LevelBlue

PRODUCT BRIEF

LevelBlue Managed Threat Detection and Response

Protect Your Customers with 24/7 Threat Monitoring and Management

LevelBlue PARTNER PROGRAM

LevelBlue

As a LevelBlue partner, your customers trust you to safeguard their businesses from sophisticated cyber threats. This means constantly monitoring across their attack surface to identify and contain threats before they cause harm. Yet, a truly effective threat detection and response program is difficult to achieve. In fact, many partners do not have the resources or expertise to do this on their own. LevelBlue Managed Threat Detection and Response (MTDR) can help you ensure that your customers' businesses are protected around the clock.

LevelBlue MTDR combines years of experience in managed security services with a proprietary open XDR platform and award-winning LevelBlue Labs threat intelligence to help our partners quickly scale to provide 24/7 services.

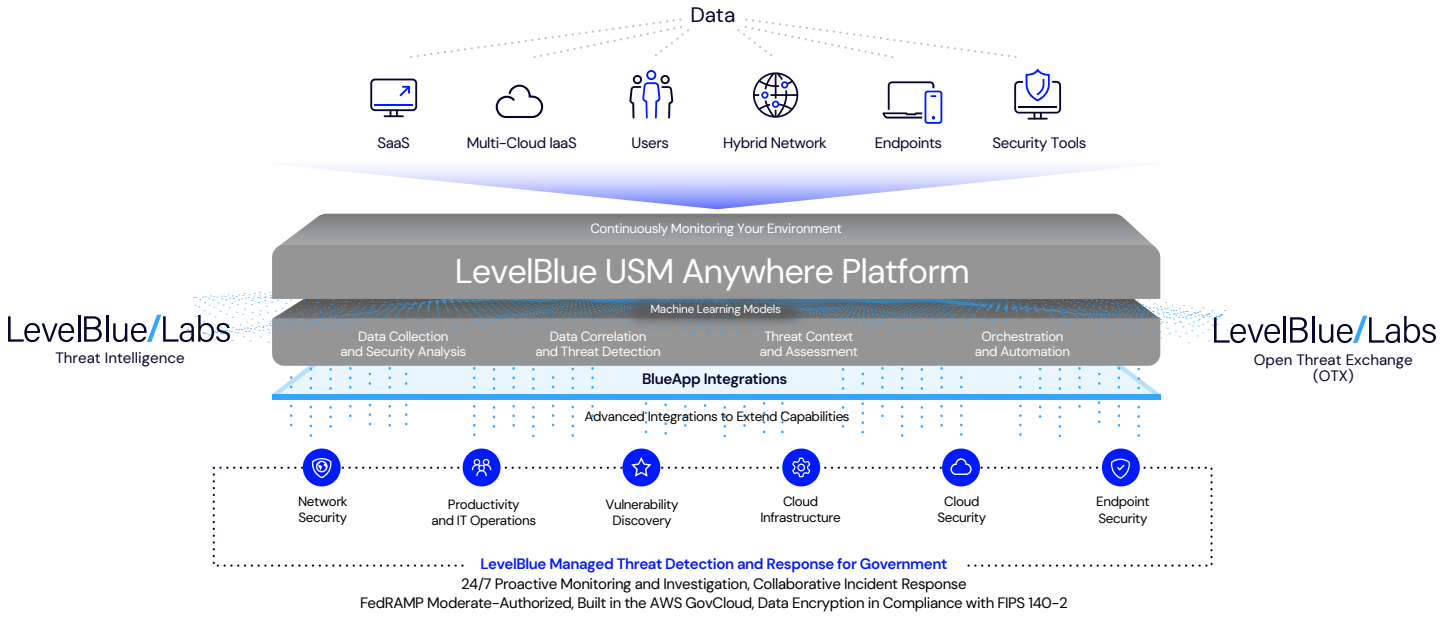
The service provides sophisticated threat management that includes 24/7 proactive security monitoring, alarm validation, and incident investigation and response.

Benefits

- **Expertise and experience**
- **24/7 threat monitoring and management**
- **Highly scalable platform accommodates changing business needs and provides one centralized view into threats**
- **Continually updated threat intelligence powered by in-product machine learning**
- **Deep integrations with hundreds of leading third-party security and productivity tools**
- **Automated and orchestrated response actions for faster response times**
- **Build stronger relationships with your customers**

LevelBlue

Extending Detection and Response Across the Attack Surface



Our managed services are built on top of LevelBlue's proprietary open XDR platform, USM Anywhere.

USM Anywhere continuously monitors across the customer's environment, collecting, correlating, and analyzing data from multiple sources. The data is provided in one view to give LevelBlue analysts the centralized visibility they need to understand what's happening in near-real-time.

The cloud-based platform readily scales to accommodate changing IT environments and business needs. It combines advanced analytics, powerful security orchestration and automation capabilities and built-in threat intelligence for faster, more accurate detection of threats and coordinated, efficient response.

USM is also highly extensible, using powerful integrations known as BlueApps to extend detection and orchestration capabilities to hundreds of third-party security and productivity tools. In addition to the standard BlueApps functionality, Advanced BlueApps offer even more robust automation and orchestration capabilities. Advanced BlueApps collect and enrich log data, perform threat analysis, and provide workflow that coordinates response actions with third-party applications to provide security orchestration, allowing your IT team to take immediate action directly from the USM platform.

Examples of Advanced BlueApps

- Akamai
- Check Point
- Cisco
- CrowdStrike
- Fortinet
- G-Suite
- Lookout
- Microsoft
- ServiceNow
- SentinelOne
- Palo Alto Networks
- Qualys
- Tenable
- VMware
- Zscaler

For a complete listing of Advanced BlueApps, click here: LevelBlue.com/BlueApps

LevelBlue

A high-touch managed service featuring proactive monitoring, in-depth investigations, and guided response to help you detect and respond to threats faster for your customers.

Timely, Tactical Threat Intelligence

The LevelBlue USM Anywhere platform integrates curated threat intelligence from LevelBlue Labs, our dedicated threat intelligence unit. This global team of security researchers and data scientists analyzes thousands of suspicious URLs, files, and threat artifacts daily, using machine learning and proprietary security technology to write and continuously update the platform's more than 2,000 detection rules.

These rules, which provide the context needed to power resilient detection and response are also mapped to the MITRE ATT&CK knowledge base of adversary tactics, techniques, and procedures (TTPs), which is integrated into the USM Anywhere dashboard.

LevelBlue Labs collects and analyzes threat data from many different sources, including from the platform's global sensor network. Advanced security analytics tie together the diverse telemetry feeds so true threats can be quickly and accurately identified (i.e., fewer false positives).

Let Our SOC Experts Help You Protect Your Customers 24/7

Building on years of experience in delivering managed security services to some of the world's largest companies, the LevelBlue Security Operations Center (SOC) is staffed by a team of security analysts who identify and disrupt advanced threats around the clock.

Let the LevelBlue team handle your customer's daily security operations, so you can focus on their strategic work. Our analysts will:

- Perform 24/7 proactive alarm monitoring, validation, and escalation
- Identify vulnerabilities, AWS® configuration errors, and other areas of risk
- Recommend policy updates and additional controls
- Investigate incidents
- Guide response
- Orchestrate response actions for integrated controls (BlueApps)
- Train your team on how to use the LevelBlue platform

Onboarding Your Customers

Our high-touch onboarding ensures that your business can offer LevelBlue MTDR services to your customers within 30 days. As part of the onboarding process, our teams will:

- Offer an optional Threat Model Workshop that's tailored to your customer's security strategy
- Install, configure, and tune the LevelBlue platform to meet customer requirements
- Integrate with security technologies in your service stack that are part of our BlueApp framework
- Collaborate with your team and customer stakeholders to develop a custom Incident Response Plan
- Train your team on how to use the LevelBlue platform

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.