LevelBlue

PRODUCT BRIEF

LevelBlue Malware Risk Assessment Services

Gain More Visibility and Control of Your Organization's Potential Impact of a Malware Attack if Deployed within Your Environment

LevelBlue

Malware is a collective name for several different types of intrusive software attacks that have been created to steal an organization's data, damage computers, and/or damage their network. A malware attack can cause serious problems for an organization that can affect daily operations and the long-term security of the company and its clients. It's important to note that a malware attack can happen at any time, anyway, and over various types of surface levels within the organization.

Now more than ever it is important that an organization evaluate their current state of various controls and practices that could have a direct impact on their resilience from a potential malware outbreak. Companies should know where they are most vulnerable to an attack and be able to remediate it as soon as possible.

Potential Benefits

- Vulnerability management assessment
- Help to avoid data breaches
- Provide actionable remediation guidance
- Control Data Leakage
- Mitigate human error with machine learning in near real-time
- Support compliance with NIST, CMMC, ISO, CCPA, etc.
- Incident Response Planning
- Uncover application vulnerabilities
- Compliance Requirements Support

LevelBlue Malware Risk Assessment

LevelBlue Malware Risk Assessment is focused on the business and technology environments in which the organization operates and takes into consideration the best practices, industry standards, and compliance issues that impact the organization. Based on the customer's need, the LevelBlue Consulting team applies multiple assessment activities and tools to evaluate internal and external threats and delivers the analysis of findings and recommendations for remediation. Areas of review include the following:

- **Endpoint Security Assessment:** Ensuring that endpoint systems are well protected from advanced malware is a foundational component of any strong malware preparedness strategy. The team will review several considerations around the security of endpoints in the environment including; product selection, completeness of coverage across the endpoint population, use of file integrity monitoring solutions, application restrictions and logging of administrative tool use, and integration with the overarching detective control framework in place within the organization.
- **Network Segmentation Review:** Flat network structures allow for malware to easily propagate throughout the compromised environment. The assessment team will evaluate the use of segmentation practices used in the environment.
- **Enterprise Patch Management:** Poor hygiene in the computing environment is a contributing factor to malware spread. The team will review the organization's patch management procedures and tools used.
- **Response Controls Review:** Being prepared to respond should a malware incident occur will lessen the time of impact on the organization. Response and reporting capabilities are essential to effectively manage and communicate during an incident.
- **Remote Connectivity Assessment:** Validating that remote users can securely connect to enterprise resources is a foundational element of a secure architecture. The assessment team will review the various remote connectivity solutions in place and identify opportunities for improvement through interviews with administrators and staff as well as technical testing. These activities will uncover potential risks associated with remote connection and terminal services such as VPN, L2TP, PPTP, SSH, SSL, and HTTPS solutions. An analysis of the attack surface presented by the identified solutions will be performed as will attempts to exploit any configuration problems and vulnerabilities identified.
- **Permissions Management**: Malware often enters the organization through email or drive-by downloads while browsing the web. The resulting code typically executes with the permissions of the user falling victim to the attack. By practicing the principle of least privilege an organization can make sure that any malicious code that is executed by an end-user has limited capabilities to act on the local system, such as disabling endpoint security packages, or on the network as a whole.
- **Detective Controls Review:** Many malware outbreaks are the result of an intruder manually deploying malicious software after having spent days or weeks undetected within the network. Having a strong web of detective controls in place

is critical to early detection and revocation of such access. The team will review the controls in place to detect suspicious activity in the environment, the supporting monitoring and review processes and tools, and look for opportunities for improvement in the environment.

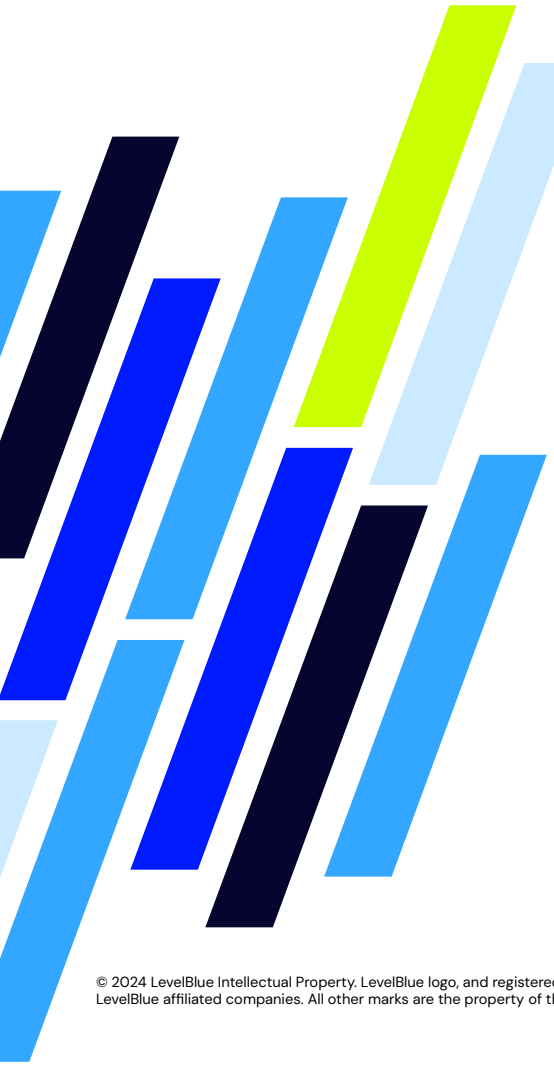
- **Application Assessments**: Identify security holes and vulnerabilities within an organization's application portfolio. Within the context of organizations with compliance requirements, specific considerations around OWASP Top 10 issues and other application best practices as they apply to multi-user and mobile applications can have a significant impact on daily operations and compliance readiness. The team will seek to identify opportunities for improvement in deployed applications while striking a balance between access needs, business requirements, and organizational security.
- **Training and Awareness**: The human element is a key component of protecting the organization against malware threats. System users must be able to recognize attempts via email or other social engineering acts and know what to do and where to report these events. The assessment team will evaluate the training program and conduct social engineering penetration testing (as an optional service).
- **Multi-Factor Authentication Review:** Most compromises involve the use of stolen or the brute-forcing of weak passwords. This allows threat actors to gain access to networks and then manually deploy malware, such as ransomware packages, to their greatest effect. The team will review the use of multi-factor authentication in the environment as it pertains to remote access, system administration, cloud environments, and user access.
- **Risk Management:** Security risks are inevitable, so the ability to understand and manage risks to systems and data is essential for an organization's success. Having a well-designed and integrated risk management program enables the protection of an organization's most critical assets against emerging cyber threats. This includes effective asset management as well as third-party management. The assessment team will review applicable documentation and interview to evaluate risk management governance and integration into security and organizational processes.
- **Backup and Restoration Controls Review:** Malware often attempts to disable, corrupt, or otherwise make unavailable through encryption data backups that would allow their victims to avoid capitulating to the demands of the threat actors responsible for the attack. By ensuring that backup solutions are properly segmented from the production environment and leveraging strong authentication mechanisms, an organization can enhance its chances of successfully recovering from a malware attack. The assessment team will review the backup controls and supporting processes through interviews and document review.

Assessment Finding Analysis

Once the LevelBlue Consulting Team has run the various malware risk assessments, the pertinent findings will be summarized. The executive summary is written in non-technical language to provide a broad understanding of information security shortcomings found, the impacts, and recommended actions that will address each finding.

Why LevelBlue

LevelBlue Consulting has a strong history of delivering comprehensive and effective security, information risk, and compliance solutions to all verticals and industries. The measure of any successful security assessment is in the rigor that is applied to each task. LevelBlue has built a rigorous consulting solution that is set for conducting security assessments. Those solutions are based on the results of the collection body of knowledge that comes from performing these services for a variety of customers over an extended period of time.



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.