



24x7x365 Managed eXtended Detection and Response for the Midmarket

secure365[®] from Softwerx is a comprehensive 'eyes-on' 24x7x365 Managed eXtended Detection and Response (MXDR) service solution, designed and built from the ground up on the future-proof, industry-leading Microsoft Security[®] technology stack.

secure365 uses the real-time detection and response functionality of Microsoft 365 Defender[®] and the security information event management (SIEM) capabilities of Microsoft Sentinel[®] as its foundation. Any suspicious events identified are then triaged and managed by our expert UK-based 24x7x365 Security Operations Centre (SOC).

But why a focus on the midmarket?

In the past, mid-sized organisations tended to be overlooked by cybercriminals in favour of targeting large enterprises. However, it's clear that things are changing rapidly. Mid-market organisations now form the majority of the critical supply chains of much larger businesses, hold huge quantities of valuable data, and operate with enough complexity to be enticing targets for cybercriminals – but often lack the skills, resources and dedicated security teams of their larger peers to combat the emerging threat.

According to the UK Government Cyber Security Breaches Survey 2025, 70% of medium-sized UK businesses experienced a cyber breach in the previous year, much higher than the 50% average across all companies.

And the risk landscape is only getting even more challenging, with AI-driven threats, mounting regulatory demands and hybrid IT-sprawl all contributing to the creation of an environment in which most businesses struggle to keep up – not only with cyber threats but also with the increasing complexity of their own defences.

Make use of what you're already paying for

Ironically, with the majority of SMBs basing their IT infrastructure on Microsoft technology such as Azure[®] and Microsoft 365[®], the cybersecurity toolsets they need are often already in their hands, part of the bundles they already use (Forrester data shows that 60% of businesses aren't using the security features included in the Microsoft licenses they paying for). Microsoft Security is enterprise-grade, offers the potential to go beyond merely reactive cyber defence, and often just needs to be turned on and configured.

For most midmarket organisations, exploiting transformational security like this represents a powerful business opportunity.

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

Matt Smith
CTO, Softwerx

That's where Softwerx and secure365 come in

With over twenty-five years of specialist expertise in Microsoft Security, **Softwerx** helps midmarket scale organisations rethink their approach – transforming existing cybersecurity investments into secure, scalable, AI-ready infrastructure.

By adopting **Softwerx secure365** as their MXDR solution, organisations can leverage the future-proofed, industry-leading Microsoft Security portfolio that they're already paying for, combined with a world-class, 24x7x365 'eyes-on' Security Operations Centre (SOC), staffed by seasoned cybersecurity experts. Building an effective in-house SOC can take years and cost millions – **we've already done it so you don't have to.**

Softwerx secure365[®] is a Managed XDR service that works with Microsoft Sentinel[®], Defender[®] and other Microsoft Security[®] tools to provide midmarket organizations with a managed 24x7x365 security solution that offers enterprise-grade protection at an affordable price.



Solution Overview

secure365 is a Managed eXtended Detection and Response (MXDR) solution using Microsoft Defender, Microsoft Sentinel and other tools to provide robust Security Information and Event Management (SIEM) as a managed service.

The **secure365** solution includes the deployment, customisation and optimisation of Microsoft Sentinel in the customer's infrastructure, along with Security Orchestration and Automated Response (SOAR), specifically tailored to the detailed needs of the organisation.

The Softwerx UK-based Security Operations Centre (SOC) team provides a 24x7x365 MXDR service, overseeing detection, investigation, and response to incidents flagged in Sentinel.

The onboarding process for customers adopting the **secure365** service is simple and assured, enabling customers to get up and running quickly by leveraging existing Sentinel, Defender and other implementations/licenses, and Softwerx will provide advice, guidance and deployment via its professional services team.

Key Benefits of secure365

- ▶ **Confidence** through financially-backed, guaranteed SLA's delivered by the Softwerx UK-based SOC.
- ▶ **Peace of mind** as no data ever leaves the customer's Microsoft environment and the Softwerx team can only gain access via a Zero Trust validated process, including multi-factor authentication as a minimum.
- ▶ All customisations, rules and SOAR processes **remain the customer's property**, and operational, even after the service ends.
- ▶ **Secure compliance and collaboration** with the customer's team takes place via Microsoft Teams, ensuring all governance requirements are adhered to.
- ▶ **Full-service transparency**, including tailored dashboards providing the customer with all information needed to help mitigate risks, enhance security posture and give full visibility of any actions taken by the Softwerx SOC.
- ▶ **Efficiencies** through automation and proactive threat hunting.
- ▶ **Triage and guidance** on mitigation of vulnerabilities in the customer's environment and its configuration.
- ▶ **Continuous security posture improvement** through regular review meetings with Softwerx consultants.
- ▶ **Cost control** through optimisation of Sentinel logs.

For more information, and to discuss your specific requirements, please contact us at: info@softwerx.com

The Softwerx SOC

Automated triage and response technologies including machine-learning and AI deliver big efficiencies in handling thousands of security events that occur in IT environments every hour. However, human threat-hunting skills and qualified investigation techniques are still essential in the final analysis stage of any suspected incident.

The Softwerx specialist Security Operations team behaves as if it were the customer's SOC and monitors their systems on a continuous 24x7x365 basis.



UK-based



Microsoft accredited



Highly qualified



Highly experienced



Security cleared



24x7x365 eyes-on

secure365 from Softwerx is ideal for midmarket organisations looking to enhance their security posture with advanced threat detection and response capabilities.

Irrespective of the type of customer, the Softwerx SOC team ensures that the organization remains secure 24x7x365