BRIEF

/ MXDR and MXDR Elite for Microsoft

LevelBlue

Unified security operations for modern threats

A 24×7 global threat detection and response solution integrated with your Microsoft Security products for faster response across your digital environment.

The landscape of cybercrime has evolved dramatically, presenting significant challenges for cybersecurity.

To defend our organisations, we deploy varying types of security technologies. However, modern cyber-attacks often involve intricate kill chains made up of numerous low-fidelity signals. Correlating these alerts across siloed solutions to gain an enterprise-wide threat view is challenging. This issue is compounded by legacy security tools which were not designed for today's hybrid environments, leading to significant visibility and coverage gaps.

Additionally, the high demand for skilled security professionals often leaves SOCs overwhelmed with a flood of alerts and a backlog of incidents that need investigation and remediation. SecOps teams grapple with disjointed security solutions, lacking the integration, intelligence, and expertise necessary for efficient incident resolution.

Modern tools for modern threats – Microsoft Defender XDR and Microsoft Sentinel

Integrated security technologies from Microsoft Security suite are essential to address these challenges and keep up with the advancement and funding of cyber threat groups.

Microsoft Defender XDR is a unified enterprise defence suite that coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications. This integration provides robust protection against sophisticated attack scenarios in concert with Microsoft Sentinel (SIEM).

By leveraging various Microsoft Security products, Microsoft Defender XDR enables security teams to piece together threat signals to determine the full scope and impact of threats. This integrated solution reveals how threats enter the environment, what they affect, and their current impact.

Cybercrime evolution

A decade ago, cybercrime's economic impact was estimated in the low billions, comparable to the global illicit drug trade. Today, cybercrime is a USD $8 trillion industry, the third largest economy in the world, growing at an alarming rate of 15% annually.

8T+

third largest economy in the world

Enhanced with LevelBlue Managed XDR (MXDR)

Having the right modern tools is only part of the equation. The other part that's needed is high-quality experts, proven SecOps process, dynamic content, and relevant adversarial threat intelligence to put organisations ahead of today's sophisticated threats.

LevelBlue MXDR for Microsoft services offer 24×7 global security operations with extended detection, investigation, threat hunts, and response across Microsoft Security products:

- Microsoft Sentinel
- Microsoft Defender XDR
  - » Defender for Endpoints
  - » Defender for Identity
  - » Defender for Cloud Apps
  - » Defender for Office 365
- Copilot for Security
- Microsoft Native and External Data Sources

LevelBlue MXDR for Microsoft service integrates with your deployment of Microsoft Sentinel and the Microsoft Defender XDR suite. This integration enables LevelBlue to take native response actions in Defender XDR for swift and effective response to security incidents across your digital environment.

LevelBlue's thorough investigation process and effective response actions aim to disrupt complex threats across the attack chain soon after detection. LevelBlue is also the first in the industry to offer accelerated investigation and response capabilities within our client's deployment of Microsoft Copilot for Security for faster resolution of threats.

LevelBlue Microsoft Security Advisors

LevelBlue MXDR for Microsoft services include preventative configurations to maximise your organisation's defensive posture and minimise overall threat exposure leveraging the Defender XDR's proactive capabilities.

Additionally, LevelBlue Microsoft Security Advisors (MSA) will enhance your team and provide co-management activities – continuous technical advisory, preventative configuration reviews, dynamic emerging threat content, customisation, and more – to maintain an optimised deployment. The MSA also conducts regular Microsoft Security and Exposure Score reviews to help you prioritise your team and mature your overall security posture.

LevelBlue MXDR for Microsoft offers a comprehensive approach to your cybersecurity mission, providing your organisation with the expertise required to actively combat the modern cyber threat.

Features

- 24×7 global threat monitoring, threat hunting, investigation, and response
- Effective, native Defender XDR response to disrupt complex threats
- Layered threat detection with SpiderLabs threat intelligence
- SpiderLabs threat research and reverse engineering
- Proven preventative configurations and continuous tuning LevelBlue Microsoft Security Advisors
- Microsoft Security and Exposure Score reviews
- Defender XDR Security Assessments

Unlock the full power of Microsoft Security with LevelBlue, and maximise your investment, reduce complexity, and boost your SecOps team's productivity with a unified stance.

Benefits

- Azure Benefits Eligible
- Maximise value from your Microsoft investments
- Eliminate active threats 24×7, globally
- Disrupt complex threats across the attack chain
- Enhance your team of Microsoft Security Advisors
- Accelerate productivity of your security operations team
- Reduce complexity and boost security posture
- Unlock the full value of Microsoft Security
- De-risk transition with rapid time-to-value
- Layer detection with SpiderLabs unique threat intelligence and research
- Accelerate security outcomes with a recognised cybersecurity leader

Your cybersecurity partner

We understand the importance of rapid time-to-value while mitigating transition risks. LevelBlue will be your objective advocate for the right technology solutions within your existing heterogeneous and homogenous environments, ensuring seamless integration and interoperability.

If you have a Microsoft licence, both Microsoft Defender XDR and Microsoft Sentinel may already be available to you as part of your security product entitlements. LevelBlue can help you understand and unlock the full value of your security entitlements under any Microsoft licence.

Let LevelBlue be your trusted partner in securing your digital landscape, today and into the future.

Microsoft credentials and certifications

LevelBlue is endorsed and validated by Microsoft as a leading cybersecurity partner:

- Microsoft Verified Managed XDR Solution
- Microsoft Copilot for Security Partner
- Microsoft Intelligent Security Association (MISA) Member
- Certified Microsoft AI Cloud Solutions Partner
- Microsoft AI Cloud Partner Programme Solution Partner for Security with a Cloud Security and Threat Protection Specialisation

LevelBlue

Contact us www.levelblue.com