LevelBlue

SOLUTION BRIEF / JUNE 2024

Detect Advanced Threats With Endpoint Detection and Response (EDR)

Extend Security Monitoring to the Endpoint with Unified Security Management® (USM)

Today, corporate endpoints represent one of the top areas of security risk for organizations, accelerated by an increasingly mobile and cloud-first workforce.

As malicious actors target endpoints with new types of attacks designed to evade traditional endpoint prevention and antivirus tools, security teams are looking to endpoint detection and response (EDR) solutions for an additional layer of security. However, enterprise EDR solutions often carry high cost and complexity, making it difficult for many organizations to implement EDR successfully.

LevelBlue USM Anywhere takes a different approach by delivering advanced EDR capabilities as part of a unified solution for threat detection, incident response, and compliance. USM Anywhere centralizes endpoint and network security monitoring across cloud and on-premises environments, enabling security teams to detect and respond to threats faster while eliminating the cost and complexity of maintaining yet another point security solution.

The LevelBlue Approach to EDR

LevelBlue USM Anywhere centralizes and automates threat hunting virtually everywhere modern threats appear so you can detect threats earlier and respond faster. Unlike point security solutions, USM Anywhere combines multiple security capabilities into a unified cloud platform, including EDR, security information and event management (SIEM), intrusion detection (IDS), vulnerability assessment, and more, giving you the essential security capabilities you need in a single pane of glass, significantly reducing cost and complexity.

The built-in EDR capabilites in USM Anywhere help:

Incorporate EDR Into Your Security Stack Without Adding Cost or Complexity

While many security teams recognize the need for endpoint detection and response, most do not have the resources to manage a standalone endpoint security solution. USM Anywhere eliminates the cost and complexity of adding yet another cumbersome point solution to your security stack. Instead, you can deploy a single platform that delivers advanced EDR combined with many other essential security capabilities in a single pane of glass, driving up the efficiency of your security operations.

Centralize Security Visibility and Monitoring of All Your Critical Assets

Siloed approaches to security monitoring are less effective and create overhead as your teams must work across multiple systems to investigate and respond to security incidents and to demonstrate compliance. With USM Anywhere, you get complete, centralized security visibility and monitoring of all your critical assets, so you can investigate your security incidents faster with a full context of what's happening on your networks, your endpoints, and your cloud environments.

Automate Threat Hunting and Detect Evasive Threats That Your Antivirus Can't

With the built-in EDR capabilities in LevelBlue USM Anywhere, you can add a layer of security to detect advanced endpoint threats that bypass your antivirus tools. The platform automatically and continuously monitors your endpoints to detect anomalous or suspicious activities that may indicate a compromise.

And, because USM Anywhere receives continuous threat intelligence from the LevelBlue Labs security research team, you can be advised of the latest endpoint threats as they emerge and evolve in the wild.

Monitor Your Workforce on and off the Network

In today's mobile workplace, your users don't stop working when they leave the office, and neither should your threat detection tools. It's essential to have continuous security visibility of your user's activities as they move on and off your corporate network, especially as they remotely connect to your network and cloud environments from insecure Wi-Fi hotspots at hotels, coffee shops, and airports.

With LevelBlue USM Anywhere, you can continuously monitor your user's endpoints and cloud activities virtually anywhere they may roam. The USM Anywere agent offers remote and bulk deployment, making it simple to deploy and manage on your users' laptops. The agent communicates directly with USM Anywhere, so you can continuously monitor your users' off-network activities.

Accelerate Your Compliance Efforts with Built-In File Integrity Monitoring (FIM)

With the built-in EDR capabilities of USM Anywhere, you can accelerate your compliance efforts without having to introduce additional file integrity monitoring (FIM) software. USM Anywhere automatically detects suspicious or anomalous changes to your critical files and registries on Windows and Linux®, as well as your cloud locations like Office 365 Sharepoint and Google Workspace. And, because the platform provides a consolidated view of up-to-date asset information, including running software and services, vulnerabilities, changes made to critical files, security events, and even pre-built compliance reporting templates, you can quickly and easily point to that information during a compliance audit.

How it works

LevelBlue USM Anywhere Agent Deployment and Management

The USM Anywhere agent underpins the EDR capabilities in USM Anywhere, performing continuous endpoint monitoring as part of the unified platform. A lightweight, adaptable endpoint agent based on osquery, the agent is easy to deploy on your Windows and Linux hosts and manage directly from USM Anywhere, so you can avoid having to integrate and manage a third-party agent to achieve endpoint monitoring.

USM Anywhere includes deployment options for Windows and Linux, with scripts for single and mass agent deployments. LevelBlue provides two configuration profiles for the agent. The optimized configuration profile – defined by the LevelBlue Labs security research team – collects only the security-relevant data from your endpoints, so you can get started quickly and maintain a small data footprint. With the full configuration profile, you can collect additional endpoint data, including syslog events.

Endpoint Log Collection

LevelBlue USM Anywhere simplifies security and compliance log management, giving you a centralized, highly secure cloud location to manage your endpoint logs as well as your network and cloud logs. The USM Anywhere agent collects information from your endpoints wherever they are, on or off the network. The agent transmits log data directly to the USM Anywhere platform, so you don't have to worry about the limitations of local storage, such as running out of space or attackers wiping local data to cover their tracks. LevelBlue stores your log data for 12 months, including time-stamped raw logs, in a certified compliant environment.

Threat Detection

USM Anywhere automatically detects advanced endpoint threats, including those designed to evade traditional antivirus tools, using continuous threat intelligence from LevelBlue Labs. The LevelBlue Labs security research team works on your behalf to research emerging and evolving threats in the wild and continuously updates USM Anywhere with the latest actionable threat intelligence, in the form of correlation rules, endpoint queries, and even step-by-step response guidance. This allows you to automate threat hunting activities so that you can focus your resources on incident investigation and rapid response.

USM Anywhere detects modern threats wherever they appear. The unified platform intelligently correlates events from the network, cloud, and endpoints, helping to give you the best position to detect threats early and confidently.

Incident Investigation and Response

When it comes to incident response, speed matters. For example, if you detect malicious activities in your network traffic, such as a host communicating with a

known command and control server, your investigation will likely include querying the host for more information, like a list of running processes and network connections. However, if you have to work across multiple security tools to collect that information and then manually correlate it, it can slow down your investigation and delay your response.

With USM Anywhere, you can investigate and respond to security incidents faster with all the relevant threat information you need in a single pane of glass. Because USM Anywhere consolidates relevant information on every alarm, including the affected asset, its vulnerabilities, related network and endpoint events, step-by-step response guidance, and even direct links to LevelBlue Labs Open Threat Exchange (OTX™) threat intelligence, you can immediately orient yourself to the incident.

LevelBlue USM Anywhere also accelerates your incident investigation and response activities through its advanced security orchestration and automation capabilities. You can proactively query your endpoints at any time to get additional information that adds context to your threat investigations. And, directly from an alarm, you can trigger other forensics and response actions. For example, you can select to shut down or disable networking on an asset, open an issue in ServiceNow® or Jira®, or notify your team through Slack or PagerDuty. With the ability to automate orchestration and response actions, you can work faster and more efficiently to contain threats.

Reporting

USM Anywhere includes a library of pre-built templates that you can use to produce rich reports to meet management requests, support your compliance audit, and/or for daily security operations. At deployment, the platform delivers reporting templates for Windows and Linux file integrity monitoring, which can help to support your PCI DSS compliance efforts. In addition, the pre-built reporting templates for USM Anywhere agent events, including for command history, Docker containers events, login activity, and more, make it simple to get the visibility you need to monitor your endpoints.

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.