softwerx
The Microsoft Cloud Security Specialists

Secure365
24x7 Managed Security

Future-proof your Security with Microsoft

A Business Insight for Security Visionaries

Introduction: Why security won't accept second place for your business

Your core business is not security. Your core business is providing a first-class experience for your customers or beneficiaries. Your focus is to deliver excellence in your products and services. You have a multitude of demanding priorities, limited resources and tight deadlines.

With all of these priorities on your plate, security might seem like something that can wait. The reality is that security cannot wait. **Security is quite likely the single biggest risk to your business.**

The UK government recently reported that 39% of businesses identified a cyber-attack in the previous 12 months and 82% of senior executives now rate a cyber-attack as a 'very high' threat to the business.[1]

The most effective approach to protect a business is using a dedicated Security Operations Centre (SOC). Until now, having a SOC has largely been the privilege of enterprise-sized organisations. A SOC centralises technology and skilled resources to continuously monitor and improve your security posture. It works by detecting, analysing, responding to and preventing cyber threats.

Disruption in the security sector is here. In the last 18 months, Microsoft has changed the security landscape. Mid-market organisations can now access affordable 'enterprise-grade' security thanks to Microsoft's advanced security stack.

[1] UK Government Cyber Security Breaches Survey 2022

The security challenge for mid-market firms

Mid-market firms may think that cyber criminals are targeting large companies to make more money, but a recent report published by the National Cyber Security Centre reveals that criminals are no longer focussing on 'big game hunting'. **Mid-market businesses are now the main target of ransomware attacks.** Threat actors also want to avoid public scrutiny from going after well-known brands.

Cyber-attacks are also becoming more sophisticated. For example, Softwerx has recently seen attacks that seem to originate from Germany and Amsterdam. In reality, these attacks are routed via VPNs to appear legitimate and bypass conditional access protocols. Some criminals go to great lengths through impersonation attacks, often scraping social media websites and forging bank mandates.

Cyber criminals do not work 'office hours'. Our own Softwerx analysts report that most ransomware attacks in the UK occur between midnight and 3am GMT. If you are not monitoring your systems on a 24x7 basis, you run the risk of being welcomed with a ransomware note on your screen and your data being encrypted.

The time to detect and remediate a cyber attack for a security team is a critical metric. **A quick response can be the difference between an effectively mitigated attack or a catastrophic business disaster.**

76%

Of ransomware infections happen outside of business hours[1]

46%

Cite competition for cyber security talent as their biggest security challenge[2]

65%

Of medium-sized businesses had experienced a cyber attack in the last 12 months[3]

[1] They Come in the Night: Ransomware Deployment

[2] UK Cyber Security Sectoral Analysis 2022

[3] Cyber Security Breaches Survey 2021, UK Government

Overcoming the security challenges with a Microsoft First approach

Security specialists and Senior Executives within mid-market firms are under extraordinary pressure to perform. Performance in this context means protecting the business, as well as growing it. **The challenge is significant.**

Overcoming this challenge is not limited to an increased frequency and sophistication of cyber-threats, more so, it's as much about trying to **'see the wood from the trees'.**

In an overcrowded and complex supplier marketplace, where 'product bloat' is rife, building an integrated and robust security posture that actually works (and doesn't cost the earth to support) is not for the faint-hearted.

Microsoft First
For Security & Compliance

There is a different way. In the past eighteen months, **Microsoft has transformed the cybersecurity marketplace for mid-market firms**, making enterprise-grade security accessible, affordable, and refreshingly simplistic.

A Microsoft First approach for security and compliance is critically about better understanding what you already have in place with Microsoft – and what you're already likely paying for. A Microsoft First approach to security is about leveraging your existing investment.

Never heard of Microsoft Security? Read on.

In this playbook, we introduce four key areas for consideration. You will discover how you can now afford to put security first, and still concentrate on your core business.

Explore the art of what is now possible with Microsoft

Microsoft is quite likely the largest security vendor that you have never heard of – or at least thought of – until now.

Through world-leading investment in research and technology, **Microsoft has quietly moved the security dial for mid-market firms** – and from a unique perspective – now offers a compelling proposition for those organisations craving for a more simplified, cost-effective, and robust approach to building an effective security posture.

A security road-map with Microsoft is a **futureproof road-map.**

- Microsoft is investing $20BN in security over the next five years
- Microsoft tracks over 1TN signals per day
- Microsoft blocks 16 million threats a day
- Microsoft now leads in five different Gartner Magic Quadrants for security
- Only Microsoft can offer a uniquely native end-user experience

> We found that with a 'Microsoft First' approach, we could seamlessly get stronger, streamlined security by just upgrading our licences to the E5 SKU. This meant that we did not have to scope other products or run training and monitoring across multiple security vendors.
>
> **– Colin Manson, Cyber Security Associate, Factor**

Discover why a modern approach to security makes sense

Most mid-market organisations have an eclectic security posture, built over many years of adding different products, technology, and resources. For many organisations, the net result is a security posture that doesn't quite fit together, or that has holes; and that is often expensive to manage and maintain.

A modern approach to security means the consolidation and organisation of purposeful technology and qualified resources into one place – a Security Operations Centre (SOC).

To date, the only option for security conscious firms has been to try and build their own SOC. To do this properly **costs millions and takes years**, which is why an in-house SOC has largely been the cartel and privilege of much larger organisations such as national banks and high profile FTSE500 firms.

There is a different way. By utilising Microsoft technology (which you already own) and working with expert niche security partners (like Softwerx), mid-market firms can now also get peace of mind on a 24x7 basis, albeit – for a fraction of the cost.

Cybersecurity is a 24x7 problem.
Most attacks in the UK occur between midnight and 3am (GMT).
Organisations with a SOC (Security Operations Centre) are generally able to prevent more successful attacks in and out of hours, and they also have faster reaction times to data breaches. According to a recent report, organisations with a SOC/high security recovered within seven days.[1] But those with no SOC and/or low security took more than 90 days to recover. In your industry, where time is money, it makes sense to consider a SOC approach.

IT Security is not IT Support.
Many mid-market businesses will likely already have some level of internal IT Support – and the question is often asked: 'Shouldn't our own people already be doing that?' Apart from the fact that the in-house team is probably only working normal office hours, senior management should understand that IT Security is not IT Support. They are related in that both are concerned with technology, but an IT Security Analyst has different training and skills to an IT Support Engineer.

[1] Varonis Data Breach Response Times

Minutes matter

Within the context of building a robust security posture minutes really matter – and quite simply can be the difference in successfully identifying and mitigating a breach, versus an attack becoming successful and causing catastrophic damage.

MTTD (Mean Time to Detect) is the average time it takes to detect an incident. MTTR (Mean Time to Respond) measures the average time it takes to control and mediate a threat. Both are critical performance metrics for professional MDR (Managed Detection and Response) services, such as **Microsoft secure365** from Softwerx.

Incident timeline

“

With a Microsoft First approach and **secure365** from Softwerx, we can find our information quickly. We do this by leveraging a simplified information architecture, which saves us around £500,000 a year. We have also saved around £30,000 in equipment so far by adopting cloud first. We’re now looking forward to future benefits such as BI and analytics.

– Chris Holden,
Head of Information Services,
Kidney Research UK

Explore the commercial case for change

1

Microsoft First. The cybersecurity marketplace is overcrowded, complex and expensive. Taking a 'Microsoft First' approach makes business sense. Mid-market organisations have typically built (or grown) an eclectic mix of 'next-best' products or solutions. These may not be the best for very long, often work largely in isolation, and are difficult and costly to maintain.

Adopting a 'Microsoft First' approach to security is all about two things. Firstly, it is about future-proofing your organisation with the best, most advanced security technology from Microsoft which is investing $20bn. Secondly, it is about consolidating disjointed solutions to reduce costs.

Robust security is about the best technology, combined with the best security analysts. With Microsoft and Softwerx, your organisation can achieve both, and often realise significant savings.

2

Retire redundant third-party security solutions. You can also save by eliminating third-party software that you no longer need. You can do this by simply augmenting your current Microsoft subscription, or just turning it on. Softwerx typically sees organisations achieve savings in the order of 28% through the retirement of unnecessary Endpoint, Secure Email Gateway and other Breach Detection solutions.

3

Scarce resources. It's hardly a secret that skilled cybersecurity resources are scarce, with more positions available than candidates. Building even a small 24x7 SOC will need a minimum team of 12, and then you need to keep them trained, incentivised, and motivated. If you accept that an organised and specialist approach to mitigating any security threat (a 24x7 SOC) make sense, then what also makes (commercial) sense is to seek help outside of the business.

4

The bottom line. A security breach is likely the single biggest risk to your business. A successful breach can cost millions and cause irrevocable reputational damage. Mid-market firms are arguably at a greater risk than larger firms. Unlimited spending on the 'next-best' security solution is not an option, nor is building a (multi-million) pound in-house SOC. There is a different way – a professional 24x7 SOC-as-Service solution from Softwerx starts at just £10 per user per month.

Learn why better never stops

Security is a process, not an event. Hackers continually reinvent themselves and a good security posture needs to be as dynamic as it is robust.

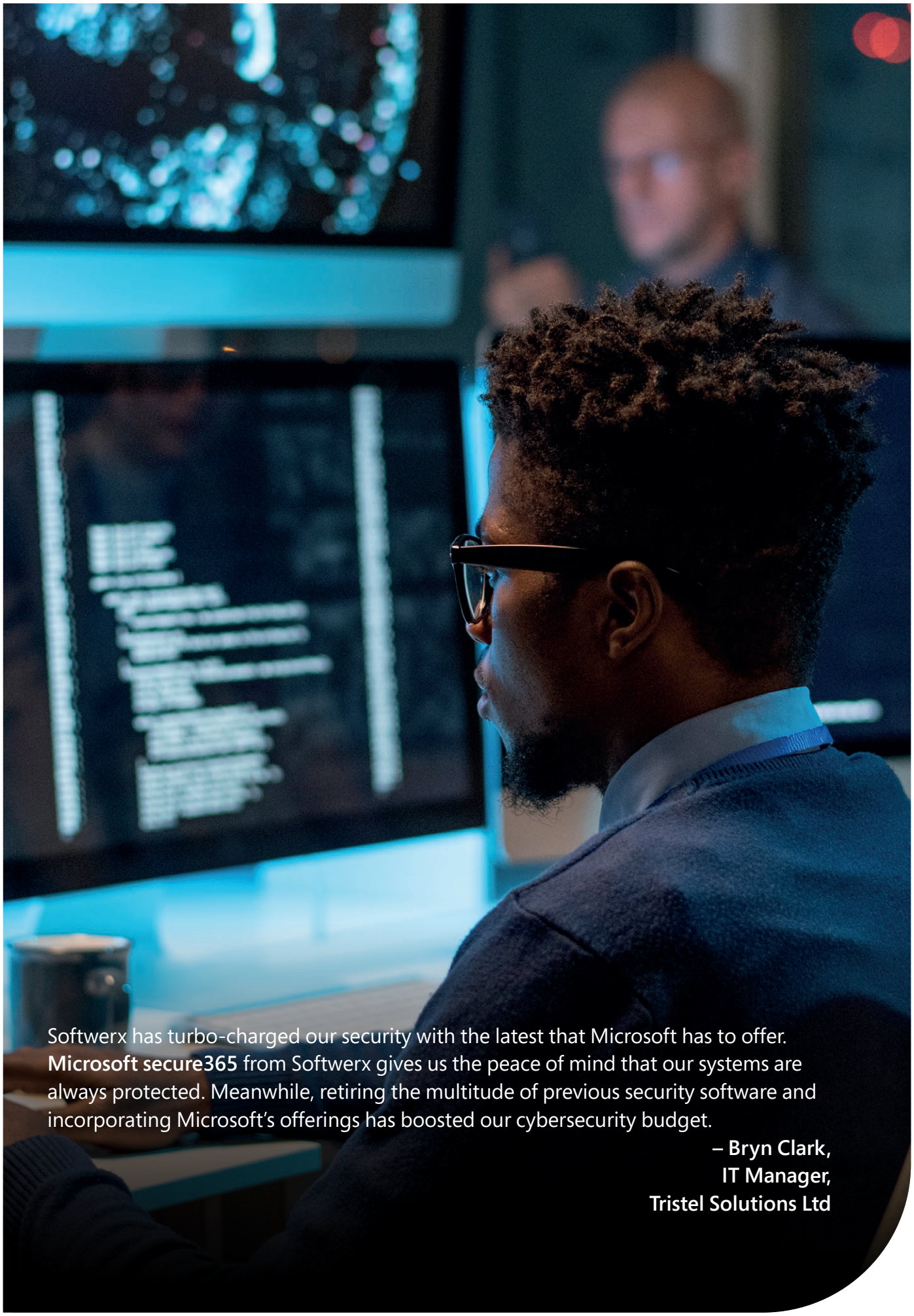
Your trust in Softwerx doesn't end with a 24x7 'eyes-on' managed security service that works on a real-time basis to mitigate serious attacks that otherwise may paralyse your business. More so, your commitment from Softwerx includes a forward-looking approach that includes the examination and improvement of your security posture on an ongoing basis.

Microsoft provides an objective benchmark called Microsoft Secure Score to understand your current security posture and offers clear recommendations for tangible improvement. With the help of qualified security specialists, your score and posture can be interpreted, actioned and improved upon.

In an industry engulfed in complexity and subjective product claims, **Microsoft Secure Score cuts through the noise**. It is a comprehensive metric that all executives can understand, manage, and measure.

"In the past year, we've leant on Softwerx's expertise to achieve a 40%+ increase in our Microsoft Secure Score posture. In fact, Secure Score and Azure Advisor now form part of our core Board metrics.

– Peter Messervy-Gross, CIO, Altum Group



Softwerx has turbo-charged our security with the latest that Microsoft has to offer. **Microsoft secure365** from Softwerx gives us the peace of mind that our systems are always protected. Meanwhile, retiring the multitude of previous security software and incorporating Microsoft's offerings has boosted our cybersecurity budget.

– Bryn Clark,
IT Manager,
Tristel Solutions Ltd

About Softwerx

With over twenty years' experience and a dedicated 24x7 Microsoft Security Operations Centre (SOC), Softwerx is one of the UK's leading Microsoft Cloud Security specialists. Softwerx is trusted by over three hundred eclectic organisations and was one of the first Microsoft Partners in the UK to be awarded the specialist Microsoft Security Solutions Partner Competency.

Microsoft Solutions Partner

Security

ISO 9001 : 2015 REGISTERED

ISO 14001 : 2015 REGISTERED

ISO 27001 : 2018 REGISTERED

ISO 45001 : 2018 REGISTERED

CYBER ESSENTIALS PLUS

INVESTORS IN PEOPLE™

HM Government G-Cloud Supplier

CIF CERTIFIED

About the Authors

Principal researcher

Faith Akinbo is a Microsoft Research Analyst with a focus on cybersecurity strategy for nonprofits. She was awarded the 2022 Apprentice of the Year Award by Cambridgeshire County Council.

Assistant researcher

Paul Njenje is a Microsoft Research Analyst with a focus on cyber resilience for the Private Equity and Venture Capital sector. Paul built his own computer from scratch and enjoys getting his teeth into anything technical.

info@softwerx.com 01223 834 333 www.softwerx.com

Cambridge Copley Hill Business Park, Babraham, Cambridge CB22 3GN
London 26 Finsbury Square, London EC2A 1DS

#secure365 #MicrosoftFirst

About Microsoft secure365

Microsoft secure365 is the brand name of the Softwerx SOC-as-a-Service offering, built on the Microsoft Defender and Microsoft Sentinel suite. **Microsoft secure365** constitutes the best in Microsoft technology (which you already own and retain), combined with our expertly qualified 'eyes-on' specialist SecOps Team, working around the clock (365 days a year) to keep you safe.

Microsoft secure365 is effectively **complete peace of mind for mid-market organisations**, starting from just £10 per user, per month.

Eyes-on

Rapid response

Guaranteed service levels

Microsoft technology

Book a demo

secure365
24x7 Managed Security

Discover how **Microsoft secure365** can help your organisation by providing around-the-clock peace of mind.

To learn more, book a personal demo today by scanning the QR code, by calling us on 01223 834 333, or by using this link:

www.softwerx.com/secure365-demo