LevelBlue

SOLUTION BRIEF

LevelBlue Managed Detection and Response (MDR)

Evolving Threats and a Lack of Expertise

As cyber attackers find new ways to exploit vulnerabilities and evade detection, organizations of all sizes are finding it more and more difficult to stay ahead of threats. A breach can have devastating financial, legal and reputational impacts. Research published this year indicates that the global average cost of a data breach is now a staggering USD 4.88 million.[1] But most organizations do not have the time, resources, or expertise to manage across their hybrid IT environments and find and respond to threats before they cause damage.

A Suite of Services

LevelBlue is recognized as one of the world's largest security service providers. Our broad portfolio includes a suite of managed detection and response (MDR) services that draws on years of security expertise. We provide our customers with around-the-clock monitoring and management that includes proactive threat hunting, deep integrations with leading endpoint security and vulnerability management tools, and a wide menu of incident readiness and response services.

Benefits

- Expertise and experience
- 24/7 threat monitoring and management
- One centralized view across the attack surface
- Continually updated threat intelligence
- Deep integrations with hundreds of third-party tools
- Automated and orchestrated response actions for faster response times
- Highly scalable platform accommodates changing business needs
- Strategic partnerships with leading endpoint security and vulnerability management tools
- Wide menu of incident readiness and response services

1. IBM Cost of a Data Breach Report 2024

Expertise and Experience

The LevelBlue MDR security operations center (SOC) is based in the US and staffed 24/7 by skilled cybersecurity professionals who use state-of-the-art tools and curated threat intelligence to help you detect and respond to threats before they impact your business.

Our team has years of experience protecting customers across the private and public sectors. They hold multiple industry-standard certifications and US security clearances and have been recruited from top vendors in the industry, as well as from the National Security Agency (NSA) and the U.S. Department of Defense (DOD).

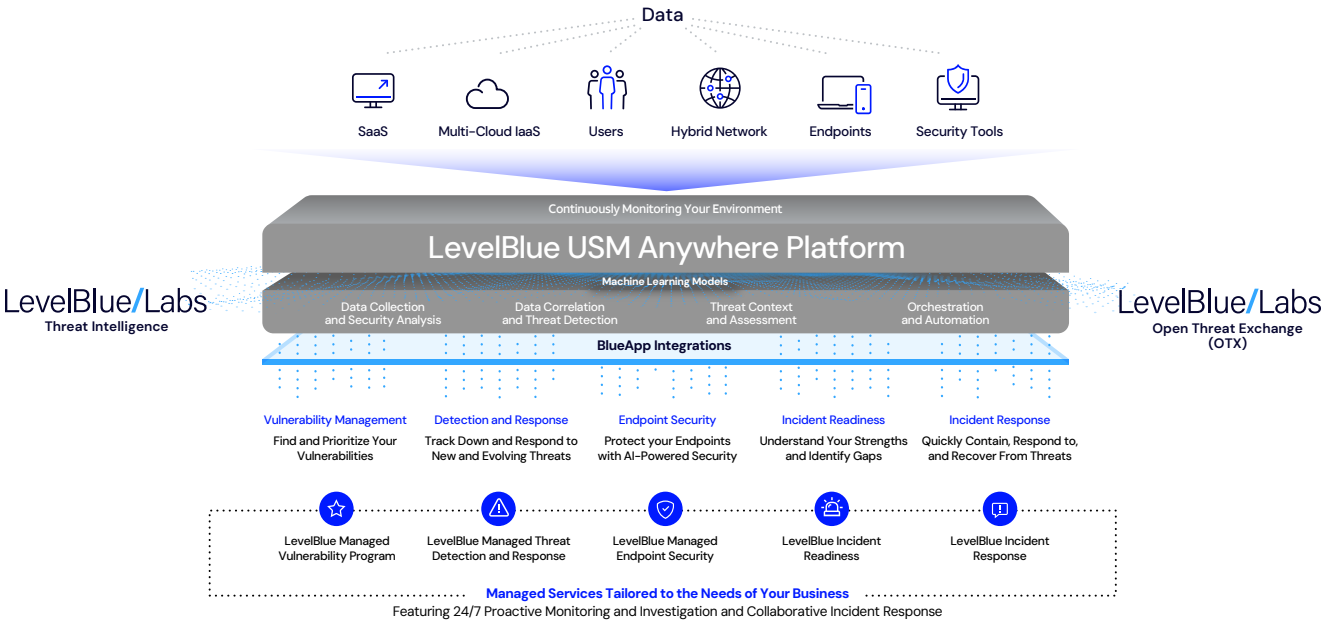
An Extension of Your Team

From initial onboarding and deployment to continuous monitoring, investigation, vulnerability management, and potentially incident response, our team functions as an extension of yours, giving you access to the skills and expertise you need to protect your critical assets.

Our SOC analysts are your first responders. They monitor our customers' environments 24/7, year round. No matter when an incident happens, this team is always on. They review alarms, conduct investigations, and advise on—or even initiate—response and remediation. They also handle day-to-day security operations so your team can focus on more strategic initiatives.

A White-Glove Service That Includes:

- High-touch deployment
- 24/7 threat monitoring and management
- Platform tuning, policy updates
- Proactive threat hunting
- Uncover vulnerabilities, misconfigurations
- In-depth investigations
- Guided response and remediation
- Regular reviews of security goals



Detection and Response Powered by a Proprietary Platform

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 and correlating, and analyzing data from multiple sources and providing it 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 your changing IT environment and growing business needs and 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.

It is also highly extensible; it uses powerful integrations, which we call BlueApps, to extend its detection and orchestration capabilities to hundreds of third-party security and productivity tools. Our advanced integrations include the capability to initiate automated and orchestrated response actions in just a few simple steps.

Timely, Tactical Threat Intelligence

The 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 more than 2,000 correlation rules based on the latest threats.

These rules, which provide context 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).

It also combines this data with threat indicators from LevelBlue Labs Open Threat Exchange (OTX), which is one of the world's largest open threat intelligence communities and currently has more than 450,000 active members.

But the Labs team goes beyond delivering threat indicators. They also perform research that provides insight into attacker tactics, techniques, and procedures, or TTPs, so we can identify and understand attacker behaviors as well as their tools. By understanding what an attacker will do when they come into a network, we can help organizations reduce risk—and respond faster to threats—even when attackers are using zero-day attacks.

The platform's user and entity behavior analytics (UEBA) machine learning models help us predictively identify insider and external threats, such as credential compromise, lateral movement, data exfiltration, and suspicious executions, with higher-confidence alerts and fewer false positives.

Next-Generation Endpoint Technology

Included within the LevelBlue MDR suite is a premium managed service that brings together two world-class technology platforms and the expertise of seasoned cybersecurity professionals. With LevelBlue Managed Endpoint Security with SentinelOne, our SOC analysts can monitor and manage the USM Anywhere and the SentinelOne Singularity platform in one view. Data from SentinelOne endpoint agents is ingested directly into the USM Anywhere platform and enhanced with threat intelligence from LevelBlue Labs to help analysts quickly understand and respond to threats on the endpoint.

Additionally, the deep integration between the two platforms allows for all alarms on the endpoint to be responded to directly from USM Anywhere. A range of automated and orchestrated response actions is available, including a powerful one-click rollback capability that allows users to restore encrypted or deleted files to a known-good state. Other actions include the ability to terminate malicious processes, quarantine suspicious files, delete source code, or disconnect endpoints from the network, and more.

Defend Across a Shifting Attack Surface

We help our customers manage risk by working with them to find and address potential weaknesses across their dynamic attack surface before they can be exploited. Our Managed Vulnerability Program gives organizations access to the skill and technology they need by combining LevelBlue expertise with best-in-class technology from a portfolio of leading vulnerability management vendors.

Organizations need to find and address potential weaknesses across their systems, networks, and applications before cyber criminals can exploit them.

Our managed vulnerability management services include asset discovery and inventory, scanning to determine which critical systems and sensitive information are vulnerable or to assess compliance with internal policies and external regulatory

requirements. We also offer continuous monitoring to identify misconfigurations, file changes, and new assets, automated threat analysis, and more.

Customers can also work on cyber resilience goals by taking advantage of our patch management, penetration testing, and social engineering assessment services.

A Trusted Partner for Incident Readiness and Response

The first few hours after an attack is discovered are critical. We provide support and forensic expertise when you need it most. Skilled incident response (IR) and forensic specialists on the LevelBlue Cybersecurity Consulting team help customers quickly identify, contain, and mitigate incidents that range from employee policy violations to insider threats, malware outbreaks, and external attacks.

In addition, if there is a security event, the SOC team ensures customers have access to immediate and adequate support by providing up to ten hours of courtesy IR per incident. If a customer requires assistance beyond these 10 hours, they can transition to working with our IR and forensic specialists.

LevelBlue also helps customers plan and prepare for incidents. Our incident readiness services help customers understand their strengths and identify where they have security gaps and include services such as custom incident response plans, tabletop and red team exercises, dark web monitoring, malware risk assessments, and more.

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.