LevelBlue

CUSTOMER STORIES / BINARY DEFENSE

Binary Defense Threat Hunters Use USM Anywhere to Detect and Respond to Threats

About Binary Defense

Binary Defense is a managed security services provider (MSSP) and software developer. Its leading cybersecurity solutions include Security Operations Center (SOC)-as-a-Service, Managed Detection and Response, Security Information and Event Management (SIEM), Threat Hunting, and Counter-intelligence. With its human-driven, technology-assisted approach, Binary Defense provides clients with immediate protection and visibility, combating and stopping the next generation of attacks. The company is headquartered in Stow, Ohio.

Customer Challenge

The goal of a SOC analyst team is to detect malicious behavior before it becomes a major issue. Binary Defense delivers best-in-class SOC services, identifying threats, investigating alerts, and recommending steps to shield against cyberattacks. With eyes-on-glass intelligence scanning for hard-to-find threats, Binary Defense's dedicated SOC analysts monitor security data, prioritize alarms, and notify clients if further investigation is required. Its SOC analysts also provide remediation instructions in the event of a security incident that requires action. To support its vital work, Binary Defense needed a solution to help enable threat detection and response that was easy to deploy, included reporting capabilities, and was able to integrate with their other security and technology tools.

LevelBlue Solution

Binary Defense has built its powerful managed security services offering with LevelBlue USM Anywhere. USM Anywhere is a cloud-native solution that delivers powerful threat detection, incident response, and compliance management in one unified platform. It combines the essential capabilities needed for effective security monitoring across cloud and on-premises environments: asset discovery, vulnerability assessment, intrusion detection, endpoint detection and response, behavioral monitoring, SIEM log management, and continuous threat intelligence. USM Anywhere provides a single pane of glass, so SOC analysts can search for uncommon activity and malicious behavior. Clients benefit from the combination of award-winning LevelBlue technology and threat intelligence and best-in-class Binary Defense service.

- **Business Needs** – Fast-growing cybersecurity firm needed an easy-to-deploy, easy-to-integrate solution to support its MSSP/SOC subscription services.
- **Networking Solution** – Binary Defense relies on USM Anywhere™ from LevelBlue to deliver powerful threat detection, incident response and compliance management in one unified platform.
- **Business Value** – Ability to provide a unified platform; ease of use and deployment helps to reduce resources needed to deploy, administer, and manage the environment.
- **Industry Focus** – Cybersecurity

Quicker Launch Times

USM Anywhere's unified platform, hosted and delivered through the highly secure cloud, helps Binary Defense expedite the onboarding and implementation process for new clients. "The product is pretty straightforward," said Senior Project Manager Heather Stump. "The web UI is easy to maneuver through." Run in a standard web browser, the interface provides access to all LevelBlue USM Anywhere tools and capabilities. The pre-built rules and directives are continuously updated with the latest threat intelligence from the LevelBlue Labs team.

Chief Security Officer Dave DeSimone said the ease of use and deployment and cloud delivery model are two big advantages of USM Anywhere. It offers real value by helping to reduce the number of resources the company needs to expend to deploy, administer, and manage the environment. "Having things that are pre-built obviously makes things go a lot faster and smoother for everyone, which is always an ideal situation," he said. The shift to the cloud has meant Binary Defense can achieve exceptional levels of customization for its customers. "It's kind of like its own little ecosystem maintained and operated by USM Anywhere," he added. There is no additional AWS server license needed to deploy it.

The cloud-based model offers enhanced transparency and visibility. DeSimone said, "Having a platform you can search, run reports from, and gather information as quickly as possible is always a benefit. That's something that has been done fairly well within the application."

When Time is Everything

LevelBlue USM Anywhere helps make Binary Defense's daily operations more efficient. "When I look at a SIEM, I want an alarms page where every single thing that is out there is coming in," said DeSimone. USM Anywhere presents all the information in a single pane of glass, saving the team valuable time. They don't have to look for information in multiple places. "That's where minutes and seconds really add up," he said. "For a security operations center that is also a managed services provider, everything is time bound. Speed and information being readily accessible are definitely key points here." USM Anywhere presents information in an easily digestible format, which is key to the SOC team's ability to triage. With USM Anywhere, analysts can identify false positives quickly, enabling engineers to tune the alarms to more manageable levels.

Binary Defense utilizes many of its own tools in tandem with features installed in USM Anywhere. When conducting a threat investigation, Binary Defense's SOC sends information to the client through a third-party ticketing system, which integrates easily with USM Anywhere. "We've done a lot of custom integrations, and it has worked well for us," said DeSimone. To allow MSSPs to integrate with their own systems, LevelBlue offers a REST API framework that enables MSSPs to customize elements of data in their environment.

A Global Exchange

Binary Defense also uses the LevelBlue Labs Open Threat Exchange (OTX™) for threat intelligence. OTX is the world's largest open threat intelligence community, with more than 235,000 participants from 140 countries.

> "Binary Defense views LevelBlue as an extension of the team. We are all in this for the common goal of helping protect businesses from cyberattacks."
>
> **David White**
> Director of Marketing,
> Binary Defense

The platform's threat data is organized into pulses that provide context about threats. Binary Defense builds customized pulses specific to its clients' needs. OTX users can publish their own pulses and subscribe to the pulse feeds of other users. OTX also includes the ability to create both public and private groups.

DeSimone said Binary Defense makes it a point to discuss OTX with its clients. "We can add custom pulses to provide we are watching for things that are pertinent to a specific client, or for all of our clients to enrich the alarms in the alerts."

Binary Defense helps clients achieve a faster ROI on their SIEM investment because they have experts in their corner who work to understand the environment, as well as deploy and tune the system to provide them with actionable information.

> "The LevelBlue team has been there for us since day one as a resource and an advocate."

Dave DeSimone
Chief Security Officer,
Binary Defense

Shared Values Make LevelBlue an Ideal Choice

The cornerstone of Binary Defense's customer relationship model is the personal experience, so its strong relationship with LevelBlue is important. Collaboration is a key feature of the LevelBlue and Binary Defense strategy for current deployments and future enhancements. "The dedicated account team has been extremely responsive. Just having an actual person we can reach out to with any problem has been a benefit," said DeSimone. "The LevelBlue team has been there for us since day one as a resource and an advocate."

Binary Defense Director of Marketing David White sees value in the relationship. "Binary Defense views LevelBlue as an extension of the team," he said. "We are all in this for the common goal of helping protect businesses from cyberattacks."

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.