



## Services Overview

The following section outlines Caliber Security Partners services. Please visit [www.calibersecurity.com](http://www.calibersecurity.com) for more information or contact Tab at [tab@calibersecurity.com](mailto:tab@calibersecurity.com) or 206-349-9162.

Service	Description	Value	Cost Structure
<b>Application Security Scanning</b>	Automated scanning with a cross section of security tools. Manual false-positive removal and reporting.	Identify production security vulnerabilities reducing time of exposure, multiple scanners deliver comprehensive coverage, expert false positive removal and mitigation recommendation.	Individual contracts or offered as a managed service for regular scanning as applications evolve over time e.g. daily or weekly scanning.
<b>Application Penetration Test</b>	Manual investigation and creative hacking to identify unique vulnerabilities.	Security experts with years of experience identify vulnerabilities that scanners miss but malicious actors may find.	Individual contracts or offered as a managed service for periodic testing as applications evolve over time e.g. quarterly or semi-annually.
<b>Static Code Analysis</b>	Static code analysis (SCA) using various tools.	SCA assesses uncompiled source code to identify vulnerabilities early in the development cycle. SAST provides excellent mitigation advice and informs training programs.	Individual contracts or integrated into your development process for immediate, incremental scanning in agile environments.
<b>Secure Development Training</b>	In person or computer based security training.	Targeted security training provides the most proactive investment to mitigate vulnerabilities early in development.	Individual contracts or semi-annual refresher and targeted training, informed by complementary assessments.
<b>Vulnerability Scanning: External</b>	Automated scanning with a cross section of security tools. Manual false-positive removal and reporting.	Identify production security vulnerabilities reducing time of exposure, multiple scanners deliver comprehensive coverage, expert false positive removal and mitigation recommendation. Complementary to change control by identifying new devices within an IP range.	Individual contracts or offered as a managed service for regular scanning as applications evolve over time e.g. daily or weekly scanning.
<b>Vulnerability Scanning: Internal</b>	Automated scanning and manual false-positive removal and reporting. Unauthenticated or authenticated scanning to include patching across application e.g. Adobe, Java.	Identify security vulnerabilities reducing time of exposure, expert false positive removal and mitigation recommendation. Complementary to change control by identifying new devices within an IP range.	Individual contracts or offered as a managed service for regular scanning as environments evolve over time e.g. daily or weekly scanning.
<b>IT General Controls Attestation</b>	Interview and evidence review utilizing industry frameworks e.g. NIST CSF, ISO 2700/2.	Comprehensive view of security to align control maturity with business risk tolerance. Inform security investments and convey	Annual review with time and cost savings leveraging previous assessments.

		security to customers and partners.	
<b>Security Integrated Sales Process</b>	Evaluate and improve sales process to ensure customer security requirements are understood and met.	Reduce sales cycle and minimize disruption of the IT and development teams.	One time engagement, utilizing evidence of complementary security services to communicate with customers.
<b>Risk Prioritization &amp; Investment Roadmap</b>	Interview based assessment incorporating control performance, Caliber experience, and business risk tolerance to develop security investment roadmaps.	Risk based security investments aligned with business drivers ensure the right amount of security at the right time to meet business needs.	Annual review with time and cost savings leveraging previous assessments.
<b>Security Staff Augmentation</b>	Complement and scale existing IT resources to execute security program activities e.g. perform internal audits, configure secure systems, author policy and standards, deliver monitoring and response services.	Jump-start security services without hiring commitments and expense. Evaluate personnel for full time employment.	Quarterly engagements with optional contract to hire arrangements.