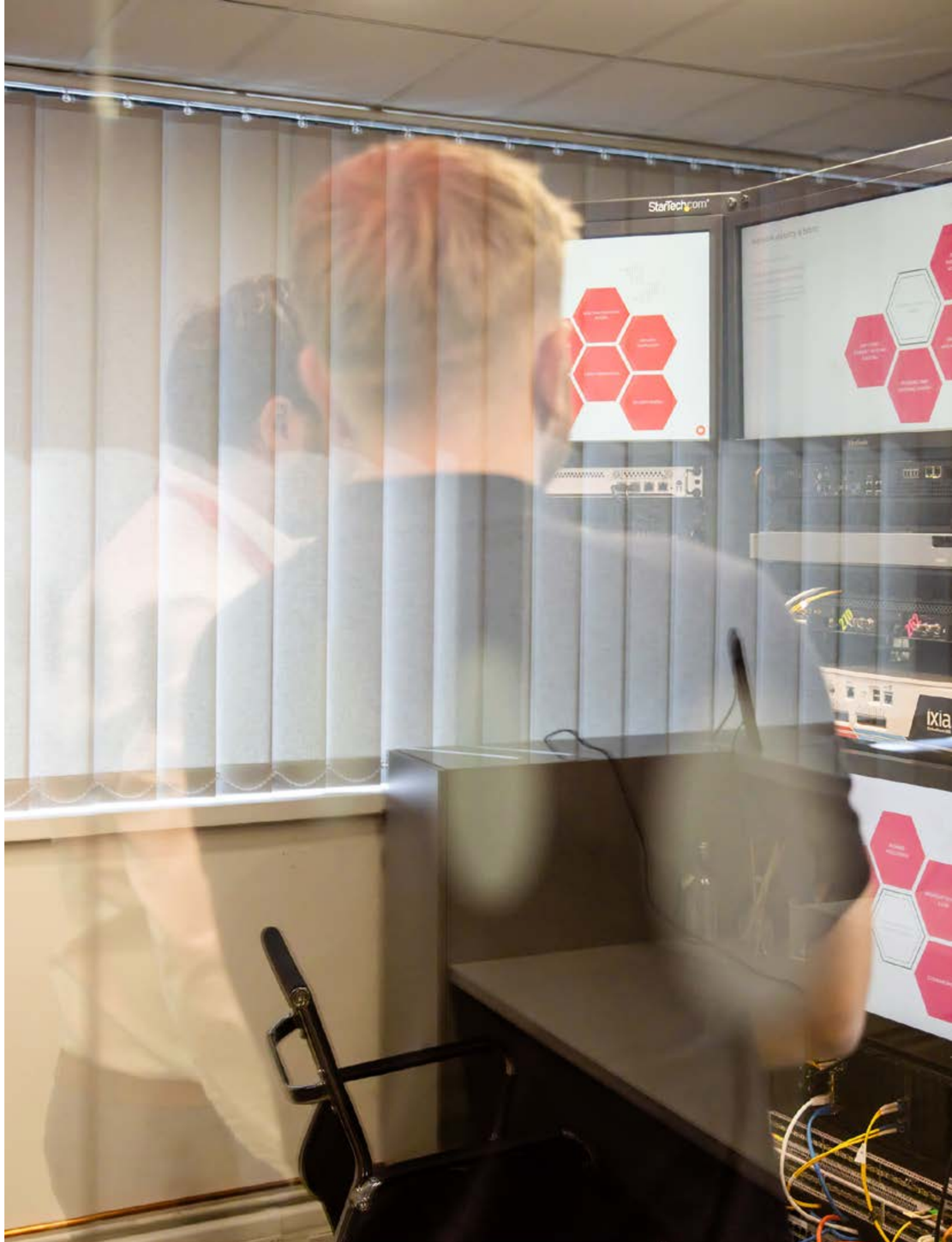
Red Helix

The Red Helix Security Intelligence Platform

Why more data is leaving organisations more exposed, and how we are closing the divide.

CONTENTS



Introduction

UK cyber security investment has never been higher, and boards are more aware of the threat landscape than at any point in history. The regulatory environment is tightening at a rapid pace. Yet, despite these factors, the breach rate continues to climb. According to the UK Government's Cyber Security Breaches Survey 2025/2026, forty-three percent of UK businesses experienced a cyber breach or attack in the past twelve months, which equates to approximately 612,000 organisations. This figure is not a failure of technology deployment; it points to something far more structural and concerning.

In the same survey, only eleven percent of UK businesses reported using or investing in threat intelligence, while fewer than one in three conducted a formal cyber security risk assessment. This is the central paradox of modern security: companies are experiencing breaches at a significant scale while investing minimally in the intelligence infrastructure that would help them understand, anticipate, or act on their exposure. Security tool adoption has grown consistently for two decades, and alert volumes have never been higher, yet the gap between what organisations know and what they need to know is widening. The problem was never the sheer volume of tools, but rather the total absence of integrated intelligence.

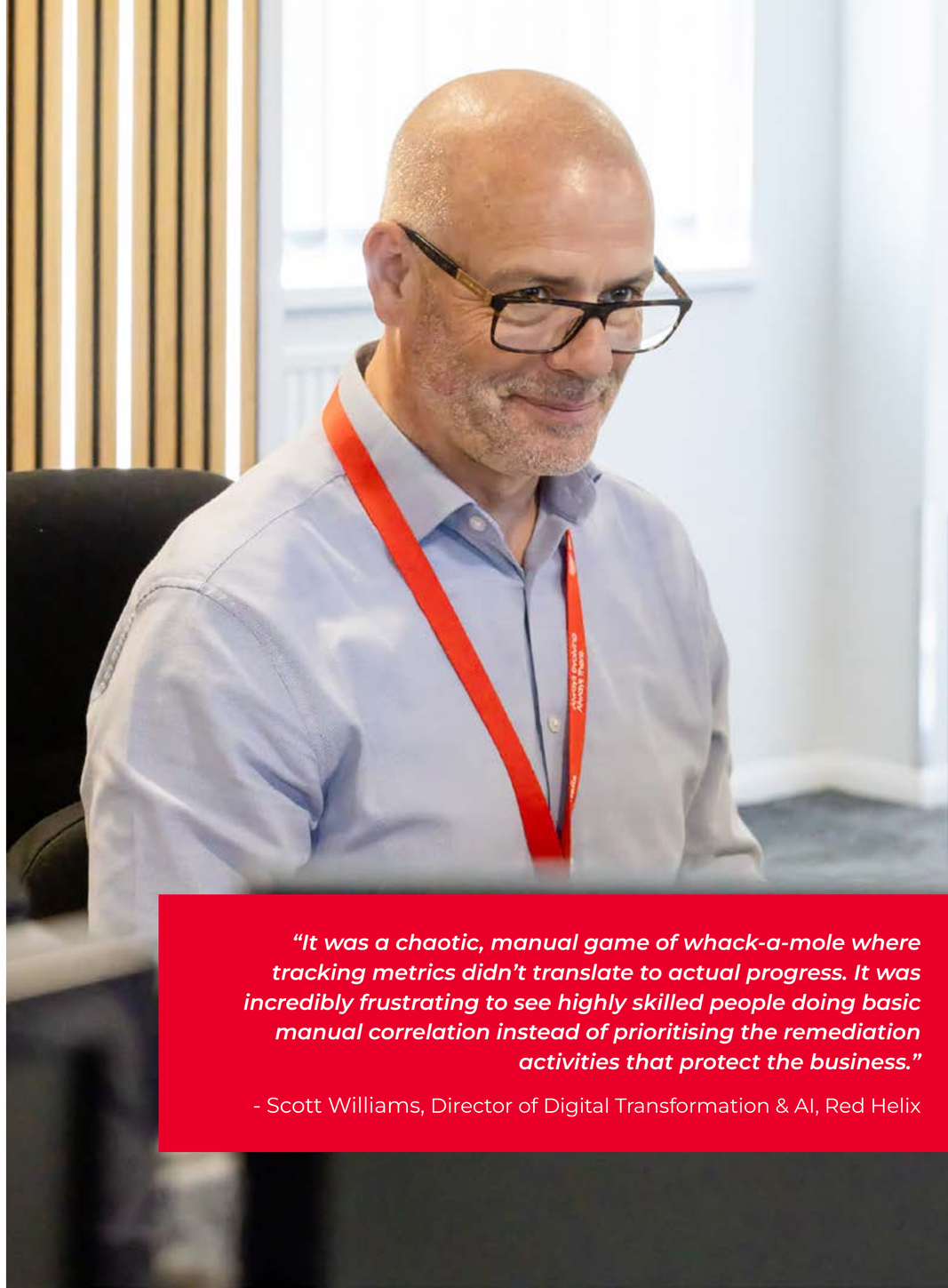
How We Got Here: The Tool Trap

The security industry's response to a decade of escalating threats was simply to deploy more tools. Each point solution addressed a real, isolated problem. Endpoint Detection and Response platforms gave visibility to the device layer, SIEM tools aggregated log data across environments, GRC platforms brought structure to regulatory obligations, and vulnerability scanners identified weaknesses. Each investment was entirely defensible in isolation, but collectively, they created fragmentation at scale.

By 2025, the World Economic Forum's Global Cybersecurity Outlook found that seventy-two percent of organisations reported an increase in cyber risk despite their tool investments. The same report revealed that thirty-five percent of small organisations now believe their cyber resilience is inadequate, a proportion that has grown sevenfold since 2022. While larger organisations have the resources to employ dedicated teams of security analysts to correlate and interpret tool outputs, the mid-market does not. This creates a deep, structural inequality where organisations that cannot afford human interpretation of tool data are generating more noise than they can process and failing to make informed decisions because of it.

This daily frustration is what drove Scott Williams, Director of Digital Transformation & AI at Red Helix, to build the Security Intelligence Platform. "For years, I watched teams drown under the weight of disjointed alerts from fragmented security stacks," Scott explains. "We were deploying the best tech on the market, but because those systems existed in silos, our analysts spent half their day just trying to piece together what was happening. It was a chaotic, manual game of whack-a-mole where tracking metrics didn't translate to actual progress. It was incredibly frustrating to see highly skilled people doing basic manual correlation instead of prioritising the remediation activities that protect the business."

Without a unified platform to centralise security telemetry and filter out background static, organisations are left constantly reacting to past events rather than preventing active threats. This operational bottleneck drove the development of the Security Intelligence Platform. By consolidating data from fragmented systems, the platform automates repetitive manual analysis, eliminates duplicated efforts across security teams, and translates complex technical telemetry into clear, actionable, business insight.



> ***"It was a chaotic, manual game of whack-a-mole where tracking metrics didn't translate to actual progress. It was incredibly frustrating to see highly skilled people doing basic manual correlation instead of prioritising the remediation activities that protect the business."***
>
> - Scott Williams, Director of Digital Transformation & AI, Red Helix

Defining the Gap and the Language of the Boardroom

To understand what is missing, it helps to be precise about what intelligence means, and how it differs from the data and information that most organisations already have in abundance. Data is what security tools produce, such as logs, alerts, telemetry, and vulnerability scores. Information is what a skilled analyst produces from that data by correlating events and contextualising incidents. Intelligence, however, is what enables a decision. It is risk-graded, business-contextualised insight that tells an organisation not just what has happened, but what it means, what it is likely to cost, and what to do next.

The intelligence gap is not a gap between alert and response; it is a gap between a technical signal and a business decision. An overwhelmed security team reviewing fifty thousand alerts a week and a CFO who cannot verify if the business is safer than it was six months ago are experiencing the same structural failure. Both are victims of a system that generates endless technical data but fails to translate it into a strategic business decision. True security intelligence requires a translation layer that speaks the language of the boardroom, which is always the language of finance.

The Red Helix platform doesn't just estimate abstract risk; it calculates real-world financial implications. This means security teams can show a Board exactly what a breach would cost in terms of downtime, regulatory penalties, and operational impact. It transforms cyber security from an expensive, reactive compliance checkbox into an active, data-driven business strategy, so organisations can quantify the precise risk of inaction.

"For too long, cyber security has been considered a highly technical IT department problem, but cyber security is a fundamental pillar of organisational risk management and business survival. As a CFO, I don't need to see CVE codes, threat signatures, or vulnerability counts. I need to know how exposed we are, how our risk posture has changed quarter-on-quarter, and what the tangible ROI is on our security spend. What we call financial security intelligence is our way of translating the technological to our stakeholders."

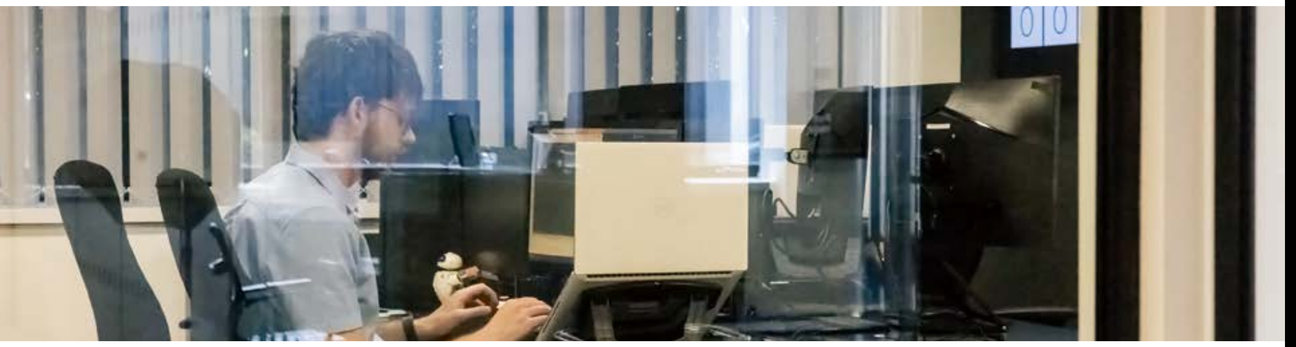
- Ben Dunn, Chief Strategy Officer, Red Helix

Threat Velocity and the AI Arms Race

What makes this intelligence gap highly dangerous is the sheer speed at which the modern threat landscape now operates. According to CrowdStrike's 2026 Global Threat Report, the average eCrime breakout time fell to just 29 minutes in 2025, which represents a 65% increase in speed from the previous year. The fastest observed breakout occurred in only 27 seconds, and in one intrusion, data exfiltration began within four minutes of initial access. Against a threat landscape moving at that tempo, reporting cycles measured in weeks or months are structurally irrelevant. The intelligence gap does not cause organisations to respond slowly; it causes them to respond to events that are already complete.

Furthermore, dominant attack methodologies make traditional detection methods obsolete. In 2025, 82% of detections were malware-free, with adversaries operating through valid credentials, legitimate identity flows, and approved application integrations. Traditional signature-based detection is largely blind to this class of attack, which requires deep behavioural intelligence to identify.

At the same time, AI-enabled adversaries increased their operations by 89% year-over-year in 2025, deploying machine learning across reconnaissance, credential theft, social engineering, and evasion. The WEF's 2026 Outlook notes that 87% of respondents identified AI-related vulnerabilities as the fastest-growing cyber risk of the past year. This is compounded by a ten-fold explosion in automated bot volume. Threat actors are utilising advanced machine learning as a primary weapon, with over eighty percent of attacks now leveraging AI and advanced models.



Who Bears the Cost?

Security professionals inherit fragmented tool estates, manage alert volumes that exceed human capacity, and are then asked to translate technical complexity into a board-level narrative. The DSIT survey found that the most common source of guidance remains external consultants and providers, with only one percent citing the NCSC by name. Operating without structured intelligence frameworks, security leaders are consistently disadvantaged in budget conversations because they cannot easily quantify risk in financial terms.

Meanwhile, following high-profile incidents, the UK government has called directly on FTSE350 chief executives and chairs to treat cyber resilience as a board-level responsibility. Yet, the DSIT survey reveals that only 31% of UK businesses have a board member with explicit responsibility for cyber security. While 72% of senior management teams report that cyber security is a high priority, priority without intelligence is meaningless. Boards are carrying greater personal and institutional exposure for a risk they cannot see.

This is being accelerated by the political landscape. Announced as part of the July 2024 King's Speech and currently progressing through Parliament, the Cyber Security and Resilience Bill aims to reform and expand the existing NIS Regulations 2018. The Bill is expected to introduce mandatory 24 hour incident reporting and enforce stricter, continuous audit requirements, moving organisations away from an annual compliance view and toward a live view of security risk. It will hold the Board directly accountable for remediation, ensuring real engagement rather than passive delegation.

The intelligence gap is sharpest at the middle of the market. DSIT data shows that 64% of small businesses and seventy percent of medium businesses outsource their cyber security to external providers. However, outsourcing operational security is not the same as accessing strategic intelligence. The mid-market faces enterprise-grade threats without the analytical infrastructure or the budget to hire expensive in-house threat analysts, risk quantification specialists, and detection engineers. The scale of the UK threat context underscores what is at stake, as the NCSC's Annual Review 2025 recorded 204 nationally significant cyber incidents in the year to August 2025, meaning the UK experiences an average of four nationally significant cyber attacks every single week.

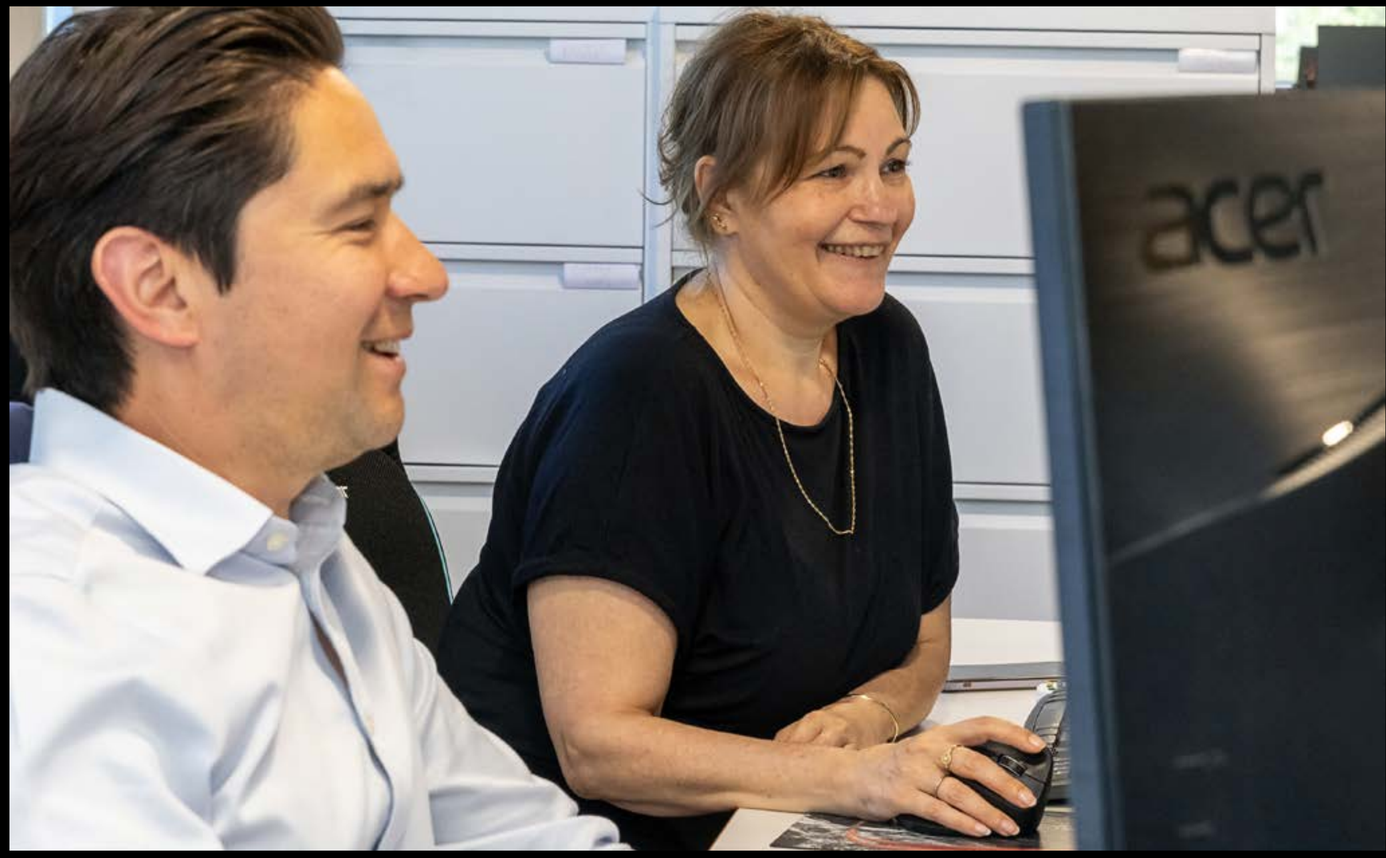
Closing the Gap: The Red Helix Security Intelligence Platform

The Red Helix Security Intelligence Platform is a unified command centre designed to turn raw technical telemetry into actionable business intelligence. Rather than forcing organisations to deploy more disconnected tools, our platform consolidates risk reporting into a centralised, single-pane-of-glass hub.

We have designed our approach around a simple methodology that we call Find, Fix, and Prove. First, our platform and AI identify your specific security and compliance gaps. Second, our expert SOC, consultants, and penetration testers provide the direct human capital needed to remediate and close those gaps. Finally, our 24/7 autonomous hunting and SLA timers provide constant, quantified proof of your resilience.

To counter AI-driven threats, the industry is moving toward Agentic AI, where systems operate through multiple specialised AI agents to reduce human analyst workloads. Our platform serves as a progressive gateway to these advanced AI capabilities, feeding alerts into the SOC and cycling them back to enable continuous, tailored learning for your environment. The platform unifies your entire security stack into a single, intuitive interface, understanding previous rules and behaviours to generate only critical, relevant outputs rather than overwhelming technical noise.

Furthermore, the Security Intelligence Platform adapts to your specific business environment, sector context, and high-value assets, ensuring attention is focused where a breach would cause the most severe operational or financial damage. The platform provides a strong forensic audit trail, proving continuous due diligence to regulators, cyber insurers, and supply chain partners. This allows you to show the direct cost of inaction, proving to stakeholders exactly what will happen if you do not remediate a specific vulnerability.



Real-World Business Cases

Aligning Cyber Security with Business Risk

Security leaders spend too much time translating technical findings into business language, while executives struggle to understand where the organisation is genuinely exposed. Even though boards know cyber is a business risk, reporting is often fragmented across multiple tools, spreadsheets, and technical dashboards.

The Red Helix Security Intelligence Platform aggregates telemetry from across the organisation and translates it into a single, business-focused view of cyber risk. Rather than presenting thousands of alerts or technical vulnerabilities, it provides a clear understanding of risk posture, emerging trends, and areas requiring investment or intervention.

As a result, executives gain the visibility needed to make informed decisions, justify security investment, and demonstrate governance to regulators, auditors, customers, and shareholders. For example, a CFO preparing for a board meeting can quickly understand how cyber risk has changed over the quarter, where the greatest exposure sits, and whether security initiatives are reducing risk, without needing to interpret complex technical reporting.

Scaling Security Operations in the Mid-Market

Many mid-market organisations face the same threats as large enterprises but lack the resources, specialist skills, and headcount to manage an ever-growing number of security tools and alerts. Teams become overwhelmed by noise and struggle to focus on genuine threats.

The platform acts as a force multiplier for security and IT teams by consolidating telemetry into a single operating picture. Through continuous feedback from the SOC, it learns about the organisation's environment, reducing unnecessary alerts and highlighting only the issues that require action. This is unlike traditional SIEM or monitoring platforms which often generate more work; instead, the platform continuously improves its understanding of the business and prioritises outputs accordingly.

This allows security teams to spend less time investigating false positives and more time addressing meaningful risks, helping organisations gain greater security maturity without needing to significantly increase headcount. An IT manager responsible for infrastructure, security, and compliance can quickly identify the handful of issues that genuinely require attention, rather than manually reviewing hundreds of alerts across multiple systems every day.

AI-Powered Security Operations Built on Business Context

Many organisations are interested in AI-driven security but lack the foundations to deploy it effectively, as AI is only as useful as the quality, context, and accessibility of data feeding it.

The Security Intelligence Platform creates a centralised intelligence layer that understands the organisation's technology stack, operational behaviours, historical incidents, and security controls. Because the platform continuously learns from SOC activity and previous investigations, it develops an understanding of what normal looks like within that specific environment. This creates a trusted foundation for AI-driven recommendations, automation, and detection engineering.

This allows organisations to adopt AI with confidence, using it to automate repetitive security tasks, accelerate investigations, and improve threat detection without introducing unnecessary risk or noise. Rather than generating generic detection rules, the platform can recommend controls and automations specific to the organisation's vendors, infrastructure, and observed threat patterns, significantly reducing manual effort.

Turning Cyber Risk into Investment Decisions

Security leaders often know where technical weaknesses exist, but struggle to articulate which risks matter most to the business. As a result, investment decisions can become reactive, driven by the latest vulnerability, compliance requirement, or headline breach.

By bringing together telemetry from across the environment and correlating it with business context, the platform enables organisations to understand not just where threats exist, but which risks have the greatest potential operational, financial, or regulatory impact. This allows security leaders to move away from discussions about alerts, vulnerabilities, and technical controls, and towards conversations about measurable business risk.

Budgets can be allocated more effectively, remediation programmes can be prioritised based on impact, and organisations gain greater confidence that security investment is reducing the risks that matter most. Instead of treating 500 vulnerabilities as equal, the platform identifies which handful could realistically disrupt critical business services, expose sensitive data, or create regulatory consequences, enabling teams to focus effort where it delivers the greatest reduction in risk.

From Data Rich to Intelligence Led

The security industry has spent two decades solving the data problem. Most organisations now have more telemetry, more alerts, and more reporting than they can meaningfully use. The investment has not been wasted, but the strategic problem of managing cyber risk as a business risk remains largely unsolved.

Data without intelligence is noise, and noise at scale is its own vulnerability because it diverts attention, exhausts teams, and obscures the signals that matter. The threat landscape is not waiting for organisations to close this gap on their own timeline. The question is not whether your organisation needs security intelligence, but whether you access it before the cost of the gap becomes unavoidable.

Whether you are fighting to keep up with the daily deluge of security alerts, trying to satisfy upcoming compliance demands, or trying to prove to your board that your security spend is working, the answer is the same. The era of simply buying more tools is over. True business resilience requires moving past the noise of raw data and demanding clear, actionable, financial intelligence.

At Red Helix, we built our Security Intelligence Platform to bridge this exact gap. We help you find your vulnerabilities, we provide the human expertise to fix them, and we give you the continuous data to prove your resilience. The threat landscape is moving faster than ever, and the cost of the gap is only growing. Let us help you close it.

+44 (0)1296 397711

info@redhelix.co.uk

Phoenix House
Smeaton Close
Aylesbury
Buckinghamshire
HP19 8UW

Red Helix

redhelix.com