

Application Security

1. Service overview

Organizations need application security to protect their systems and data from potential cyber threats and vulnerabilities. Application security involves implementing measures and practices to protect software applications from security threats and vulnerabilities. It includes designing and developing applications with security in mind, conducting regular security testing and vulnerability assessments, and implementing controls to mitigate potential risks. The goal is to ensure that applications function securely, protecting against unauthorized access, data breaches, and malicious attacks. CyberProof provides end to end application security services to secure and protect the applications against cyber threats.

Primary services provided

- **Application Security Assessment:** Identifying vulnerabilities and weaknesses to ensure robust protection against potential threats.
- **Vulnerability Management Services:** Identifying, prioritizing, and addressing vulnerabilities to maintain a secure and resilient infrastructure.
- **Penetration Testing Services:** Performing simulating real-world attacks to identify and address security vulnerabilities in systems and applications.
- **Application Security Consulting Services:** Understanding customer security requirements, designing solution, and implementing tools such as SCA, SAST, DAST and IAST.
- **Mobile Application Security Assessment:** Evaluating and enhancing the security of mobile applications to protect against potential risks and vulnerabilities.
- **Secure Application Code review:** Analyzing application code to identify and rectify security flaws, ensuring robust protection against potential exploits.
- **Secure SDLC:** Integrating security practices throughout the software development process and tools to create secure and resilient applications.
- **API Security Assessment:** Evaluating and strengthening the security of APIs to protect against potential vulnerabilities and unauthorized access.
- **Application Security Program Strategy:** Developing a comprehensive plan to proactively manage application security risks and ensure ongoing protection.

2. Pain points (why orgs need our help)

- Protecting sensitive data
- Mitigating cyber threats
- Maintaining customer trust
- Compliance with regulations
- Protecting against emerging threats

3. Service benefits/outcomes

- Application security services to ensures the protection of sensitive data, such as customer information, intellectual property, and financial data.
- Enhanced Security Posture by assisting in improving the overall security posture of organizations.

- Assisting organizations in meeting compliance obligations and maintaining them to avoid penalties.
- Proactive threat detection services to avoid costly remediation efforts and potential financial losses associated with security incidents.
- Comprehensive security assessments and audits, application security services for risk reduction and protection against attacks.

4. Differentiators (USPs)

- Proven track record and extensive experience in application security.
- Offering a wide range of application security services such as scanning, assessment, code review and vulnerability management, one-stop solution for application security needs.
- In-depth knowledge of compliance regulations and standards, such as GDPR, ISO, NIST, and tailored services offering.
- Innovation and emerging technologies offering to address the evolving application security landscape.