DigitalXRAID
CYBER SECURITY EXPERTS

GUIDE

Microsoft Sentinel Benefits

Businesses are seeking solutions that offer cyber protection without stretching resources or compromising on efficiency.

What exactly are the benefits of Microsoft Sentinel, especially when compared with other traditional SIEM tools?

What is Microsoft Sentinel?

Microsoft Sentinel, previously known as Microsoft Azure Sentinel, is a cloud-native Security Information and Event Management (SIEM) platform that leverages the power of artificial intelligence, data analytics, and cloud computing.

Unlike traditional SIEMs, Microsoft's innovative solution is designed to provide a comprehensive solution for threat detection, event management, and security orchestration, all while being scalable and cost-effective.

How Microsoft Sentinel can improve your security posture

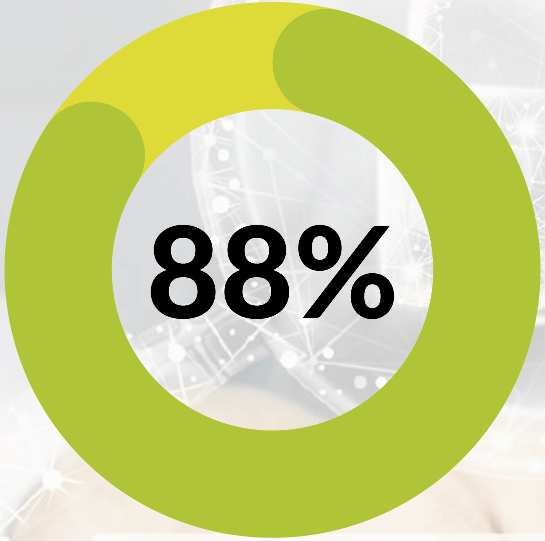
The cybersecurity landscape is an evolving one, particularly in sectors like Public Sector, Education, Financial Services, Retail, and Critical National Infrastructure (CNI).

.

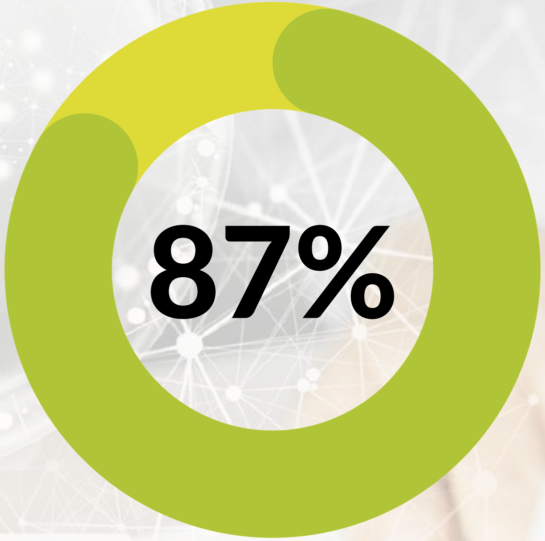
The cybersecurity landscape is an evolving one, particularly in sectors like financial services, retail, energy, utilities, and Critical National Infrastructure (CNI).

If you're looking for a solution that provides robust cyber protection without overextending your resources or impacting efficiency, Microsoft Sentinel is an option to seriously consider.

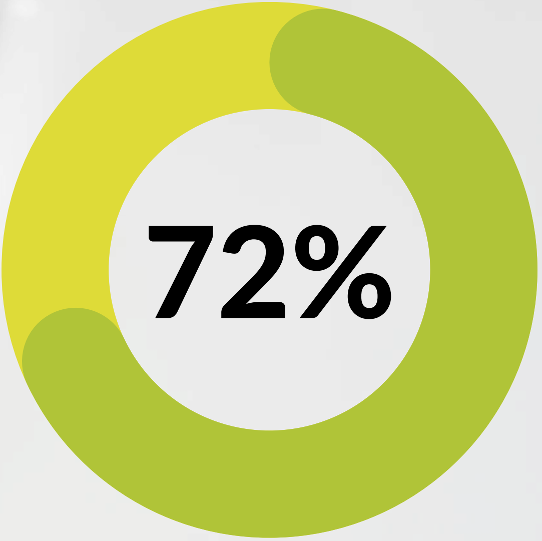
In this ebook, we'll unpack the five key ways Managed Microsoft Sentinel can give you the powerful cybersecurity solutions you need – tailored to your unique business model.



of analysts face challenges like complex processes and visibility gaps with their current SIEM solution



of businesses using Microsoft Sentinel reported a significant reduction in threat detection and response times



of companies that transitioned to Managed Microsoft Sentinel services saw a decrease in security breaches

Benefits of Microsoft Sentinel for Your Business

Traditional SIEM tools, while effective in the past, now often fall short in addressing the multifaceted threats of the modern world.

As part of a managed XDR service, Microsoft offers a suite of features tailored to combat security threats. Designed with the modern business in mind, Sentinel provides a host of benefits:

Easy Setup:

Sentinel's cloud-based nature means businesses can bypass the heavy infrastructure that traditional SIEMs demand. This ensures a hassle-free setup process, saving both time and resources.

Reduced Downtime:

The platform's proactive threat detection minimises potential downtime. It ensures that business operations run smoothly, even in the face of emerging threats.

Automated Threat Detection & Response:

The platform excels in quickly identifying correlated security events and sending alerts for immediate investigation.

This targeted approach allows the SOC team to determine if a breach has occurred and take quick action by executing your incident response plan.

This mitigates any threats in real time, thereby minimising potential damage. The advanced machine learning algorithms present only the most critical security incidents to analysts. This efficient filtering reduces noise and ensures that genuine threats are prioritised.

Integration with the Microsoft Graph Security API allows for the importation of custom threat intelligence feeds. This enhances threat detection and customises alert rules.

Hybrid Environment Management:

Sentinel stands out in its ability to manage data sources across hybrid environments. Whether your data is on-premises, in Microsoft Azure, AWS, Google Cloud, or other platforms, this platform offers seamless integration and management.

Data Normalisation:

One of Sentinel's standout features is its ability to normalise data from various sources.

By reformatting data into a consistent format, it can be easily correlated as part of log management. This simplification ensures that data analytics is more accessible and actionable for security teams.

Seamless Data Collection with Connectors:

Sentinel boasts a host of built-in connectors. These connectors ensure that data collection from various platforms is seamless, further enhancing its data analytics capabilities.

Data Aggregation:

SIEM solutions centralise security event data from across the network, presenting it through a unified dashboard. Sentinel streamlines the process of gathering security data from every corner of your hybrid organisation, be it devices, users, apps, or servers across any cloud platform.

Leveraging the prowess of artificial intelligence, it swiftly pinpoints genuine threats. Being an Azure-native solution, it harnesses the vast scalability and speed of the cloud to cater to all your security requirements.

Better Data-Driven Decisions:

The advanced data analytics and query language capabilities empower businesses to make informed, data-driven decisions. This ensures that businesses are not just reactive but proactive in their approach to threats.

Better Threat Hunting:

By integrating seamlessly with tools like Microsoft Defender, businesses can proactively search for and neutralise threats.

Single Pane of Glass:

Consolidating security data from across the enterprise into one unified view allows for streamlined monitoring and management. This centralised approach facilitates faster decision-making and more efficient threat response.

Alerts and Incident Organisation:

Genuine threats can be prioritised, reducing the noise often associated with security alerts.

Security Threat Root Causes Investigation:

Sentinel's in-depth investigative capabilities ensure that threats are not just neutralised but understood. By understanding the root causes of threats, businesses can better prepare for future challenges.

Scalability & Compliance:

The cloud-native design ensures unparalleled scalability to meet evolving security needs, without incurring significant costs.

The SIEM solution assists businesses in adhering to various regulatory standards. Through detailed security control reports, companies can effectively showcase their alignment with these mandates.

The Microsoft Sentinel benefit that makes this solution stand out amongst other cybersecurity solutions is its advanced real-time threat detection capabilities.

Understanding Microsoft Sentinel Benefits

This powerful tool actively monitors your network and swiftly identifies and responds to security incidents as they occur. This immediate detection is crucial, as every second counts in a cyberattack.

A key Microsoft Sentinel strength is its automated response feature, so the time taken to respond to known threats is significantly reduced, which mitigates potential damages.

This feature means that threats are handled even outside of regular monitoring hours.

By analysing and correlating the vast amounts of data across your network, you receive actionable insights.

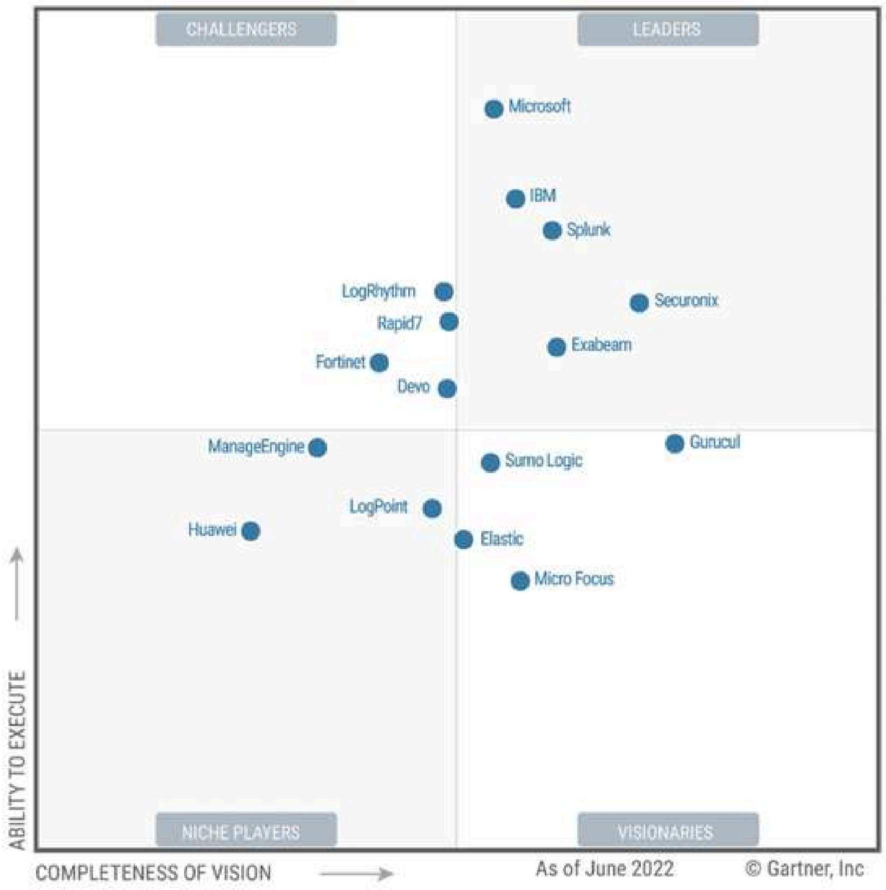
This deep analysis helps you to understand complex threat patterns and to develop more effective defence strategies.

Contrary to some beliefs, Microsoft Sentinel is not just for large organisations. It is designed to be scalable and can be effectively used by businesses of all sizes.

Another myth is that Sentinel can only integrate with Microsoft products as it's quite flexible and can work with a variety of non-Microsoft data sources and applications.

Microsoft named a Leader in the Gartner® Magic Quadrant™ for Security Information and Event Management

Figure 1: Magic Quadrant for Security Information and Event Management



As of June 2022

© Gartner, Inc

Microsoft has been recognised as a Leader in the Gartner Magic Quadrant for Security Information and Event Management.

Their top-tier position on the Ability to Execute axis underscores their commitment to delivering a state-of-the-art, AI-driven, cloud-native SIEM.

Clients such as iHeartMedia and Pearson VUE have already reaped Microsoft Sentinel benefits.

iHeartMedia chose Sentinel for its cost efficiency. iHeartMedia's CISO, Janet Heins, praised its all-encompassing visibility and intelligence to combine data from multiple systems, including firewalls, domain controllers, and more.

Pearson VUE's Enterprise Architect, Vladan Pulec consolidated visibility by migrating to Microsoft Sentinel, while benefitting from reduced infrastructure costs.

Innovations & The Future

Microsoft's recent enhancements, including its unique blend of SIEM and extended detection and response (XDR) capabilities, offer a comprehensive security operations platform.

.

Clients using Microsoft 365 Defender even benefit from data ingestion discounts.

As the threat landscape evolves, Microsoft remains committed to refining innovation, ensuring it remains at the forefront of security solutions. Microsoft has pledged to invest up to $20 billion in its cybersecurity development over the next 5 years.

Pros and Cons of Microsoft Sentinel

⊕

- Its integration with Microsoft 365 and Azure services. This allows you to capitalise on your existing Microsoft ecosystems for a more unified security management experience.

- Advanced threat detection and real-time analysis, combined with automated response capabilities, certainly positions this solution as an attractive option.

⊖

- There is an initial learning curve, especially for teams that are not used to working with advanced security systems.

- Because you need to configure comprehensive data during initial setup, there can be issues surrounding customisation.

Drawbacks of Traditional SIEM Tools

To fully understand the benefits of Microsoft’s SIEM tool, it's also essential to understand the drawbacks of traditional SIEM tools:

Infrastructure Overheads:

Traditional SIEM tools often require heavy investment heavily in infrastructure and teams of developers, leading to increased costs and complexities.

Limited Scalability:

As your business grows, traditional SIEMs can struggle to scale, leading to performance issues.

Complex Management:

They often come with a steep learning curve, requiring specialised training and expertise, or a dedicated team of specialists, which incur additional cost and overheads.

Delayed Threat Detection:

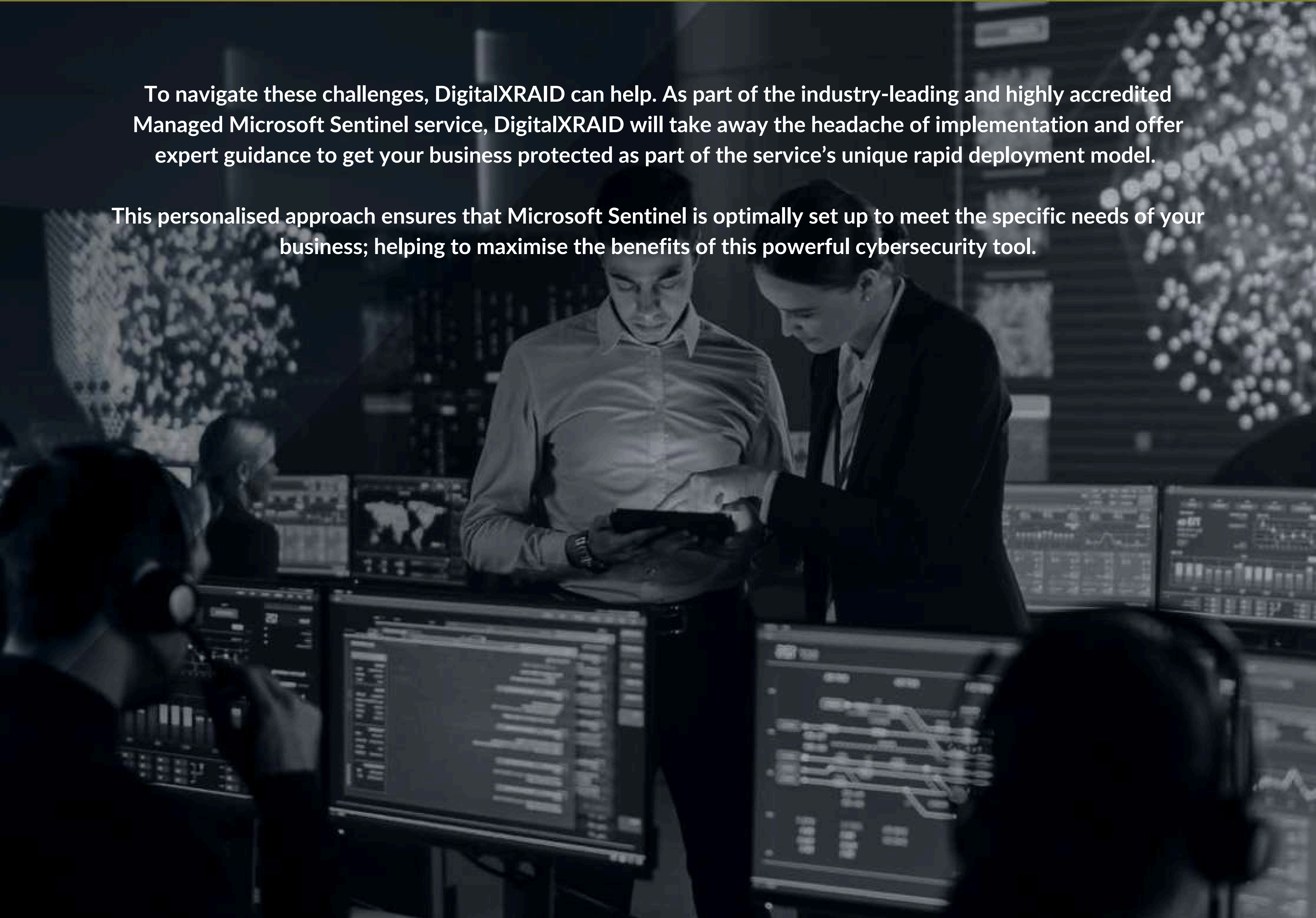
Without the power of cloud computing and AI, traditional SIEMs can sometimes lag in real time threat detection.

Integration Challenges:

Integrating traditional SIEM platforms with other tools can be cumbersome, often requiring manual configurations by developers, straining your in-house resources further.

To navigate these challenges, DigitalXRAID can help. As part of the industry-leading and highly accredited Managed Microsoft Sentinel service, DigitalXRAID will take away the headache of implementation and offer expert guidance to get your business protected as part of the service's unique rapid deployment model.

This personalised approach ensures that Microsoft Sentinel is optimally set up to meet the specific needs of your business; helping to maximise the benefits of this powerful cybersecurity tool.



Microsoft Sentinel vs Other Security Solutions

So, how does Microsoft Sentinel stack up against other security solutions on the market? The obvious benefit of playing well with the other Microsoft products is ideal if you're already in that ecosystem.

Its capacity to provide comprehensive security analytics and automated threat detection can result in significant long-term cost savings and a substantial return on investment.

This is particularly true if you compare it to other solutions that might require you to pay extra for similar functionalities.

In contrast to many traditional security solutions that might need additional infrastructure or struggle with complex integrations, Sentinel's cloud-native architecture ensures it remains adaptable and responsive to evolving cybersecurity challenges.

While other tools might offer similar basic functionalities, Sentinel's edge lies in its ability to provide comprehensive, real-time security insights and automate responses to threats – making it a more efficient and forward-thinking choice for modern enterprises.

The use case for Microsoft Sentinel

This solution is perfect for the financial space, as it is highly capable of combating advanced cyber threats such as fraud, data breaches, and network intrusions.

Financial institutions are prime targets for cybercriminals due to handling sensitive financial data. Some banks' existing security infrastructure is robust, but they often struggle with the sheer volume of data and the sophistication of new threats.

In these instances, a managed Microsoft Sentinel service is deployed to monitor a bank's vast network, including online banking platforms, transactional databases, and internal communication networks.

Its advanced analytics and AI capabilities can detect unusual patterns indicative of APTs or fraudulent activities.

These can include irregular transaction volumes or suspicious login attempts from unrecognised locations.

Upon detecting a potential threat, Microsoft Sentinel can automatically initiate predefined response protocols.

For instance, if a potential data breach is detected, Sentinel could automatically isolate the affected network segment and initiate a forensic investigation, while alerting the cybersecurity team.

If a new threat is detected, your managed service security analysts will take action immediately, programming Microsoft Sentinel to recognise this new form of attack in the future.

Microsoft Sentinel plays a crucial role in safeguarding a bank's assets and reputation by providing scalable, advanced, and efficient cybersecurity solutions tailored to financial organisations' specific challenges.

Managing Your Threat Detection and Response

While Sentinel SIEM offers many benefits, the management can be challenging, especially for businesses without a dedicated security team. .

In the ever evolving threatscape, tools like Sentinel are not just beneficial but essential.

By understanding its benefits and leveraging the expertise of managed Microsoft Sentinel service providers, businesses can ensure security protection for their entire organisation in an efficient and cost-effective manner.

Utilising Microsoft's Sentinel solution as part of your managed XDR service provides organisations with a comprehensive and effective solution to the growing threat of cyber-attacks.

Businesses benefit from:

- Ensuring that their security operations are overseen by experts
- Focusing on core business operations, leaving the intricacies of security management to specialists
- Efficient use of the tool's features, eliminating unnecessary costs

When you choose DigitalXRAID for your Managed Microsoft Sentinel service, you're not just selecting a service – you're partnering with an industry leader.

Managing Your Threat Detection and Response

DigitalXRAID is here to manage every step of your Microsoft Sentinel integration and deployment.

With the CREST-certified Security Operations Centre (SOC) service, DigitalXRAID offers a cutting-edge Managed Microsoft Sentinel service for proactive threat detection, investigation, and response.

> **DigitalXRAID - Helping you to secure your digital landscape with confidence and ensuring the bad guys don’t win.**

How can we help?

When you choose DigitalXRAID for your Managed Microsoft Sentinel service, you're not just selecting a service – you're partnering with an industry leader. Here's just a few of the reasons why our offering stands out:

CREST Accreditation: Our CREST certification is a testament to our commitment to the highest standards of security and professionalism. It's a globally recognised seal of approval, and we wear it with pride.

Round-the-Clock Monitoring: With our 24/7/365 monitoring, threats don't stand a chance. Day or night, our team is on hand to ensure your business remains protected.

Unparalleled Expertise: Our team's extensive experience and qualifications in cybersecurity position us to uniquely harness the full potential of your security services across offensive, defensive and compliance.

Diverse Client Portfolio: We protect a wide range of organisations, from central government departments and critical national infrastructure to esteemed educational institutions like universities. Even international football clubs trust us with their security, underscoring our versatility and prowess.

Cost-Effective & Comprehensive: Our close partnership with Microsoft ensures cost-effective security management. Plus, clients using solutions like Microsoft 365 Defender benefit from exclusive discounts on data ingestion.

Future-Proof Your Security: The digital threat landscape is ever-evolving, but with DigitalXRAID, you're always a step ahead. Our commitment to continuous adaptation and learning ensures your security measures are always at the industry's forefront.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence
Against Cyber Threats?
Call us now on 0800 090 3734

info@digitalxraid.com digitalxraid.com

ISO 27001 ISO 9001 CYBER ESSENTIALS CERTIFIED PLUS IASME CONSORTIUM CREST

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing