eBOOK / JUNE 2024

LevelBlue

Unlock the Promise of Open XDR

Power Up Your Cybersecurity with Managed Extended Detection and Response

LevelBlue

Table of Contents

Evolve Your Threat Detection and Response

One Command Center for Intelligent Cyber Defense

Extended detection and response, or XDR, is a holistic approach to threat detection and response. It helps break down security silos by collecting and correlating network, endpoint, and cloud telemetry from across the attack surface in one centralized location.

XDR:

- Expand visibility and context
- Correlate data from multiple sources
- Use advanced security analytics and machine learning
- Automate and orchestrate security processes
- Simplify reporting

LevelBlue

Keep the Freedom to Implement Best-of-Breed Products

Open XDR Gives You a Vendor-Neutral Platform Unified Under a Centrally Coordinated, Intelligent Home Base

Native XDR solutions require purchase of all components from one vendor, but with open XDR, you can work with security products from multiple vendors.

In an open XDR solution, the core platform provides the central management console. Through it, you can integrate and manage numerous third-party solutions. That means not only can you keep the tools you already have in place, but you also have the flexibility to add or remove tools.

What to Watch For:

Some open XDR solutions will offer more third-party integrations than others – even the most comprehensive open solutions cannot integrate all the tools available in the market.

Integrations can be complex to build and are not always smooth; look for expertise in the provider and seamless functionality.

Open XDR:

- Avoid vendor lock-in
- Integrate smoothly with best-of-breed tools
- No need to rip and replace — can evolve organically
- Flexibility to swap out different technologies

LevelBlue

Find and Neutralize Threats Before They Impact Your Business

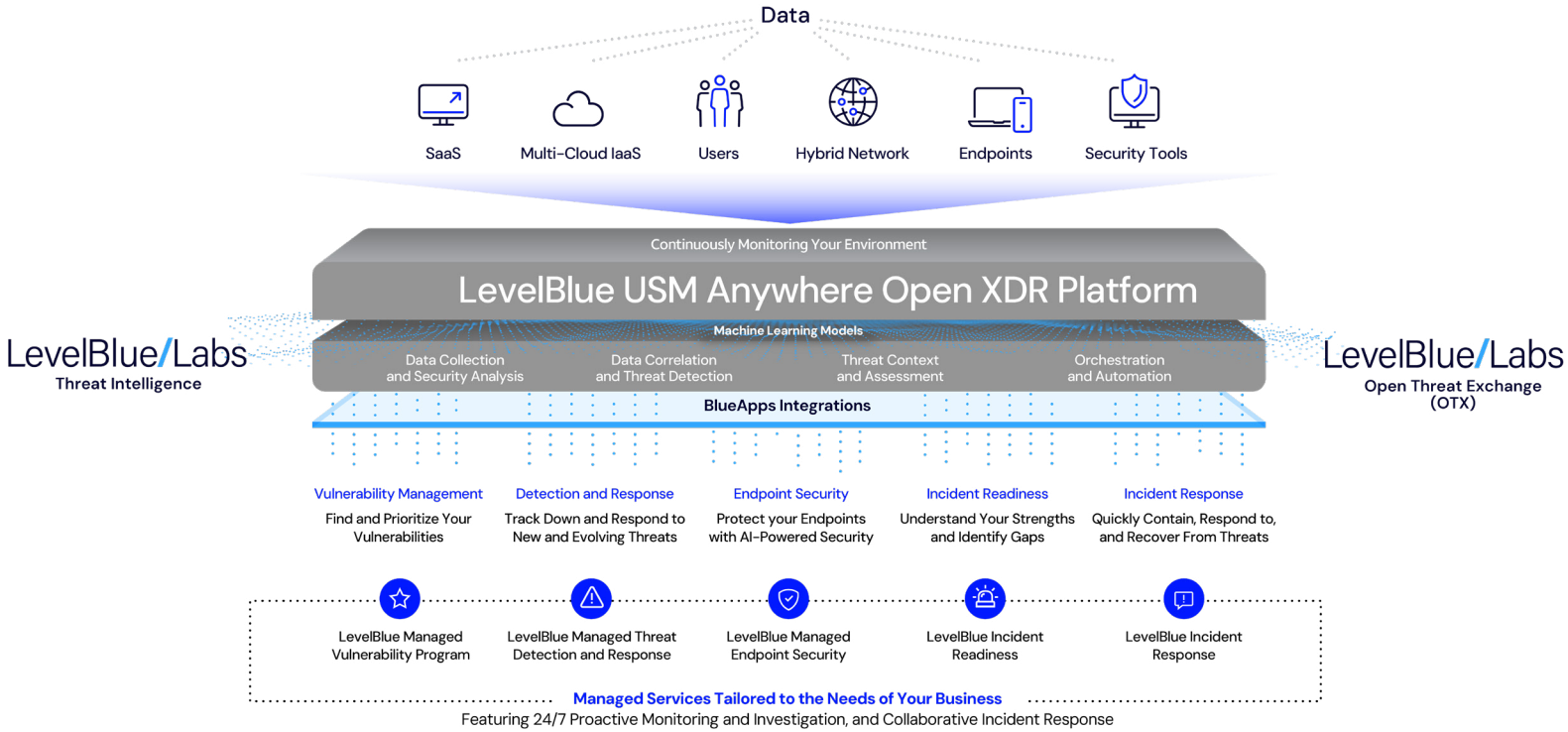
An Ecosystem That Helps You Get More Out of What You Have Already Invested In

Powerful Advanced BlueApp integrations extend our solution's capabilities to a growing number of industry-leading security and productivity tools.

Managed Extended Detection and Response (XDR) combines award-winning threat detection and response capabilities from the USM Anywhere platform with leading endpoint security from SentinelOne.

Protect your business with a comprehensive solution that incorporates advanced security analytics, built-in security orchestration and automation capabilities, and continually updated threat intelligence from LevelBlue Labs.

LevelBlue Managed Detection and Response Services



LevelBlue

Get the Visibility and Context You Need to Protect Intelligently

Multiple Solutions Working as One to Keep Your Network and Data Safe

A managed XDR service helps you protect users, devices, and security tools across your organization with automated and orchestrated response actions that can be executed with just the click of a button.

Protect Your Business from Emerging and Evolving Threats

- Gather and analyze data from across your environment so you can find and respond to threats in your network faster and more efficiently.
- Leverage the technology and expertise of a managed service to gain access to the skills and resources you need.
- Prevent malware and ransomware on your endpoints; perform automated remediation actions with just the click of a button thanks to powerful endpoint security from SentinelOne.
- Address operational challenges and remove security silos with one centralized view into assets and vulnerabilities across your network.
- Embrace digital transformation with a flexible, cloud-based solution that can scale to support your changing business needs.

LevelBlue

We've Got You Covered

Extend Your Threat Detection and Response Capabilities with BlueApps

With BlueApp integrations, you can extend the comprehensive threat detection and response capabilities of the USM Anywhere platform to other security and productivity tools.

What's the difference between a BlueApp and an Advanced BlueApp?

The platform has close to 800 built-in BlueApps that work to translate raw log data into normalized events for analysis.

The more powerful Advanced BlueApps provide bi-directional integration. Not only can they pull in data from different tools, but they can also push orchestration actions to other tools.

"Open XDR is different than conventional detection and response in the sense that it enables our MSSP partners to build solutions based on the platforms their customers already use in order to make the best out of their investments. Partners can also pair the LevelBlue USM Anywhere platform's next-gen SIEM capabilities with SentinelOne endpoint protection to offer industry-leading managed XDR for their customer businesses."

Michael Vaughn
Product Management, Global MSSP and Channel, LevelBlue

LevelBlue

Power Up Your Security with Advanced BlueApps

Get Data Collection with Robust Automation and Orchestration Capabilities in One Platform

Our Advanced BlueApps let you monitor your security posture and orchestrate response actions directly from the USM Anywhere platform.

Every app has a built-in interactive dashboard, so you can visualize your attack surface and receive alerts on possible issues. Our apps collect, correlate, and enrich log data, perform threat analysis, and provide workflow that coordinates response actions with third-party applications.

- **Centralized Monitoring:** Collect data from your network, endpoint, cloud, and SaaS environments to help you respond to threats more efficiently.
- **Advanced Orchestration and Automation:** Define and execute automated investigation and response processes whenever threats are detected.
- **Enriched Data and Analytics:** Receive continual threat intelligence updates from LevelBlue Labs and the Open Threat Exchange (OTX) to help you identify and prioritize immediate threats.
- **Agility:** Easily access new technologies with a flexible architecture that allows for the rapid development and delivery of new Advanced BlueApps.

LevelBlue

Broad Support Across Industry-Leading IT and Security Tools

Expand and Customize Your Defenses with Advanced BlueApps

Endpoint Security	Vulnerability Management	Productivity and IT Operations	Cloud Security	Network Security	Cloud Infrastructure
SentinelOne	Qualys	Jira Software	Akamai	Akamai	aws
SOPHOS	FORTRA	servicenow	FORTINET	FORTINET	Azure
CISCO	tenable	box	zscaler	CISCO	Google Cloud
VMware Carbon Black	**Mobile Security**	Google Workspace	paloalto NETWORKS	paloalto NETWORKS	**Identity**
McAfee	Lookout	Microsoft 365	**Email**	CHECK POINT	SpyCloud
Microsoft 365	ivanti	salesforce	mimecast	CLOUDFLARE	okta
CROWDSTRIKE					

Check out our Advanced BlueApps

LevelBlue

Manage and Defend Your Endpoints

Every desktop, laptop, server, or mobile device can be a vector for attack. Securing the endpoint is often considered an organization's first line of defense.

As attacks have increased, and as attackers have become more sophisticated, the need for more advanced endpoint security has grown. Today's solutions have evolved from traditional antivirus protection to comprehensive tools that use machine learning to protect against ransomware, malware, and zero-day threats.

Integrations

- SentinelOne
- Cisco AMP for Endpoints
- Crowdstrike
- McAfee
- Microsoft Defender ATP
- Mimecast
- VMware Carbon Black
- Ivanti
- Lookout

Use Advanced BlueApps to Detect and Respond to Threats on the Endpoint Directly from the USM Anywhere Platform

- Centrally monitor, aggregate, and analyze events and alerts gathered from all your endpoint products.
- Detect endpoint threats across your on-premises, cloud, and SaaS environments.
- Easily identify your at-risk, business-critical endpoints.
- Trigger manual and automated response actions, such as isolating a compromised device, quarantining a file, or rolling back an infected device to a prior clean state.
- Stay ahead of the latest endpoint threats with continuous intelligence updates from LevelBlue Labs and the Open Threat Exchange (OTX).

LevelBlue

Enable a More Cyber-Resilient Network

The modern network must be secured from the core to the edge, but today's complex network infrastructures are challenging to manage and defend.

On top of that, you face a constantly changing, rapidly expanding threat environment that includes breaches, intrusions, malware, spyware, adware, trojans, botnets, computer worms, and distributed denial-of-service attacks (DDoS).

In addition to these threats, we've seen accelerating cloud adoption, an increasing number of Internet of Things (IoT) connections, and the rapid shift to a remote workforce. To meet these security challenges requires a more agile, automated approach to defending your data and network.

Integrations

- Akamai ETP
- Check Point
- Cisco ASA Firewall
- Cisco Umbrella
- Palo Alto Networks PAN-OS
- Palo Alto Networks Panorama
- Fortinet FortiGate
- Fortinet FortiManager
- Sophos

Use Advanced BlueApps to Detect and Respond to Threats in the Network Directly from the USM Anywhere Platform

- Automatically collect logs.
- Manually or automatically use firewalls or cloud-based firewalls to block malicious IP addresses, compromised internal hosts, and other threats.
- Get visibility into what's happening on your network and identify potential threats.
- Utilize real-time threat intelligence from LevelBlue Labs and the OTX.

LevelBlue

Protect Access to Business-Critical Data in the Cloud

While the cloud facilitates better collaboration and sharing, both of which are essential requirements for today's globally dispersed workforce, cloud platforms are not inherently secure.

Cyber actors are taking advantage of increased opportunities to infiltrate systems and steal data and credentials such as through misconfigured cloud services, inadequate identity and access management controls, APIs that contain security vulnerabilities, and cloud malware.

Secure access to your systems by following security best practices such as using multifactor authentication and implementing least-privilege principles.

Additionally, a next-gen security information and event management (SIEM) platform can detect risky connections from the internet and store logs to help maintain business continuity in the event of a breach.

Integrations

- Zscaler
- Akamai EAA
- Palo Alto Networks
- Fortinet
- Cloudflare

Use Advanced BlueApps to Protect Remote Access to Cloud Applications and Data Directly from the USM Anywhere Platform.

- Collect security event data.
- Trigger alarms when threats are detected.
- Quickly respond to alarms by changing policies directly from the platform.
- Automate detection and response actions, such as blocking users, apps, or IP addresses.
- Show relevant security events from a dashboard in the platform.
- Leverage ongoing threat intelligence updates from LevelBlue Labs and the Open Threat Exchange (OTX).

LevelBlue

Detect and Remediate Vulnerabilities Before They Cause Damage

Businesses need to evaluate and secure their networks with tools that simplify and automate the process of vulnerability management so that vulnerabilities in operating systems, applications, and browsers can be identified and remediated before cybercriminals exploit them. Modern vulnerability management tools provide visibility into assets and vulnerabilities across the attack surface.

Integrations

- Forta
- Qualys
- Tenable

Use Advanced BlueApps to Help Organizations Manage Vulnerabilities Directly from the USM Anywhere Platform.

- Get deep visibility into network assets and their vulnerabilities through active scanning, passive monitoring, and database integrations.
- Combine vulnerability data and threat intelligence to rapidly assess risk and understand which vulnerabilities to fix first.
- Uncover hidden malware artifacts that often go undetected by endpoint monitoring.
- Detect missing or disabled endpoint security tools.
- Protect against cyber actors gaining unauthorized access or control with prioritized remediation and patching recommendations.
- Track dynamic, virtual, and mobile assets.
- Use orchestration actions to scan networks and streamline incident response activities.
- See detailed information on your risk posture in one dashboard within USM Anywhere.
- Get a complete inventory of known and unknown IT assets.
- Get access to continuous tactical threat intelligence from LevelBlue Labs and the Open Threat Exchange (OTX).

LevelBlue

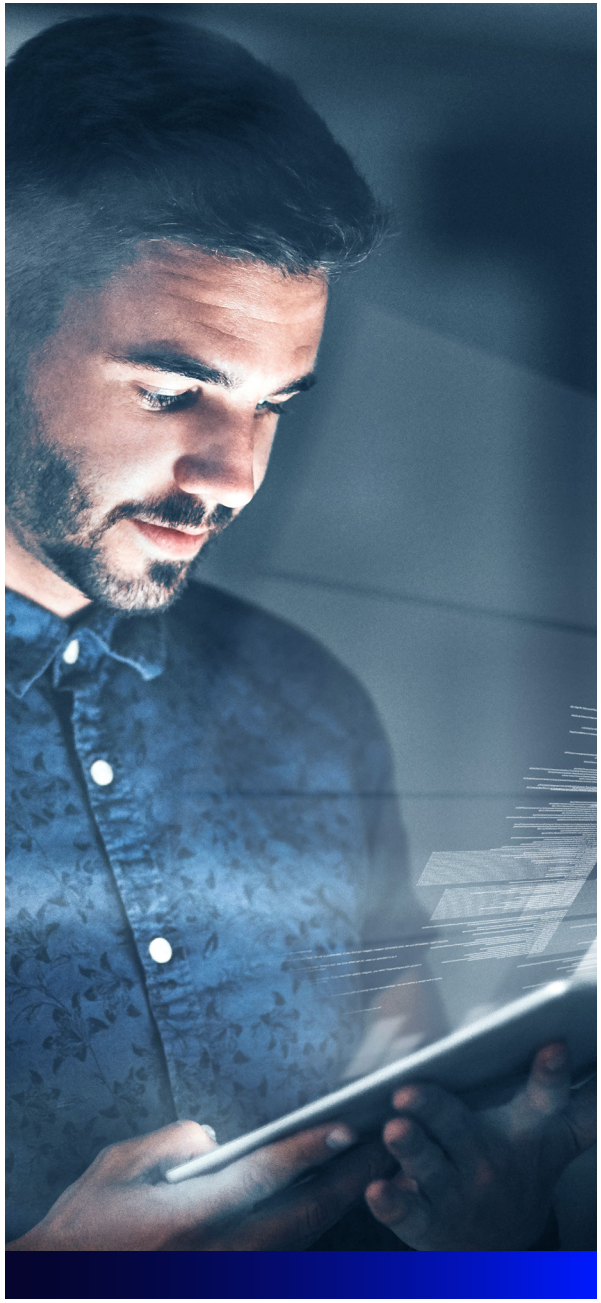
Get Operational Visibility into Your Cloud Infrastructure Environment

The elastic infrastructure of the public cloud is transforming business, but along with this flexibility comes loss of visibility into and lack of control over the data flowing in and out of the cloud.

Organizations must manage security and compliance challenges such as cloud platform misconfiguration, exfiltration of sensitive data, unauthorized access, and insecure interfaces.

Integrations

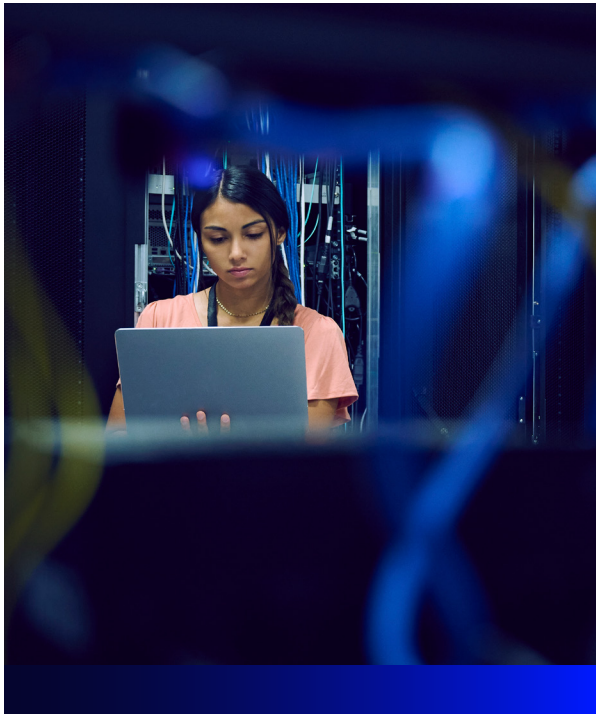
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform



Use Advanced BlueApps to Gain Visibility into Your Public Cloud Environments Directly from the USM Anywhere Platform.

- Get deep visibility into network assets and their vulnerabilities through active scanning, passive monitoring, and database integrations.
- Combine vulnerability data and threat intelligence to rapidly assess risk and understand which vulnerabilities to fix first.
- Uncover hidden malware artifacts that often go undetected by endpoint monitoring.
- Detect missing or disabled endpoint security tools.
- Protect against cyber actors gaining unauthorized access or control with prioritized remediation and patching recommendations.
- Track dynamic, virtual, and mobile assets.
- Use orchestration actions to scan networks and streamline incident response activities.
- See detailed information on your risk posture in one dashboard within USM Anywhere.
- Get a complete inventory of known and unknown IT assets .
- Get access to continuous tactical threat intelligence from LevelBlue Labs and the Open Threat Exchange (OTX).

LevelBlue



Manage Your Business Risk and Easily Integrate with Help Desk Systems

Cloud-based productivity software and applications increase efficiency and facilitate better collaboration and sharing, but they also bring security challenges. Security teams need visibility into administrator and user activities and the assurance that adequate controls are in place to keep corporate data and resources secure.

Integrations

- ServiceNow
- Google Workplace (formerly G Suite)
- Microsoft 365 (formerly Office 365)
- Salesforce
- Jira
- Box
- Connectwise
- Okta
- SpyCloud

Use Advanced BlueApps to Secure Your Productivity and IT Operations Software Directly from the LevelBlue USM Anywhere Platform.

- Track user login activities and identify anomalous login attempts.
- Insert USM Anywhere alarms into cases on help desk platforms to integrate with IT tools for incident response, such as opening a ticket for reimagining of an infected system.
- Get alerts on potential threats such as credential abuse, data exfiltration, brute-force attacks, or malware infection, and launch automated response actions directly from the alarm in the platform.
- Learn about changes to security settings that increase risk exposure, such as disabling multifactor authentication.
- Get alerts on administrator actions, such as account creation or deletion, escalation of privilege, and policy changes.
- Detect policy violations and compromised user credentials.
- Audit user activities at a glance with pre-built, interactive dashboards, such as file editing and deletion, or file sharing with known malicious entities.
- Know when compromised user credentials are discovered on the dark web, and take immediate action to prevent a breach.
- Receive ongoing threat intelligence updates from LevelBlue Labs and the Open Threat Exchange (OTX).

Defend Your Network and Your Data

Leverage the technology and expertise of a managed security service provider to help protect your business around the clock. Get the data from across your attack surface automatically collected, correlated, analyzed, and provided in one view so threats can be found and neutralized before they impact your business.

Learn More About How Managed Security Service Providers Can Help Protect Their Customers.

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.