LevelBlue

LevelBlue USM Anywhere

Unified threat detection and compliance

LevelBlue USM Anywhere delivers unified threat detection, incident response, and compliance management across cloud and on-premises environments.

Complete security visibility

LevelBlue USM Anywhere provides comprehensive visibility across your infrastructure, enabling faster detection, simplified compliance, and elimination of blind spots, all from one platform.

- **Asset Discovery:** API, network, and software or service discovery
- **Vulnerability Assessment:** Network, cloud, and infrastructure scanning
- **Intrusion Detection:** Network and cloud-based detection
- **Endpoint Detection and Response:** HIDS, FIM, and continuous monitoring
- **Behavioral Monitoring:** Access and activity logs across AWS, Azure, and VMware
- **SIEM and Log Management:** Event correlation, log analysis, and integrated threat intelligence from LevelBlue SpiderLabs and OTX

Streamlined detection, response, and analytics

USM Anywhere centralizes detection, response, and analysis across your environment with automation, analytics, and a cloud-native design.

- **Automated Response Orchestration:** Suppress alarm noise, trigger custom alerts, auto-respond to events, and integrate third-party actions
- **Security Analytics:** Search, pivot, and analyze data across assets, vulnerabilities, and events for rapid investigations and compliance reporting
- **Cloud-Native Architecture:** Built in the cloud to leverage API integrations for richer data, faster setup, and complete visibility
- **Graph-Based Correlation:** Run ad-hoc queries and uncover relationships between users, assets, and activities for deeper insight

Scalable and simple by design

LevelBlue USM Anywhere grows with your business needs. Add or remove sensors and agents, expand cloud coverage, and scale log management as your environment evolves without complex upgrades or hidden costs.

- **Flexible Scalability:** Adjust coverage and capacity instantly
- **Simple Subscription Model:** Tiered plans starting at 250GB per month, including support, maintenance, threat intelligence, and cold storage
- **All-in-One SaaS Model:** No separate licensing for features or storage

Expanded orchestration with BlueApps

Extend orchestration through BlueApps integrations with tools like Cisco Umbrella and Palo Alto Networks. Extract and visualize external data, trigger automated actions, and expand capabilities as new BlueApps are introduced.

Integrated threat intelligence

Stay protected with continuous threat intelligence from LevelBlue SpiderLabs and the global OTX community, powered by more than 330,000 researchers contributing over 20 million indicators daily. LevelBlue SpiderLabs curates and validates these indicators to deliver the latest, most relevant intelligence directly into USM Anywhere.

Fast and simple deployment

Deploy lightweight sensors and agents in your cloud or on-premises environment, connect to your USM Anywhere instance, and start detecting threats in minutes. Sensors collect and normalize network, log, and cloud data for centralized analysis and correlation. Agents, built on osquery, extend detection, file integrity monitoring, and EDR capabilities to Windows, Linux, and macOS endpoints.

LevelBlue USM Anywhere Environment