LevelBlue

SERVICE BRIEF

LevelBlue Exposure and Vulnerability Management

Technology Should Help, Not Hinder

Vulnerability management has been a key part of cybersecurity for decades, helping organizations identify security weaknesses in their networks. While this approach has worked well in the past, today organizations face new challenges as they advance with their digital transformation initiatives, causing rapid expansion of their attack surface. According to IDC, by 2027, "41% of an enterprise's revenue will come from digital products and services." The adoption of operational technology (OT), Internet of Things (IoT) devices, mobile solutions, cloud services, and diverse endpoints, coupled with growing supply chain dependencies, has created more entry points and exposures that sophisticated threat actors can exploit. This expansion has made it increasingly difficult for organizations to maintain comprehensive security visibility and control. Organizations must transition from isolated vulnerability management to an integrated exposure management program, which incorporates comprehensive discovery, and continuous monitoring to minimize gaps adversaries can target.

Key Challenges

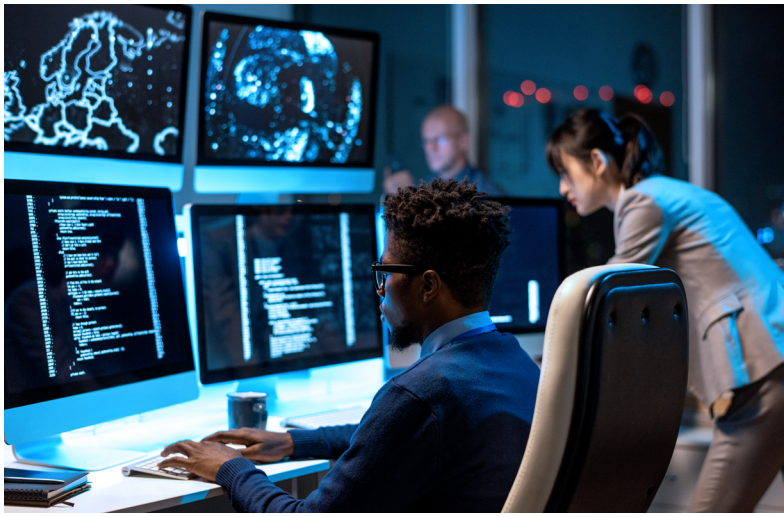
Many organizations lack comprehensive visibility across their attack surface due to legacy tools and point solutions. When combined with irregular and incomplete security scanning practices, this provides attackers with extended windows of opportunity to exploit undiscovered vulnerabilities. This reactive approach not only increases risks but also lacks an effective process for prioritizing and mitigating high-risk vulnerabilities and exposures when they are found.

Resource constraints make matters worse, with many organizations struggling to maintain the right expertise in-house. This makes it difficult to support continuous monitoring and effectively prioritize vulnerability remediation efforts. Without the proper context and prioritization frameworks, security teams often find themselves overwhelmed, and unable to determine which vulnerabilities pose the greatest risk to their environment and business objectives.

Regulatory compliance adds another layer of difficulty. Organizations are challenged with maintaining comprehensive visibility for accurate reporting, while navigating the complex industry-specific standards, privacy regulations, and security

Benefits

- Streamlines processes to enhance productivity and reduce manual efforts.
- Offers comprehensive insights and detailed reports on vulnerabilities and risks.
- Strengthens the overall security posture and provides better control over IT environments.
- Reduces the time and cost associated with protecting your network.
- Adapts to new security and compliance requirements as your business expands.
- Provides immediate access to trusted advisors to fill gaps in IT staff or resources.
- Reduces the need for re-scanning dynamic hosts and eliminates manual tracking.
- Delivers continuous scans with minimal performance impact, leading to accurate risk assessments and prioritized remediation.
- Identifies and alerts on communication attempts from external sources.
- Enables quick incident response and proactive compliance with internal and external regulatory bodies.
- Integrates across the LevelBlue portfolio for a cohesive security strategy.



frameworks. The tasks of generating timely and accurate compliance reports becomes increasingly burdensome as environments grow more complex, highlighting the critical need for automation and mature security processes. Failed compliance can result in hefty fines, legal consequences, and reputation damage.

LevelBlue Exposure and Vulnerability Management

Mitigating exposures requires a holistic approach with the right combination of people, processes, and technology. This is where a managed security service provider like LevelBlue can help, providing a cost-effective and all-encompassing solution for organizations to address issues around compliance and close security gaps.

LevelBlue delivers enterprise-grade exposure and vulnerability management through a combination of vulnerability management tools, continuous monitoring capabilities, and specialized consulting services. LevelBlue Exposure and Vulnerability Management empowers organizations to identify, assess, and remediate security weaknesses across their entire technology landscape through four stages: discover, prioritize, validate and mobilize.

Discovery

We configure platforms and service modules that offer continuous visibility into an organization's attack surface through asset discovery and inventory. This approach enables organizations to maintain a comprehensive inventory of all assets, including OT systems, IoT devices, mobile endpoints, SaaS applications, and traditional IT infrastructure. It ensures no component goes unnoticed, whether on-premises, in the cloud, remote, or in containers. Our discovery processes identify and catalog every networked asset, application, and potential entry point, while continuous monitoring tracks changes and identifies new assets as they are added to the environment. Through continuous vulnerability scanning and sophisticated assessment techniques, we provide visibility into potential security gaps across both external and internal attack surfaces, ensuring no vulnerability goes undetected.

Prioritization

Once vulnerabilities are discovered, LevelBlue helps organizations focus on what matters most. We analyze each vulnerability to determine its risk level (high, medium, or low) and evaluate the effort required for remediation. This practical approach ensures security teams can focus first on actively exploited vulnerabilities that pose the greatest risk to critical systems and sensitive data. Our prioritization process helps organizations to find the most-effective way to reduce risks, whether through patching, mitigation, or other security controls.

Validation

We provide several different testing methods to confirm how a potential attacker could exploit a known vulnerability and assess how the monitoring and control systems would respond. Our team conducts vulnerability validation to verify identified issues and performs both external and internal penetration testing to understand how real-world attackers could exploit these weaknesses. We also offer:

- Red team exercises where our ethical hackers simulate real-world cyber-attacks to test an organization's defense mechanisms. These exercises mimic the tactics, techniques and procedures used by malicious attackers.
- Purple team exercises will integrate both the red (attackers) and blue (defender) teams, to promote collaboration and coordination between the two groups, resulting in a more comprehensive and resilient security approach.

This hands-on testing helps uncover weaknesses in security systems before they can be exploited and provides practical experience in handling cyber incidents.

Mobilization

In the mobilization stage, we transform security findings into actions through streamlined, automated response workflows. Our tools integrate with existing IT service management systems, providing patch management capabilities and clear remediation strategies. Comprehensive reporting keeps stakeholders informed and helps demonstrate compliance with regulatory requirements, while our automated workflows ensure swift, consistent response to identified vulnerabilities and exposures.

Service Tiers

LevelBlue offers customers flexibility through three tiers on Exposure and Vulnerability Management with Essentials, Advanced, and Premium.

The Essentials tier establishes a strong security foundation by ensuring ongoing protection through constant vigilance, timely identification of security gaps, testing defenses, and continuous monitoring of cloud environments. The Advanced tier offers enhanced risk management with targeted testing across IT and OT environments, preventing threats before exploitation and providing additional vulnerability assessments for better threat handling. The Premium tier delivers elite-level protection against evolving cyber threats through comprehensive scanning and realistic attack simulations, ensuring assets are safeguarded from emerging risks, and alignment with industry best practices.

LevelBlue Exposure and Vulnerability Management			
	ESSENTIALS	**ADVANCED**	**PREMIUM**
Unlimited Vulnerability Scanning (Internal and External)	Included	Included	Included
External Network Pen Test	Included	Included	Included
Cloud Security Monitoring	Included	Included	
Asset and Attack Surface Management		Included	Included
Web Application Scanning		Included	Included
Internal Pen Test		Included	Included
Wireless Pen Test		Included, based on **two sites with three SSIDs per site**	Included, and based on **sites with three SSIDs per site**
Social Engineering Assessment		Included with **email and text-based scenarios**	Included with **email, text, and phone-based scenarios**
Red Team or Purple Team		Red Team: Included, **Six-week** test engagement. Purple Team pricing is based on 2 advanced persistent threat scenarios	Red Team: Included, **Eight-week** test engagement. Purple Team pricing is based on 2 advanced persistent threat scenarios
OT Pen Test		Included with a 4-week engagement	Included with a 4-week engagement
Web Application Pen Test			Included and based on the number of pages, inputs per page, and user roles. (3 roles, 20 pages and 40 inputs)

Exposure and Vulnerability Management Service Components

Unlimited Vulnerability Scanning
Continuous scanning to detect vulnerabilities and weakness within an organization's internal network as well as systems and applications exposed to the internet. Price is based on the number of assets.

Cloud Security Monitoring
Continuous monitoring of an organization's multi-cloud environment for misconfigurations and non-standard deployments, including for Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Oracle Cloud Infrastructure. Price is based on the number of cloud connectors, or number of assets.

External Penetration Testing
Simulated cyberattacks that identify vulnerabilities and security weaknesses in external-facing network components, such as web servers, firewalls, and routers, that could be exploited by attackers to breach your network, steal sensitive data, or disrupt operations. Price is based on asset count and testing frequency.

Asset and Attack Surface Management
Continuous identification and monitoring of all assets visible on the internet, including previously unknown and potentially vulnerable systems paired with analysis to detect and address potential security risks. Price is based on number of assets.

Web Application Scanning
Automated scanning of web applications to detect security weaknesses and vulnerabilities, including dynamic application security testing (DAST), API security, deep learning-based web malware detection and AI-powered scanning. Detect runtime vulnerabilities, OWASP Top 10 exposures, OWASP API Top 10 exposures, misconfigurations, PII and sensitive data exposures, web malware, compliance issues, and more. Price is based on the number of applications.

Internal Penetration Testing
Testing performed on an organization's internal networks to validate that security controls are working as expected, identify access to sensitive data, validate access management controls, and identify potential lateral movement and insider threats. Price is based on number of assets, testing frequency and a toolset fee.

Wireless Penetration Testing
Wireless penetration testing simulates attacks won an organization's wireless network to uncover vulnerabilities, access flaws, unauthorized device connections, encryption weaknesses, or misconfigurations that could leave the network exposed to attackers. The advanced and premium service tier differ from number of sites, and SSIDs per site.

Operational Technology (OT) Pen Test
A 4-week engagement that simulates advanced cyberattacks within industrial control environments, without disrupting operations. It targets critical components like PLCs, SCADA systems, RTUs, and HMIs to uncover vulnerabilities unique to OT, such as insecure protocols, weak segmentation, and outdated firmware. The assessment blends passive analysis and controlled testing to evaluate how well the environment can detect, respond to, and withstand real-world threats, providing clear remediation guidance aligned with safety and availability requirements. Pricing is based on number of assets and toolset fee.

Red Team or Purple Team
A full-scale security assessment involving ethical, simulated adversary attacks (red team) to evaluate the effectiveness of defensive strategies. Simulations are designed to help an organization identify exposures and weaknesses and improve its security defenses. A purple team exercise fosters collaboration between an organizations defense (blue) and attack (red) teams to enhance detection, response, and remediation strategies through joint simulations. The Advanced and Premium service tiers for red teaming differ in terms of the length of engagement.

Social Engineering Assessment:
Security test designed to assess the human element of security by using tactics such asphishing, pretexting, and baiting. Tests can include email, text, and phone-based scenarios. Pricing based on test scenarios, the Advanced and Premium service tiers differ with scenarios.

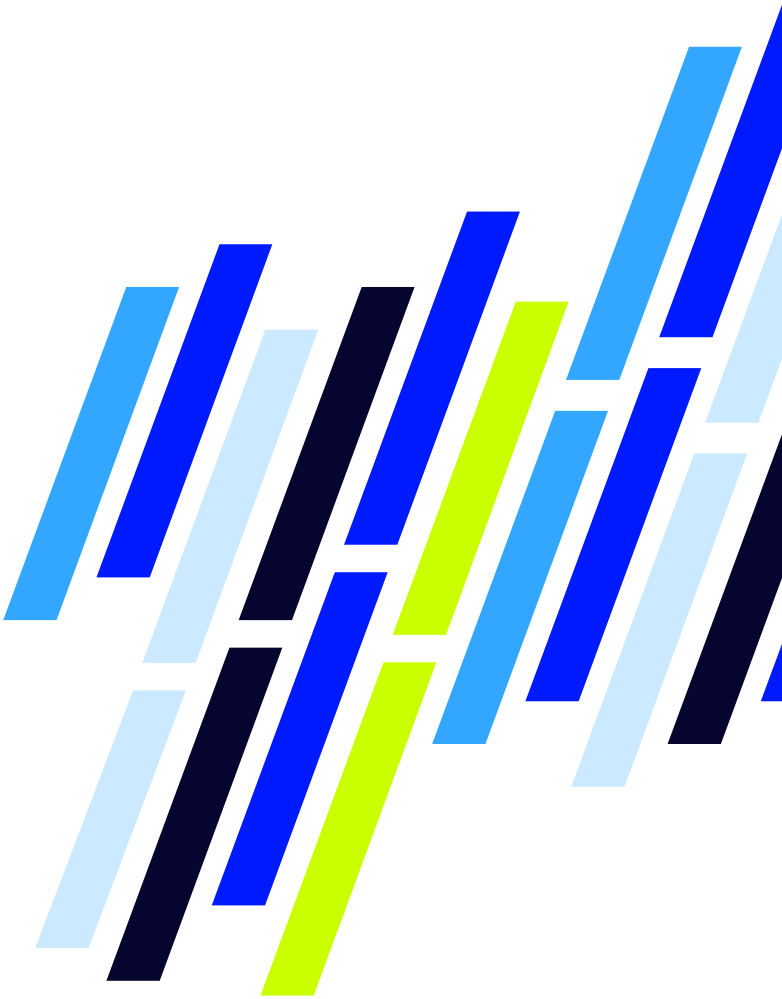
Web Application Penetration Testing
In-depth testing of web applications to uncover vulnerabilities that automated scans may not detect, including authentication and authorization bypasses,

automated tools that may not follow or understand business flows. Pricing is based on the number of pages, inputs per page, and user roles for application(s).

Integration with Other Security Technologies

Our solution integrates with advanced security technologies, particularly our Managed Detection and Response (MDR) portfolio. By incorporating MDR into an exposure and vulnerability management program, organizations benefit from real-time threat detection, continuous monitoring, and rapid incident response, significantly reducing security risks.

By taking this integrated approach with LevelBlue Exposure and Vulnerability Management paired with LevelBlue's Managed Detection and Response (MDR) service, organizations can not only identify and mitigate exposures that put them at risk, but also rapidly detect and respond to any threats that attempt to exploit these vulnerabilities.



Why LevelBlue

LevelBlue's comprehensive approach to exposure and vulnerability management delivers the visibility and control organizations need in today's complex threat landscape. Through complete asset inventory across IT, OT, IoT, and cloud environments, coupled with real-time monitoring and intelligent vulnerability prioritization, we help organizations stay ahead of emerging threats while focusing resources where they matter most. Our proven methodology goes beyond basic scanning by adopting an attacker's perspective, enhancing incident response capabilities, and ensuring regulatory compliance – all while providing the strategic insights needed for informed security investments. Partner with LevelBlue to transform your security posture from reactive to proactive, ensuring your organization remains resilient against cyber threats.

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.