TAG SOLUTIONS
We make IT work. We make IT easy. No excuses.

Penetration Testing

WHO IS IT FOR?

- **Regulated Industries**
  PCI-DSS (Payment Card Industry Data Security Standard) specifically mentions penetration testing. HIPAA calls for Covered Entities to "conduct an accurate and thorough assessment of potential risks and vulnerabilities" facing health-related data. All industry-specific cybersecurity regulations exist to shrink risk. Penetration testing is a valuable way to uncover areas of weakness and vulnerability, which in turn, can be remediated to reduce the risk of a breach or other cyber event.
- **Everyone Else**
  Anyone who wants to answer the following questions should consider penetration testing:
  - "How hackable is my network edge by a bad actor with Internet access?"
  - "If my edge defenses allow something bad through, what vulnerabilities or footholds could a hacker or malicious software leverage to damage or steal private information?"
  - "Is my Internet-facing website susceptible to code injection or cross-site scripting?"

WHY IS IT IMPORTANT?

- **Identify weaknesses, vulnerabilities and exploits** in the organization's information systems, networks, and applications.
- **Improve the overall security posture of the organization** – Penetration testing plays a critical role in an organization's ability to defend against security threats.
- **Reduce organizational risk** – Vulnerability scanning can identify existing vulnerabilities and exploits in an organization's information technology assets, including operating systems, applications, and devices.
- **Support compliance** – Penetration testing can satisfy an organization's regulatory, commercial, and organizational compliance requirements.
- **Test security investments** – Penetration testing measures the effectiveness of the security controls that are currently in place.

WHAT IS INCLUDED?

There are three types of penetration testing. Depending on your environment, budget, current security needs, and past assessments, you may want to consider one or more of them.

- **External Penetration Testing** – Identifies weaknesses that could be exploited at the network edge. We perform reconnaissance on the weaknesses and then attempt to

actively exploit weaknesses using an advanced mix of automated and manual tools that are both open- and closed-source.

- **Internal Penetration Testing** – Like external penetration testing, but performed on internal IP-enabled devices.
- **Web Application Penetration** – Following the OWASP (Open Web Application Security Project) Top Ten framework, our security engineers perform a series of in-depth security tests such as cross-site scripting, SQL injection, authentication bypass, or invalid redirects to bypass security controls. Detailed reporting and remediation recommendations will help you secure your web application from real world hackers.