wanstor

Automatically detect and disrupt cyberattacks

Microsoft Security

Cyber threats are increasing in volume and sophistication

Ransomware attacks	200%	Increase in human-operated ransomware attacks
Business email compromise (BEC) attacks	156K	Increase in BEC attacks from 2022 to 20231
Adversary-in-the-middle (AitM)	4K	Identity attacks blocked per second

How to protect your organisation

Stop attacks with an integrated, unified security operations platform from Wanstor and Microsoft.

- Prevent attacks across your multiple-platform, multi cloud environment
- Detect and defend against threats across your systems
- Investigate and respond faster with generative AI

The Microsoft unified security operations platform with **Wanstor** brings together the full capabilities of SIEM, XDR, exposure management, generative AI, and threat intelligence, empowering your security teams with a unified solution that works across your use cases.

Anatomy of a real-life Octo Tempest attack chain

A company uses the Microsoft unified security operations to detect, investigate, and respond to attempt to exfiltrate data, prior to extortion or ransomware operations.

1:52 PM — Self-service password reset

2:00 PM — TA temper victim's MFA

2:04 PM — First login by TA (attributed as Octo Tempest)

2:04–3:26 PM — TA accesses victim's SharePoint + Teams chats

3:05 PM — Microsoft Entra ID IP alert

3:18 PM — Microsoft Defender XDR alert

3:19 PM — Auto IR "disable user" playbook triggered

2:04–3:26 PM — User disabled by Microsoft Defender XDR

As a Microsoft Partner we provide

Comprehensive security management across your environment—identities, endpoints, data, email, cloud apps, and infrastructure. We also help with diverse regulatory, industry, and local requirements. Whether you need an assessment, help with licensing, or managed services, we can deliver the security solutions you need to succeed.

Contact us for more details

info@wanstor.com | www.wanstor.com