JULY 2025

inside zhero

Robots for Cyber

Robotic Patch Management

Our Cyber Civilisation

An Ongoing Digital Evolution

Windows 10 EOL

The Clock is Ticking

amazon

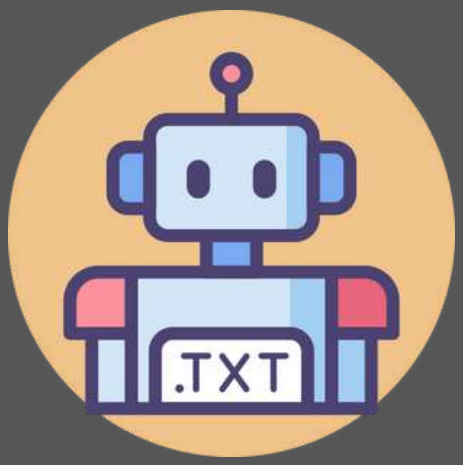
Win £50 voucher

Message from Izak

Welcome to our exciting July edition of Inside Zhero.

This month, we are looking at all things cybersecurity, as we explore our cyber civilisation and look at the role of robotics in security. Also, a reminder that Windows 10 end-of-life is fast-approaching.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author



In this issue

Our feature “Robots for Cyber” gives you an in-depth look at how robotic security management can rid us of boredom, save time and eliminate error for security experts.

Deloitte’s global Robotic Process Automation survey shows us that 53% of businesses have implemented the technology.

"Robotic Process Automation (RPA) has quickly evolved from a budding innovation into a vital catalyst for digital transformation. The adoption of RPA is at an all-time high, driven by AI, hyper-automation, and the ever-growing demand for operational efficiency. For modern businesses like mine, RPA is no longer merely a choice; it's an absolute necessity."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

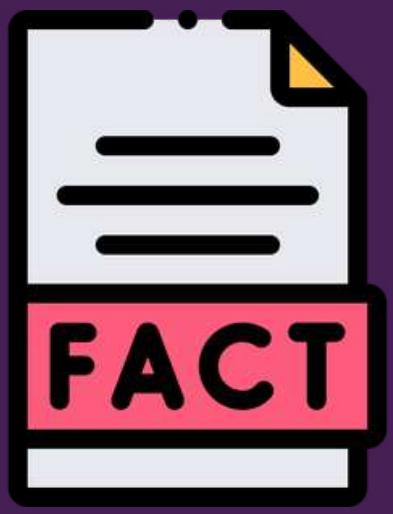
30% discount **cyberzhero542**

ROBOTS FOR CYBER

Robotic Process Automation (RPA) is a type of business process automation that relies on software robots (bots) or AI agents. However, RPA should not be mistaken for AI, as it operates through automation technology that follows a predefined workflow. In conventional workflow automation tools, a software developer creates a sequence of actions to automate a task and connects to the back-end system using internal application programming interfaces (APIs) or a specific scripting language. In contrast, RPA systems generate the list of actions by observing a user carrying out the task within the application's graphical user interface (GUI) and then automate the process by mimicking those actions within the GUI. This approach can make automation more accessible, especially in systems that do not provide APIs for integration. RPA tools share many technical similarities with GUI testing tools, which also automate interactions with the user interface, often by replicating a set of recorded user actions. However, RPA tools go further by enabling the handling of data across multiple applications. For example, an RPA system might receive an email with an invoice, extract the relevant information, and input it into an accounting system.

How does RPA work?

RPA services are hosted in a way that mirrors how software robots work—each robot runs on its own virtual workstation, similar to how a human would use a computer. The robot performs tasks using virtual keyboard and mouse actions to interact with applications through the GUI. These tasks usually take place in a virtual environment, with the robot reading the screen electronically, so there's no need for a physical monitor. Modern RPA systems are highly scalable thanks to virtualisation technology. Without it, businesses would face the high cost and difficulty of managing physical machines for each robot. Compared to traditional manual processes, RPA has helped many organisations reduce costs significantly. However, RPA does come with some challenges. Critics have noted that it can increase system complexity and potentially slow innovation. Existing software systems weren't originally designed to interact with the GUI through automation, which can create extra maintenance work and technical issues.



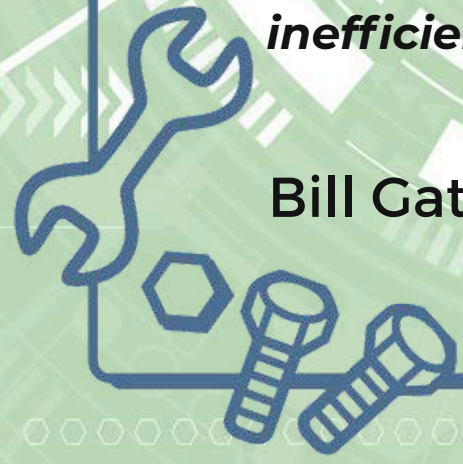
- 92% of businesses report improved compliance with RPA.
- 86% experience increased productivity.
- 89% of employees feel more satisfied with their jobs due to automation.
- 83% believe AI-powered automation reduces burnout.
- 91% of employees state that automation improves work-life balance.

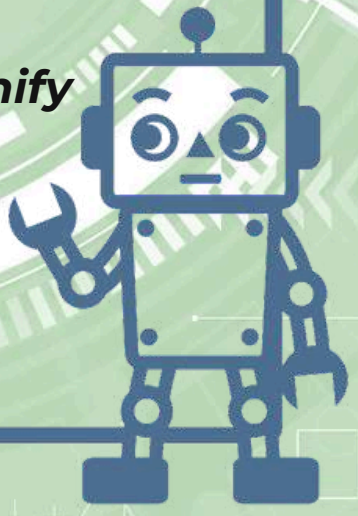
RPA applications

- **Data entry and processing** – Automating the input of data from various sources into different systems.
- **Invoice processing** – Automating the extraction of data from invoices and the handling of payments.
- **Customer service** – Automating tasks such as responding to frequently asked questions and processing routine requests.
- **Financial reporting** – Automating the extraction and consolidation of financial data for reporting purposes.
- **HR processes** – Automating tasks including the onboarding of new employees, managing leave requests, and processing payroll.

"The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency."

Bill Gates





RPA in cybersecurity

The applications of RPA in cybersecurity extend well beyond basic task automation; they strengthen the overall security framework, enhance efficiency, and reduce human error in critical processes. As cyber threats grow increasingly sophisticated, RPA offers organisations a powerful means of handling repetitive tasks, optimising resources, and reinforcing their defences.

- **Conducting Security Tests Efficiently** – RPA can automate routine security testing, such as penetration tests, by simulating cyberattacks and assessing system defences.
- **Automating Software Updates** – RPA automates the detection and installation of software updates, ensuring systems stay current and secure. This reduces human error and protects against vulnerabilities caused by outdated software.
- **Automating Log Analysis** – By scanning log files for anomalies or suspicious patterns, RPA accelerates threat detection and alerts teams in real-time. This frees security professionals from manually reviewing vast amounts of data.
- **Enhancing Incident Response** – RPA can monitor for suspicious activity and initiate immediate, pre-set responses—such as isolating systems or notifying teams—helping to contain threats swiftly and consistently.
- **Real-Time Breach Detection** – RPA continuously monitors networks, identifies potential breaches, and alerts teams for fast action.
- **Maintaining Security Compliance** – RPA supports regulatory compliance by tracking data access, logging changes, and flagging discrepancies.
- **Managing and Categorising Data** – RPA ensures data is accurately classified and stored securely, reducing the risk of mismanagement or data loss.

RPA benefits

- **Increased efficiency and productivity** – RPA can automate time-consuming and repetitive tasks, enabling employees to concentrate on more complex and strategic work.
- **Reduced operational costs** – By automating routine activities, organisations can lessen their dependence on manual labour and reduce operational expenditure.
- **Improved accuracy and consistency** – RPA bots follow predefined rules and procedures, ensuring tasks are completed with consistent accuracy. RPA Bots are often built to repeat the painfully boring workflows everyone hates.
- **Enhanced compliance** – RPA can assist organisations in meeting regulatory requirements by automating compliance-related processes.
- **Faster turnaround times** – RPA can significantly shorten the time required to complete tasks, leading to improved turnaround times overall.

"I don't buy into the dystopian scenarios of self-aware robots enslaving mankind but you don't have to be a sci-fi conspiracy theorist to acknowledge that plenty of good, well-paying jobs are being taken over by machines."

Marco Rubio

Boosting MSP capabilities

Zhero was looking for a solution that would make their SecOps more efficient and help them dedicate more time to better serving our clients. We partnered with Atomatik to implement a tailored intelligent automation solution for patch management and T1 alerts triage. This project strengthened the workflows and productivity within Zhero and helped consolidate our cybersecurity processes.

Solution

The Atomatik team worked closely with Zhero to understand their existing patch management routine and where it was falling short, mainly around manual effort, visibility across sites, and consistency. Based on this, our team developed an automated workflow tailored to their needs.

We deployed Atomatik's digital SOC Analyst Agents and connected them to Zhero's MSP platform, N-Central Patching. Our agents automatically gathered a list of devices from each of Zhero's locations. For each device, the agents checked for available software updates. If updates were found, they applied the patches without requiring any manual intervention. After patching, our digital SOC Analyst Agents created a clear, structured report with statistics around patches to be installed and patches that were already installed since the last check. This report was then sent to a human analyst, making it easier for them to be in the loop about the actions taken, without digging through multiple locations and thousands of end-points.

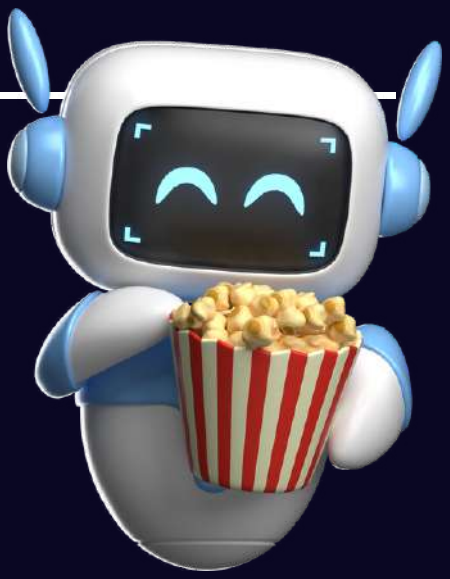
The results

Zhero significantly improved its operational efficiency and key performance indicators as a managed service provider, benefiting from increased transparency into its workflows. This setup reduced the time Zhero spent on routine checks, helped them catch missed patches more reliably, and gave their analysts more time to focus on other tasks.

Implementing Atomatik enabled them to reduce manual workload by delegating the highly manual process of patching to digital SOC Analyst Agents and allowed staff to focus on higher-value activities. Atomatik seamlessly integrated with Zhero's existing tech stack and enhanced SecOps efficiency by more than 90%.

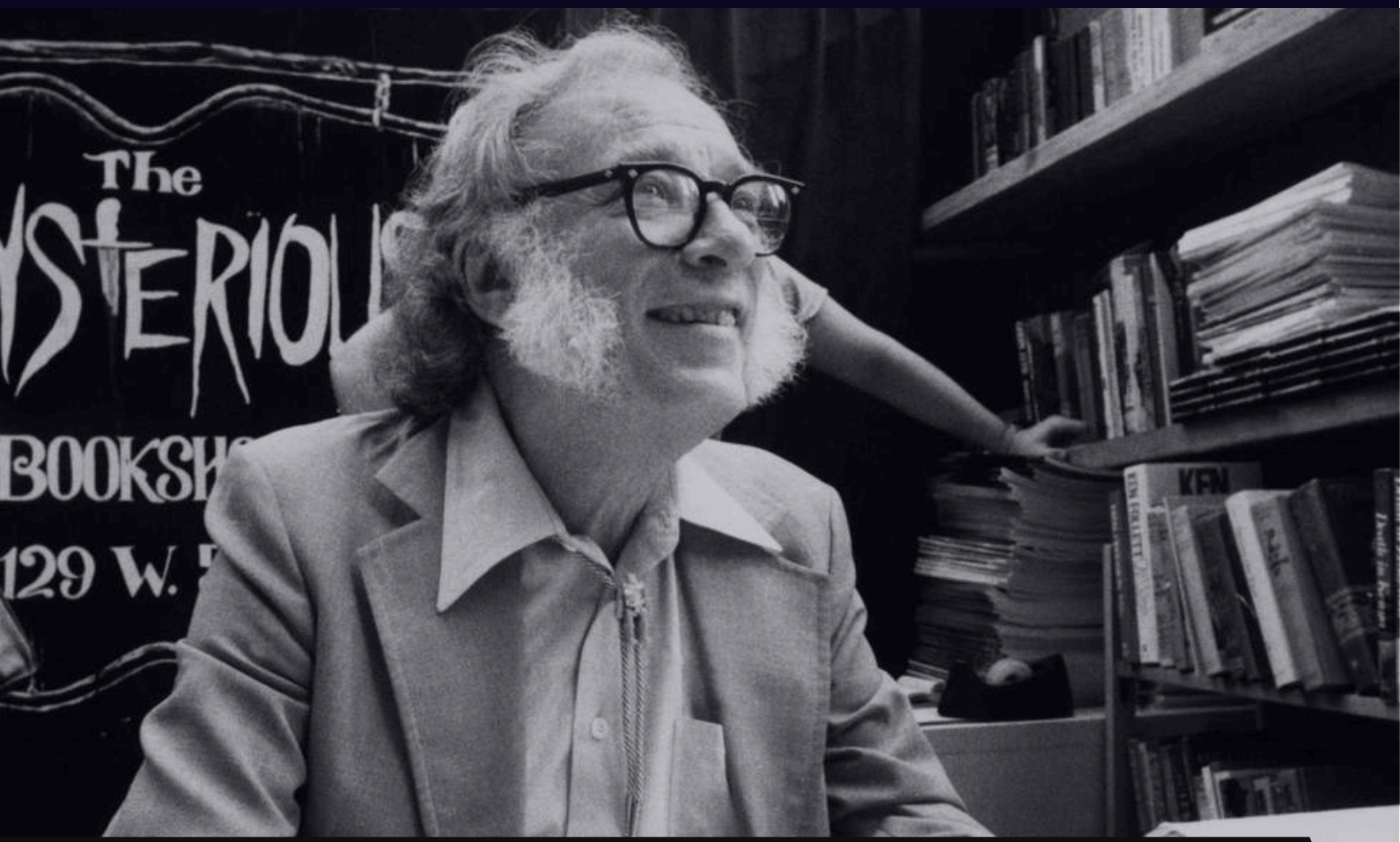
"We are always on the lookout for reliable, cost-effective solutions to improve our key KPIs while delivering best-in-class security protection to our clients. Atomatik helps us cut through operational noise by automating tedious tasks that no one wants to do."

Izak Oosthuizen



“Let’s start with the three fundamental Rules of Robotics… We have: one, a robot may not injure a human being, or, through inaction, allow a human being to come to harm. Two, a robot must obey the orders given it by human beings except where such orders would conflict with the First Law. And three, a robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.”

Isaac Asimov



OUR CYBER CIVILISATION

The term Cyber Civilisation arose from the rapidly evolving nature of digitalisation. Since the advent of the internet, our world has been in a state of continual transformation. Put simply, the internet revolutionised the way we live and interact, suddenly granting us access to vast amounts of information and accelerating our development as never before. Alongside the early internet, basic digital tools began to emerge to meet new demands. Each evolutionary step towards Cyber Civilisation builds upon its predecessor. For example, the rise of cloud technology was soon followed by an increase in data breaches, which in turn prompted heightened security awareness, the integration of artificial intelligence (AI), and the growing adoption of Zero Trust and automation frameworks. Due to the increasing frequency of data breaches, adaptation has become not merely necessary but inevitable. However, this shift represents more than simple adaptation — it marks the beginning of what can be described as Cyber Civilisation. It is believed that many organisations can take a crucial step towards more effective cybersecurity strategies once they fully understand the true scale and complexity of cyber threats.

Cyber threat landscape

Six major categories of cyber threats have been identified, each capable of significantly impacting both organisations and individuals. When these threats are overlooked or underestimated, the consequences can be catastrophic, ranging from financial loss and operational disruption to reputational damage and legal liabilities. To mitigate such risks, it is essential to adopt a proactive and comprehensive approach to cybersecurity. This includes conducting regular security assessments, delivering ongoing employee training, and implementing clear, organisation-wide security protocols. These measures must be fully embedded at every level, from executive leadership to frontline staff, to ensure a resilient and security-conscious culture throughout the organisation. These are the primary threats:

- **SQL injection** – By exploiting vulnerabilities in data-driven applications, attackers can manipulate or steal data from databases.
- **Denial-of-Service (DoS) attacks** – These attacks aim to overwhelm systems, networks, or servers with traffic, rendering them unusable.
- **Malware** – This encompasses various malicious software, including viruses, worms, and ransomware, which can disrupt operations, steal data, or damage systems.
- **Zero-Day exploits** – These occur when attackers take advantage of previously unknown vulnerabilities before developers have had a chance to address them.
- **Phishing attacks** – These scams involve sending fraudulent communications that appear to come from a reputable source, often via email, to steal sensitive information.
- **Man-in-the-Middle attacks** – Attackers intercept and relay messages between two parties, manipulating them for malicious purposes.

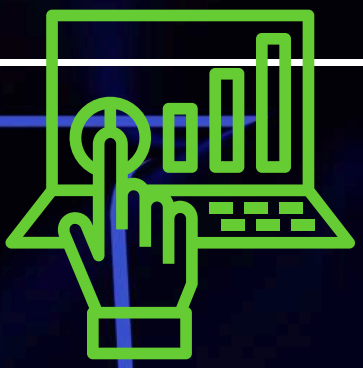
Cyberattack aftermath

The consequences of a successful cyberattack are both severe and far-reaching. Such incidents can erode stakeholder trust, result in regulatory penalties, cause substantial financial damage, and disrupt essential business operations. Crucially, no organisation, regardless of size, sector, or geography, is exempt from these risks. This assertion is substantiated by a growing body of empirical evidence, including industry-wide threat intelligence reports and internal risk assessments. Given the scale and complexity of the threat landscape, cybersecurity must be treated not as a reactive function but as a strategic imperative that is embedded at the core of organisational governance, risk management, and operational resilience.

Cyber civilisation necessity

With a comprehensive understanding of the primary cyber threats, it becomes imperative to address a broader and more strategic question: Why does cybersecurity constitute a critical priority in the digital era? Why is a Cyber Civilisation a necessity? In recent years, cybersecurity has emerged as a central focus not only for multinational corporations, but also for academic institutions, research bodies, and government agencies. Its importance lies in its capacity to protect digital infrastructure, sensitive data, and critical systems from an ever-evolving array of cyber threats. These threats have the potential to compromise the confidentiality, availability, and integrity (CIA) of information assets, the foundational pillars of information security.

Technology dependence



Cybersecurity is no longer a luxury or a specialised concern but it is an operational necessity that transcends industry boundaries. Cyber threats do not originate from isolated sectors; they span the entire digital ecosystem, exploiting vulnerabilities wherever they exist. While each industry faces distinct challenges, a common denominator persists: a deep reliance on digital technology and interconnected systems. In a landscape where more than 60% of interactions and operations now take place online, the critical importance of cybersecurity cannot be overstated. It serves as a fundamental pillar in safeguarding digital integrity, ensuring business continuity, and maintaining stakeholder trust. Cybersecurity is also central to the broader paradigm shift towards what is increasingly defined as Cyber Civilisation, a digitally driven world where security, situational awareness, and technological innovation must evolve in unison. In this emerging era, robust cybersecurity frameworks are not simply protective mechanisms, but strategic enablers of sustainable digital transformation.

"As organisations accelerate digital transformation- embracing cloud computing, the Internet of Things, and remote work—attack surfaces expand considerably. This creates new vulnerabilities that often aren't fully understood or safeguarded."

Andrei Pusoiu

Cybersecurity trends

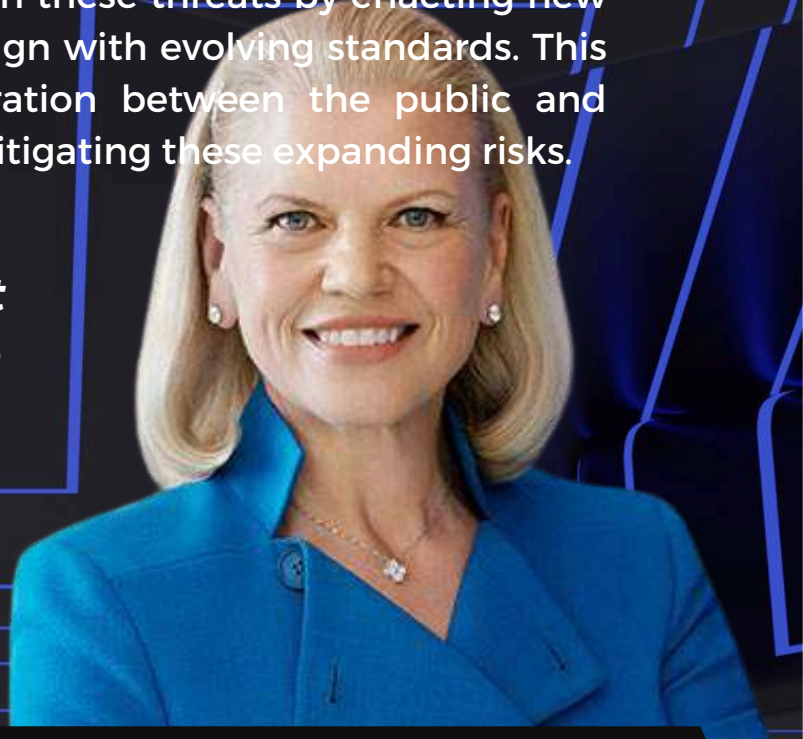
Three major trends have been identified as having the most significant impact on the cybersecurity sector: the escalation of cyber threats, the emergence of the Zero Trust security model, and the evolving role of AI in cybersecurity. Organisations that comprehend and proactively adapt to these trends will be far better equipped to safeguard their digital assets, mitigate emerging risks, and sustain operational resilience in an increasingly hostile and unpredictable cyber environment.

Growing threats

The increasing prevalence of cyber threats is recognised as part of a global cybersecurity trend, fuelled by extensive discussion and mounting relevance in the digital landscape. Today, governments are placing heightened emphasis on these threats by enacting new laws, policies, and regulations to align with evolving standards. This underscores the growing collaboration between the public and private sectors in addressing and mitigating these expanding risks.

"Cybercrime is the greatest threat to every company in the world."

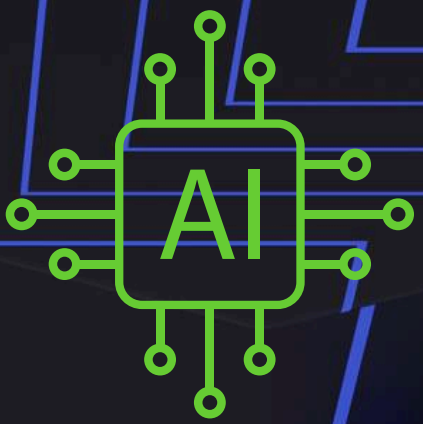
Ginni Rometty



Zero Trust model

The maxim “Never trust, always verify” lies at the heart of the Zero Trust Model, which was developed with the primary aim of strengthening security. This approach is founded on the principle that no entity — whether a user, device, or application — should be trusted by default. In recent years, organisations have embraced this model to mitigate the risks posed by cyber threats, emphasising the importance of stringent access controls and continuous verification. The shift towards Zero Trust highlights why cybersecurity has become a global imperative. Governments, corporations, and even individuals are placing greater priority on cybersecurity, recognising it as a fundamental component of modern digital infrastructure. The widespread adoption of the Zero Trust Model reflects a collective commitment to protecting sensitive data and maintaining resilience against evolving cyber risks.

AI and cybersecurity



Although AI offers substantial benefits in enhancing cybersecurity, it also introduces a range of complexities, particularly about data privacy. The very algorithms designed to monitor user behaviours, detect anomalies, and identify potential threats require access to and processing of vast amounts of sensitive and personal data. This extensive data handling inevitably raises significant concerns regarding privacy, data protection, and compliance with regulatory frameworks. Moreover, the use of AI in cybersecurity necessitates careful consideration of how data is collected, stored, and utilised to prevent misuse or unauthorised access.

Windows 10 EOL

On 14 October 2025, Windows 10 Home and Pro will reach end of support or end of life (EOL). End of Life (EOL) is when a software application is taken off the market or not renewed. The manufacturer may still provide some support, such as security patches and updates. End of Support (EOS) is the complete discontinuation of all support services for the software.

WHAT THIS MEANS

- No more free updates - After October 14, 2025, Windows 10 users will not receive any further free security updates, feature updates, or technical support from Microsoft.
- Security risks - Running Windows 10 without security updates will expose your device to potential security threats, malware, and vulnerabilities.
- Upgrade or replace - Microsoft advises users to either upgrade to Windows 11 (if their hardware is compatible) or replace their devices with new ones that support Windows 11.
- Extended Security Updates (ESU) - Microsoft offers an ESU program for Windows 10, which provides paid security updates for a limited time after the EOL date, but it's not a long-term solution and doesn't include new features.
- Windows 11 advantages - Windows 11 offers a modern and efficient experience with enhanced security features, designed to meet current demands.
- Free upgrade - Upgrading from Windows 10 to Windows 11 is free for eligible devices.
- PC Health Check - If you're unsure whether your PC is compatible with Windows 11, you can use the PC Health Check app to check its eligibility.

Windows 10 EOL

WHAT WILL HAPPEN

Your PC will continue to work, but all support for Windows 10 is discontinued.

WHAT YOU CAN DO

- You could ignore the EOL deadline completely. This is NOT recommended as your PC is no longer receiving updates and security patches from Microsoft. This means your PC is vulnerable to malware infections and other cyber threats. You will also experience performance and compatibility issues.
- You can pay Microsoft for security updates for Windows 10. With the Extended Security Updates package you can keep your current Windows 10 device fully protected for up to 3 years. According to Microsoft, the first year of protection will cost £50. This increases to £100 in the second year and £150 in the final year of cover.
- You can upgrade your existing PC to Windows 11 or buy a new laptop with this latest OS already installed.

WHAT WE WILL DO

Zhero recommends switching to Windows 11. We will assess whether your existing PC can be upgraded and is capable of running Windows 11 or if you will need a new workstation. While making the change to a new OS may seem daunting, we are here to support and assist you in every way we can.

Digital Defender Giveaway

amazon

Win £50 voucher

- *I scan the web night and day*
- *I keep bad actors far away*
- *Through files and code, I make my way*

What am I?

Enter our monthly draw and stand a chance of winning a £50 Amazon voucher. The winner will be announced in the next edition of Inside Zhero. It only takes seconds to enter. Competition closes 11 August 2025 at midnight. Good Luck!

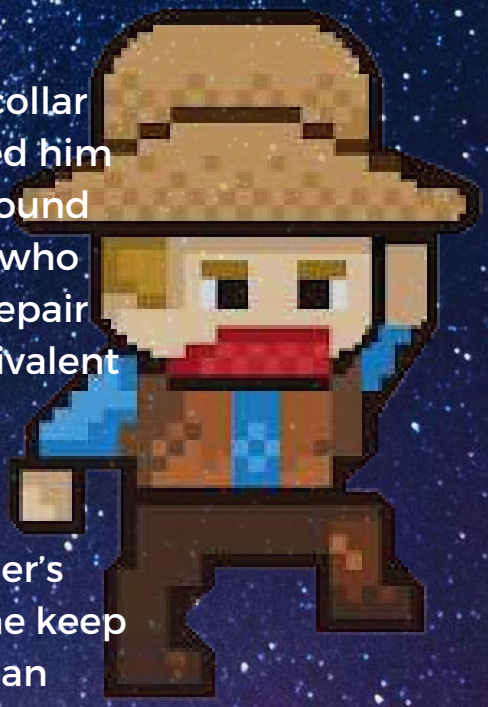
Enter Now

zhero

A Journey into Cybersecurity

This month, one of our amazing Escalation Engineers, Lovemore Gurungo, reveals his incredible journey into cybersecurity. Lovemore shows how determination, hard work and education all pay off in the end, especially for somebody wanting to pursue a career in the IT and cybersecurity industries

My father passed away in 1999, and I have only vague memories of the time we spent together. What I do remember clearly is that he was a hardworking blue-collar man, doing welding and plumbing jobs, which allowed him to leave us with a roof over our heads. Without him around for career guidance, I looked up to my older brothers, who had carved their own paths as self-taught computer repair technicians. After completing my O-Level exams (equivalent to GCSEs), I couldn't afford to continue my education immediately, so I took a gap year.



During that time, I started working at one of my brother's computer repair shops. He motivated me by letting me keep the money from any repairs or sales I brought in. I began selling computer games like Galactica, Dangerous Dave, and Super Mario to my more well-off friends. I'd often upsell them RAM upgrades, hard drive optimizations (good old chkdsk /f), and Windows OS repairs.

zhero

A Journey into Cybersecurity

This was my first exposure to Windows 2000, XP, Vista, and 7 systems that made me feel ahead of my peers and deepened my love for IT. However, one thing became clear: I didn't enjoy hardware repairs. I began brainstorming ways to stay in IT without having to deal with hardware. The answer was education.

I enrolled in a professional course called Microcomputer Technology (City & Guilds), which helped me discover my passion for Network Engineering. Determined to excel in my chosen specialisation, I began researching how to stand out, especially since I hadn't followed the traditional four-year degree path due to financial constraints.

To bridge that gap, I pursued industry-recognised certifications, starting with the Cisco Certified Network Associate (CCNA) and later advancing to the Cisco Certified Network Professional (CCNP) certification. These professional courses opened doors for me, and I soon began working for a local Internet Service Provider (ISP). At the ISP, I was rotated through various departments, including: Access Network, Network Planning, Helpdesk, WiMAX, Core Network, Research & Implementation of Network and Security vendor solutions.

Across all these rotations, one constant remained: Security. Whether it was Network Security, Endpoint Protection, or Cybersecurity Awareness, I was always involved in helping clients understand how to protect their data. We educated users to prevent common complaints like unexplained data usage or suspicions that the ISP was tampering with their information. By this point, I had become somewhat of a network and cybersecurity nerd. Although I'm an introvert, I came alive when explaining tech and cybersecurity concepts. That passion led me to my next role as a Group Network Security and Infrastructure Administrator, supporting over 64 branches.

zhero

A Journey into Cybersecurity

The platform I was managing became both broader and more complex, requiring me to upskill further to protect users and infrastructure effectively. I went on to complete certifications in Sophos XG Administrator, Fortinet NSE4 (Network Security), CEH Practical, and Darktrace Cyber Analyst. These pursuits allowed me to delve deeper into cybersecurity, where I implemented an Onion Security Model—a layered defence strategy designed to protect the organisation at multiple levels. This model helped secure data at rest and data in transit, perimeter security, Access Control & Identity management, Security Patching & System hardening, Email & Web Security, while also leveraging Darktrace as an AI-powered threat visualizer to detect anomalies in real time. In addition to technical implementations, I was also tasked with training both internal Junior IT teams and end users on cybersecurity awareness. After all, a thousand-dollar security system can be rendered useless by a ten-pound flash drive—or worse, an uninformed attitude.

Just before joining Zhero, I took on a role as a Linux Server Administrator—an opportunity I earned through my natural curiosity and willingness to explore. During this time, I also explored DevSecOps, which gave me a broader view of how security integrates into development and operations pipelines. These nine and a half years in fast-paced, high-responsibility environments ultimately led me to the doorstep of Zhero, where I now serve as an Escalations Engineer. In this role, I act as the final point of escalation for complex technical issues, ranging from network outages and infrastructure failures to advanced cybersecurity incidents. I work closely with Tier 1 and Tier 2 support teams, conducting in-depth root cause analysis to ensure that client environments remain secure, stable, and resilient. Security remains a central part of my responsibilities. I manage and monitor endpoint protection, firewall configurations, and patch management across multiple client systems. At Zhero, I've found a space where my passion for networks and cybersecurity continues to grow, where every challenge is an opportunity to learn, lead, and make a meaningful impact.

CYBER LONDON

NATIONAL HEALTHCARE CYBERSECURITY CONFERENCE

IGPP

At the beginning of the month, Izak represented Cyber London at the Annual Healthcare Cyber Security Conference and Exhibition 2025 in Manchester. Hosted by the Institute of Government & Public Policy, cyber experts addressed the real cybersecurity challenges facing the NHS, including resilience strategies and emerging threats to innovation, collaboration, and creating a stronger cyber culture across UK healthcare. Izak took the stage twice. First, he gave the lowdown on Cybersecurity Governance in Healthcare Organisations. Later in the day, things got a bit more technical with Izak's presentation on Enhancing Healthcare Cyber Resilience Through Integrated Tooling and XDR.

Meet the team

Popina Khumanda

SERVICE DESK ENGINEER

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

I originally applied to study Electrical Engineering, with no intention of pursuing IT. But when an administrator unexpectedly suggested IT during registration, I accepted without hesitation. I'm grateful I did.

What's your most-used productivity tool?

Active Directory. It's a powerful tool that allows me to work efficiently and support users effectively within the IT infrastructure.

How would you describe yourself?

Il've learned to embrace change as naturally as the seasons shift. Just like nature around me adapts to both abundance and scarcity, I thrive in dynamic environments and find strength in flexibility and growth.

What do you enjoy the most about your role?

I have the opportunity to work with international companies and solve real-world challenges. It's rewarding to contribute to global operations and learn about cutting-edge technologies

Do you have any hidden talents or hobbies?

I'm fascinated by reading and writing. There's something magical about how the human mind can imagine the unimaginable, how a simple thought can be transformed into words.

What is your favourite movie or TV show?

My favourite TV show is Westworld. It's more than just science fiction it mirrors so much of human vulnerability, identity, and our relationship with control and freedom.

CRUSH IT CHAOS

Tune in here:

zhero | PODCAST

LONDON
162 Farringdon Road
London
EC1R 3AS

SPEAK TO US
+44 20 7183 3975

START THE PROCESS

zhero
crush the chaos