LevelBlue

PRODUCT BRIEF / MAY 2024

Provide Agency Mission Success with Threat Detection and Response

LevelBlue

LevelBlue Threat Detection and Response for Government is built on our FedRAMP-authorized, industry-leading USM platform, which combines multiple essential security capabilities and enables fast deployment and broad visibility across your whole environment.

Due to the sheer volume of sensitive data, the aggressive posture of nation-state threats, and the need to support critical infrastructure, the public sector is one of the most susceptible to digital risk. As departments and agencies go through a digital transformation to modernize legacy systems and embrace cloud computing, the need for effective security monitoring is more significant than ever. LevelBlue Threat Detection and Response for Government is purpose-built to meet the evolving security needs and challenges of governmental entities.

LevelBlue Threat Detection and Response for Government is FedRAMP-authorized at the Moderate Impact Level and built on our award-winning Unified Security Management (USM) platform, which combines threat detection, incident response, and compliance management. Featuring built-in integrations with other IT and security tools, our single-pane-of-glass view provides visibility across your environment, both on-premises and in the cloud. LevelBlue Threat Detection and Response for Government is faster to deploy and easier to use than other threat platforms, allowing your security teams to begin discovering threats sooner.

LevelBlue Threat Detection and Response for Government helps to reduce risk and protect data from advanced threats, enabling agencies to focus on their mission.

Multiple essential security capabilities in a single SaaS platform

LevelBlue Threat Detection and Response for Government provides multiple essential security capabilities in a single SaaS solution, providing a single pane of glass for threat detection, incident response, and compliance management. With LevelBlue Threat Detection and Response for Government, you can focus on finding and responding to threats, not managing software.

A flexible, cloud-based security solution, LevelBlue Threat Detection and Response for Government can readily scale to meet your threat detection needs as your IT environment changes and grows.

Asset discovery

- API-powered asset discovery
- Network asset discovery
- Software and services discovery

Vulnerability assessment

- Network vulnerability assessment
- Cloud vulnerability scanning
- Cloud infrastructure assessment

Intrusion detection

- Network Intrusion Detection (NIDS)
- Cloud intrusion detection

Endpoint detection and response

- Host-based Intrusion Detection (HIDS)
- Continuous endpoint monitoring and proactive querying

Behavioral monitoring

- Asset access logs
- Cloud access and activity logs (Microsoft Azure® Monitor, AWS®: CloudTrail®, CloudWatch, S3, ELB)
- AWS VPC Flow monitoring
- VMware® ESXi access logs

SIEM and log management

- Event correlation
- Log management with log retention for the subscription term
- Incident response
- Integrated threat intelligence from the LevelBlue Labs security team and the LevelBlue Labs Open Threat Exchange (OTX™)

© 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. | 095-PB 05-2024

Key product features and highlights

Helping to protect your data

LevelBlueThreat Detection and Response for Government builds on the existing security measures of the USM platform with additional security, including:

- FedRAMP Moderate authorized
- Built in the AWS GovCloud
- All data is encrypted in accordance with FIPS 140-2
- U.S.-based support
- NIST 800-171 compliance

Centralized security monitoring for your cloud and on-premises environments

LevelBlue Threat Detection and Response for Government gives you powerful threat detection capabilities across your cloud and on-premises landscape, simplifying security monitoring, and helping you eliminate security blind spots. As you modernize your infrastructure and migrate workloads and services to the cloud, you have the benefit of virtually seamless security visibility.

LevelBlue Threat Detection and Response for Government monitors:

- AWS, Microsoft Azure, and Google Cloud Platform™ commercial environments
- AWS GovCloud, Microsoft Azure Government, and Google Cloud Platform™ government environments
- Cloud applications like Office 365 and G-Suite™
- Windows, Linux®, and macOS endpoints in the cloud and on premises
- Virtual on-premises IT on VMware / Hyper-V
- Physical IT infrastructure in your data center
- Other on-premises facilities

Stay ahead of the latest threats

LevelBlue Threat Detection and Response for Government is fueled with continuous threat intelligence from the LevelBlue Labs security research team, so your defenses are up to date and better able to detect emerging threats. LevelBlue Labs, the threat intelligence unit of LevelBlue, produces and delivers timely, tactical threat intelligence directly to the USM

platform, so you always stay up to date without having to conduct your own research or write your own correlation rules or queries.

Additionally, LevelBlue Labs utilizes community-sourced threat intelligence from the OTX. OTX is the largest crowd-sourced threat intelligence exchange in the world, providing security research for you that is powered by a global community of threat researchers and security professionals. LevelBlue Labs analyzes raw OTX data with a powerful discovery engine that is able to granularly analyze the nature of the threat, and a similarly powerful validation engine that continually curates the database and certifies the validity of those threats.

© 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. | 095-PB 05-2024

LevelBlue

Automated response orchestration

LevelBlue Threat Detection and Response for Government provides advanced security orchestration rules that automate actions and responses according to your needs, making your work more efficient. You can:

- Reduce alarm 'noise' with suppression rules
- Generate alarms based on custom parameters
- Auto-respond to events with orchestration rules
- Create orchestration rules for third-party apps

Built natively in the cloud for the cloud

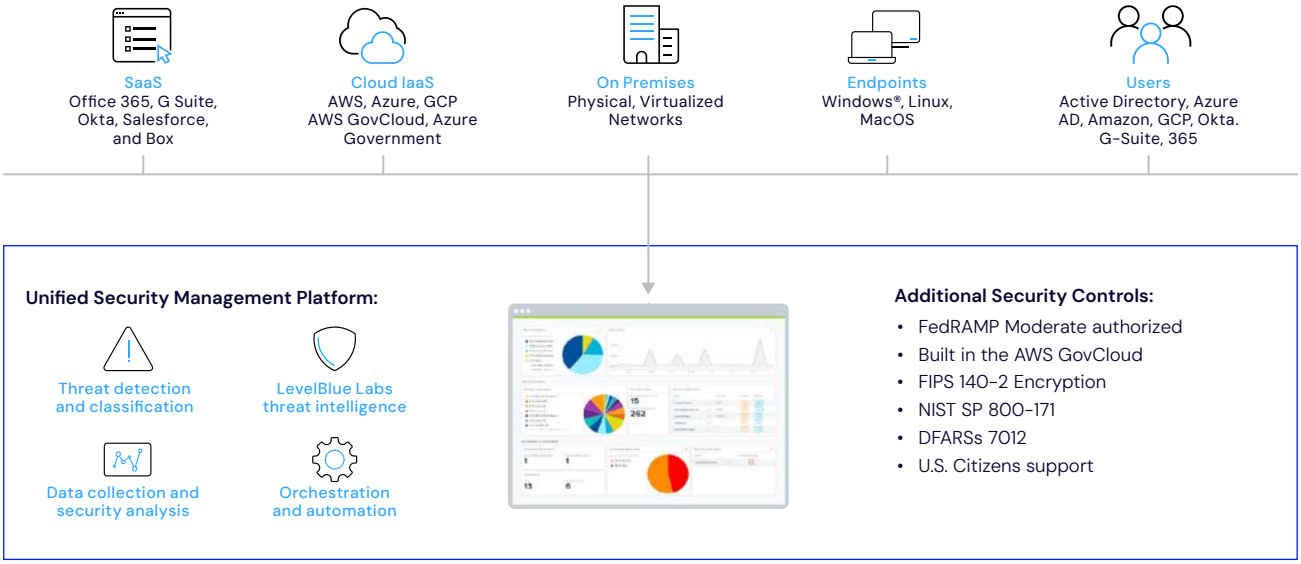
Unlike other legacy security solutions that have been modified to work in the cloud, LevelBlue Threat Detection and Response for Government is a truly cloud-native security monitoring solution that utilizes the additional security capabilities of the government cloud infrastructure. It uses direct hooks into cloud APIs to give you a richer data set, greater control over the security of your cloud infrastructure and SaaS applications, and more immediate visibility across your entire environment which may be as early as within minutes of installation.

Extended security orchestration with BlueApps

LevelBlue Threat Detection and Response for Government is built on our highly extensible USM platform that utilizes BlueApps—integrations with third-party security and productivity tools—to extend your security orchestration capabilities. With BlueApps, you can:

- Extract and analyze data from third-party security applications
- Visualize external data within LevelBlue Threat Detection and Response for Government's rich graphical dashboards
- Push actions to third-party security tools based on threat data analyzed by LevelBlue Threat Detection and Response for Government
- Gain new security capabilities as new BlueApps are introduced into LevelBlue Threat Detection and Response for Government

How does it work?



To learn more about how LevelBlue Threat Detection and Response for Government can help reduce your risk and protect your data, contact your sales representative or visit our website.

© 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. | 095-PB 05-2024

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.

© 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. | 095-PB 05-2024