secure365®

24x7 Microsoft Managed Detection and Response Security Solution

softwerx
The Microsoft Security Specialists

Our Business.
100% Microsoft Security.

Your Business.
Safe.

secure365 is a comprehensive 'eyes-on' 24x7 Managed Detection and Response (MDR) Solution, designed and built on the future-proof Microsoft Security technology stack.

secure365 leverages the real-time detection and response features of Microsoft 365 Defender and the security information event management (SIEM) capability of Microsoft Sentinel. Identified suspicious events are then triaged and managed by our expert (UK-based) Security Operations Team.

"My original vision for **secure365** was to make enterprise-grade security accessible and affordable for the Midmarket. I also wanted to ensure that key elements of the solution, such as full control, transparency and interoperability were all included at a design level.

Matt Smith
Microsoft Services Director
Softwerx

The Security Challenge for the Midmarket

- Budget Limitation
- Complex Support
- 24x7x365 Threats
- Task Saturation
- Increasing Threats
- Increasing Regulations
- Crowded Marketplace
- Uninsurable Risk

Understanding Microsoft Security

Microsoft has changed the security landscape. Microsoft's enterprise-grade security solutions are now accessible and affordable for the Midmarket, bundled within Microsoft Business Premium, and Microsoft's 365 E5 and Microsoft E5 Security licences.

Microsoft offers comprehensive security covering extended detection and response (XDR), security information and event management (SIEM), threat intelligence, identity and access management (IAM), endpoint management, cloud security, and data protection and compliance.

Microsoft is now investing more in security than any other security vendor. Only Microsoft offers a truly integrated, end-to-end comprehensive solution that natively connects the systems you have.

Microsoft is, quite possibly, the largest security solutions provider you have ever heard of, or least considered, until now.

65 trillion signals analysed daily by Microsoft to better protect against cybercrime

135 million managed devices providing security and threat landscape insights

4,000 identity attacks blocked per second

300+ threat actors tracked

* https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

#SimplifySecurity

Why Adopt a 'Microsoft First' Approach?

A 'Microsoft First' approach to security and compliance simply means better understanding, and better leveraging, your existing Microsoft investment. Before you bolt on even more security products, stop and consider building on what you already have.

1. Microsoft is now a leading and credible security vendor, leading in five Gartner Magic Security Quadrants.

2. A decision to consider Microsoft for security is a future-proof decision.

3. You already likely own and are paying for security features that are simply not configured.

4. Quickly and cost effectively augment your subscription to add advanced security features.

5. Gain a net commercial benefit by retiring unnecessary third-party solutions.

6. Your users and support teams will thank you for not having to learn yet another product.

Winning with a Microsoft First Approach

Peter Messervy-Gross
Chief Information Officer
Altum Group

Altum Group, an international financial services firm, was a finalist of the 2022 Microsoft First Awards for Security and Compliance hosted by Softwerx. Altum pioneered a streamlined security posture using the latest Microsoft technology. As the champion of this approach, Peter Messervy-Gross was endorsed as a 'Security Visionary' by Microsoft.

Peter explains how the company gained the accolade by saying, "Softwerx supported our 'Microsoft First' journey by helping us to align our commercial strategy with Microsoft's technology stack. Thanks to this, we've streamlined security, reduced vendor overlap and realised concrete security gains including a 40%+ increase in our Microsoft Secure Score."

#MicrosoftFirst

A Security Operations Centre (SOC): Build or Buy?

Most Midmarket 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 dislocated security posture that is a risk in itself and, typically, expensive to support.

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. Doing this properly costs millions and takes years, which is why an in-house SOC has, largely, been the privilege of much larger organisations, such as national banks and high-profile FTSE500 firms.

There is another way. We have built a dedicated 24x7 'eyes-on' Microsoft Security Operations Centre for the Midmarket – so that you don't have to.

Cybersecurity is a 24x7 problem.
Statistics from our own SOC clearly indicate that most serious cyberattacks occur outside of normal office hours. Criminals operate on a 24x7 basis, so you should to. In the initial detection and response of a breach, minutes really do matter. According to a report by Varonis, organisations with a SOC and a focus on security recovered within seven days, but those without a SOC, or a poor security posture, took more than 90 days to recover.*

Building a SOC takes years and costs millions.
We know because we've done it. You don't have to though. With Softwerx and secure365 you can achieve a total peace of mind for just a fraction of the cost, also allowing your organisation to focus on its core business.

* https://www.varonis.com/blog/data-breach-response-times

#MinutesMatter

Discover **secure365**

Too many Managed Detection and Response (MDR) solutions are aimed at enterprise-sized organisations, requiring enterprise-sized budgets. Typically, these solutions are based upon a proprietary platform and are, normally, hosted supplier-side, meaning control is always and, ultimately, with the vendor. Anything 'outside of the box' normally attracts an additional fee, and in an overcrowded marketplace in which acquisitions can seemingly occur overnight, you can't be sure who you will be dealing with in the morning.

secure365 is Different by Design

1

Secure
Underpinned by industry-accepted Zero Trust principles, **secure365** is based around a fundamental principle of not, unnecessarily, moving data between environments. **secure365** interrogates data only within one secure environment – your environment. No data is ever taken from your Microsoft portal and our SecOps Team can only access your environment through a zero-trust validated process, including MFA as a minimum.

2

Transparent
Most MDR offerings are based on a proprietary vendor portal, which imports, interrogates and manipulates threats (and your data) behind closed doors. As we only access your environment, you have complete visibility of our analysts' and engineers' actions. We believe that absolute transparency is a fundamental principle of a trusted security solution. Transparency is essential to ensure a collaborative approach with your IT, security and compliance teams.

3

Full Control
It's yours. Every action that we take, every incident that we investigate, all logs that we create, all bespoke analytics rules that we build, all custom watchlists that we configure – quite literally everything that we do, is yours – forever. We tailor everything to your organisation and build it into your Microsoft and Azure environments to ensure you own everything and retain full control. Unlike other MDR offerings and vendors, you are never locked-in with **secure365**.

4 Non Proprietary

A principle design feature of **secure365** is one of interoperability. By this, we mean **secure365** will work with almost any device, entity or user that generates a signal. We have already built hundreds of custom connectors to work with all types of devices, applications and technology. Microsoft's forward-thinking open technology policy ensures that this principle is future-proof.

5 Affordable

secure365 is an MDR solution engineered for the Midmarket. In this respect, cost of ownership is a critical principle. It's great to build the most comprehensive, flexible, scalable and effective MDR solution in the market, but not if its unaffordable. With secure365, a 300-seat organisation can achieve total peace of mind on a 24x7 basis for about the same cost as employing just one junior Security Analyst.

6 Future-proof

In a complicated and fast-moving marketplace, in which many security vendors are working toward an exit or acquisition, Softwerx wanted a technology partner that it could trust for the long term. With a committed security investment of $20BN over the next five years, and now leading in the Gartner Magic Quadrant for Security Information and Event Management (SIEM) Solutions*, Microsoft could be the most significant security provider you've yet to consider.

* https://www.gartner.com/doc/reprints?id=1-2FFCXFP9&ct=231025&st=sb

Keeping You Safe

Core to **secure365** is the fast detection and response to events on a 24x7 basis. Literally millions of security events occur in your IT environment every day, which is why we combined Microsoft's technology with our expert team to triage and respond to these events before they become a serious incident.

secure365 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 and alert our security operations team.

The security operations team investigate every suspicious event using our proven methodology and continuously feed their discoveries back into the service in the form of enhanced analytics rules and threat intelligence data.

We select real-time detection technologies that fit your environment (Defender for Endpoint, Defender for Office 365, Defender for Cloud Apps and Defender for Cloud) and connect all your other security systems, such as firewalls, web security gateways and network access controllers to Microsoft Sentinel.

Analytics combined with Threat Intelligence feeds in Microsoft Sentinel scour this central repository of security events to identify threats and weaknesses across your entire IT estate.

If, and when, an event becomes a serious incident we alert you promptly, and if necessary, full Disaster Recovery* can be invoked.

For a more detailed solution description, please see our **secure365** Solutions Document.

Our Service Promise

Severity Level	Response Time
High	15 minutes
Medium	4 hours
Low	12 hours
Informational	24 hours

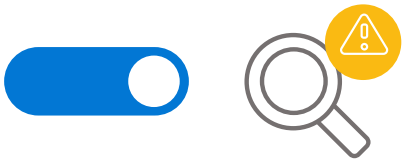
Severity Levels applied by Analytics Rules

** Disaster Recovery sold separately*

Under the Bonnet

Here's a glimpse into how we have designed and built the underlying **secure365** technology to keep you safe. For more information, please ask to see our **secure365** Technical Data Sheet, or just speak to our Technical Team.

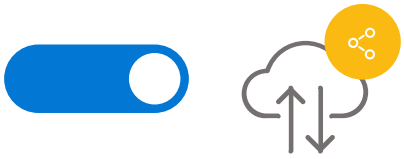
Analytics rules for understanding threats and triaging alerts automatically with AI



Threat hunting for pinpointing risks and anomalous behaviours

Threat intelligence enhanced 'hive mind' by Microsoft's global threat lists

Bespoke log collection feeds are built and maintained to ensure enriched and relevant data



SOAR orchestration (Security Operations Automation and Response) streamlines and automates tasks with custom workflows.

Automated ticketing critical for case management and seamless event coordination.

Live dashboards allow you to view the precise status of your environment 24x7

Watchlist maintenance to identify your most critical assets, systems and VIP users

Your Specialist Security Operations Team

Automated triage and response technologies offer significant efficiencies in handling the thousands of security events that occur in your IT environment every hour. However, human threat-hunting skills and qualified investigation techniques are still essential in that final analysis stage of a suspected incident.

Consider our specialist security operations team to be *your* specialist security operations team – and, rest assured, we are watching your systems on a 24x7 basis.

- UK-Based
- Microsoft Accredited
- Highly Experienced
- Highly Qualified
- Security Cleared
- 24x7 Eyes-On

A Night in the Life of a Microsoft Security Analyst

Name: Helio Tareco
Role: Security Analyst
Typical Shift: 8 hours
Hobbies: Bass guitar and travel

"As a SOC Analyst, I need to be able to quickly figure out if an alert or action is the result of a potential attack, a normal business process, a mistake, or a harmless anomaly, because time counts. Working with Microsoft's deeply integrated tools, such as Defender and Sentinel, makes this so much easier thanks to their built-in AI-driven threat correlation rules and out-of-the-box automations. Other than that, I protect end-users against themselves, since they can be the greatest risk to their organisation!

7:45 pm	Make a large cup of coffee!
8:00 pm	Log into portals, get briefed on current status by outgoing analysts
8:38 pm	High-level alert flagged – start investigation
8:45 pm	Triage alert as a false positive
9:14 pm	Review bespoke customer threat alert rules
12:39 pm	Update system logs
1:52 am	Review global attack vectors from Microsoft's Threat Intelligence Centre
2:21 am	Investigate new medium alert
3:03 am	Identify source as malicious and notify customer
3:03 am	Quarantine device and remediate
4:09am	Update logs, hand over to relieving analysts and sign out

#SecurityNeverSleeps

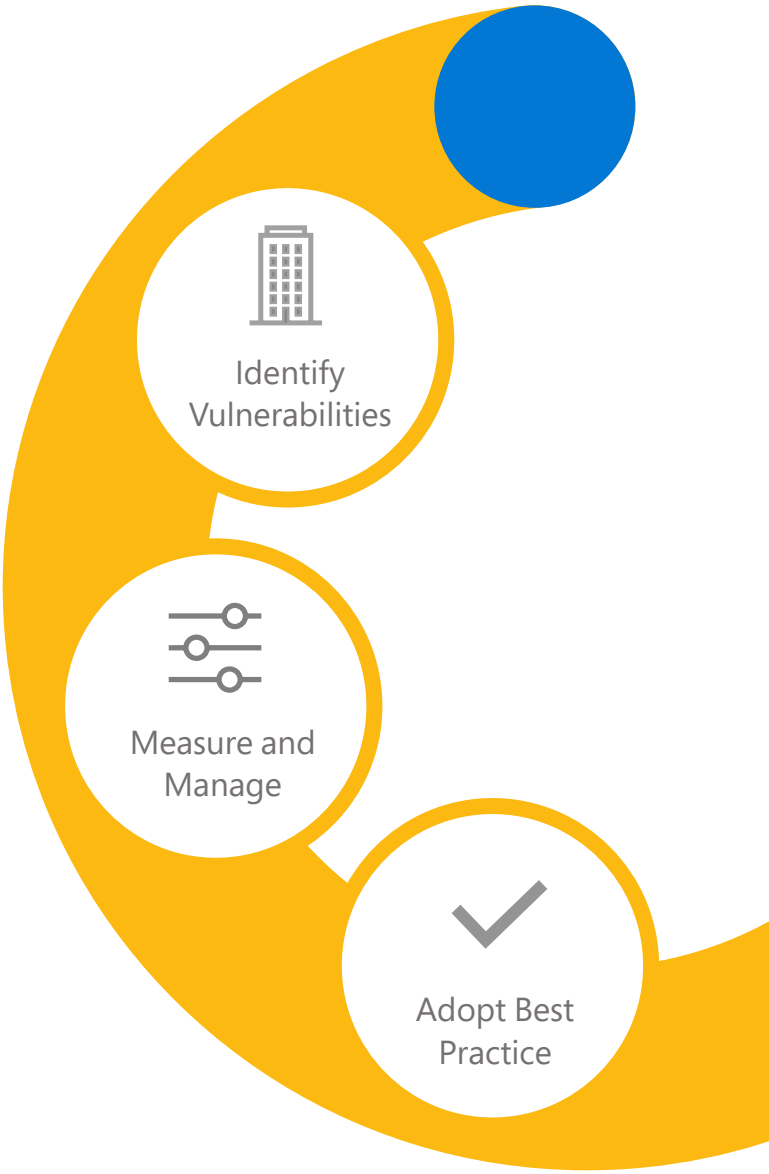
Better Never Stops

Security is a process, not an event. Continual improvement is critical. As part of your **secure365** solution with Softwerx, we constantly monitor and review your systems for both vulnerabilities and improvements.

Through regular Security Solution Reviews, we highlight weaknesses and suggest improvements to maintain a strong security posture.

We leverage Microsoft Secure Score as a measure. Microsoft Secure Score is a widely accepted, comprehensive and objective gauge that can be used by technical teams, but also understood at a headline level by the Board.

Your improving Microsoft Secure Score can be shared externally with customers, suppliers, and any regulatory bodies. You can also benchmark your progress and achievements against your peers.



Devices are managed centrally and are protected by a 24x7 Security Operations Centre from Softwerx called secure365. With that, we have MFA and real-time detection in place. As a result, our Microsoft Secure Score is currently well above the industry average, and it continues to climb.

Head of Information Services, Leading Charity

Security Bundles

Bundles

Essential	Standard	Advanced	Sentinel
For smaller organisations seeking a first step into next-generation security	Best Bundle for sub-300 user organisations with the Business Premium licence	Best Bundle for plus-300 user organisations with the full M365 E5 Security licence	Included in all solutions except Essential
• Defender for Endpoint • Defender for Office 365	• Defender for Endpoint • Defender for Office 365 • Microsoft Intune • Microsoft Purview Information Protection	• Defender for Endpoint • Defender for Office 365 • Defender for Identity • Microsoft Intune • Microsoft Purview Information Protection • Defender for Cloud Apps	• Defender for Cloud • Uses Microsoft Sentinel • Sign-in logs • Threat Intelligence • Windows Security • Azure activity • Optional Feeds • Playbooks

Getting Started

Getting started couldn't be easier. Simply click on the link below to book a demo, or call us directly on 01223 843 333 to understand more.

In a rush? Depending on your current Microsoft licence subscription and configuration, we can typically get you up and running – and protected – in a matter of weeks.

Book a Demo

Book a 45-minute demo to understand how you can transform your organisation's security with Microsoft and **secure365**.

To book a personal demo today, scan the QR code, call us on 01223 834 333, or use the link below:

softwerx.com/secure365-demo/

A Matter of Trust

Our business is 100% Microsoft security – and has been for more than twenty years. We've grown up with Microsoft, we've shared the journey with them and we've specifically shaped our business and expert SecOps Team around the Microsoft Security stack. Our 24x7 Cambridge-based 'eyes-on' dedicated Microsoft Security Operations Centre is trusted by some of the best known names in the UK.

Kidney Research

hollywood bowl

Tristel™

FinTrU

ALTUM

RRG GROUP

About Softwerx

Softwerx is one of the UK's leading Microsoft Cloud Security Specialists and one of the first Microsoft Partners in the UK to be awarded the Microsoft Security Solutions Partner Designation. Softwerx runs 24x7 a Microsoft Security Operations Centre (SOC) based in Cambridge.

Microsoft Solutions Partner
Security
Specialist
Threat Protection

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Infrastructure
Azure

CYBER ESSENTIALS PLUS

CIF CERTIFIED

INVESTORS IN PEOPLE™

QMS ISO 9001 : 2015 REGISTERED

QMS ISO 14001 : 2015 REGISTERED

QMS ISO 27001 : 2018 REGISTERED

QMS ISO 45001 : 2018 REGISTERED

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

Cambridge Copley Hill Business Park, Babraham, Cambridge CB22 3GN

softwerx

The Microsoft Security Specialists