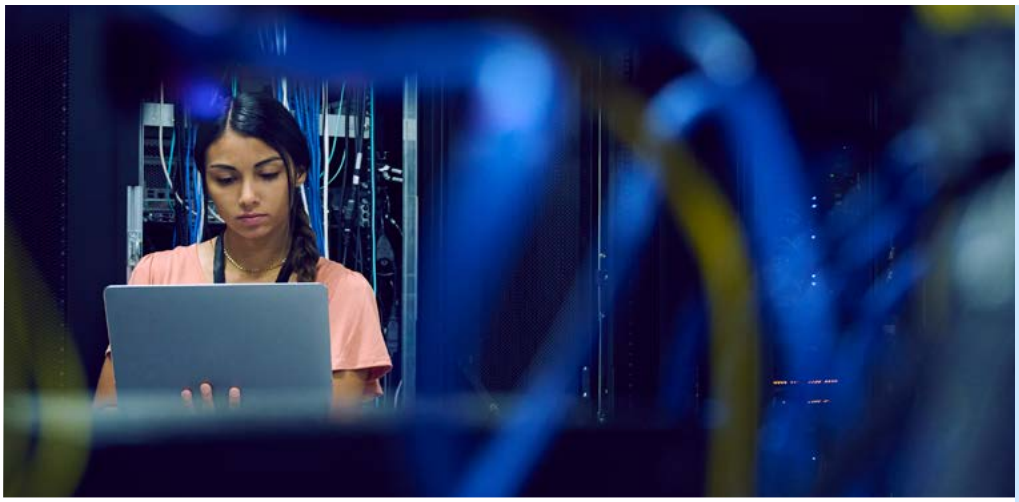
LevelBlue

PRODUCT BRIEF / MAY 2024

LevelBlue Managed Threat Detection and Response

Protect your business with 24x7 threat detection and incident response from LevelBlue



Start detecting and responding to advanced threats sooner with LevelBlue.

To defend against modern cyber threats, organizations must be able to constantly monitor their critical networks and devices on premises, in the cloud, and in remote locations to identify and contain potential threats before they cause harm. Yet, a truly effective threat detection and response program is difficult to achieve. Most organizations do not have the time, resources, or expertise to do so on their own. LevelBlue can help.

With LevelBlue Managed Threat Detection and Response, we can help you detect and respond to advanced threats and exposed risk to protect your business and your brand. A sophisticated managed detection and response (MDR) service, it provides threat management in one turnkey service, including 24 x 7 proactive security monitoring, alarm validation, and incident investigation and response. With it, you can quickly establish or augment your threat detection and response strategy while helping reduce cost and complexity.

LevelBlue Managed Threat Detection and Response combines decades of experience in managed security services, our Unified Security Management® (USM) platform for threat detection and response, and LevelBlue Labs threat intelligence to deliver an unrivaled MDR solution.

Potential benefits:

- Help protect your business with highly effective threat detection and incident response services
- Gain centralized security visibility across your critical cloud and on-premises environments
- Move towards your security and compliance goals faster with less complexity and greater cost efficiency
- Protect your security investment with a solution that scales and adapts to your changing business and IT environment

Product features:

- 24 x 7 security monitoring by a dedicated LevelBlue SOC team
- Built on LevelBlue's award-winning unified security management (USM) platform
- LevelBlue Labs delivers continuous threat intelligence to help keep your defenses up to date
- Security orchestration and automation helps to streamline and accelerate response
- Response support extends to change management with other LevelBlue managed security services
- Threat Model Workshop conducted by LevelBlue Consultants

LevelBlue

Built on unified security management

LevelBlue Managed Threat Detection and Response takes advantage of our award-winning USM platform. Unlike other managed detection and response solutions that may be based primarily on a SIEM log management or endpoint detection and response (EDR) tool, the USM platform combines multiple security capabilities that are essential for effective threat detection and response in one unified console.

Key capabilities include asset discovery, vulnerability assessment, network intrusion detection (NIDS), endpoint detection and response (EDR), SIEM event correlation, and long-term log management, incident investigation, compliance reporting, and more. With these capabilities working in concert, the USM platform is able to provide broader threat coverage and deeper environmental context than point solutions alone, helping to enable early detection, reduce false positives, and streamline incident investigations.

Fueled with LevelBlue Labs threat intelligence

LevelBlue Managed Threat Detection and Response is fueled with continuous threat intelligence from LevelBlue Labs, so your defenses are up to date and better able to detect emerging threats. LevelBlue Labs, the threat intelligence unit of LevelBlue, produces and delivers timely, tactical threat intelligence directly to the USM platform.

LevelBlue Labs has visibility into the LevelBlue Labs Open Threat Exchange (OTX™), and other sources of threat data. This team goes beyond simply delivering threat indicators to performing deep, qualitative research that provides insight into adversary tools, tactics, and procedures (TTPs). By identifying and understanding the behaviors of adversaries, LevelBlue Labs helps power resilient threat detection, even as attackers change their approach and as your IT systems evolve.

Managed 24 x 7 by our SOC experts

Building on decades of experience in delivering managed security services to some of the world's largest and highest-profile companies, the LevelBlue Security Operations Center (SOC) has a dedicated team of security analysts who are solely focused on helping you to protect your business by identifying and disrupting advanced threats around the clock.

The LevelBlue Managed Threat Detection and Response SOC analyst team handles daily security operations on your behalf so that your existing security staff can focus on strategic work.

Responsibilities include:

- 24 x 7 proactive alarm monitoring, validation, and escalation
- Identifying vulnerabilities, AWS® configuration errors, and other areas of risk
- Incident investigation
- Response guidance and recommendations
- Orchestrating response actions towards integrated security controls (BlueApps)
- Reviewing your security goals regularly and providing recommendations on policy updates and additional security controls
- Implementing changes in response to identified threats within other LevelBlue services managed by the LevelBlue SOC

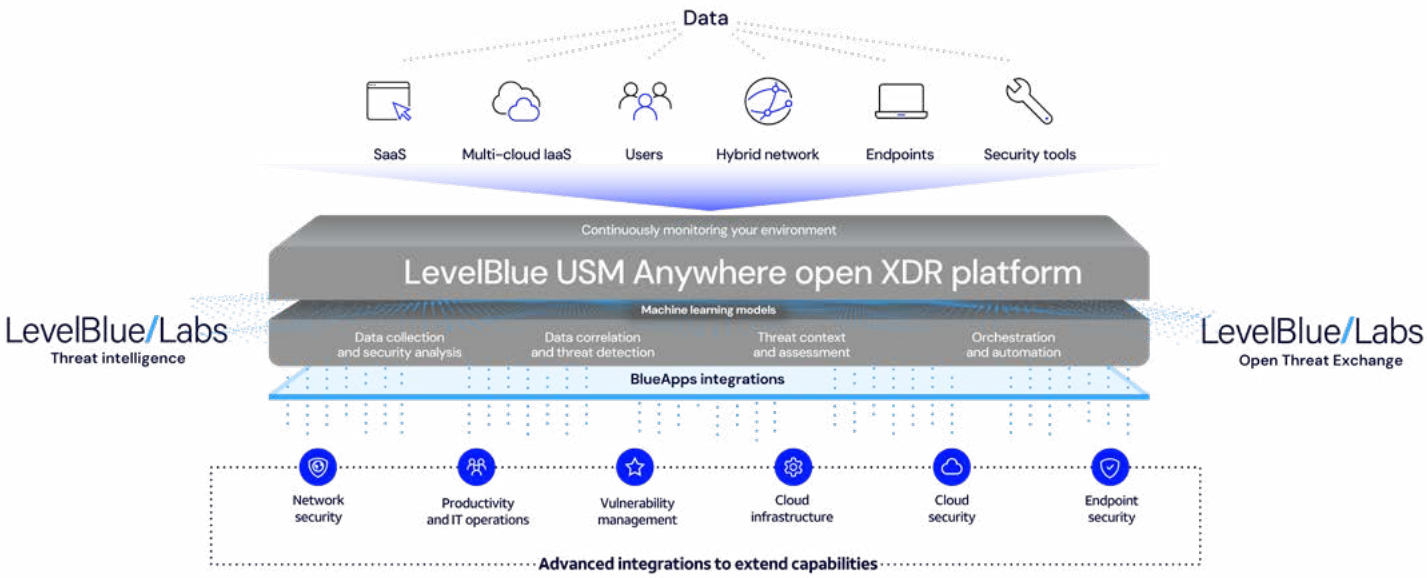
High touch service delivery

Deployment is fast and simple, thanks to our high-touch service delivery model and a modern SaaS platform deployment model. Within 30 days of signing the contract, our SOC analysts can be monitoring your critical infrastructure and responding to threats according to your individualized Incident Response Plan. Onboarding includes:

- Threat Model Workshop conducted by LevelBlue Consultants
- Installation, configuration, and tuning of your USM Anywhere to meet your requirements
- Integrate with other security technologies that are in scope of our BlueApp Framework
- Development of a custom Incident Response Plan in collaboration with your security team
- Training your personnel on the LevelBlue USM Anywhere platform

How it works

LevelBlue managed detection and response services



LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us to learn more, or speak with your LevelBlue sales representative.