FLEXENTIAL

External Vulnerability Assessment

Mature cyber resiliency and advance your organization's security posture

External vulnerability management is a crucial component of a robust cybersecurity program. It helps businesses identify and address potential weaknesses before malicious actors can exploit them and breach the organization's perimeter. For many organizations, vulnerability management is also a required compliance activity for frameworks, certifications, or regulations such as ISO 27001, SOC2, PCI DSS, and GLBA.

Our External Vulnerability Assessment is designed to help organizations stay ahead of threats, mature their cyber resiliency, and advance their overall security posture in the increasingly dangerous cyber landscape.

Features

- Comprehensive scanning of external-facing assets
- In-depth vulnerability reports with prioritized remediation steps
- Expert analysis and recommendations from our experienced cybersecurity team
- Integration with compliance frameworks (e.g., SOC 2, ISO 27001, PCI DSS, HITRUST)
- One-time or regular automated scans with customizable frequency

Problems we solve

- Identification of unknown security weaknesses in external-facing infrastructure
- Resource constraints for executing regular vulnerability scanning
- Limited visibility into the organization's external attack surface
- Compliance gaps in regulatory requirements

Outcomes we create

- Reduced risk of external attacks and data breaches
- Proactive detection of security vulnerabilities
- Detailed mitigation recommendations prioritized by criticality and risk
- Verification of previous vulnerability remediations
- Vulnerability trend tracking for measuring program effectiveness
- Enhanced cyber resilience through proactive vulnerability management
- Cost avoidance through active prevention of potential breaches
- Improved compliance with regulatory and industry requirements
- Increased confidence in the organization's security posture

32%

of ransomware attacks were caused by unpatched vulnerabilities[1]

Last year, cyber-attacks targeting known vulnerabilities surged[2]

54%

Mature cyber resiliency

Proactive threat mitigation: By identifying vulnerabilities before they can be exploited, our service helps organizations stay one step ahead of potential attackers

Risk-based approach: Our prioritized remediation recommendations allow for optimal resource allocation to address the most critical vulnerabilities first.

Compliance adherence: The service supports compliance with your regulatory requirements, reducing the risk of penalties and legal consequences.

Continuous improvement: Regular scans provide insights into the organization's security trends, enabling continuous improvement of an organization's security posture.

Advance cybersecurity posture

Comprehensive visibility: Our service provides a clear view of the organization's external attack surface, enabling better-informed security decisions.

Timely identification: Regular scans identify new vulnerabilities quickly allowing for fast resolution and a reduced window of opportunity for attackers.

Incident response preparedness: By understanding potential vulnerabilities, organizations can better prepare for and respond to potential security incidents.

Security ROI measurement: Tracking vulnerability trends over time provides tangible metrics for measuring the effectiveness of security investments.

Contact us for more information on how our **External Vulnerability Assessment** and the Flexential NIST CSF-Aligned Portfolio for Ransomware can enhance your organization's cyber resiliency.

39%

increase in Common Vulnerabilities and Exposures (CVEs) last year, averaging 109 per day[3]

20%

20% increase in exploited CVEs for 2024 over 2023, from 639 to 768 CVEs[4]

1. *Indusface Cybersecurity Statistics*
2. *Sophos, The State of Ransomware 2024*
3. *JerryGamblin.com, CVE by the Numbers*
4. *Vulncheck, 2024 Trends in Vulnerability Exploitation*