LevelBlue

PRODUCT BRIEF / MAY 2024

LevelBlue Extended Detection and Response for MSSPs

Comprehensive visibility and end-to-end threat detection and response capabilities

As cyber actors continue to find new ways to exploit vulnerabilities and evade detection, it is becoming more and more difficult to protect against destructive attacks that result in disruption to business. Security teams today must manage and protect users and devices across networks, endpoints, and cloud environments. But disconnected security tools have resulted in security siloes, and without centralized visibility, security teams lack the context they need to detect, investigate, and respond to potential threats quickly and effectively.

A holistic approach to threat detection and response

Evolving with the needs of the security market, LevelBlue extended detection and response (XDR) for managed security service providers (MSSPs) delivers the end-to-end threat detection and response that business customers want.

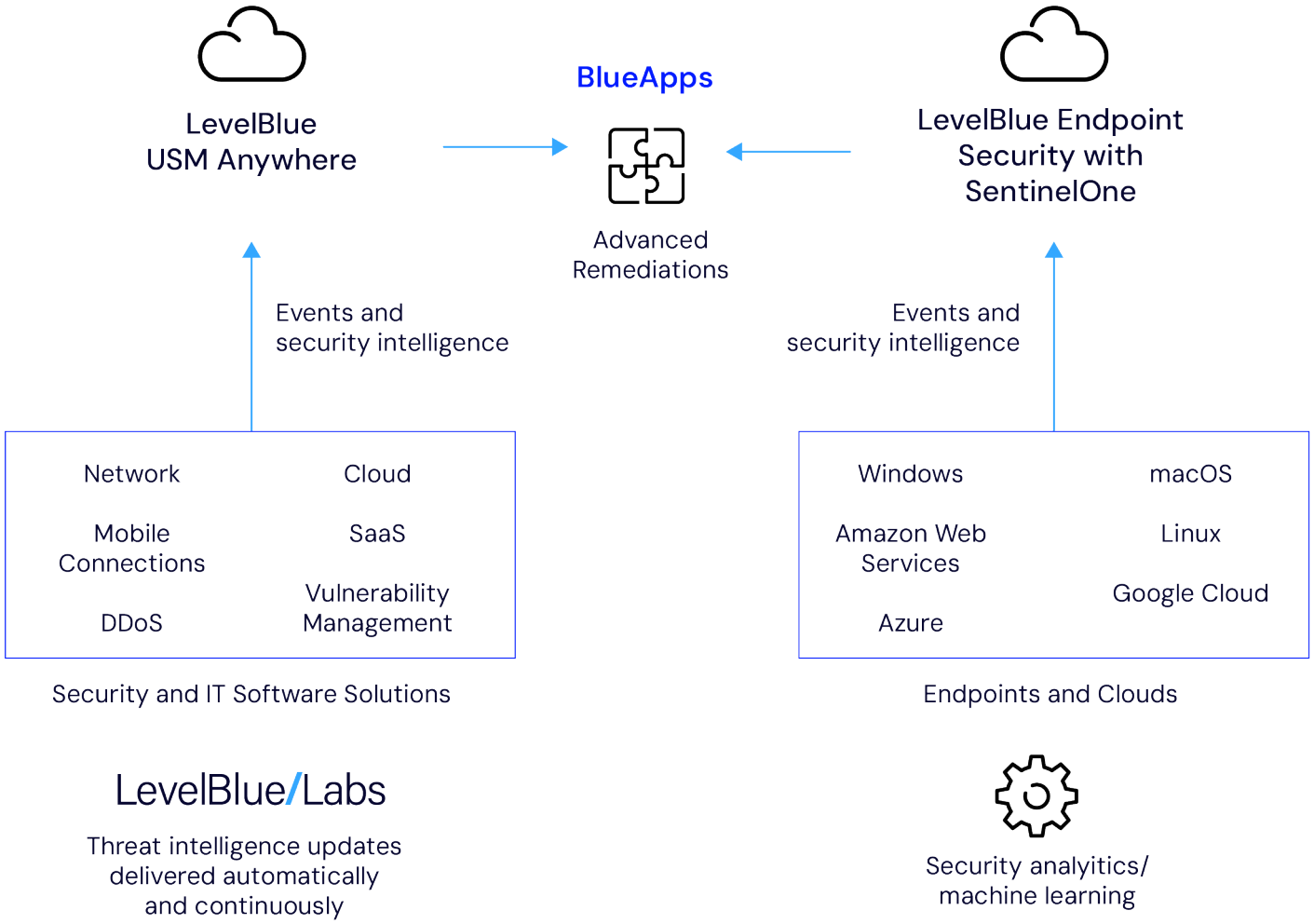
With this XDR solution, you can better protect your customers and ensure their business operates without interruption.

Our solution automatically collects, correlates, and analyzes Information about threats, vulnerabilities, and assets from across the customer's attack surface and provides it to you in one unified view. Not only can you see and take action against threats in your customer's network, but you can also detect and respond to threats such as malware and ransomware on their endpoints.

Our vendor-agnostic, open XDR solution features a wide variety of integrations through the BlueApps framework with industry-leading third-party technologies. In addition to this, the solution incorporates robust threat intelligence via LevelBlue Labs and automated threat detection and response. The LevelBlue USM Anywhere platform's broad, inherent toolset enables security service providers to deliver on their promise to help protect customer networks, endpoints, cloud infrastructure, and cloud applications in an ever-changing security landscape.

Benefits

- Continually updated LevelBlue Labs threat intelligence that utilizes built-in correlation rules for faster triaging of alerts and more efficient identification of threats
- Single pane of glass provides one centralized view into alarms, vulnerabilities, and assets across customer's attack surface
- An open platform that integrates with best-of-breed security and IT tools
- Automated threat detection and response for faster, more efficient incident response
- Extensible platform that can accommodate customers' changing business needs



An open platform that can scale with your business

Our XDR solution employs our award-winning LevelBlue USM Anywhere platform to surface ongoing attacks against the customer's network, both in the cloud and on premises. The platform automates collection and analysis of data across your attack surface to deliver context for faster and more accurate detection of threats and coordinated, efficient incident response. Hosted in our elastic cloud environment, the highly extensible platform readily scales to accommodate your changing IT environment and growing business needs.

Through the BlueApps framework, LevelBlue USM can integrate with a large ecosystem of best-of-breed security and productivity tools for orchestrated and automated incident response.

Identify threats based on behaviors rather than signatures

Through a robust integration with SentinelOne, our XDR solution for MSSPs incorporates next-generation endpoint technology, which includes both endpoint protection and endpoint detection and response (EDR), to help protect against known and unknown threats. The technology autonomously defends

endpoints using machine learning and artificial intelligence (AI)—even when users are working offline and endpoints are not connected to the cloud.

The solution utilizes its integration with SentinelOne to monitor processes in real time and identify threats based on behaviors rather than signatures. Signature-based antivirus, which helps protect networks from known threats, is no longer sufficient to defend against malware, ransomware, and fileless attacks. With our solution, you can uncover abnormal activity and patterns that are consistent with the presence of ransomware.

And you can take automated remediation actions to neutralize threats, such as deleting source code, killing malicious processes, quarantining suspicious files, or even disconnecting endpoints from the network. You can even roll back customer endpoints to a previous clean state without having to reimage machines, restore from external backup solutions, or write scripts.

Fueled with LevelBlue Labs threat intelligence

Our XDR solution brings together your customer's network and endpoint data in one view and enhances it with continually updated tactical information from the LevelBlue Labs threat intelligence team. With this solution, you get the information you need to quickly understand and respond to threats in your customer's environment.

LevelBlue Labs collects and analyzes threat data from many different sources, including the LevelBlue Open Threat Exchange (OTX™), which is the world's largest open threat intelligence community.

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

Award-winning partner program

As industry leaders, we believe it is critical to invest in relationships that accelerate growth, remain cutting-edge, and deliver on customer expectations. We understand your customers rely on your expertise to deliver world-class security solutions, and we work with you to build your business.

Our award-winning MSSP Partner Program is designed to foster profitable and long-lasting relationships. Join us and gain access to industry-leading technology and expertise so you can deliver end-to-end, enterprise-grade cybersecurity solutions.

Partner portal

Develop a meaningful, growth-minded relationship with LevelBlue and receive 24/7 support, access to a partner portal fully equipped with training and co-marketing content, and a dedicated channel account manager.

Through our partner portal, you will receive access to:

- Free trials
- Product and solution resources
- Pricing and quote tools
- Videos, webcasts, and training
- Professional services, support, and forums
- Marketing collateral, blogs, case studies, data sheets, and e-Books

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.

LevelBlue works with you and your team to take your business to the next level. Click here to learn more.