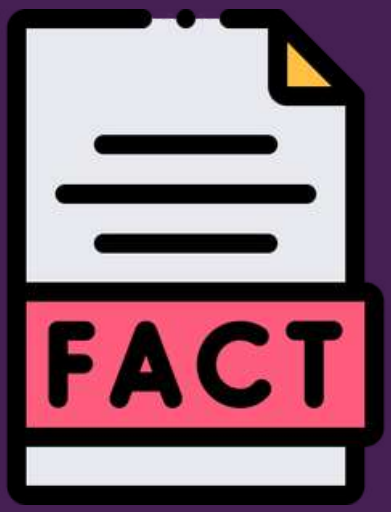
For many UK SMEs, the biggest cybersecurity risk is not the technology, but everyday human behaviour. End-user risk is the potential for employees, contractors, or customers to unintentionally create security vulnerabilities through things like phishing emails, weak passwords, accidental misconfigurations, or unsafe online activity. Even with strong technical protections in place, cybercriminals frequently target people as the easiest way into a business.

Core Risk Drivers

- **Human error & negligence** - Clicking phishing links, opening malicious attachments, or losing devices like laptops and phones.
- **Social engineering** - Attackers trick users into sharing sensitive data via phishing emails, SMS scams (smishing), or impersonation tactics.
- **Credential mismanagement** - Weak, default, or reused passwords make accounts easy to compromise through guessing or brute-force attacks.
- **Physical security lapses** - Allowing unauthorised access to secure areas through tailgating or poor access control.
- **Cloud/system misconfiguration** - Incorrect settings that unintentionally expose data or services to the public internet.

Cost of End User Risk

- **Data breaches** - Theft of sensitive company or customer information, often leading to legal, regulatory, and financial consequences.
- **Ransomware infections** - Malware that locks systems or encrypts data, causing downtime, operational disruption, and potential ransom payments.
- **Reputational damage** - Loss of trust from clients and partners, which can impact relationships, revenue, and long-term business growth.
- **Financial loss** - Direct costs from fraud, ransom demands, recovery efforts, and lost productivity during downtime.
- **Regulatory penalties** - Fines and sanctions for failing to protect personal or sensitive data under regulations such as UK GDPR.
- **Business interruption** - Critical systems or services going offline, delaying operations and affecting customer service delivery.
- **Intellectual property theft** - Loss of proprietary data, designs, or business plans that can damage competitive advantage.
- **Legal liability** - Potential lawsuits from affected customers or partners following a security incident.



- 43% of UK businesses experienced a cyber breach or attack in the last year, with phishing the most common entry point.
- 67% of UK employees admit to behaviours that put organisations at risk, such as unsafe clicking or poor security habits.
- 38% of users reuse passwords across accounts, increasing the risk of credential compromise from a single breach.

zhero

Mitigate IT Better

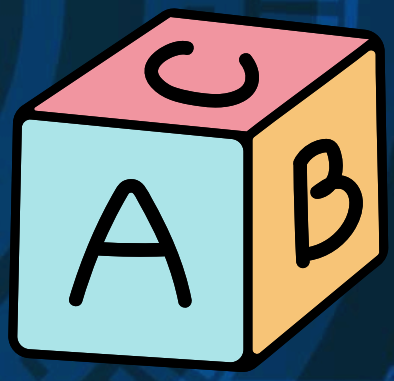
Zhero's end-user risk mitigation, Mitigate IT Better, focuses on turning cyber weakness into cyber strength by identifying risky behaviours and embedding security awareness directly into daily workflows. This includes:

- Lightweight phishing and email simulations to highlight high-risk behaviours
- Embedded, ongoing security awareness training that reduces human error
- Clear visibility for leadership into user-level vulnerabilities and risk trends
- Automated, policy-driven training for users who need additional support

Mitigate IT Better means behaviour-driven security, transforming employees into confident, proactive defenders. With continuous monitoring running quietly in the background, you get superlative protection, minimal operational disruption, and clearer insight into how human behaviour impacts overall cyber risk. The bottom line is that your critical data is protected, operational resilience strengthened, and your team becomes a coordinated first line of cyber defence for the business.

SMART CYBER DEFENCE

As data risks and attacks continue to mount, compliance and regulations impose additional operational responsibilities, yet budgets do not increase in parallel. At the core of data risk mitigation are detection and response capabilities that help you identify threats, investigate them, and contain them before they disrupt your business. The majority of SMEs prefer to outsource complex security operations and services, such as Endpoint Detection and Response (EDR), Managed Detection and Response (MDR), and Extended Detection and Response (XDR). From a bird 's-eye view, these solutions seem remarkably similar and offer interchangeable business benefits like greater protection, lowered operating costs, and simplified operations.



ABC of EDR, MDR and XDR

EDR, MDR, and XDR are cybersecurity frameworks that differ primarily in scope of coverage and how they are managed.

- **EDR (Endpoint Detection and Response)** monitors individual devices like laptops and servers.
- **XDR (Extended Detection and Response)** is an advanced platform that expands EDR monitoring across your entire network, cloud, and email systems.
- **MDR (Managed Detection and Response)** is an outsourced service that provides human experts to manage these security tools for you 24/7.

The Threat Reality

As a business owner, you might question the need for implementing XDR and MDR. These eye-opening numbers speak for themselves. In 2025:

- 67% of UK SMEs experienced a cyberattack
- 19,000 UK businesses were hit by a ransomware attack
- 1 in 3 SMEs paid the ransom demand
- £6,400 was the average cost of a cyber breach for UK SMEs
- 43% of SMEs had no incident response plan in place when attacked

"Attackers only have to get it right once. Defenders have to get it right every time."

Kevin Mitnick,
Global Cybersecurity Influencer

Full Spectrum Security

We know that UK SMEs are facing an evolving threat landscape where attacks are continuous, automated, and increasingly hard to detect with traditional monitoring tools. Fragmented security leaves gaps across email, endpoints, and external exposure, giving attackers opportunities to slip through unnoticed. This is why integrated protection through XDR and MDR is becoming essential, not optional. Key layers include XDR for Darknet Exposure Protection, Mail Security, and Mailbox, and MDR for Perimeter Defence. Together, these create a unified approach that strengthens visibility, speeds up detection, and improves response before threats can disrupt operations.

Mail and Mailbox Security

Mail security is the front door guard, focusing on protecting email before and during delivery and gatekeeping incoming/outgoing email traffic. By contrast, mailbox security is the inside-the-house monitoring, focusing on protecting what's already inside a user's mailbox. N-able's Mail Assure is a cloud-based email security XDR solution to protect inbound and outbound email from threats like phishing, malware, and ransomware. Mail Assure offers:

- Protection and Security - It uses collective threat intelligence to safeguard against spam, viruses, and ransomware.
- Integration - It offers seamless integration with Microsoft 365 via an add-in.
- Functionality - It includes 24/7 email continuity, allowing users to access email during outages, and offers long-term, encrypted email archiving.

UK SMEs benefit from this layered approach because email remains the most common entry point for cyberattacks, yet many smaller organisations lack the resources to monitor and respond to threats in real time. By separating mail security (front door protection that filters and blocks phishing, malware, and ransomware before delivery) from mailbox security (internal monitoring of what lands inside users' inboxes), SMEs gain both prevention and detection in one model.

"For SMEs, email is both the most valuable business tool and the most targeted attack surface. Securing the inbox is fundamental to business continuity."

Perimeter Defence

N-able's perimeter defence is not a single tool, but a layered, defence-in-depth approach designed to protect UK SMEs across their entire attack surface, including endpoints, email, identity and network activity. Key components include:

- EDR - Uses behavioural AI to detect and respond to threats, including automated rollback of malicious changes
- Attack Surface Management (ASM) - Identifies and isolates unknown, rogue, or IoT devices connected to the network
- DNS Filtering - Blocks access to malicious websites, phishing domains, and harmful online destinations
- Mail Assure - Stops phishing, spam, and malware before they reach users or the network
- Firewall and Network Monitoring - Ensures security devices are correctly configured, patched, and functioning as intended
- MDR - Provides 24/7 monitoring and expert threat response for continuous protection

Perimeter defence reflects the modern reality that the "perimeter" is no longer a fixed boundary. Instead, UK SMEs get AI-driven, always-on protection that covers users, devices, cloud services, and identities, helping reduce blind spots and improve response times against fast-moving cyber threats.

"Perimeter security is the digital equivalent of locking the front door. Without it, every other security investment is compromised from the start ."

Darknet Protection

N-able's Darknet Exposure Protection is a proactive security feature, typically delivered via MDR/XDR with Adlumin, an AI-powered security operations command centre. The platform scans the dark web for stolen employee credentials and leaked company data. It continuously monitors criminal forums, marketplaces, and data breaches to identify exposed usernames, passwords, and sensitive information before attackers can use them. When risks are detected, it can trigger alerts and, in some setups, even automated password resets to prevent account takeover. It provides organisation-wide visibility across both privileged and standard accounts, helping reduce the risk of ransomware, phishing, and malware attacks by addressing exposure at the source. For UK SMEs, this is particularly valuable because it reduces the need for large in-house security teams while helping them detect and neutralise threats early, before stolen credentials can be used to access systems or disrupt operations.

zhero

Cyber Defence Partners

N-ABLE

By partnering with N-able, Zhero brings together MDR and XDR capabilities into a unified, always-on defence model that connects detection, intelligence and expert response across every layer of the business. This means threats are not only identified earlier but actively contained before they escalate into operational disruption. For SMEs, the benefit is immediate and practical, offering enterprise-grade protection without enterprise overhead. From uncovering hidden exposure on the dark web to securing email, endpoints and network perimeters, this partnership reduces blind spots, strengthens resilience and simplifies security management. In a world where one missed alert can become a major breach, Zhero and N-able offer UK businesses something far more powerful than tools alone, delivering confidence, continuity and control in an increasingly hostile digital environment.

Meet the team

JUSTIN GEORGE

SERVICE DESK COORDINATOR

Hi Justin! What made you realise you want to go into the IT industry?

Hi! I've always enjoyed playing computer games and wanted to understand how programs are created. I started opening computers and was amazed by all the small parts inside them.

What's your most-used productivity tool?

Obsidian is my go-to productivity tool because I take a lot of notes, and it helps me keep everything organized and easy to find.

How would you describe yourself?

I am an introverted-leaning but socially open person. I enjoy a balance between comfort and exploration. I like relaxing indoors and watching movies, but I also enjoy meeting new people & trying new experiences.

What do you enjoy the most about your role?

Learning new ways to troubleshoot various systems and expanding my knowledge in IT and cybersecurity.

Do you have any hidden talents or hobbies?

Some of my hobbies are reading comic books, playing football and skateboarding.

What is your favourite movie or TV show?

Tough to choose, but my current favourite TV show will have to be The Office, US version. My favourite movie of all time is 1994's The Crow.

LONDON
162 Farringdon Road
London
EC1R 3AS

SPEAK TO US
+44 20 7183 3975

START THE PROCESS

zhero
crush the chaos