



SAPPHIRE™

Unlock the Power of your Security Budget with Sapphire's XDR for Microsoft

Sapphire's XDR service for Microsoft integrates into your business to develop enhanced visibility, rapidly identifying and shutting down cyber threats.

Sapphire's Managed mXDR (Microsoft Extended Detection and Response) is a holistic approach to cybersecurity that takes full advantage of your Microsoft security subscriptions to provide comprehensive cyber defence for your business.

Our analysts leverage world class threat intelligence, dedicated advanced analytics, AI, and custom automation to deliver defences aligned specifically to your business needs.

Our service provides proactive threat detection, investigation, and response across endpoints, identities, applications, and cloud services. When an incident occurs, we act fast, with active responses that are configurable by your business. Our SLA for the highest risks is less than 15 minutes, giving you confidence, we will be there when you need us most.

Benefits of Sapphire's Managed Microsoft XDR Solution

We are Always There:

We protect you 24x7x365, monitoring, detecting, analysing and responding throughout your business. We provide direct access to cybersecurity professionals with extensive experience in managing and mitigating complex threats. We are an extension of your team, delivering continuous incident handling, investigation and analysis.

We Value your Time:

We understand your focus is on running your business, so we mitigate the risks and support and guide you on incidents that need your attention the most. We collect and analyse information to support detections from low noise events, and we will advise you on what is important, who it happened to, what happened, and how to stop it from happening again.

We Leverage Existing Technology:

Our mXDR service integrates with all existing technology investments to leverage and extend value. We will work with you on everything from configuring the latest Microsoft add-on, to tuning what you have already deployed. We combine advanced automations, machine learning and AI to create more effective and efficient results, so our human experts focus more on your security and less on repetitive tasks.

We Deliver Value Fast:

From the first day of working with Sapphire our threat intelligence systems identify potential

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

SAPPHIRE™

risks that could impact you. Our deployment is automated through CI/CD pipelines, building sentinel, configuring connectors and deploying our custom detections improving efficiencies by 95%.

We Help Grow your Business:

We provide continuous evidence of how you defend your customers' personal data, financial transactions and any access to their systems – increasing their confidence.

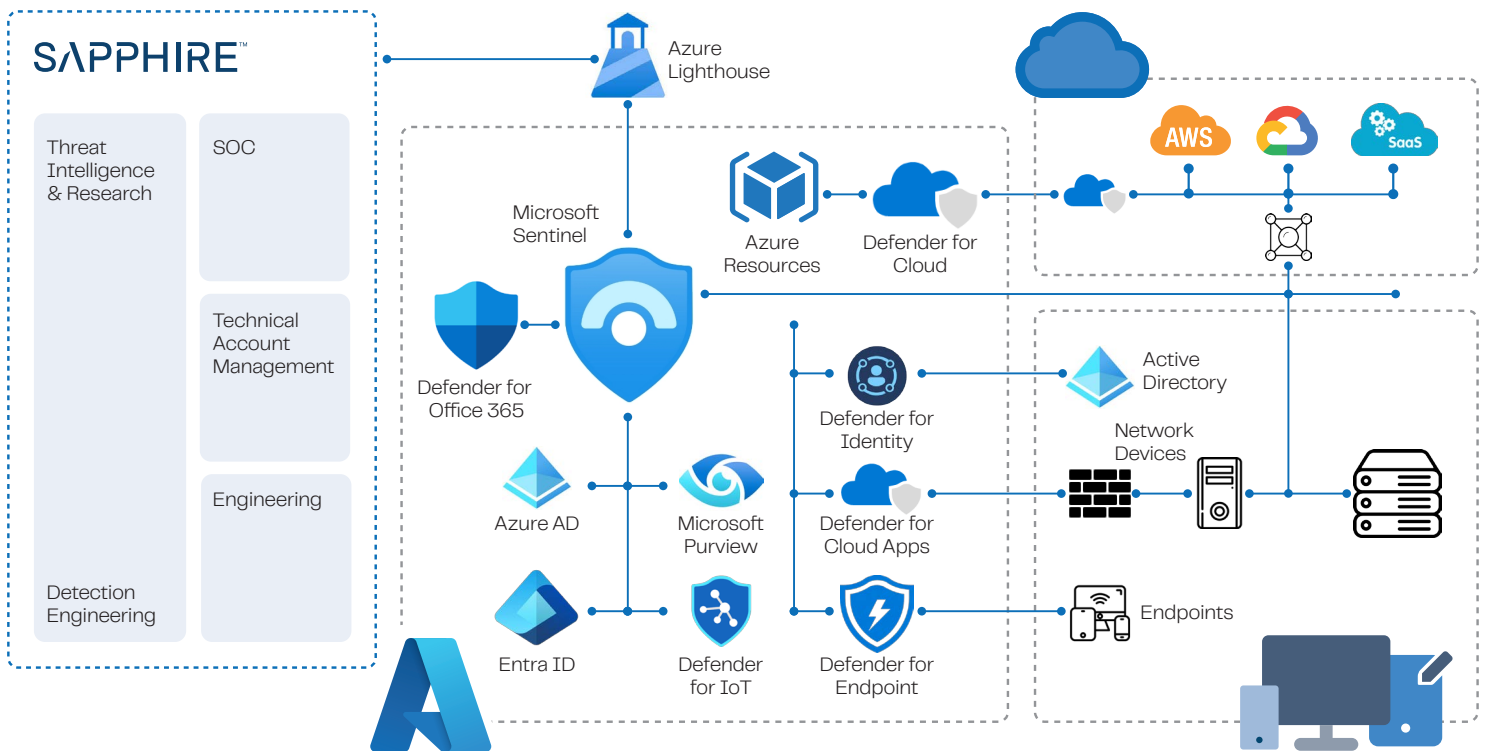
We Continue to Strengthen your Defences:

With a holistic view of your organisation and business, combined with security expertise on the latest attacker techniques and tactics.

Sapphire continues to improve and adapt our service. We extend these improvements to our client's delivering recommendations and advice on the security roadmap, investments and coverage.

How does Sapphire Managed Microsoft XDR Solution work?

The service provided includes a comprehensive cybersecurity solution encompassing various components.



To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001



SAPPHIRE™

Integrates with Existing Technology

Sapphire's mXDR service integrates a Microsoft Sentinel Security Information & Event Management (SIEM) system within your tenancy, skilfully correlating diverse data types like system logs, endpoint data, anomalies, and behaviour analytics to enhance cyber defence and maturity. The Sapphire Security Operations Centre (SOC) delivers mXDR Services through a team of expert security analysts, detection engineers, threat intelligence specialists and engineers. The SOC defends systems, data, processes, and people against cyber incidents, leveraging security controls, expertise, and threat intelligence, underpinned by a robust set of accredited procedures.

An Extension of Your Team

The SOC, acting as an extension of your security team, operates 24x7x365, focusing on networks, servers, endpoints, databases, and cloud systems to detect anomalous activities indicative of security incidents. All customer data is securely stored in your Azure tenancy, ensuring control, governance, and resilience. We can build significant individual context about your organisation to prioritise and target defences, including threat modelling for contextual awareness and prioritisation, a dedicated Technical Account Manager for operational matters, and active containment and security remediation automations within your governance framework.

Evolving to Your Security Needs

Almost all security technologies and platforms can be leveraged, including the Microsoft Defender suite, Azure security tooling, and appropriate third-party solutions are utilised for comprehensive defence, awareness and insight. We can provide flexible options for managing data ingest and continue to iterate tooling and configurations adapting to evolving security needs.

Boosted with Threat Intelligence

To further enhance your defences, Sapphire has significantly invested in threat intelligence. The threat intelligence platform plays a crucial role in contextualising security events, aiding in better understanding of threats and facilitating faster, more informed decision-making. This includes integration with Recorded Future for comprehensive threat intelligence data, and a partnership with Check Point for access to ThreatCloud™. Additionally, our threat intelligence analysts conduct extensive research, leveraging both open and closed source intelligence. Our mXDR service uses this intelligence to enhance alert analysis, leveraging automation capabilities for efficient threat handling. This combination of enriched data and automated processes enables analysts to effectively validate, triage, and respond to threats, enhancing operational efficiency, and reducing detection and response times.

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001