

Stay one step ahead: unifying your Security Operations



wanstor

The current state of security operations

Growing frequency, speed, and sophistication of threats


Cyber threats are evolving fast – and so are we. At Wanstor, we cut through the noise to keep your business secure and focused. Just as important is the exponential expansion of enterprise attack surfaces resulting from the adoption of cloud services, bring-your-own devices, increasingly complex supply chains, Internet of Things (IoT), and more.

Disconnected tools waste time. We bring everything together – so your team can act fast and stay ahead.

Switching between multiple dashboards and siloed data can significantly slow down the average time needed to discover and respond to threats. Simply put, security operations centre (SOCs) teams have too much security data distributed in too many places to quickly react to issues.

Making matters worse is an ever-growing gap in supply and demand of cybersecurity professionals.

With issues like these, something needs to change.



We deliver seamless protection that keeps your business ahead of threats. It spans identities, endpoints, data, email and collaboration, cloud apps, and hybrid and cloud infrastructure.

We know how to help

To address modern attacks crossing multiple domains, security teams need a unified solution that enables them to detect and respond to threats across their company's entire digital estate. Extended detection and response (XDR) can help your SOC teams transition from a reactive approach to a proactive defence strategy, improving threat detection and response times. Most important, it frees up time for analysts to focus on proactive hunting and prevention.

The benefits of an XDR solution

XDR gives your team the full picture – fast. No more guesswork, just smart, streamlined defence, protecting organisations against advanced attacks. SOC teams gain a more complete view of the kill chain for more effective investigation. XDR can also provide automatic remediation across multiple domains using vast sets of intelligence and built-in AI.



Endpoint detection and response (EDR) solutions are **not enough**

XDR

- Holistic security and signal correlation across identity, email, endpoint, cloud app, data loss prevention (DLP) security, and more
- Incident-based investigations and response experience
- Protection against advanced attacks such as ransomware and business email compromise (BEC)

EDR

- Endpoint security only
- Siloed endpoint alerts
- Only fends off endpoint-specific attacks
- Lacks the big picture to help with advanced attacks

XDR offers a new way to drive process and cost-efficiency across your operations by focusing on five critical capabilities:



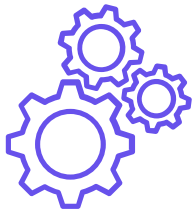
01. Advanced kill chain visibility and protection

XDR solutions cover different asset types and unify security for critical threat entry points like email and identity. They also protect endpoints, cloud apps, and DLP data. By consolidating these data sources, XDR solutions correlate low-level alerts into a single incident and help uncover the full kill chain of a sophisticated attack often overlooked by point security solutions.



02. Unified investigation and response

Effective XDR solutions enable incident-based investigation showing the end-to-end view of attack, contextual deep dives, and response playbooks with best practices. These are all critical in making it easier for SOC teams to investigate and respond to attacks more efficiently.



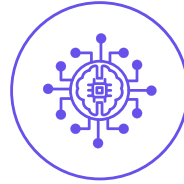
03. Exposure management

Approximately 99% of attacks can be prevented with basic cybersecurity hygiene, highlighting the importance of hardening all systems.¹ Issues like security silos make it more difficult and time-consuming to uncover, prioritise, and eliminate vulnerabilities.

Wanstor and Microsoft strive to ensure data protection and privacy, helping you avoid penalties and maintain trust with stakeholders



04. Broad intelligence and threat vector visibility



An XDR solution draws insights from a broad set of sources to analyse signals and better understand the threat landscape. This enhances the ability to see and understand more threat vectors, quickly identify an attack at an early stage, and reduce the amounts of alerts and incidents.

05. Improved total cost of ownership



XDR enables vendor consolidation for organisations by integrating multiple siloed security tools into a unified solution. It removes the need to purchase from various vendors and eliminates the manual work needed to correlate signals, reducing acquisition costs and process overhead.

Spot threats early. Shut them down fast. That's how we keep you secure. We harness Microsoft's powerful tools, then layer on our expertise to deliver results that matter. We monitor and mitigate risks, ensuring minimal impact on business operations.

Supercharge your SOC with **Wanstor** and the **Microsoft** unified security operations platform

The Microsoft unified security operations offer a comprehensive, AI-powered unified platform for detecting, investigating, responding to, and protecting against cyberthreats across your platforms, clouds, and hybrid infrastructure.

The Microsoft unified security operations delivers a single incident queue, equipped with robust out-of-the-box rules, that saves time, reduces alert noise, and improves alert correlation, delivering a full view of an attack.

Improve security outcomes at machine speed and scale

Microsoft Security Copilot is embedded in the analyst experience, right into the workflow, helping analysts optimise security management and level up their skills. According to Microsoft research, analysts using the solution work, on average, 22% faster, accelerating time to resolution.

Simplify your defence against modern threats

Microsoft Sentinel offers a modern, cloud-native security information event management (SIEM) powered by AI, automation, and the deep understanding Microsoft has of the threat landscape. Customers get a complete SecOps solution at a fraction of the cost and hassle of standalone SIEM and security orchestration automated response solutions.

We take the pressure off your team – our experts handle security so you can focus on growth. This reduces the need for in-house security resources, which can be costly and hard to find.

Defence with a host of key capabilities to stay ahead of attackers, so you can:

1

Rapidly respond with prioritised incidents in a unified queue

Wanstor's security solutions and the Microsoft unified security operations correlate native signals across multiple-platform endpoints, hybrid identities, email, collaboration tools, software-as-a-service apps, and DLP insights. AI-generated decoys and lures help you coordinate defence across security layers and prevent attackers from reaching critical assets, disrupting the kill chain in the early stages, and automating responses to significantly reduce dwell time.

Stay ahead of advanced attacks

By bringing together the full capabilities of SIEM, XDR, exposure management, generative AI, and threat intelligence, security teams gain unified, comprehensive features that work across use cases, not security tool siloes.

Additionally, to make sure automations help you respond even faster, XDR and SIEM support near real-time custom detections.

Enable a data-centric SOC with DLP signal

Integrating DLP alerts into the incident investigation experience gives your SOC analysts an entirely new way to prioritise, based on the sensitivity of affected data.

The Microsoft unified security operations reduce mean-time-to-respond by

88%

Total Economic Impact™ Of Microsoft SIEM And XDR

78
trillion signals

synthesised daily,
using sophisticated
data analytics and AI
algorithms to
understand and
protect against
digital threats and
criminal
cyberactivity

Wanstor's security solutions and the Microsoft unified security operations platform take advantage of the XDR signal and AI-driven detection capabilities to identify advanced attacks like ransomware, providing automatic response at the incident level with automatic attack disruption that disables or restricts devices and user accounts used in an attack—stopping progression and limiting impact.

Scale your SOC team with automatic containment of affected assets

Harnessing the power of XDR and AI helps disrupt advanced attacks like ransomware, business email compromise, and adversary-in-the-middle attacks with automatic attack disruption, a game-changing technology that remains exclusive to Microsoft Security. Attack disruption automatically stops the progression and limits the impact of the most sophisticated attacks in near real-time.

Build efficiencies on the industry's widest insight into attack vectors

Microsoft Security has visibility into more threat vectors than any other vendor. When paired with the Microsoft natively integrated XDR platform and SIEM, SOC teams have better real-time protection against sophisticated threats and can respond more quickly.

We help you optimise the SIEM, XDR, and GenAI capabilities of the Microsoft unified security operations platform, maximising your return on investment

3

Unified XDR security and identity access management

Wanstor and Microsoft combines identity protection capabilities from our industry-leading identity access and management platform and our XDR solution, providing a single integrated experience for protecting identities and defending against threats. This powerful combination offers capabilities such as conditional access, built directly into the identity platform Microsoft Entra ID. Combined with XDR, it protects hybrid-user and workload identities, as well as the underlying identity infrastructure.

Create operational efficiencies and reduce cost

Wanstor's security solutions and the Microsoft unified security operations platform offers one solution for protecting identities on-premises and in the cloud, and it combines those signals with all the other sources for the full XDR view of the attack kill chain. It's a cost-effective approach to consolidating vendors, delivering industry-leading identity and XDR capabilities in a single package.

Gartner named Microsoft a Leader in the 2022 Gartner® Magic Quadrant for Endpoint Protection Platforms

Microsoft, "Microsoft is named a Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms," March 2, 2023.

We have deep knowledge and extensive experience in deploying the Microsoft unified security operations to help you address complex security challenges.

What businesses are saying



ING uses Microsoft 365 Defender to reimagine banking for a digital audience. The IT team can now better recognise phishing attempts and block them right from the start, building on its own intelligence by using query data to identify additional risks.

“

A single layer of detection isn't strong enough and is prone to some level of false positive... On the other hand, Microsoft 365 Defender correlates signals across endpoints, email, documents, identity, apps, and more.

We consider it a game-changer that Microsoft 365 Defender combines signals for threat hunting because it connects data from the identity and endpoint perspectives to pinpoint truly malicious events.

— Krzysztof Kuźnik, Product Owner at ING

G&J Pepsi-Cola Bottlers used Microsoft 365 Defender, to expand its security over after recovering from a ransomware attack in 2021. Microsoft 365 Defender is uniquely able to help detect and respond to such ransomware threats.

Having a strong security posture focused on protecting physical security and the security of devices, identities, and data is critical to company stability and were key components to a successful defence against cyberattacks.

— Eric McKinney, Enterprise Infrastructure Director at G&J Pepsi-Cola Bottlers



What businesses are saying

Summary

Wanstor and the Microsoft unified security operations provide comprehensive security that spans identities, endpoints, email and collaboration, cloud apps, data, and hybrid and cloud infrastructure. Utilising the platform, security teams gain SIEM, XDR, exposure management, and generative AI, delivering an integrated approach that delivers better protection, efficiency, and resiliency.

Defender XDR, the only XDR that combines a leading identity and access and management platform with its XDR solution, protects identities and defends against threats, consolidating costs with a single vendor. Sentinel delivers an intelligent and comprehensive solution for SIEM with cyberthreat detection, investigation, response, and proactive hunting, for a bird's-eye view across your enterprise.

Security Copilot provides end-to-end support for analysts from summaries of incidents and response, to assessment of incident impact, to actionable recommendations for faster investigation and remediation.

Get the threat protection you need today

We have a robust security practice, along with the expertise you need to assist you with every stage of your security strategy.

Whether you need an assessment, help with licensing, or managed services, we can deliver the security solutions you need to succeed.

Let's get your security sorted. Talk to us today and take the first step toward smarter protection.

Contact us