



Transform your security operations center with simplified threat detection and response

Table of Content

- 01** [Traditional SIEMs](#)
- 02** [Microsoft Sentinel: The Next-Gen SIEM Solution](#)
- 03** [Simplifying Your Defense Against Threats](#)
- 04** [The Use Cases](#)
- 05** [Flexibility and Cost Efficiency: The Affordable Solution](#)
- 06** [Why Netwoven](#)

Traditional SIEMs are inefficient

The frequency and intensity of cyberattacks continue to increase. Criminals use ever-evolving strategies to take advantage of vulnerabilities. Even simple single-PC ransomware has ballooned and can take down entire networks. Meanwhile, the attack surface continues to expand because of larger and larger data estates, and organizations are embracing hybrid workstyles. Now more than ever, Security Operations teams need new ways to integrate cybersecurity with their business continuity strategies.

But there's a real gap. The traditional Security Information and Event Management (SIEM) solutions organizations once relied on can no longer keep up. They're slow to scale. They can leave gaps due to siloed tools and limited capabilities. They can also be expensive to maintain and expand; for instance, increasing storage can be extremely expensive, forcing organizations to choose between cost control or visibility and increased risk.

And for the Security Operations Center (SOC), outdated SIEM solutions create an overwhelming amount of additional work, leading to increased risk. The enormous amount of data they generate can leave security teams scrambling to analyze potential threats—often requiring manual analysis—and wading through massive numbers of alerts, many of which are false positives.

In short, your SOC could be missing an important insight from:

- Incomplete visibility
- Missing contextual awareness
- Inability to handle big data
- No threat intelligence integration
- Slow analysis and limited integration

Isn't there a better way?



You need a stronger defence

Microsoft Sentinel is a modern approach to a growing problem. It uses the power of the cloud and AI to help you detect cyber threats *before* they impact your business.

As a Microsoft partner, we can help you start using Microsoft Sentinel quickly and easily, so you can transform your security operations.

Microsoft Sentinel: the next-gen SIEM solution

As a technology advisor to businesses like yours, we are deeply embedded in the security space -and we recommend Microsoft Sentinel precisely because it isn't yesterday's SIEM. Instead, it's a next-generation, cloud-native SIEM solution that taps into the power of AI, automation, and deep threat intelligence from Microsoft. Microsoft Sentinel is designed to be proactive, not reactive. Our customers that use Microsoft Sentinel have a solution that helps protect large digital estates before threats occur - and it works across data, apps, infrastructure, or even any custom data or use case.

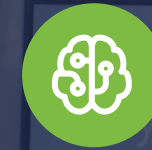
Microsoft Sentinel acts as a consolidated Security Operations platform for your SOC team too. Not only will security personnel get a complete view of the entire data estate in a single location, but they can also hunt and resolve critical threats at machine speed.

Microsoft Sentinel is highly integrated with Microsoft XDR solutions - that is, Microsoft 365 Defender, Microsoft Defender for Cloud, and Microsoft Defender for IoT. This integration keeps incidents synchronized between both portals for complete visibility from within Microsoft Sentinel.



Help protect your digital estate

Secure more of your digital estate with scalable, integrated coverage for a hybrid, multi-cloud, multiplatform business.



Help protect your digital estate

Secure more of your digital estate with scalable, integrated coverage for a hybrid, multi-cloud, multiplatform business.



Detect, investigate, and respond effectively

Stay ahead of evolving threats with a unified set of tools to monitor, manage, and respond to incidents.



Lower your total cost of ownership

Get started faster while reducing infrastructure and maintenance with a cloud-native SaaS solution.

It's time to simplify your defence against threats

Defending against threats doesn't need to be as complicated as it is. Our security experts know that today's SOC simply doesn't have time, staff, or budget to triage, investigate, and remediate threats manually. We also understand the limitations of SIEMs that aren't cloud-based; they simply cannot protect organizations that have embraced hybrid workstyles or that use multiple clouds. And we've seen time and again that adding more security solutions just adds complexity and cost. That's why your SOC needs solutions that help them simplify its defence against cybersecurity threats. We recommend Microsoft Sentinel. Let us help you deploy it so your SOC can streamline security operations.

Secure more, stress less

Microsoft Sentinel offers a wide variety of features and capabilities designed to help your SecOps team be more efficient, strategic, and effective.

Cloud-scale protection increases flexibility

Now, you can secure your hybrid, multi-cloud environments with increased flexibility to uniquely address your business needs.

- Cost reduction with cloud-native SaaS
- Out of the box (OOTB) that's ready to go and customizable content
- Cloud-scale data collection and analysis
- Scaled data collection, flexible data access options, access management, and robust business continuity and disaster recovery.

A unified solution delivers more robust security

Stop reacting to evolving attacks and start being proactive with a unified set of tools to detect, investigate, and respond to incidents.

- Enhanced user and entity behavior analytics (UEBA), security orchestration, automation, and response (SOAR), hunting capabilities, and threat intelligence (TI) built into your day-to-day operations
- Built-in case management for SOC teams
- OOTB bi-directional integration into Microsoft 365 Defender, making Microsoft Sentinel the only true SIEM and XDR offering on the market
- The ability to extend and expand capabilities with extensive customization

AI and automation increase efficiency

Empower your SecOps team with advanced AI, world-class security expertise, and comprehensive threat intelligence.

- AI trained scoring and tuning
- Machine Learning (ML) that automatically correlates alerts into prioritized incidents.
- Automation via OOTB and custom SOAR playbooks
- Bring-your-own-machine-learning (BYO ML) to stay ahead of evolving attacks.

Microsoft Sentinel use cases



Increasing attacks

In order to stop and prevent the attack, you need to have visibility into your entire digital attack surface and the ability to secure it. That means your SIEM needs to be able to ingest any type of data known today or yet to come. As a software-as-a-service offering, Microsoft Sentinel can take in any kind of data, stored for up to seven years for compliance, and quickly and easily augmented and customized with out-of-the-box content, connectors, additional solutions, workbooks and more.



Multiple regions

You cannot be everywhere and observe everything, but your organization needs to have the latest threat intelligence information to help prevent and detect threats and attacks. Microsoft processes more than 65 trillion signals every day, which combined with AI and the expertise and more than 8,000 dedicated security professionals, provides deep security insights to prevent catastrophic breaches. All this information is embedded into Microsoft Sentinel to help prevent and detect attacks. If an attack gets in, the affected pieces are isolated for simpler remediation.



Sophisticated attacks

Every minute matters in your investigation. Microsoft Sentinel uses cutting-edge Microsoft AI and ML, trained at scale to give your SOC enhanced tools to speed their threat detection and remediation. Built-in intelligence can reduce signal noise, and pinpoint attacks, correlate the mass amounts of alerts into incidents that can span the entire attack kill chain in an attack. Then, ML prioritizes alerts can be taken right from the incident page.



Quick identification

To remediate threats, you first need to know if something is malicious or not—and finding that out often takes the most amount of time. Microsoft Sentinel features investigation tools that help you understand the scope and root cause of threats. Plus, an identity mapping graph enables analysts to ask interesting questions for a specific entity and drill down more deeply.



Lurking threats

Security analysts want to be more proactive about looking for security threats. That means you need to be able to hunt and see if anything comes back as unusual. Microsoft Sentinel provides powerful hunting search and query tools across all your data sources.

The flexibility you need, at an affordable total cost of ownership

Your enterprise needs modern security solutions—and to be their best, your SecOps team needs a full-featured, cloud native SIEM solution that enables flexibility and nimbleness. That solution is Microsoft Sentinel, and it's much more cost-effective than you might think.

There are many reasons that Microsoft Sentinel offers an exceptional total cost of ownership.

For one, you'll be able to free your teams to focus on higher-value activities, and you won't need to pay data scientists to run analysis on threats.

For another, you simply get more—like low-cost storage that meets compliance regulations and native XDR integration.

Lastly, you'll be able to eliminate multi-vendor solutions, which can save up to 60 percent on security technology expenditures.²



We're here to help you transform your security operations center

Now is the time to stop cyberattacks and coordinate response across all your assets. And there's no better way than by establishing Microsoft Sentinel as the guardian of your digital estate. Give your SOC a true command and control center designed with AI front and center. Get the benefit of our experience as a trusted Microsoft partner that understands best practices and can design and customize a solution specifically for your needs.

We are uniquely positioned to help you streamline all your security operations modernization projects through our robust security service offerings. Whether you need an assessment, migration, hunting expertise, incident response, or managed security services, we're ready to help.



Why Netwoven?

Data Protection execution is full of challenges, but you can overcome them using Netwoven's proven methodology and experience.

- Implemented a comprehensive Information Protection program to protect sensitive data for a Fortune 1000 company
- Migrated 45000 Mailboxes and migrated M365 tenant for a large Fortune 1000 hospital



Microsoft Solutions Partner
Security
Specialist
Identity and Access Management
Information Protection and Governance



Microsoft Solutions Partner
Microsoft Cloud

Member of
Microsoft Intelligent Security Association
Microsoft



The client has taken a comprehensive approach to protecting sensitive information both inside and outside the organization while ensuring there was no impact on collaboration. Netwoven's extensive technical expertise and willingness to work with Microsoft's product engineering combined with their unique approach to designing solutions with a business-centric view allowed them to make the best use of Microsoft's offerings to meet the company's information protection needs. "



Enrique Saggese
Microsoft

Next Steps

Book a complimentary security workshop with our experts to understand the Microsoft security stack and learn how you can modernize your security infrastructure and improve your security posture.

+1 877 638 9683

info@netwoven.com

netwoven.com

About Us

Netwoven

We shepherd organizations safely through the cloud transformation journey by unraveling complex business problems.

By partnering with us, our clients securely collaborate globally, improve business operations, build new products and solutions with deeper insights, and reduce cyber security risks.