LevelBlue

SOLUTION BRIEF

# LevelBlue Managed Threat Detection and Response for Government

## Resource Constraints Create Security Gaps for Agencies Tasked with Protecting Sensitive Data

Maintaining effective defenses across an increasingly diverse and distributed attack surface is critical, particularly for federal, state, and local government agencies or for companies handling sensitive public sector data. When this data is exfiltrated, it can threaten national security and public safety, disrupt essential services, compromise critical infrastructure, cause significant economic impact, and erode public trust.

But resource constraints, in particular the ongoing global shortage of skilled cybersecurity professionals, continue to create security challenges. These challenges are amplified for government agencies that typically have more limited security budgets than their private sector counterparts.

**Positioned as a Leader in the 2024 IDC MarketScape for U.S. National Government Professional Security Services**[1]

## A 24/7 Managed Service Architected to Protect Sensitive Public Sector Data

LevelBlue Managed Threat Detection and Response for Government (LevelBlue MTDR for Gov) can help you protect highly regulated data and ensure critical services are delivered without disruption. A year-round, 24/7 managed security service, LevelBlue MTDR for Gov offers US-based managed security expertise and a proprietary platform that is certified FedRAMP Moderate to meet regulatory and compliance objectives.

## Key Features

- 24/7 proactive monitoring by LevelBlue Security Operations Center
- FedRAMP Moderate authorization
- Built in AWS GovCloud (US-West region)
- All data encrypted according to US government standards for cryptography in technology products (FIPS 140-2)
- US citizens only support

## Expertise and Experience

With this service, experienced cybersecurity professionals from the LevelBlue security operations center (SOC) augment or complement in-house security teams with proactive security monitoring and management, threat hunting, and incident response.

The service is available to federal, state, and local government entities as well as US-based companies (including Alaska, Hawaii, Puerto Rico, and Guam). It is managed and supported by US citizens only (located in the 48 contiguous United States and the District of Columbia).

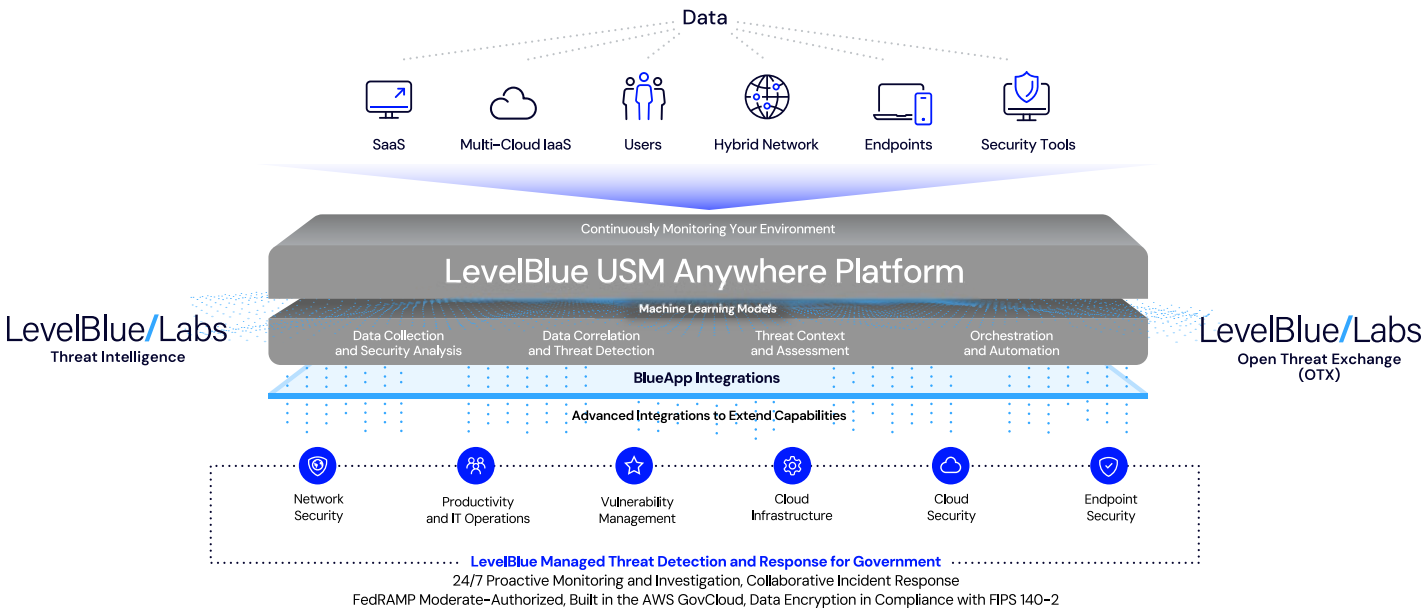
## Customers Receive:

- Hands-on onboarding (we manage the complex and costly technology integrations)
- 24/7 Monitoring, ongoing alarm validation, proactive threat hunting, and integrated threat intelligence
- Rapid, collaborative incident response
- A dedicated point of contact to regularly review and understand their needs and facilitate changes as their environment evolves
- Event and alarm tuning, advisory on risk posture adjustments, address compliance needs or potential capacity adjustments
- In-depth investigation reviews with LevelBlue threat hunters and the customer's incident response team

1. 2024 IDC MarketScape for U.S. National Government Professional Security Services

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 331SB 08-2024

## Built to Address Regulatory and Compliance Requirements




Our analysts have extensive experience utilizing advanced technology to protect data that is subject to government regulations and requirements.

We have personnel with the highest levels of government clearance and have recruited staff from agencies such as the National Security Agency (NSA) and Department of Defense (DoD).

## Centralized Visibility and a Wide Integration Ecosystem

The service is built on LevelBlue's proprietary USM Anywhere platform, which simplifies security operations by providing a single dashboard for our analysts to monitor across the agency's environment. USM Anywhere delivers centralized visibility, advanced analytics, security orchestration and automation, and curated threat intelligence. The platform extends its powerful detection and orchestration capabilities to other leading security and productivity tools through its BlueApps integration ecosystem.

In addition, USM Anywhere can securely manage workloads that contain Controlled Unclassified Information (CUI) and government-oriented, publicly available data across a hybrid attack surface.

**The platform:**

- Authorized at the FedRAMP Moderate impact level to indicate that it has the security controls needed to protect federal data
- Validated against National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 standard, which confirms that it meets specific security requirements, including being production-grade with externally tested algorithms, tamper-evident technology, and role-based authentication
- Stores customer data in the AWS GovCloud (US-West region) to address specific regulatory and compliance requirements, including regional, national, or state data residency requirements

2. Strong third-party test results confirm LevelBlue as XDR leader, p.15

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 331SB 08-2024

> "… broad compliance management, risk assessment and mitigation capabilities."[2]

- Continuously integrates curated threat intelligence from LevelBlue Labs, pulling in enriched threat indicators from the LevelBlue Labs Open Threat Exchange (OTX), a global open threat intelligence sharing community of more than 400K security professionals
- Delivers 2,000+ continuously updated detection rules aligned to the MITRE ATT&CK framework, which is built into the USM Anywhere dashboard

## Evolve to a More Resilient Security Posture

MTDR for Gov helps support SOC modernization initiatives, including augmenting functions for exposure management.

The USM Anywhere platform combines extensive data collection and orchestration capabilities and integrates with industry-leading vulnerability management tools.

LevelBlue also provides a vulnerability and risk management service to help customers find and address vulnerabilities and meet compliance mandates. The service combines the expertise of our security consultants with a portfolio of solutions that includes vulnerability, asset, and patch management as well as threat and risk prioritization.

## Meet Requirements for Risk Identification, Mitigation, and Governance

Organizations handling data that is subject to government regulations and requirements face new and upcoming requirements for reporting on risk identification, mitigation, and governance. This includes US Securities and Exchange Commission (SEC) rules requiring organizations to disclose material cybersecurity incidents and to provide annual disclosures about their cybersecurity risk management, strategy, and governance.

But complying with the additional reporting burdens can create operational challenges for organizations with limited resources. MTDR for Gov gives organizations the tools they need to report on how risk is being identified, mitigated, and governed, so they stay in compliance.

Our SOC teams help customers build reports or will share best practices for creating reports. They will also help customers understand how to use the platform to gather the data they need.

The LevelBlue USM Anywhere platform has several preset compliance templates, including PCI DSS v4:2022, ISO 27001:2022, NIST 800-53, NIST 800-171, and HITRUST, to help customers meet reporting requirements in the case of an incident. Custom reports can also be created from standard or custom dashboards, alarms, events, and custom event filters and attached to investigations, produced in PDF or CSV format, downloaded, or emailed directly from the platform.

## A Partner for IRR Planning and GRC

Often, government agencies have gaps in their incident readiness and response (IRR) planning that put them at risk. Partnering with a service provider can give them the broader IRR coverage and advanced vulnerability management they need to better manage their risk.

LevelBlue Cybersecurity Consulting has years of experience providing a wide menu of services to help organizations identify and address security gaps, improve resiliency, address governance, risk, and compliance (GRC) challenges, and meet unique government mandates with less complexity and greater cost efficiency.

> "… high-fidelity threat detection, correlation, and classification"[3]

3. Strong third-party test results confirm LevelBlue as XDR leader, p.2

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 331SB 08-2024

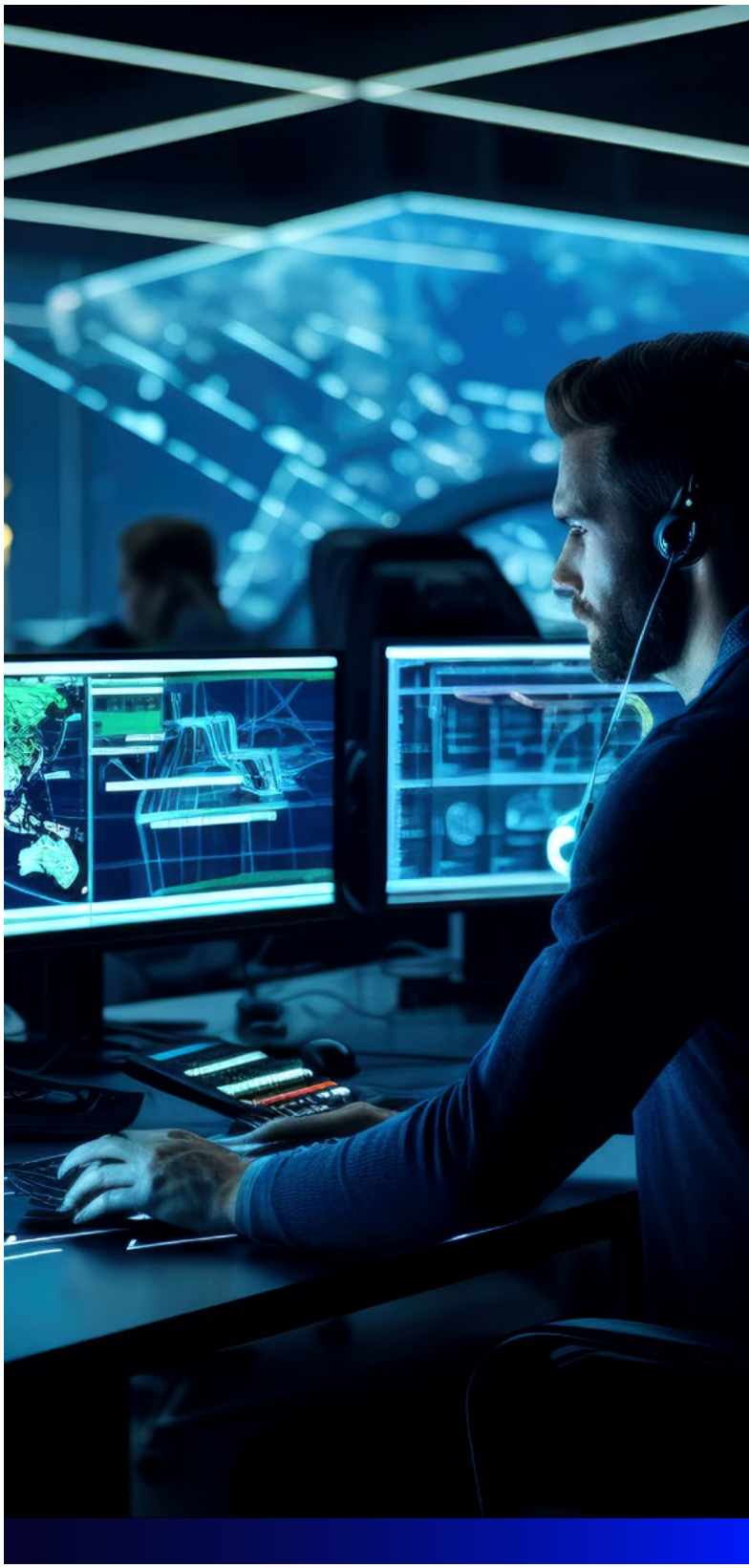
## Externally Validated Technology

The LevelBlue USM Anywhere platform was recently evaluated in third-party extended detection and response (XDR) testing, and the results firmly validate our claims about its capabilities. The platform achieved an overall score of 96.3% for its capability to accurately detect threats, provide context for attacks, and respond to incidents.

The platform demonstrated that it is highly effective at filtering out noise to produce relevant, actionable alarms (99.98%) and at accurately identifying non-malicious traffic, i.e., resistance to false positives (100%).

The platform also scored very well when assessed on its time to detect and attack dwell time metrics. Throughout the evaluation, both metrics were essentially the same (less than or equal to one hour), indicating no significant gap in time between when the platform detects an attack and when it triggers an alarm.

**NOTE:** LevelBlue also offers threat detection and response built on our FedRAMP Moderate-authorized platform as a self-managed service: *LevelBlue Threat Detection and Response for Government.*



© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 331SB 08-2024

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.**

**Contact us to learn more, or speak with your LevelBlue sales representative.**

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 331SB 08-24