



# Proactive protection for peace of mind

Secure your business with tailored Managed Extended Detection and Response services built upon Microsoft Sentinel and Microsoft Defender XDR and delivered by KMicro with Microsoft



# Contents

Identify tomorrow's risks, not just today's threats .....2

Enhance threat hunting with MXDR for Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Defender for Cloud .....3

Fine-tune your Microsoft Security product portfolio .....4

Reduce alert fatigue and improve threat response .....6

Simplify compliance and data protection .....8

Case Study: MBC Group secures media and broadcast operations with KMicro Sentinel360 MXDR solution .....10

Experience what it's like to have a partner in the fight ..... 12

# Identify tomorrow's risks, not just today's threats

## Finding the right security solutions while reducing IT complexity and meeting everyone's needs is not easy

"Security is like an onion," says the CIO of Wedgewood LLC, a real estate company that has invested in both Microsoft Sentinel and KMicro's Managed Extended Detection and Response (MXDR) services. He goes on to share that he wanted to peel back every layer of this onion, identifying the areas where his organization needed a solution for security. But the challenge is more than just identifying gaps to close – security teams must also work to eliminate overlapping layers of security investments while also ensuring the continuity of required business operations. People need the freedom to work productively using their preferred applications and methods. Companies need greater visibility and control to reduce exposure to cyber threats and downtime caused by cyber events. Meeting everyone's needs can feel overwhelming.

Organizations looking to strengthen their security defenses without overcomplicating their IT ecosystem, overburdening their in-house analysts, or disrupting critical business processes can find relief in knowing that they don't have to walk this cybersecurity journey alone. In fact, the cost-effective, simple solutions are often found in collaborative partnerships with trusted MXDR solution providers who intimately know the platforms and systems that sustain your business.

50%

With the right help, you can tailor existing investments to extend their value: 50% of organizations admit that their security tools are only somewhat or slightly effective due to a lack of skilled personnel and complex configuration.<sup>1</sup>

54

Bringing in outside expertise can complement your security investments and standardize processes: Many organizations lack a coordinated incident response plan, which is crucial for managing cybersecurity threats efficiently. Organizations with both an incident response team and a plan identify breaches 54 days faster than those without.<sup>2</sup>

# Enhance threat hunting with MXDR for Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Defender for Cloud

In today's ever-evolving threat landscape, cybersecurity is non-negotiable. But it doesn't need to be a solo undertaking, with the KMicro Sentinel360 MXDR solution, that puts next-generation Microsoft Security products to work for you. Sentinel360 is tailored for Microsoft Sentinel, Microsoft's cloud-based Security Information and Event Management (SIEM) solution. It is designed to optimize Microsoft 365 Security and E5 licensed products with an integrated suite of managed services that fortify and streamline the security of your technology portfolio. Customize the design and deployment of Microsoft Sentinel instances tailored to your organization's risk profile. Develop and fine-tune analytics rules, watchlists, and playbooks to super-charge threat detection and response. Tag-team with a fully equipped Security Operations Center (SOC) that works on your behalf around the clock to investigate alerts.

Identify, investigate, and remediate today's most advanced cyberattacks with the help of an elite SecOps team



## **Fine-tune your Microsoft Security product portfolio**

Tailor your Microsoft Security and Microsoft 365 products according to your business requirements.



## **Reduce alert fatigue and improve threat response**

Address the core pain of alert overload, skills gaps, and compliance burdens.



## **Simplify compliance and data protection**

Enhance regulatory compliance, reduce downtime, and prevent data breaches.



# Fine-tune your Microsoft Security product portfolio

## Take full advantage of your Microsoft Security suite by tailoring solutions to your needs

If you are using Microsoft 365 and Azure for your business, you know how powerful and versatile these platforms are. They enable you to work from anywhere, collaborate seamlessly, and scale your operations. But as with any complex ecosystem of products, security configuration and management often require specialized expertise and solutions. If you want your organization to maximize the potential of any technology, you need to first make sure that the technology is designed with both the end users and the organization in mind. Your Microsoft ecosystem has a lot to offer you, with incredibly robust built-in security capabilities. But cybersecurity is not a one-size-fits-all – you need to set up your tools based on your unique business needs and requirements.

KMicro Sentinel360 MXDR is tailored to meet your specific Microsoft Security needs. With a deep understanding of the Microsoft ecosystem, including Microsoft Sentinel, Microsoft Azure, and Microsoft 365, the team ensures your security measures are optimized for maximum protection. Move beyond standard configurations to customized solutions that fit your organization's risk profile and compliance requirements. This continuous optimization process adapts to emerging threats and your evolving business landscape, keeping your security strategy current.

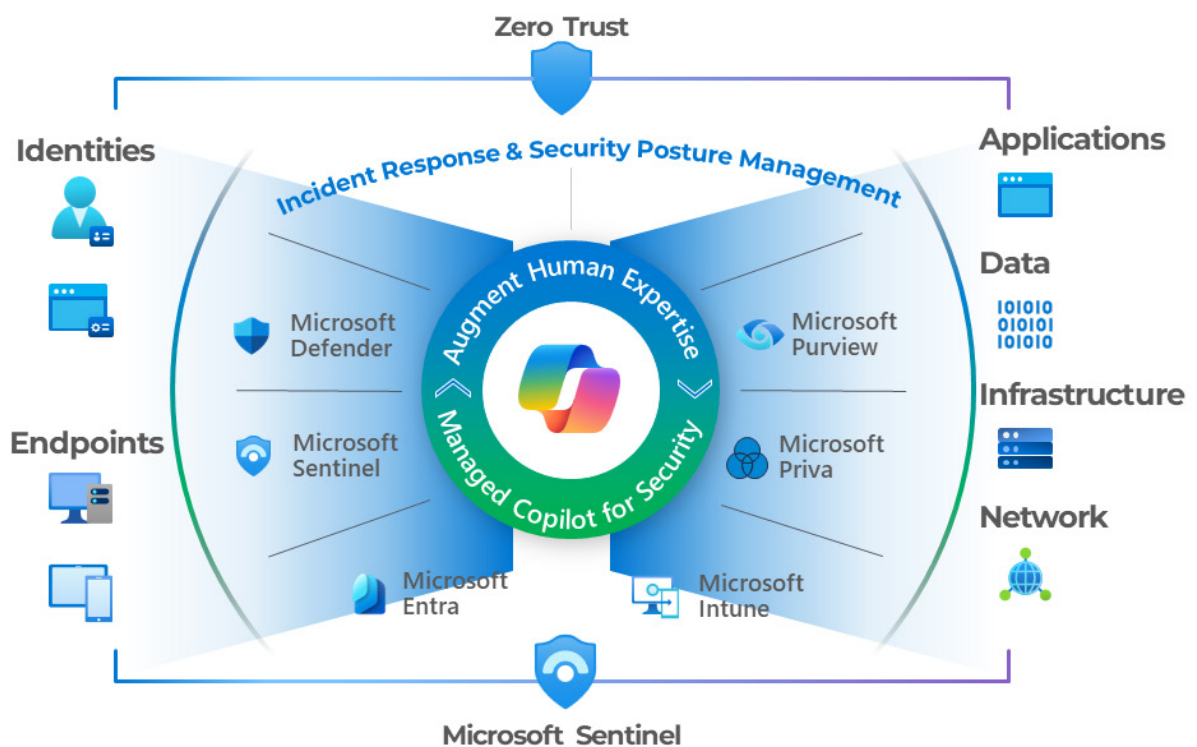
## Collaborating with a premier Microsoft Gold Partner for cybersecurity

As a member of the Microsoft Intelligent Security Association, KMicro provides expert guidance and training to help organizations like yours strategically leverage their Microsoft Security products. They focus on aligning your security measures with your business objectives, ensuring your Microsoft investments are not just managed, but optimized. With KMicro, you gain a partner who understands the dynamic nature of your business and helps you navigate your security needs with confidence and efficiency.





## Sentinel360 MXDR





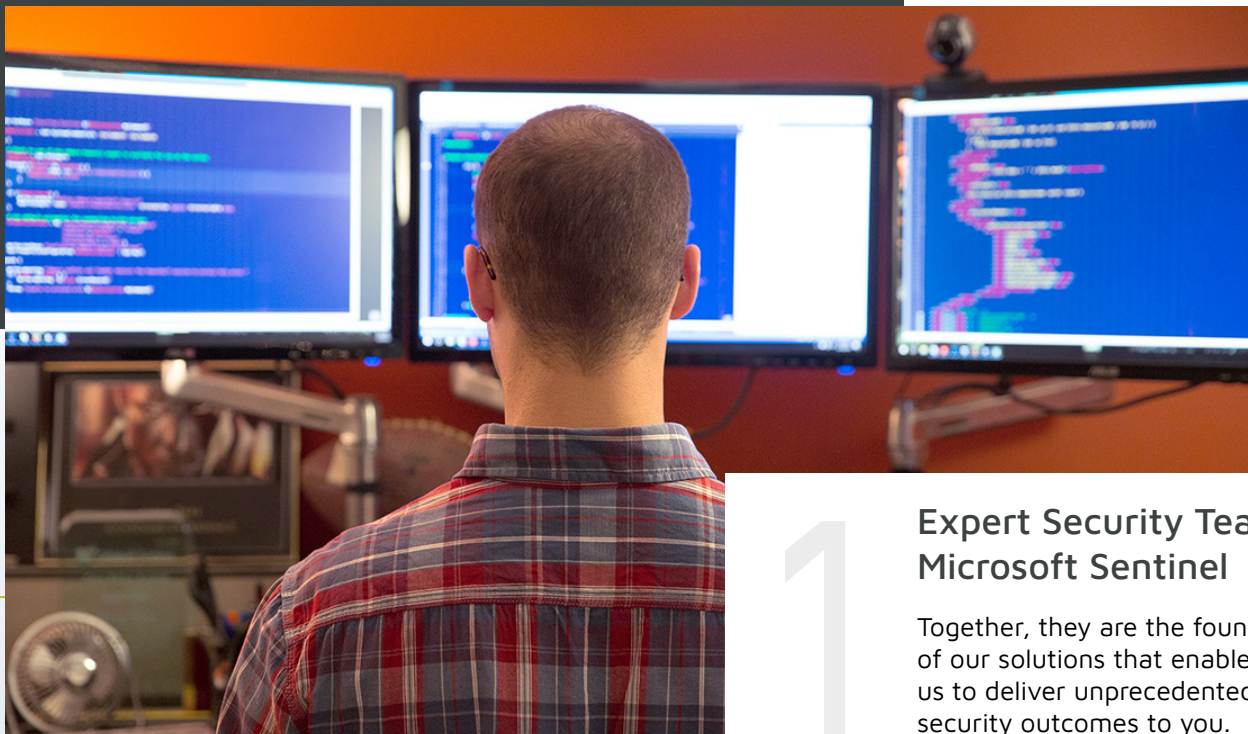
# Reduce alert fatigue and improve threat response

Cut through the noise of security alerts and weed out false positives to find and stop real threats

Do you feel swamped by the sheer volume of tasks and alerts that trickle in every day? If you've answered yes, you're not alone. One of the biggest challenges in cybersecurity today is alert fatigue with over 97% of Security Analysts admitting they are concerned about missing relevant security events due to the volume of alerts generated by various security tools in their ecosystem.<sup>3</sup> This level of noise, combined with a flood of false positives (an unfortunate and typical byproduct of maintaining a layered security environment), can often be a huge distraction for your security team, making it difficult to find and stop real threats.

Discover the impact of proactive human-led false positive analysis and threat hunting


- 79% decrease in false positives.<sup>4</sup>
- 80% reduction in investigation labor effort.<sup>4</sup>



1

## Expert Security Team & Microsoft Sentinel

Together, they are the foundation of our solutions that enable us to deliver unprecedented security outcomes to you.



Imagine a quieter workday where you can delegate the painstaking task of sifting through notifications to a trusted resource that combines the power of human expertise with automation, intelligence, and analytics. Sentinel360 MXDR, built around Microsoft Sentinel and integrated with the broader Microsoft ecosystem, makes that vision a reality. Through expert fine-tuning and bespoke configurations, KMicro's comprehensive MXDR solution reduces the number of alerts your tools generate, ensuring that security teams receive only the most relevant and critical notifications. Additionally, proactive threat hunting and actionable insights offered by Sentinel360 MXDR mean that potential issues are identified and addressed before they escalate into alerts, further reducing the burden on security personnel. By configuring and updating your Microsoft Security investments to align with specific organizational needs, KMicro can help you transform the deluge of alerts into a manageable flow of pertinent information, enabling security teams to act more efficiently and effectively.

# KMicro Sentinel360 MXDR

Experience what it's like to have a partner in the fight!

Safeguard your people, data, and infrastructure. Get visibility and respond to threats before they cause harm with 24/7 Managed Security tailored for your business.

2

## The Human Element to Cybersecurity

Qualified security experts alongside the right technology is essential. Microsoft Sentinel coupled with human-led analysis speeds threat detection and response.

3

## Take full advantage of your Microsoft Security suite

Deploy the Microsoft Security tools and the Defender stack you already have and eliminate the headaches and cost of disparate security products.





# Simplify compliance and data protection

## Customize and continuously optimize tools to comply with regulations

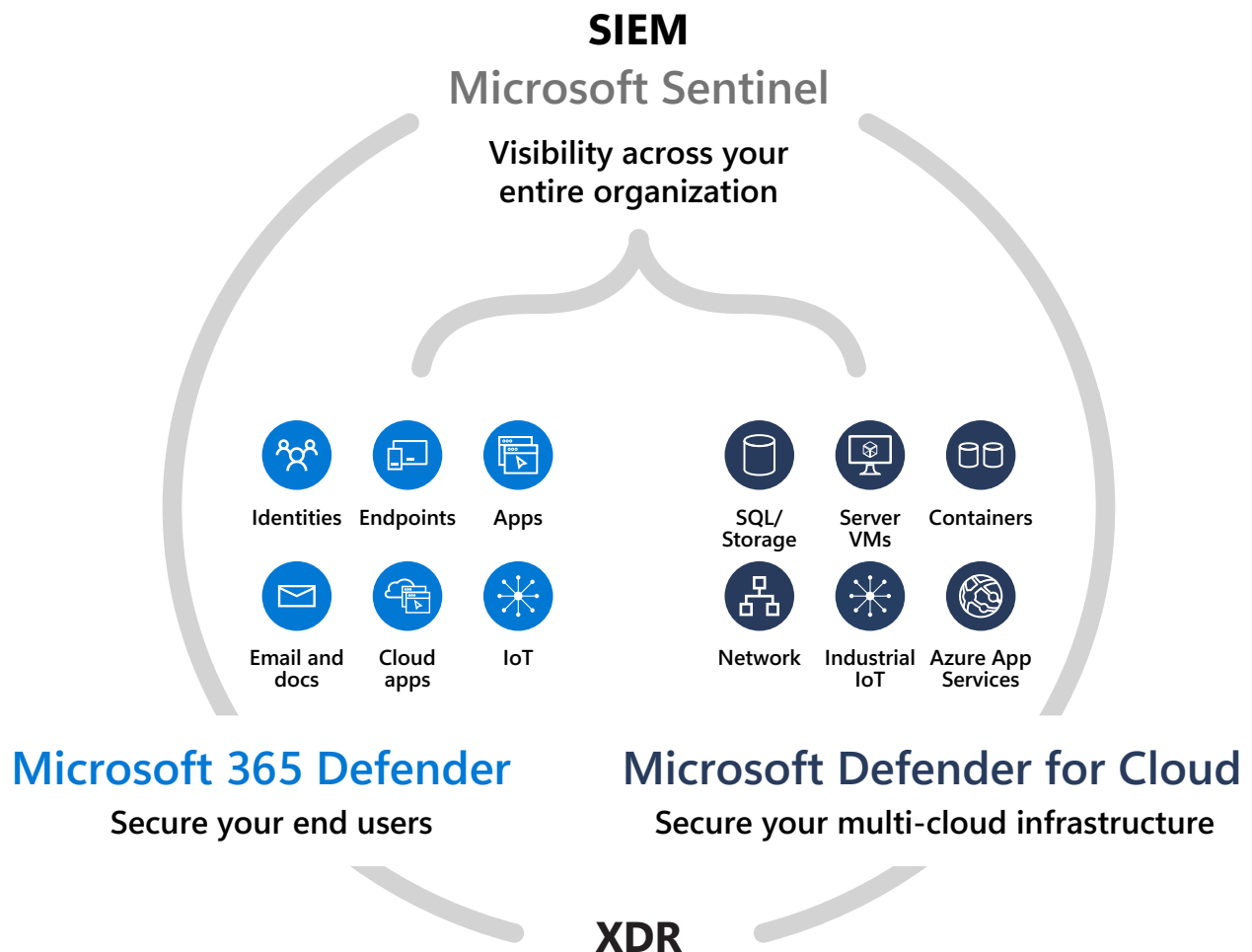
It can be hard to manage compliance and safeguard confidential data that's scattered across your IT environment, especially when you have limited resources and in-house expertise. For many security teams, this isn't simply a challenge – it's a reality they face daily. KMicro Sentinel360 eases that burden.

Navigating Microsoft's Security landscape requires more than just a surface-level understanding. It helps to have dedicated personnel on hand who have made it their mission to stay up to date on the latest features, best practices, and protocols for optimizing your investments. KMicro introduces experience and knowledge of Microsoft's Security solutions and compliance frameworks to your team. This expertise can be deployed to configure products like Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Defender for Cloud to align with your organization's specific compliance requirements – be it HIPAA, NIST, ISO 2007, GDPR, CCPA, or others.

But compliance is an ongoing journey, not a one-time destination. You can't just configure tools once and expect them to stay compliant with changing legislation and requirements. Highly regulated organizations need to constantly fine-tune their security controls and conduct clear, concise reporting that not only demonstrates their compliance posture to auditors but also ensures security measures evolve alongside the business. To ensure you remain compliant and secure, Sentinel360 delivers ongoing optimization and reporting. When it comes to proactive threat detection within Microsoft environments, KMicro's team combines a deep understanding of security attack vectors with Microsoft's robust Security features to offer superior detection capabilities, helping to prevent non-compliance events before they occur.



# KMicro MXDR: Harnessing Next-Generation Microsoft Security to Empower Your Defense.



**K•MICRO>**

Member of  
Microsoft Intelligent  
Security Association

Microsoft Security

Microsoft Verified  
Managed XDR Solution



## CASE STUDY

# MBC Group secures media and broadcast operations with KMicro Sentinel360 MXDR solution

**mbc**

G R O U P

### Situation

MBC Group is a leading media and entertainment company in the Middle East and North Africa. They leverage Azure for cloud-based content storage and delivery and Microsoft 365 for internal collaboration. MBC was facing increasing cybersecurity risks as their growing reliance on cloud services and the shift to remote production models created new attack surfaces.

### Challenge

MBC needed to ensure compliance with complex and evolving regional and international data protection regulations, especially regarding the handling of sensitive viewer data. They also needed to prevent leaks and unauthorized access to pre-release content and intellectual property. Comprehensive security and visibility were a challenge, as their IT ecosystem spanned on-premises and multi-cloud environments, multiple production facilities, and partner systems.





## Result

With KMicro's Sentinel360 MXDR service and Microsoft Security solutions, MBC successfully:

- **Reduced risk of data breaches:** Rapidly detected and mitigated several attempts to steal intellectual property.
- **Improved cloud security posture:** Optimized Azure security settings and implemented continuous monitoring to prevent vulnerabilities from being exploited.
- **Demonstrated compliance:** Generated clear reporting to satisfy regulations and maintain strong relationships with content partners.
- **Enhanced visibility:** Centralized the view of threats across MBC's complex environment, allowing for faster response times.

## Solution

KMicro Sentinel360 MXDR combined the power of Microsoft Sentinel and Microsoft Defender XDR with 24/7 security expertise to provide MBC with a comprehensive defense against sophisticated cyberattacks. This included:

- Rapid investigation, containment, and remediation of security threats from KMicro's security experts.
- Automated reporting and recommendations from Sentinel360 MXDR to help MBC stay ahead of evolving regulatory requirements.
- Integration with data classification tools to ensure MBC's most sensitive information is safeguarded with the appropriate security measures.
- Continuous monitoring and threat hunting by KMicro to identify and address vulnerabilities *before* they become major incidents.
- Offloading security tasks from MBC's IT team to Sentinel360 MXDR, allowing them to focus on core business priorities.



# Experience what it's like to have a partner in the fight

Products like Microsoft Sentinel, coupled with human-led analysis and expertise, are a great way to speed up threat detection and response. But the best news is that you don't have to overextend your own resources or find and hire expensive talent to introduce this highly specialized human element to your cybersecurity strategy. Augment your existing resources and safeguard your people, data, and infrastructure with KMicro Sentinel360 MXDR. Get visibility and respond to threats before they cause harm with 24/7 Managed Security tailored for your business.

Schedule a free consultation and discover how Sentinel360 can transform your Microsoft Security posture.

Contact us

See Sentinel360 MXDR in action by requesting a personalized demo.

Request demo

Ready to get started? Find us on the Microsoft commercial marketplace.

Learn more



<sup>1</sup> Revealing New Opportunities for the Cybersecurity Workforce, Cybersecurity Research | ISC2

<sup>2</sup> New Microsoft Incident Response team guide shares best practices for security teams and leaders | Microsoft, 2023

<sup>3</sup> 2023 State of Threat Detection, Research Report | Vectra

<sup>4</sup> Managed XDR for Defender (MXDR) | KMicro

Member of  
**Microsoft Intelligent  
Security Association**



Microsoft Verified  
Managed XDR Solution



Copyright © 2024 KMicro and Microsoft Corporation.  
All rights reserved.