

APPLICATION SECURITY ASSESSMENT SERVICES

Reduce the Attack Surface of Running Applications

Applications represent one of the largest and most dynamic segments of the attack surface. Without regular, expert-driven validation, exploitable vulnerabilities persist in production, accumulating unquantified risk with every release and integration.

Gain validated evidence that production applications meet security and compliance standards across every platform and application type. GuidePoint Security Application Security Assessment (ASA) services deliver structured, non-disruptive evaluations that are tailored to each application, environment, and organization's goals. Organizations receive exploitability-rated findings, real-time critical vulnerability communication, and verified remediation confirmation, translating directly into measurable risk reduction and documented application security posture improvements.

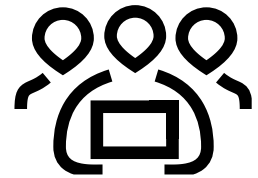
Turn Unknown Exposure Into Documented Risk Reduction

Regulatory bodies, board members, and executive leadership increasingly demand validated evidence that production applications meet security and compliance standards. Every unassessed application represents unquantified exposure that compounds with continued development, continuously increasing potential breach impact.

GuidePoint Security Application Security Assessment (ASA) services quantify application risk in traditional and AI applications, transforming unknown vulnerabilities into documented, prioritized findings tied to business impact. Organizations gain third-party validated evidence of security posture that satisfies regulatory requirements, supports audit readiness, and provides leadership with measurable proof application security improvements.

When to Consider an Application Security Assessment

- ✓ Before deploying new applications or major features to production
- ✓ After integrating AI, large language models (LLMs), or third-party components into existing applications
- ✓ When compliance or audit timelines require third-party validated evidence of application security
- ✓ Following a security incident that exposes application-layer vulnerabilities
- ✓ During mergers, acquisitions, or onboarding of inherited application portfolios
- ✓ After significant architectural changes or platform migrations
- ✓ As part of a regular cadence to maintain ongoing security posture



Stronger Together. Protecting What's Next.

Working with GuidePoint, your organization will be backed by our elite team of highly trained cybersecurity engineers, architects and consultants who come from organizations of all sizes, including Fortune 100 companies, the Department of War, and the U.S. Intelligence Community.



A Proven Methodology for Identifying Exploitable Risk

Each GuidePoint Security ASA is tailored to the organization's application environment, technology stack, and security objectives. GuidePoint's applications security experts follow a structured progression from initial scoping through verified remediation.

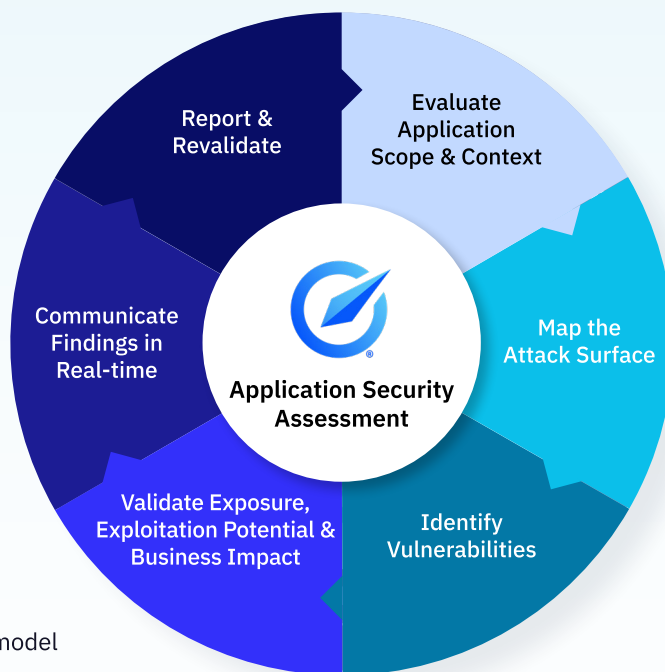
Engagements combine manual and automated techniques within time-boxed, non-disruptive testing windows, communicating critical findings in real time and delivering exploitability-rated results. Remediation guidance and ongoing advisory support ensure greater impact, with 90-day remediation verification to document evidence of improvements.

Validated Security Across Every Application Type

Each ASA adapts methodology, tooling, and testing focus to the specific application type, platform, and technology stack. Engagements address general and platform-specific vulnerabilities across authentication, authorization, session management, business logic, cryptographic implementation, and API security. For AI-integrated applications, testing additionally covers prompt injection, data leakage, model manipulation, and adversarial input handling.

Application types assessed include:

- ✓ Agentic and generative AI applications
- ✓ Web applications
- ✓ Mobile applications (iOS and Android)
- ✓ Application programming interfaces (APIs)
- ✓ Thick client applications
- ✓ Third-party integrations
- ✓ Custom large language model (LLM) implementations



Put AI to Work and Accelerate Findings Without Sacrificing Scope

For organizations requiring broader coverage or accelerated timelines, optional AI-augmented workflows accelerate expert-led assessments by up to 60 percent. Consultant oversight validates every AI-generated finding for accuracy, contextual relevance, and elimination of false positives. The same structured methodology, real-time communication, and remediation verification apply.

Why GuidePoint Security

When application vulnerabilities threaten the business, organizations need the best by their side. GuidePoint Security delivers application security advisory, testing, and training services that uncover the critical flaws automated tools alone cannot find. Credentialed consultants bring real-world development experience and deep security expertise across web, mobile, API, and AI applications. GuidePoint assesses, advises, and validates so organizations can deploy with confidence and protect what matters most.

About Us

GuidePoint Security brings together proven expertise, great relationships, and leading technologies to solve our client's most complex cybersecurity challenges. As a trusted cybersecurity advisor and partner, GuidePoint keeps people, data, and operations safe. We deliver tailored cybersecurity services that adapt to safeguard the nation's leading organizations today and provide complete confidence in their cybersecurity tomorrow. Stronger Together. Protecting What's Next.