softwerx
The Microsoft Security Specialists

Secure the advantage: A mid-market playbook for cyber resilience and growth

How Softwerx and Microsoft Security help turn risk into opportunity

Table of contents

Foreword:

Security at a turning point for the mid-market by David Smart, CEO, Softwerx

The rules of cybersecurity have changed – and mid-market organisations are now at the centre of the storm.

Once overlooked by cybercriminals in favour of large enterprises, mid-sized companies are now firmly in the crosshairs. Why? Because they power critical supply chains, hold valuable data and operate with just enough complexity to present opportunities – but often lack the dedicated security teams of their larger peers.

According to UK government data, 70% of medium-sized UK businesses experienced a cyber breach in the past year – significantly higher than the 50% average across all companies – underlining the mid-market's growing exposure.

And the risk landscape is only intensifying. AI-driven threats, mounting regulatory demands and hybrid IT sprawl have created a volatile environment where most businesses are struggling to keep up – not just with threats but with the complexity of their own defences.

But in this storm lies **a powerful opportunity**.

The tools many SMBs need are already in their hands. Microsoft's enterprise-grade security technologies – already in use across much of the mid-market – offer untapped potential to go beyond reactive defence. The challenge is no longer just about access, but about knowledge, clarity and confidence.

This is where Softwerx makes the difference.

With specialist expertise in Microsoft Security, Softwerx helps mid-sized organisations rethink their approach – transforming existing investments into secure, scalable, AI-ready infrastructure. By cutting through complexity with practical strategies and tailored guidance, we enable security to become a business enabler, not a blocker.

This eBook is here to help you do exactly that.

Many ambitious mid-sized businesses already own powerful Microsoft Security capabilities – but too few are maximising their value. In fact, only 30% of organisations feel they're effectively using the data they collect (Accenture Technology Vision 2024), and 60% aren't using the advanced Microsoft 365 security features they're already paying for (Forrester 2024).

Across the chapters ahead, we explore today's most urgent cybersecurity challenges – and the strategic advantage you can unlock by addressing them. From identity protection to Zero Trust, AI governance to data resilience, we'll show you how to protect your business while enabling growth, agility and innovation.

Because in a world of growing threats, security shouldn't just protect the business. It should power it.

1. Prime targets:

Why mid-market firms face growing cyber threats and how to gain the upper hand

Turn on the news and you're going to see a breach reported somewhere. It's a constant in the headlines. We're seeing businesses completely crippled and nobody wants to be the next cautionary tale.

Dan Burborough, Head of IT Security, **Hollywood Bowl**

The UK Government 2024 Cyber Security Breaches Survey found that 45% of medium sized businesses experienced cybercrime in the last 12 months, a rise from 26% in the previous year's survey.

Armed with AI-driven tools and operating as commercial enterprises, threat actors are launching relentless attacks on mid-market businesses, at scale and with precision.

Their weapons of choice? Social engineering, ransomware, phishing and vishing.

And the reason for this shift? Because mid-market businesses are vulnerable and have an ever increasing digital footprint.

They hold valuable data but often lack the hardened defences, rapid response plans and recovery capabilities of larger enterprises. This makes them easy targets – and profitable ones. With no clear path to threat detection, containment or recovery, many mid-sized businesses are forced to pay the threat actor's ransom.

The game has changed. Mid-market companies are no longer flying under the radar. They are now prime targets: exposed, unprepared and increasingly under attack.

Cyberattacks on mid-market businesses in the UK increased by 26% in 2024.

UK Government 2024 Cyber Security Breaches Survey

Most mid-market firms rely on Microsoft software and already have access to powerful, enterprise-grade security tools which are often included in what they're already paying for. The problem isn't access, it's activation. These tools are underutilised, misconfigured or simply switched off. What they need is expert guidance to unlock their full potential.

Making sense of existing Microsoft Security investments is where Softwerx comes in. We're not generalists. We're Microsoft Security specialists for the mid-market.

Microsoft's security stack offers a powerful strategic advantage but unlocking its full potential requires a shift in mindset. Softwerx helps organisations rethink how they use the tools they already have, transforming security from a cost centre into a business enabler.

The question isn't "*What do we need?*". It's "*How far can we go with what we've already got?*"

2. AI:

The new cyber weapon
but also your greatest ally

One of the things we're seeing is that our threat model is changing due to AI. We are having to shift from a perimeter-based security model to identity and intent aware defences.

William Wilson, Head of Threat Protection & Governance, **Altum Group**

AI has radically reshaped the threat landscape, giving cybercriminals powerful new tools to exploit organisations at speed and scale. Malicious actors are weaponising AI to automate phishing, vishing, deepfakes, malware creation and password cracking – making attacks faster, more convincing and harder to detect.

These AI-driven tactics are creating unprecedented challenges for mid-market businesses with Microsoft reporting an increase of 30% in AI-driven phishing attacks in 2024 (Microsoft Digital Defence Report, 2024).

But AI can play a dual role. When harnessed effectively through Microsoft's security stack, AI becomes a force multiplier for defence, helping identify and respond to threats in real time to enhance business operations through greater efficiencies and better agility.

To stay ahead, mid-market organisations must evolve. Yesterday's defences won't stop today's AI-powered threats. Static strategies no longer work in a dynamic threat landscape. Agility, adaptation and smarter detection are now essential.

Microsoft Security Copilot processes some 84 trillion signals per day, according to Microsoft, enabling real-time threat detection at unprecedented scale. By automating processes with AI threats are detected faster with more intelligent response, improving Security Operations Center (SOC) efficiency and reducing incident response times to minutes, instead of hours or days.

At Softwerx, we help mid-market organisations harness the full power of Microsoft's Defender suites, which leverage AI and are further enriched via Microsoft Security Copilot. Our expert guidance enables you to optimise threat detection, simplify security workflows and strengthen your overall cyber resilience, turning advanced technology into real-world protection.

A strong Microsoft Security foundation enables secure AI integration, now a strategic board-level initiative (Evanta, 2024).

AI is no longer just a buzzword. It's here, it's real and it's ready to be used. It's about driving efficiency, streamlining operations and strengthening defences. Mid-market firms must take advantage of the tools that are available to them.

There is significant investment going into Microsoft Security Copilot and it's time for businesses to realise the potential of what it can do.

Dan Burborough, Head of IT Security, **Hollywood Bowl**

3. AI:

From shadow IT to strategic IT: Taming app sprawl

App sprawl, unvetted third-party tools and weak vendor controls quietly introduce serious vulnerabilities, particularly in mid-market organisations which often lack the systems, processes and oversight to detect and manage shadow IT. Furthermore, employees may be less familiar with governance practices, further increasing exposure.

That's why visibility is critical.

Delivering clear visibility into the applications and services in use across the organisation is essential for assessing risk and making informed, strategic decisions. With the right insights, businesses can identify vulnerabilities, reduce shadow IT and take control of their digital environment.

At Softwerx, 1596 different apps are currently in use across our business – and we have complete visibility into every single one of them.

This insight empowers us to assess risk, eliminate redundancy and make smarter, data-driven decisions.

Leveraging Microsoft Defender for Cloud Apps, Microsoft Intune and Microsoft Purview, we help mid-market firms use what's already available in their licence subscriptions to deliver end-to-end visibility and risk reduction.

By discovering what applications are being utilised and assessing their risk and compliance levels, IT security teams can make more informed decisions to accept, block or reject the applications.

If a problem is lack of clarity, the solution isn't more tools. It's better insight, clearer data and trusted expertise to make sense of it all.

With more than 25 years' experience in Microsoft licensing, infrastructure and security we help teams uncover what they already have, identify what's working (and what's not) and realise what's truly possible.

A lot of SMEs are being underserved by complex enterprise grade tools. This is often due to increased configuration complexity, which means they never end up leveraging all of the toolsets available. What I've seen with the Microsoft toolset is the secure-by-default starting points and secure baselines, which allow new adoptees to get a head start on this strategy.

William Wilson, Head of Threat Protection & Governance, **Altum Group**

4. Identity

is the new battlefield and
Zero Trust is your best defence

One of the things that surprised me recently around the modern attack surface is how threat actors are targeting staff using their home email addresses to try and get around our corporate controls. What we've done to prevent this and reduce the risk is a series of staff awareness programs and making sure that our identity controls remain secure and robust.

William Wilson, Head of Threat Protection & Governance, **Altum Group**

The attack surface has never been larger. Every employee represents a potential entry point. Credential theft, insider threats and unmanaged access significantly amplify the risk of a breach, making identity governance and access control more critical than ever.

Mid-market organisations currently make up just 24% of the total Zero Trust market share leaving them disproportionately vulnerable to cyber threats and regulatory risks.

It only takes one person to open the door and trigger a cyber breach. That's why identity governance is critical, especially in a world of remote and hybrid work. Verifying and managing every user, right from the start, ensures that access is granted only to trusted individuals.

For mid-sized businesses, where one misstep can have outsized consequences, strong identity controls aren't optional, they're foundational.

Relying on traditional password-based authentication is no longer enough. For mid-market organisations, adopting a Zero Trust security model and moving to passwordless authentication is not just a best practice, it's a necessity.

Identity is the new battlefield and Zero Trust is your best defence.

By leveraging Microsoft's advanced security features, mid-market businesses can strengthen their defences, reduce risk and protect against increasingly sophisticated cyberattacks.

Many mid-market organisations already have access to powerful identity and security features through Microsoft Entra ID Plan 1 and Plan 2 but are not using them to their full potential. For example, did you know that new starters working remotely can be verified using government-issued ID through Entra Verified ID?

By activating and properly deploying these built-in tools, businesses can establish enterprise-grade security without the complexity or cost of additional platforms.

And Softwerx's Zero Trust enablement with Microsoft Entra ID and Defender for Identity (hybrid) can help mid-sized businesses to do just that.

Identity management has become a top priority as we've seen a sharp rise in impersonation attacks. By adopting a Microsoft-first security strategy and partnering with Softwerx, we've been able to leverage enterprise-grade tools to protect our entire estate. This approach has allowed us to both strengthen our security posture and maximise the value of our existing Microsoft investments.

William Wilson, Head of Threat Protection & Governance, **Altum Group**

5. Data is the new frontier:

Valuable asset or dangerous liability?

Your data is your most valuable asset. But unstructured, unprotected data poses a serious risk. Without proper visibility, classification and access controls, data becomes an easy target for cybercriminals and a major compliance concern. Particularly for mid-sized businesses that may lack enterprise-grade defences.

One of the most common questions we get asked by mid-market clients when it comes to data security is – *"Where do I start?"*.

70% of medium-sized UK businesses experienced a cyber breach in the past year, compared to 50% of all companies, highlighting the increasingly targeted mid-market segment.

(Cyber security breaches survey 2024).

Most mid-sized businesses struggle to classify their data, because they don't know where it is. You need to be able to identify and document where your data sits so that it can be controlled and secured effectively.

The first step towards effective data protection is simple but critical.

Identify it, map it and then manage it.

Start with tools such as Microsoft Purview where you can gather insights that help to deduce what data you have and where it sits. Sensitivity labelling in Microsoft Purview helps you to classify sensitive data within your organisation. You can then govern what can be accessed by whom and apply labelling to identify files or emails as public, general, confidential or highly confidential. From here, data flows can be mapped out and protection settings put in place

Once the data handling processes are in place, data loss prevention can be adopted helping the organisation to secure the data, supporting growth, building confidence with customers and creating trust, which can become real market differentiators in the SMB space.

With our encyclopaedic knowledge of Microsoft Security and the current threat landscape, we help mid-market organisations to gain clarity from complexity. Simplifying security through Microsoft Purview and Softwerx data governance, we help you protect IP, meet regulatory standards and unlock business value.

The biggest area of exposure for us is our cloud infrastructure. Since our team are global and all our data is on SaaS applications, that's where our security needs to be. Not only on the cloud, but on the endpoints.

Waseem Raad, Head of Information Technology, **Lightrock**

6. Regulatory pressure is rising:

Turn compliance into competitive advantage

Regulatory compliance pressures are increasing, and it can be challenging at times to ensure they don't become merely a tick-box exercise. We try to embed those KPIs into the business and, where possible, automate many of these processes as well as using tools such as Microsoft Secure Score to streamline reporting.

William Wilson, Head of Threat Protection & Governance, **Altum Group**

Mid-market businesses face growing pressure to meet complex regulatory and compliance demands. Evolving requirements like GDPR, NIS2 and DORA coupled with stricter cyber insurance standards and the pressures that come from being part of a supply chain, mean that the cost of inaction is higher than ever.

Staying compliant demands proactive planning, specialised expertise and ongoing vigilance, yet many SMBs don't know where to begin.

The best first step? Maximise the value of the tools you already own.

According to Forrester, 70% of SMBs achieve compliance with regulations like GDPR by using Microsoft tools (Forrester, 2024).

But many mid-market businesses lack the resources or in-house expertise to fully leverage the Microsoft Security tools they already own to meet regulatory compliance requirements.

At Softwerx, we help mid-market organisations turn Microsoft Security into a true business advantage. Harnessing the full capabilities of the Microsoft Security ecosystem provides deep insight into vulnerabilities and strengthens your overall security posture. This not only improves protection against evolving threats but also simplifies the path to demonstrating compliance.

By aligning with Microsoft's baseline security recommendations through the Extended Detection and Response (XDR) platform, organisations can more easily meet regulatory standards such as Cyber Essentials and ISO 27001.

Our Microsoft-first approach bridges knowledge gaps, streamlines security operations and simplifies regulatory compliance, so you can innovate with confidence and without compromising on protection.

70%

of SMBs achieve compliance with regulations like GDPR by using Microsoft tools

(Forrester, 2024)

7. People

are your weakest link and your first line of defence

48% of SMBs have experienced an attack in the last year. It's no longer a question of whether a business will encounter threat actors, it's a question of when.

Attackers continue to exploit the simplest and most reliable entry point – people.

Social engineering and phishing remain the most common and effective tactics. Whether it's an unexpected phone call, a convincing email or a spoofed identity someone always takes the bait.

The solution? Implement strong security controls and educate your employees on how to avoid cyber threats.

I've always found that security sticks when it's simple. So, reinforcing messages to our team members is important. We drip feed security principles throughout the year rather than leaning on a security test once a year. We recognise and reward as well. So, if somebody spots a phishing email, we thank them for it. If somebody makes a mistake, we don't chastise them. We offer knowledge and guidance so that together, we can do better.

Dan Burborough, Head of IT Security,
Hollywood Bowl

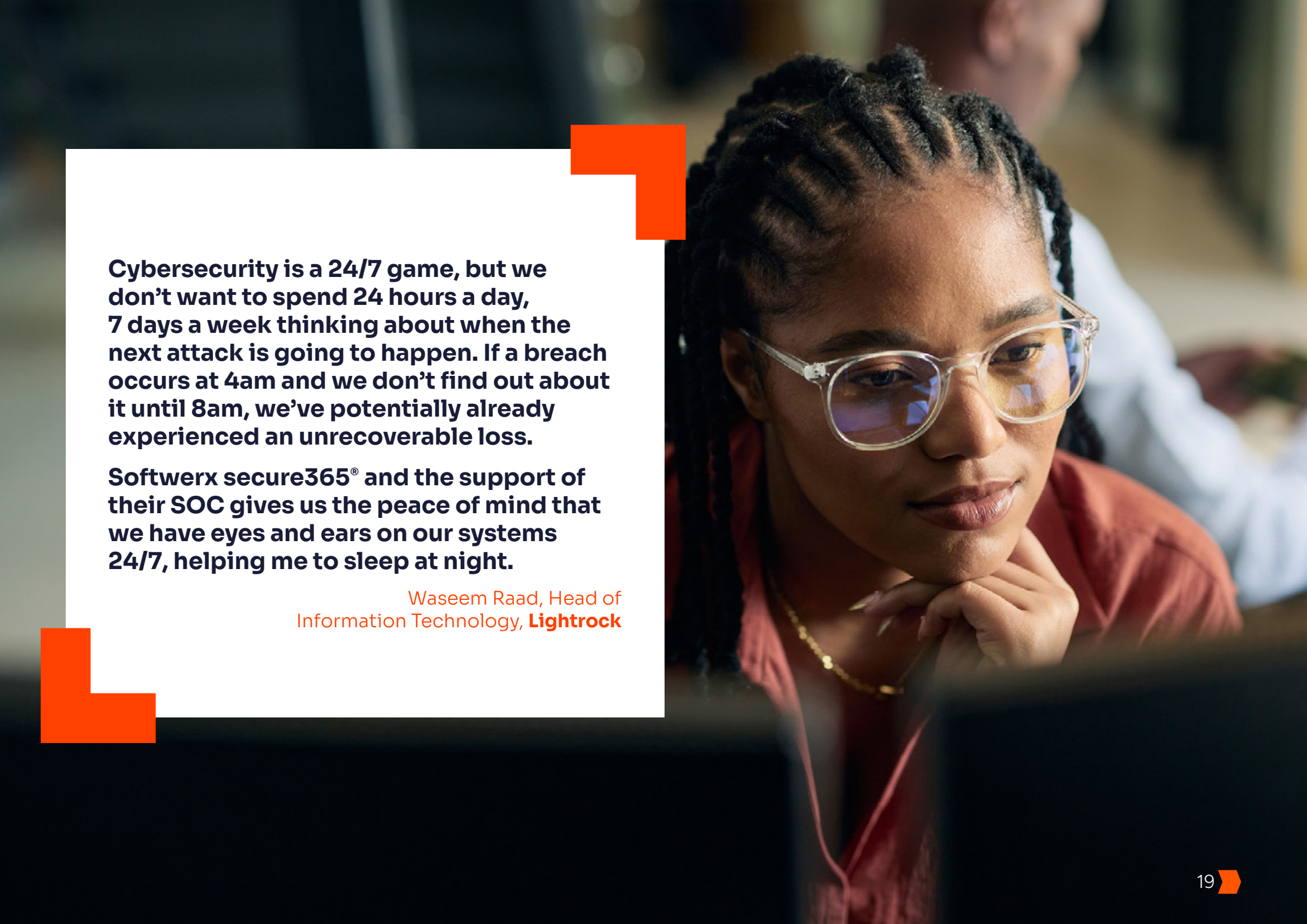
Reinforce your Zero Trust approach, operating on the assumption that every user, device or access request may already be compromised.

Ongoing employee education is essential. Regular training builds awareness, sharpens instincts and turns your workforce into a frontline defence.

At the same time, make sure you're getting the most from your Microsoft Security tools. Too many organisations underutilise the capabilities of Microsoft Defender for Office, missing out on powerful protections against phishing and impersonation. With proper configuration, Microsoft Defender for Office can significantly reduce your risk through tools like Impersonation Protection, Safe Links, Safe Attachments and Defender for Endpoint.

And remember – minutes matter, and cyber criminals don't work office hours. Consider partnering with a specialist Microsoft MSP (Managed Service Provider) to give you 24/7 Security Operations Team (SOC) support.

Our secure365® offering leverages the real-time detection and response features of Microsoft 365 Defender and the Security Information Event Management (SIEM) capability of Microsoft Sentinel to identify suspicious events which are then triaged and managed by our expert UK-based SOC. Our SOC is truly eyes-on with our analysts active 24/7 to enable rapid triage and reduced SLAs, keeping our customers secure around the clock.



Cybersecurity is a 24/7 game, but we don't want to spend 24 hours a day, 7 days a week thinking about when the next attack is going to happen. If a breach occurs at 4am and we don't find out about it until 8am, we've potentially already experienced an unrecoverable loss.

Softwerx secure365® and the support of their SOC gives us the peace of mind that we have eyes and ears on our systems 24/7, helping me to sleep at night.

Waseem Raad, Head of Information Technology, **Lightrock**

8. Detecting unseen risks:

Turning reactive threat response into proactive Managed Detection and Response (MDR) management

Building and operating an in-house SOC for a mid-sized business typically cost $1.95 million per year (Cyber Security News).

For most mid-market organisations, that level of investment simply isn't feasible. Yet the need for continuous monitoring and effective threat detection has never been greater.

So how do you stay ahead of threats when resources are limited and your security team is drowning in alerts?

In 2024, 22% of cybersecurity professionals admitted to ignoring security alerts due to alert fatigue (The Supply Chain Report). The volume and noise make it easy to miss real threats but the consequences of doing so can be severe.

A security analyst's role is to surface the unseen. To cut through the noise and transform alerts into actionable intelligence that protects both data and reputation, proactively hunting down threats, rather than waiting for the inevitable breach and then firefighting.

To do that effectively, businesses need smarter tools, leaner processes and a trusted security partner – not just more alerts.

Microsoft Defender XDR empowers proactive threat detection by consolidating signals across endpoints, identities, email, cloud apps and infrastructure, all into a unified, single-pane-of-glass view.

Paired with secure365®, you gain the capabilities of a fully operational internal security function at a fraction of the cost of building and running an in-house SOC.

We had so many tools generating alerts that we were overwhelmed, suffering from serious alert fatigue. Around 90% of the notifications were false positives, making it hard to focus on the real threats.

Partnering with Softwerx and leveraging their secure365® SOC changed everything. Their team helped us cut through the noise and zero in on the critical 10% of alerts that actually mattered. That clarity and support have been absolutely invaluable.

Waseem Raad, Head of Information Technology, **Lightrock**

9. Securing

the supply chain through
a Microsoft-first approach

We've got brand recognition and trust in Microsoft as a Gartner Magic Quadrant organisation and we have Softwerx as an extension of our internal IT team, helping us to make sense of our Microsoft Security investments and driving operational efficiency and security resilience.

William Wilson, Head of Threat Protection & Governance, **Altum Group**

Supply chains have become a critical cybersecurity focus for mid-market businesses. Interconnected vendors, partners, cloud platforms and service providers have access to sensitive systems or data, making them high-risk attack vectors. Ensuring supply chain security isn't easy and is an ever-evolving challenge but it's crucial in maintaining operational integrity and in turn, business growth.

By adopting a Microsoft-first approach, organisations can leverage Microsoft's integrated security ecosystem to protect every link in the chain – from suppliers and partners to internal operations.

By using tools like Microsoft Defender for Endpoint, Microsoft Entra for identity governance and Microsoft Purview for data protection you can gain end-to-end visibility and control over supply chain interactions. Microsoft Sentinel adds an additional layer of intelligence by correlating signals across the environment, enabling rapid detection of anomalies or breaches. This approach not only strengthens compliance and risk management but also fosters a more resilient and trusted supply chain network.

By aligning with Microsoft's best practices and security guidance you not only demonstrate to your customers that their data is protected but also gain confidence that your own organisation is safeguarded through secure interactions with suppliers and clients.

10. Security as a value driver:

From cost centre
to business enabler

Security is evolving from a cost centre into a strategic value driver. But often, security is seen as a blocker rather than a business enabler, particularly among mid-market firms, where a significant opportunity is being missed.

A lack of in-house expertise, growing complexity and mounting compliance pressures, now amplified by uncertainty around AI, leave many SMBs struggling to keep pace. However, by shifting their mindset around cybersecurity and unlocking the full potential of their existing Microsoft Security investments, these businesses can transform their posture.

The outcome is enterprise-grade protection, responsible and secure AI adoption, measurable ROI, enhanced compliance and most importantly, a stronger foundation of trust and long-term competitive advantage.

With more than 25 years of experience across Microsoft licensing, infrastructure and security, we show mid-market organisations what's already there, what's working, what's not – and what's truly possible.

By partnering with Softwerx, mid-market organisations can protect their business and innovate freely, unburdened by outdated or underutilised security constraints.

The true outcome isn't just better security. It's better business.

Your roadmap to resilience:
Take the next step with Softwerx

At Softwerx, we empower mid-market organisations to unlock the full potential of Microsoft Security.

Through expert consultancy, strategic guidance and hands-on support, we help businesses optimise their Microsoft infrastructure, security posture and licensing. Our UK-based 24/7 Security Operations Centre (SOC), alongside our flagship Managed Detection and Response (MDR) service, secure365®, leverages Microsoft 365 Defender and Microsoft Sentinel to deliver real-time threat detection, rapid incident response and intelligent security event management.

We make enterprise-grade cybersecurity both **accessible and affordable** – tailored specifically for the needs of security-conscious mid-market organisations.

Our approach guides you on a clear, tailored security journey – from initial audit to actionable outcomes – all shaped around your business's unique needs. Powered by Microsoft technologies and enriched by deep domain expertise, we take you through a structured process of discovery, assessment and expert advisory.

We transform insight into measurable impact – helping you build a resilient, future-ready security posture with confidence, clarity and the ability to protect what matters most while driving innovation forward.

Get in touch to explore how Softwerx can help secure and strengthen your business.

softwerx
The Microsoft Security Specialists

Merlin Suite, Middle Court, Copley Hill Business Park, Babraham, Cambridge, CB22 3GN Cambridgeshire

www.softwerx.com
+44 (0) 1223 834 333
info@softwerx.com