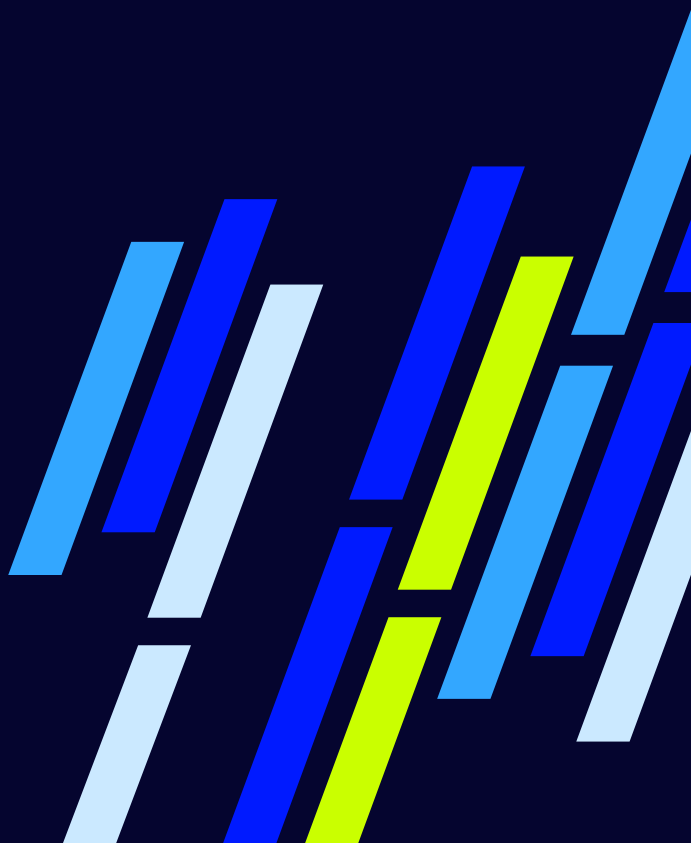
LevelBlue

SERVICE GUIDE

FCC Cybersecurity Pilot Program

LevelBlue Eligible Services



LevelBlue

Table of Contents

Advanced/Next-Generation Firewalls

Equipment and services that implement advanced/next-generation firewalls, including software-defined firewalls and Firewall as a Service, are eligible. Specifically, equipment, services, or a combination of equipment and services that limit access between networks, excluding basic firewalls that are funded through the Commission's E-Rate program, are eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

FEATURES	AVAILABLE IN LEVELBLUE SERVICE
Advanced Threat Detection and Prevention	Yes
AI/ML Threat Detection and Response	Yes
Application Awareness and Control	Yes
Cloud-Delivered Threat Intelligence	Yes
Comprehensive Network Visibility Software-defined Firewalls	Yes
Deep Packet Inspection (DPI)	Yes
Distributed-Denial-of-Service (DDoS) Protection	Yes
Firewall as a Service (FWaaS)	Yes
Integrated Intrusion Prevention Systems (IPS)	Yes
Internet of Things (IoT) Security	Yes
Intrusion Prevention/Detection	Yes
Malware Detection	Yes
Network Segmentation	Yes
Patch Management Systems	Yes
VPN	Yes

Network Based Firewall and Premises Based Firewall Services

LevelBlue offers managed firewall services including on-prem and network-based firewalls. LevelBlue's firewall services are fully managed and easily scalable to any environment. LevelBlue's firewall solutions provide app usage visibility, intrusion prevention and antivirus, logging, and reporting functions. Our firewall services include the installation, configuration, and 24/7 support from LevelBlue cybersecurity experts.

SSE (Security Service Edge)

LevelBlue helps organizations design, implement, and manage resilient network security solutions that help ensure safe access to the web, cloud services and private applications. We can tailor each solution to the unique needs of your customer through a full suite of security services delivered using the industry's top SSE platforms.

Security Services Edge (SSE) incorporates four main security components used to protect business systems and workforce. These capabilities are cloud-based to support distributed systems and workforce. SSE capabilities include the following:

- **Zero Trust Network Access (ZTNA) –** Provides segmentation of organization systems and users through access control policies.
- **Firewall as a Service (FWaaS) –** Centralized security policy enforcement that can be applied across multiple locations to give security greater visibility into the network traffic and provide consistent policy enforcement across systems and users.
- **Secure Web Gateway (SWG) –** Centralized web-based policy enforcement that blocks unapproved Internet traffic while protecting the distributed workforce.
- **Cloud Access Security Broker (CASB) –** CASB enforces and unifies security policies when users access cloud-based resources, ensuring data protection and compliance while providing secure access to services.

SASE (Secure Access Service Edge)

LevelBlue helps organizations to design, realize, and manage a converged network and security architecture that help ensure safe access to the web, cloud services and private applications. Combining security with SD-WAN enables intelligent, secure routing that keeps users safe while load-balancing connections across the network. Incorporating SD-WAN allows for fast speeds and low-latency access to data and work apps. LevelBlue tailors each solution to the unique need of the customer through a full suite of security services delivered using the industry's top SASE platforms.

Secure Access Service Edge (SASE) combines the four main security components

of SSE with a deployed Software-Defined Wide Area Network (SD-WAN) network to provide better network performance, greater security visibility, and a better overall user experience.

The components of SASE are:

- **Software-Defined Wide Area Networking (SD-WAN)-SD-WAN** improves network traffic management by moving away from hardware and premises to next-generation software in the cloud.
- **Zero Trust Network Access (ZTNA) –** Provides segmentation of organization systems and users through access control policies.
- **Firewall as a Service (FWaaS) –** Centralized security policy enforcement that can be applied across multiple locations to give security greater visibility into the network traffic and provide consistent policy enforcement across systems and users.
- **Secure Web Gateway (SWG) –** Centralized web-based policy enforcement that blocks unapproved Internet traffic while protecting the distributed workforce.
- **Cloud Access Security Broker (CASB) –** CASB enforces and unifies security policies when users access cloud-based resources, ensuring data protection and compliance while providing secure access to services.

Vendors we use to deliver these services:

- Palo Alto Networks
- Fortinet
- Checkpoint
- Zscaler

DDoS Mitigation

DDoS security solutions from LevelBlue help protect network infrastructure and internet-facing properties from being ambushed with DDoS attacks. LevelBlue provides a comprehensive and flexible suite of DDoS solutions with reactive and proactive controls that re-route volumetric DDoS attacks before they disrupt your customer's organization. With more than 20 years of proven DDoS mitigation, LevelBlue provides 30 globally distributed cloud scrubbing centers, over 20 Tbps of dedicated defense capacity, customized service-level agreements (SLAs) with response times below one second during an attack, and always-on or on-demand mitigation solutions based on the organization's requirements. Our global DDoS operations team uses proactive defensive controls to monitor the environment 24/7, reducing the organization's attack surface and decreasing time to mitigate.

Our DDoS services come in four variations:

- **Level Blue Reactive DDoS Defense –** This service is on demand where a customer calls the Security Operations Center to initiate a mitigation. It protects US-based internet circuits up to 1GB only (no most of world). Access to DDoS portal is included.
- **LevelBlue Proactive DDoS Defense –** This service provides 24/7 monitoring and is available in several mitigation options: Manual, Pre-Authorized, Platform Initiated Mitigation (PIM), and Emergency. It protects US-based dedicated internet circuits. Access to DDoS portal included and 15-minute response times.
- **Level Blue Prolexic DDoS –** Proven always-on DDoS defense to protect data centers/carrier hotel, SD-WAN branch locations, and cloud against large, complex attacks, and minimize threats to sensitive data. It protects carrier agnostic circuits with a global footprint including US, EMEA, APAC, and LATAM internet circuits.
- **Emergency DDoS Defense –** We offer emergency mitigation through DDoS Defense and Prolexic DDoS for customers who are actively under a DDoS attack and do not have DDoS protection.

Vendors we use to deliver this service:

- Arbor
- Radware
- Akamai

Microsegmentation with Guardicore

LevelBlue Guardicore offers network insight at depth that helps customers visualize network activity, implement precise and relevant microsegmentation policies, and detect possible breaches quickly. Guardicore prevents and contains lateral movement and malicious attacks by enforcing zero trust across the customer's environment. Segmenting network assets helps protect and isolate critical workloads and application in the event of a cyber-breach, such as ransomware.

Zero Trust Readiness Assessment

With LevelBlue's Zero Trust Readiness Assessment, our team of experts will execute a prescriptive delivery methodology to provide a technology roadmap to modernize an organization's Zero Trust architecture. The team will consider optimization of the current technical estate as well as augmentation and/or refresh of the current environment with technologies and solutions emerging/maturing in the marketplace. Examples of these technologies include Secure Access Service Edge (SASE), Software-defined, Automation and Cloud.

Endpoint Protection

Equipment and services that implement endpoint protection are eligible. Specifically, equipment, services, or a combination of equipment and services that implements safeguards to protect school- and library-owned end-user devices, including desktops, laptops, and mobile devices, against cyber threats and attacks are eligible.

Eligible equipment and services may include the following features, substantially similar features or their equivalents:

FEATURES	AVAILABLE IN LEVELBLUE SERVICE
Anti-Malware	Yes
Anti-Ransomware	Yes
Anti-Spam	No
Anti-Virus	Yes
Endpoint Detection & Response (EDR)	Yes
Extended Detection & Response (XDR)	Yes
Insider and Privilege Misuse	No
Privileged Access Management	No
Secure Sockets Layer (SSL) Inspections	No
Target Intrusions	No
Web Application Hacking	Yes

Managed Endpoint Security

LevelBlue delivers advanced endpoint detection and response (EDR) with continuously updated threat intelligence to identify, investigate, and respond to threats across desktops, laptops, servers, virtual machines (VMs), and cloud containers. Customers benefit from a fully managed service with 24/7 monitoring and threat hunting delivered by the LevelBlue SOC.

Vendors we use to deliver this service:

- SentinelOne (MES)

Unified Endpoint Management (UEM) and Mobile Threat Defense (MTD)

LevelBlue offers unified endpoint management (UEM) and mobile threat defense (MTD) solutions to manage and protect corporate data and applications on mobile devices. LevelBlue partners with leading vendors to deliver advanced mobile security that identifies, isolates, and remediates threats targeting mobile devices. LevelBlue offers 24/7 help desk support and a remote administration service for UEM to provide proactive recommendations and ongoing consultation on UEM design, implementation, and administration. UEM and MTD solutions are co-managed with 24/7 help desk and a remote admin service for UEMs.

Vendors we use to deliver this service:

- Omnissa/VMware Workspace One (UEM)
- Ivanti Neurons for MDM (unmanaged)
- IBM MaaS360 (unmanaged)
- Mobile Security with SentinelOne (unmanaged)
- Lookout Mobile Endpoint Security (unmanaged)
- Ivanti Blue (UEM and MTD bundle, unmanaged)
- IBM Security MaaS360 Threat Management (unmanaged)

Web Application and API Protection (WAAP) Services

LevelBlue provides a comprehensive and flexible suite of web application and API protection (WAAP) services, including App and API protection, API Security, Bot Management, Client Reputation, and Client-Side Protection and Compliance. Protect against volumetric distributed denial of service (DDoS), automated botnets, injection, and API-based attacks to defend the customer's network and applications. Validate legitimate client behavior to protect against credential abuse, card balance checking, and other forms of web fraud. Protect against end-user data exfiltration and shield websites from JavaScript threats.

Vendors we use to deliver this service:

- Akamai

Identity Protection and Authentication

Equipment and services that implement identity protection and authentication are eligible. Specifically, equipment, services, or a combination of equipment and services that implements safeguards to protect a user's network identity from theft or misuse and/or provide assurance about the network identity of an entity interacting with a system are eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

FEATURES	AVAILABLE IN LEVELBLUE SERVICE
Active Countermeasure Tools	No
Cloud Application Protection	Yes (DDoS and WAAP, Segmentation)
Cloud Services	Yes (WAAP)
Credential Stuffing	Yes (WAF)
Content Blocking and Filtering/URL Filtering	Yes (SSE and Email Security Solutions)
Content Caching Systems and Service	No
Customer Portal Services	Yes (DDoS and WAAP)
Digital Identity Tools	No

FEATURES	AVAILABLE IN LEVELBLUE SERVICE
Distributed-Denial-of-Service (DDoS) Protection	Yes
DNS/DNS-Layer Security, Blocking, and Filtering	Yes (Firewall, SSE)
Email and Web Security	Yes
Identity Governance & Technologies	No
Intrusion Detection Systems (IDS)	Yes
Logging Practices / Event Logging	Yes (MDR, Firewall, SSE)
Network Access Control	Yes
Offsite/Immutable back-ups	No
MFA/Phishing-Resistant MFA	No
Patching	Yes
Password Spraying	No
Privileged Identity Management	No
Products with TPM Chips	No
Secure Access Service Edge (SASE)	Yes
Secure-By-Design Equipment and Services	Yes (WAAP/PCI Compliant)
Security Information and Event Management (SIEM)	Yes (MDR and WAAP)
Security Updates	Yes
Single Sign-On (SSO)	Some (SSE & WAAP)
Trusted Platform Module (TPM)	No
Web Content Controls	Yes (SSE &WAAP)
Wireless Access Controllers	No
Zero Trust Architecture	Yes

Offerings that include identity protection and authentication capabilities: SSE and SASE Services (Security Service Edge and Secure Access Service Edge)

SSE (Security Service Edge)

LevelBlue services for access management and control include capabilities for identity protection and authentication. LevelBlue services can connect and secure remote workers, regardless of their location or device, and implement data loss prevention (DLP) policies to protect sensitive information and maintain compliance with data protection regulations. These security services are cloud-delivered and designed to address the modern network security challenges of securely connecting employees wherever they are. LevelBlue integrates multiple capabilities for secure web gateway (SWG), cloud access security Broker (CASB), zero trust network access (ZTNA), and firewall-as-a-service (FWaaS), protection for web, cloud, and private applications. These services continuously monitor user and device behavior and permissions, mitigate threats, enforce access to approved websites, and ensure proper configuration of infrastructure-as-a-service (IaaS). Additionally, users are only given access to the specific data and applications needed to do their jobs, segmenting the network and mitigating the risk of lateral spread.

Vendors we use to deliver this service:

- Zscaler
- Palo Alto Networks
- Fortinet
- Check Point

SASE (Secure Access Service Edge)

LevelBlue's Secure Access Service Edge (SASE) services are designed to enhance both network performance and security by converging the two technologies. By adding managed SD-WAN intelligent routing to security service edge technology, LevelBlue ensures secure connectivity across various environments, including remote users, data centers, branch locations, IoT devices, and both public and private clouds. LevelBlue managed SD-WAN intelligently connects users, data centers, and cloud apps in the most efficient way possible while LevelBlue's cloud delivered security stack protects the users and data within the network, providing unparalleled performance while maintaining tight defenses. LevelBlue's SASE service helps to improve network reliability and resiliency, strengthens security against threats, and provides consistent, secure access for users regardless of their location.

Vendors we use to deliver this service:

- Palo Alto Networks
- Fortinet

Distributed Denial of Service (DDoS) Mitigation and Web Application and API Protection (WAAP) Services

DDoS security solutions from LevelBlue help protect network infrastructure and internet-facing properties from being ambushed with DDoS attacks. LevelBlue provides a comprehensive and flexible suite of DDoS solutions with reactive and proactive controls that re-route volumetric DDoS attacks before they disrupt your customer's organization. With more than 20 years of proven DDoS mitigation, LevelBlue provides 30 globally distributed cloud scrubbing centers, over 20 Tbps of dedicated defense capacity, customized service-level agreements (SLAs) with response times below one second during an attack, and always-on or on-demand mitigation solutions based on the organization's requirements. Our global DDoS operations team uses proactive defensive controls to monitor the environment 24/7, reducing the organization's attack surface and decreasing time to mitigate.

Our DDoS services come in four variations:

- **Level Blue Reactive DDoS Defense –** This service is on demand where a customer calls the Security Operations Center to initiate a mitigation. It protects US-based internet circuits up to 1GB only (no most of world). Access to DDoS portal is included.
- **LevelBlue Proactive DDoS Defense –** This service provides 24/7 monitoring and is available in several mitigation options: Manual, Pre-Authorized, Platform Initiated Mitigation (PIM), and Emergency. It protects US-based dedicated internet circuits. Access to DDoS portal included and 15-minute response times.
  ***Note:** In Canada, EMEA and APAC DDoS is limited to coverage of AT&T dedicated internet circuits only, no Latin America coverage.
- **Level Blue Prolexic DDoS –** Proven always-on DDoS defense to protect data centers/carrier hotel, SD-WAN branch locations, and cloud against large, complex attacks, and minimize threats to sensitive data. It protects carrier agnostic circuits with a global footprint including US, EMEA, APAC, and LATAM internet circuits.
- **Emergency DDoS Defense –** We offer emergency mitigation through DDoS Defense and Prolexic DDoS for customers who are actively under a DDoS attack and do not have DDoS protection.

Web Application and API Protection (WAAP)

LevelBlue provides a comprehensive and flexible suite of web application and API protection (WAAP) services, including App and API protection, API Security, Bot Management, Client Reputation, and Client-Side Protection and Compliance. Protect against volumetric distributed denial of service (DDoS), automated botnets, injection, and API-based attacks to defend the customer's network and applications. Validate legitimate client behavior to protect against credential abuse, card balance checking, and other forms of web fraud. Protect against end-user data exfiltration and shield websites from JavaScript threats.

Vendors we use to deliver these services:

- Arbor
- Radware
- Akamai

Email Security

LevelBlue Email Security with Check Point provides comprehensive, in-depth protection for Microsoft 365 and Google Workspace. It extends its robust security measures to cover the entire collaboration environment, including file sharing and chat, as well as platforms like Slack and Microsoft Teams.

This solution ensures seamless security through an easy-to-deploy, cloud-enabled platform that requires no proxy, appliance, or endpoint agent. Organizations can take advantage of automated workflows designed to enforce regulatory compliance, ensuring adherence to standards such as PCI, HIPAA, and PII.

Bundles are available that include:

- SmartPhish Anti-Phishing
- Takeover Protection
- Configuration security
- URL clicktime protection
- Policy enforcement
- Shadow IT

- Malware Sandboxing
- Data Loss Prevention
- Encryption for Office 365

Vendors we use to deliver this service:

- CheckPoint

Managed Detection and Response

Managed Threat Detection and Response for Government (MTDR for Gov) is a managed service built on the FedRAMP Moderate-authorized version of our USM Anywhere platform. The service is supported by a US-citizens-only security operations team that provides year-round, 24/7 threat monitoring and management to help protect sensitive and highly regulated data and ensure critical services are delivered without disruption

- Support from a deep bench of cybersecurity talent that includes personnel with government clearances, and recruits from agencies such as the National Security Agency (NSA) and the Department of Defense
- A platform that delivers extended detection and response and meets US Government cybersecurity standards and requirements for cloud services:
  - FedRAMP Moderate-authorized platform implements security controls required to protect federal data
  - Validated against FIPS 140-2, US Gov't standard for cryptography in technology products
  - All customer data stored in AWS GovCloud (US-West region) to address specific regulatory and compliance requirements, including regional, national, or state data residency
- The platform integrates curated threat intelligence from the LevelBlue Labs threat intelligence unit, which collects threat data for analysis and interpretation from one of the largest sensor networks in the world, as well from as the LevelBlue Open Threat Exchange (OTX), which is the world's largest open threat intelligence community
- Every customer receives up to 10 hours of courtesy incident response (IR) engagement from the LevelBlue MDR IR Team, after which they can transition to working with dedicated responders from LevelBlue Consulting Services
  - LevelBlue Consulting offers a wide menu of incident readiness and response services to help customers plan and prepare for incidents and to provide them with a trusted partner to provide the support and forensic expertise they need if there is a breach.

Monitoring, Detection, and Response

Equipment and services that implement monitoring, detection and response are eligible. Specifically, equipment, services, or a combination of equipment and services that monitor and/or detect threats to a network and that take responsive action to remediate or otherwise address those threats is eligible.

Eligible equipment and services may include the following features, substantially similar features, or their equivalents:

FEATURES	AVAILABLE IN LEVELBLUE SERVICE
Advanced Attack Surface Management and Asset Management Solutions Bug Bounty Solutions and Services	Yes (Through MVP and MDR), No Bug Bounty
Compliance Assessment	Yes
Dark Web Scanning	Yes
Data Loss Prevention	Yes
Internal/External Vulnerability Scanning	Yes (Internal)
Network/Device Monitoring and Response	Yes
Network Security Audit	Yes
Network Traffic Analysis	No
Managed Detection and Response (MDR)	Yes
Managed Service Providers	Yes
Maturity Models	Yes
Network Detection Response (NDR)	No
Penetration Testing	Yes
Security Operations Center (SOC) for Around the Clock (24/7) Monitoring, Detection, and Response	Yes
Threat Hunting/Updates and Threat Intelligence	Yes
Vulnerability Management	Yes

Exposure and Vulnerability Management Services

LevelBlue offers a comprehensive approach to exposure and vulnerability management by utilizing the advanced technologies of Qualys and Tenable, combined with the expertise of our managed security services and cybersecurity consulting teams. We help organizations enhance their security posture by providing complete visibility across their attack surface, identifying and prioritizing vulnerabilities that are actively exploited, and implementing effective mitigation strategies.

Our suite of exposure and vulnerability management services includes the **LevelBlue Managed Vulnerability Program (MVP)**, which is a vulnerability management program that helps organizations identify, prioritize, and mitigate vulnerabilities.

It is designed for on-cloud environments, on-premises infrastructure, SaaS applications, and IT/OT systems. LevelBlue Managed Vulnerability Program delivers service support with:

- **Continuous Monitoring and Assessment:** Constantly monitors and evaluates vulnerabilities to ensure up-to-date protection.
- **Automated and Manual Vulnerability Scanning:** Utilizing both automated tools and manual techniques to thoroughly scan for potential vulnerabilities.
- **Risk-Based Prioritization:** Prioritizes vulnerabilities based on their risk and impact, ensuring critical issues are addressed first.
- **Detailed Reporting and Insights:** Provides comprehensive reports and actionable insights to inform security strategies.
- **Remediation Support and Guidance:** Offers expert support and guidance to help organizations effectively remediate identified vulnerabilities.

LevelBlue's Managed Vulnerability Program ensures organizations are proactively managing their security posture and mitigating risks effectively with the below features and capabilities such as:

- Asset Discovery and Inventory
- Vulnerability Scanning (Internal and External)
- Policy Scanning
- Web App Scanning
- IT/OT Scanning
- Continuous Monitoring
- Threat contextualization
- PCI Vulnerability Scanning
- Patch Management
- Pen Testing (Internal and External)

Additional capabilities we offer for exposure management outside of MVP are Adversary Simulation Testing, Cyber Governance and Risk Assessment, Managed Threat Detection and Response, Managed Endpoint Security, Incident Readiness and Response, Incident Readiness, Incident Response and Recovery and USM Anywhere (unmanaged).

Adversary Simulation Testing:

Our team of cybersecurity experts perform different adversary simulation tests, leveraging our security operations and detection capabilities against the advanced penetration testing techniques used by threat actors today. These tests are performed to assess the effectiveness of existing security measures and identify areas for improvement. These tests enhance preparedness and resilience against potential threats through continuous feedback and knowledge sharing between a united offensive and defensive team.

- **Red Team:** simulating realistic adversarial attacks to assess and improve an organization's security posture.
- **Blue Team:** focus on protecting an organization's IT infrastructure from attacks, by monitoring systems, detecting intrusions, and responding to incidents in real-time.
- **Purple Team:** implementing a true purple team strategy that brings together both the red and blue teams as one unit.

Cyber Governance and Risk Assessment:

Our team of cybersecurity experts perform a comprehensive risk assessment of an organization's security posture, focusing on effective governance, security risk management, and compliance with industry standards. We offer organizations a complete view of their risks and deliver recommendations and measures for improvement. This allows them to make more informed decisions, quickly anticipate and respond to potential threats, and operate with accountability and transparency.

We offer several different risk and governance assessments ranging from:

- Cyber risk posture
- Third-party risk
- Mobile security risk
- AI cyber governance and risk
- Regulatory framework or compliance (ex ISO 27001, NIST, HIPPA, PCI-DSS

Vendors we use to deliver this service:

- Qualys
- Tenable

Managed Threat Detection and Response

Managed Threat Detection and Response for Government (MTDR for Gov) is a managed service built on the FedRAMP Moderate-authorized version of our USM Anywhere platform. The service is supported by a US-citizens-only security operations team that provides year-round, 24/7 threat monitoring and management to help protect sensitive and highly regulated data and ensure critical services are delivered without disruption

- Support from a deep bench of cybersecurity talent that includes personnel with government clearances, and recruits from agencies such as the National Security Agency (NSA) and the Department of Defense
- A platform that delivers extended detection and response and meets US Government cybersecurity standards and requirements for cloud services:
  - FedRAMP Moderate-authorized platform implements security controls required to protect federal data
  - Validated against FIPS 140-2, US Govt standard for cryptography in technology products
  - All customer data stored in AWS GovCloud (US-West region) to address specific regulatory and compliance requirements, including regional, national, or state data residency
- The platform integrates curated threat intelligence from the LevelBlue Labs threat intelligence unit, which collects threat data for analysis and interpretation from one of the largest sensor networks in the world, as well from as the LevelBlue Open Threat Exchange (OTX), which is the world's largest open threat intelligence community
- Every customer receives up to 10 hours of courtesy incident response (IR) engagement from the LevelBlue MDR IR Team, after which they can transition to working with dedicated responders from LevelBlue Consulting Services
  - LevelBlue Consulting offers a wide menu of incident readiness and response services to help customers plan and prepare for incidents and to provide them with a trusted partner to provide the support and forensic expertise they need if there is a breach.

Threat Detection and Response for Government (TDR for Gov) is built on top of the FedRAMP-Moderate authorized instance of our proprietary platform, USM Anywhere, which delivers extended detection and response capabilities and meets US Government cybersecurity standards and requirements for cloud services:

- FedRAMP Moderate-authorized platform implements security controls required to protect federal data
- Validated against FIPS 140-2, US Gov't standard for cryptography in technology products
- All customer data stored in AWS GovCloud (US-West region) to address specific regulatory and compliance requirements, including regional, national, or state data residency

- USM Anywhere continuously monitors across the customer's environment, collecting and correlating data from multiple sources and providing it to our analysts in one view to give them real-time, centralized visibility into the customer's environment.
- The platform is highly extensible; it currently has more than 800 integrations, or "BlueApps," that extend its detection and orchestration capabilities to a large ecosystem of third-party security and productivity tools.
- The platform integrates curated threat intelligence from the LevelBlue Labs threat intelligence unit as well as the LevelBlue Open Threat Exchange (OTX), which is the world's largest open threat intelligence community

***Note:** Schools and libraries should be considering a solution that offers the same protections that are required for government agency data; therefore, the FedRAMP-authorized instance of the USM Anywhere platform should be prioritized. However, if the customer is seeking a less expensive solution, you can offer the non-FedRAMP version of USM Anywhere

Managed Endpoint Security

LevelBlue delivers advanced endpoint detection and response (EDR) with continuously updated threat intelligence to identify, investigate, and respond to threats across desktops, laptops, servers, virtual machines (VMs), and cloud containers. Customers benefit from a fully managed service with 24/7 monitoring and threat hunting delivered by the LevelBlue SOC.

Vendors we use to deliver this service:

- SentinelOne (MES)

Incident Readiness and Response

LevelBlue offers a comprehensive suite of incident readiness and response services, including risk assessments, vulnerability management, incident response planning, breach investigations, and employee training. These are customized to meet an organization's specific requirements, ensuring proactive prevention and mitigation of cyber incidents. By leveraging top-tier solutions and technology, we help organizations react to threats and proactively prepare to respond effectively.

Incident Readiness
We offer a range of Incident Readiness services designed to help organizations take proactive steps to prevent security breaches and enhance operational readiness. By implementing these measures, companies can improve asset discovery and visibility across their attack surface, centralize configuration and policy management, and accelerate mitigation processes. Our services assist organizations in understanding their strengths, identifying gaps in their security programs, and enhancing their readiness for security events through the following activities:

- Risk Assessments
- Incident Response Plan Creation and Review
- Playbook Creation and Review
- Tabletop and Cyber Range Exercises for Technologists and Executives

- Red Team Exercises
- Dark Web Monitoring
- SOC Optimization
- Architecture and Deployment of Preventative and Detective Controls
- Incident Response on Retainer

Incident Response and Recovery

We offer comprehensive incident response services designed to expedite an organization's response to cyber threats and minimize their impact. Our experienced security specialists provide guidance and assistance to resolve security vulnerabilities and incidents, helping organizations effectively manage and remediate threats. LevelBlue's suite of incident response services include:

- External or Internal Breach Response
- Disk Analysis and Image Acquisition
- Incident Management
- Incident Triage
- Malware Containment and Eradication
- Log Analysis and Correlation
- Rapid Deployment of Investigative Tools
- Communication Support
- Reporting to Key Stakeholders
- Remediation Support

USM Anywhere (unmanaged)

LevelBlue USM Anywhere delivers powerful threat detection, incident response, and compliance management in one unified platform. LevelBlue USM Anywhere provides multiple essential security capabilities in a single SaaS solution, giving you what you need for threat detection, incident response, and compliance management—all in a single pane of glass. Built for today's resource-limited IT security teams, LevelBlue USM Anywhere is more affordable, faster to deploy, and easier to use than traditional solutions. It eliminates the need to deploy, integrate, and maintain multiple point security solutions in your data center. A cloud-hosted platform delivered as a service, LevelBlue USM Anywhere offers a low total cost of ownership (TCO) and flexible, scalable deployment options for teams of any size or budget.

USM Anywhere Capabilities:

- Asset Discovery
- Vulnerability Assessment
- Intrusion Detection
- Endpoint Detection and Response
- Behavioral Monitoring
- SIEM and Log Management

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.