

Application Security Posture Management

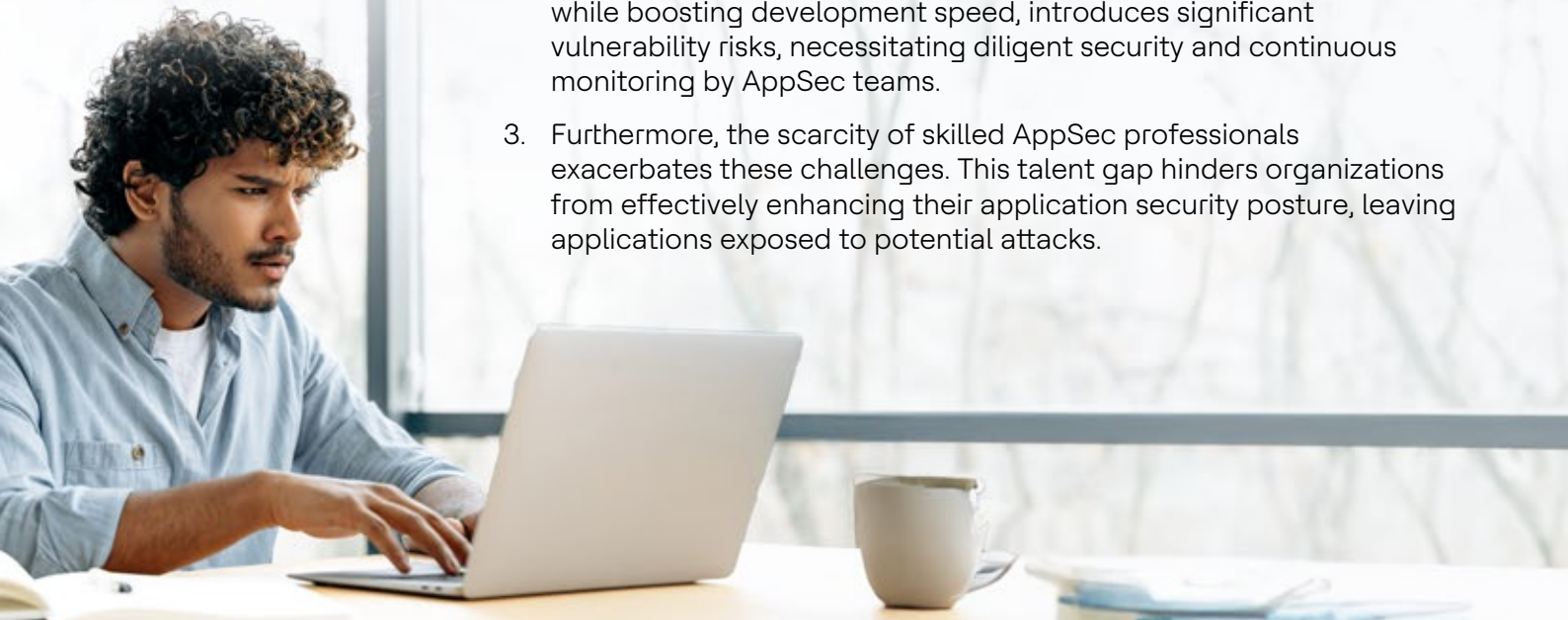


Protecting business critical applications

In today's fast-paced digital landscape, organizations face pressure to innovate and embrace new technologies like AI, the cloud and IoT. This rapid development and adoption drive escalates security risks to business applications, revealing critical vulnerabilities in an alarming 80% of them, and this figure jumps to nearly 90% with open-source code. The stakes stand high, with data breaches costing an average of \$7.2 million and taking about 80 days to detect. Such events impose not only financial loss but also significant reputational damage. The rush to market frequently leads to insufficient security checks, leaving sensitive customer and enterprise data dangerously exposed to cyberattacks.

Key challenges confronting Application Security (AppSec) teams

1. Today's software development scene is complex, blending Agile, DevOps, and cloud-based solutions, alongside DevSecOps, APIs and microservices demanding high coordination and tackling numerous security hurdles.
2. The growing reliance on open-source and third-party components, while boosting development speed, introduces significant vulnerability risks, necessitating diligent security and continuous monitoring by AppSec teams.
3. Furthermore, the scarcity of skilled AppSec professionals exacerbates these challenges. This talent gap hinders organizations from effectively enhancing their application security posture, leaving applications exposed to potential attacks.

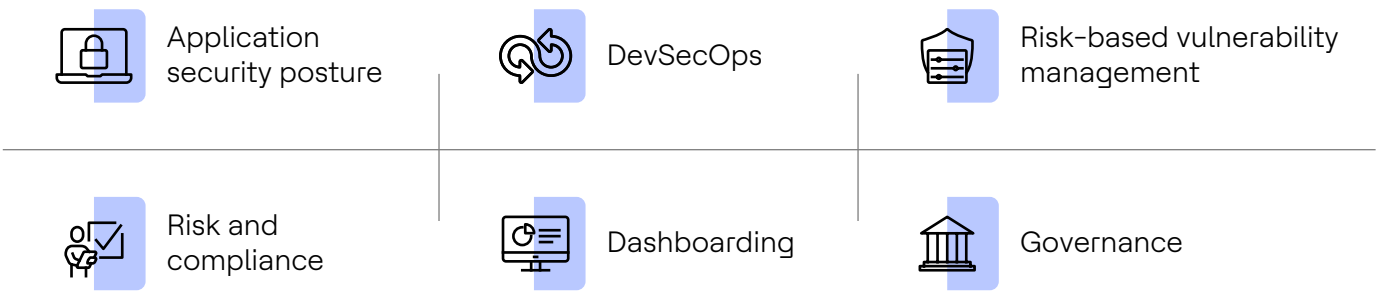


A fresh approach

In the current complex environment, the traditional method of securing applications by isolating them in silos falls short of effectively managing security challenges. There is a pressing need for a more innovative approach that is robust, scalable and capable of seamlessly integrating with the dynamic nature of applications. This approach necessitates the careful selection of appropriate tools that are capable of accurately identifying vulnerabilities. Furthermore, it's essential to have a team of skilled professionals with the necessary expertise to analyze, interpret and implement solutions to these security challenges. Our services are designed to address these needs through a comprehensive, multi-stage strategy to safeguard your applications.



ASPM platform



Application Security Posture Management (ASPM) benefits

Application Security Posture Management (ASPM) offers significant advantages for organizations looking to bolster their cybersecurity defenses. These benefits encompass a range of critical areas, ensuring comprehensive protection and streamlined security processes.



Enterprise application inventory identification and classification

The ASPM platform allows organizations to identify and categorize all enterprise applications comprehensively. This process is crucial for understanding the entire software asset landscape, enabling better security management.



Effective and efficient tools integration

One of the standout features of ASPM is its ability to integrate seamlessly with a wide array of security tools and platforms. This integration capability facilitates a more streamlined and cohesive security strategy.



Visibility of vulnerabilities

Visibility into vulnerabilities is essential for maintaining a strong security posture. ASPM solutions provide clear and comprehensive visibility into the security vulnerabilities within an organization's application portfolio.



Elimination of duplicates

Duplicate vulnerabilities can clutter security reports and dashboards, leading to inefficiency and potentially overlooking critical issues. ASPM helps identify and eliminate duplicate vulnerability findings, streamlining the vulnerability management process.

Vulnerability tracking and reduction



Effective vulnerability management is a dynamic process that involves ongoing tracking and mitigation efforts. ASPM platforms enable organizations to track the progress of vulnerability remediation activities, providing a clear overview of how vulnerabilities are being addressed over time.

What we deliver?

Our solution combines market-leading technology with the deep security expertise of our people. The ASPM platform sits within our cybersecurity portfolio and perfectly complements our wide range of established cybersecurity services. We will support your digital transformation, providing you with the reassurance you need to embrace new ways of working. Our approach at HCLTech is uniquely holistic, covering every critical phase from discovery to transformation. Here's a detailed view of how we assist you in your journey of maturity.



How HCLTech leads your journey to maturity



Discover

Assess customer ecosystem applications
discovery understand application security
maturity identify security tools discover
compliance requirements



Establish

Application security best practices integrated
security tools configure security policies CIO
vulnerability dashboard security process and tool
recommendations tools retiring
recommendations



Run by phase

Aggregate security findings – SAST.DAST/PT/
infra/cloud application-level risk analysis
remediation guidance and automation
vulnerability governance- tracking made easy
compliance monitoring and reporting



Continuous transformation

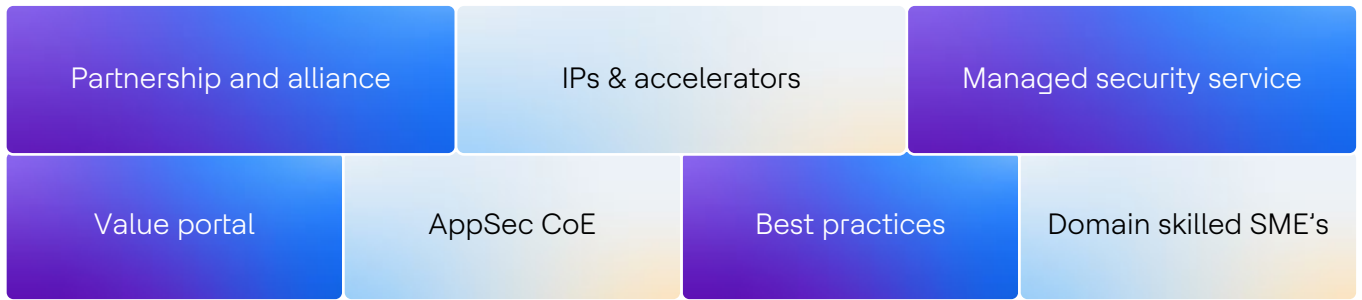
New tools onboarding new application
onboarding process improvements training
assets creation app modernization

Improve



Security orchestration and correlation across tools integration with DevSecOps pipeline
tool Rationalization metrics , KPI's, SLA tracking audit proof reporting's cyber insurance
rationalization security tool finetuning

Enablers



HCLTech | Supercharging
Progress™