HCLSoftware

eGuide: Procuring an Application Security Testing Partner

HCL **AppScan**

Summary

We live in an era of digital transformation.

Organizations around the world are using digital technologies to create new employee cultures, business processes and customer experiences that reflect rapidly changing business and market requirements. The exponential growth of remote work, cloud computing, online banking and shopping, and so many more web-based services is unprecedented.

And with all of this has come unforeseen vulnerabilities, threats, and crime.

Identity theft, data breaches, hacking, etc. are all common news stories today and businesses have a lot to lose. In a 2022 Cost of Data Breach Report by IBM and the Ponemon Institute Report, data breaches cost companies on average $4.35 million.

Data breaches cost companies on average $4.35 million.

To avoid these monetary and reputation costs, companies are increasingly purchasing application security testing software that can assist with scanning and fixing vulnerabilities in application code so that they can more effectively secure their data.

This eGuide provides valuable insights into procuring an application security testing partner including gaining an understanding of use cases, critical technologies, and best practices.

Table of Contents

04 | Introduction: Choosing the Right Solution

05 | Application Security Today

06 | Application Security Testing Technologies – a Quick Introduction

07 | Choosing the Right Technology and Platform

08 | Additional Features and Strategies

09 | Considering Cost

10 | Finding the Right Vendor

11 | Setting Expectations

12 | Conclusion

13 | About this e-Guide

Introduction: Choosing the Right Solution

Application security testing encompasses a broad array of technologies, platforms, and services, all used to find and fix the vulnerabilities in application code. Choosing the right solution depends on many factors.

It is important to determine who will be responsible for securing the applications and their code, when this is best done to ensure effectiveness and efficiency, and what the guidelines need to be when implementing a testing and remediation program.

Choosing which technology or suite of technologies to use is based as much upon how they work as who will be using them, and at what stage in the application development life cycle.

Educating stakeholders about potential security threats and setting expectations about costs is critical, as is considering both short and long-term strategies that account for growth and change.

Gaining an understanding of all these factors puts organizations in a better position to choose the right application security testing partner with the right solutions for its business needs.

> Solutions must balance the needs of development speed with effective application security.

Application Security Today

Culture

Security-focused companies that develop web applications are finding ways to prioritize application security as early as possible in the application development life cycle. This is referred to as "shifting left" and increasingly places more responsibility for security on developers.

Application security testing software helps developers write secure code without slowing down the speed of delivery. It helps DevOps teams and security teams review and test both the code and the completed applications to ensure there are no vulnerabilities.

"Shifting left" and prioritizing application security as soon as possible is key to success in reducing business risk.

Security Stakeholders

Application security that was the domain of third-party security experts in the past is increasingly being handled in-house by companies that develop their own applications.

Developers, as previously noted, are being asked to analyze their code as they write it. DevOps teams now continuously test and analyze applications throughout development and implement policies and checks and balances to reduce vulnerabilities. Overseeing policy, pen testing, and providing one more layer of expertise are security analysts. In charge of all security is the company's CISO (Chief Information Security Officer).

Companies should be able to identify all their application security stakeholders and make sure that the software solutions they choose allow everyone to work together successfully.

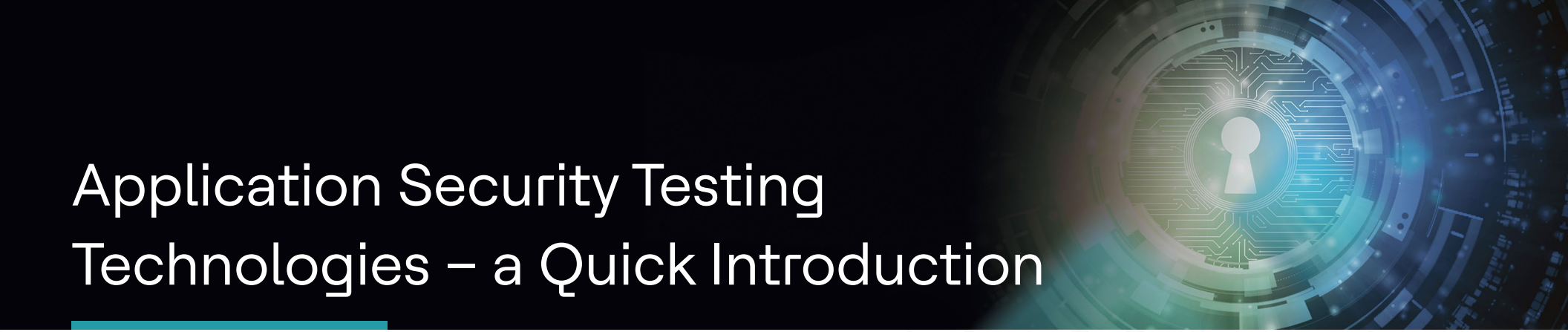
Policy

As the need for security and privacy have increased, so have government and industry regulations, designed to hold companies accountable for the data they handle. It is important that the application security solutions one uses can incorporate both external and internal security policy requirements.

When considering application security testing needs, ask the following questions:

- Where is my business risk?
- Is my private sensitive data exposed by apps?
- How do I set internal policy requirements for application security?
- How do I check for and demonstrate application compliance?

Application Security Testing Technologies – a Quick Introduction



SAST (Static Application Security Testing)

SAST analyzes an application from the "inside out" in a nonrunning state by reviewing each line of source code for security vulnerabilities.

DAST (Dynamic Application Security Testing)

DAST is used to run a variety of tests on running applications to identify potential security vulnerabilities and architectural weaknesses.

IAST (Interactive Application Security Testing)

IAST monitors web applications for security vulnerabilities while the application is run by an automated test, human tester, or any activity "interacting" with the application functionality.

SCA (Software Composition Analysis)

SCA automatically locates and analyzes open-source software and packages that have been incorporated into an application's codebase.

API TESTING (Application Program Interface)

API Testing sends requests to program interfaces in order to check their security, functionality, performance, and relability.

Since each technology scans for vulnerabilities differently, they are often best used together to ensure not only that vulnerabilities are found, but also to validate fixes, and correlate results to prioritize more easily what needs to be fixed.

Choosing the Right Technology and Platform

Technology

The scanning technology or combination of technologies that is chosen is influenced by the development environments and integration models that are used.

For developers, finding a SAST technology that will function seamlessly with a preferred IDE (Integrated Development Environment) is critical, since this is where they are already working most efficiently.

For DevOps and security teams using a traditional waterfall software development life cycle, SAST is again an important option, but DAST technologies testing running applications can also be used to validate fixes.

Since IAST monitors and provides feedback on running applications without slowing development time, it is favored more in both Agile development environments and in those using a continuous integration/continuous delivery (CI/CD) model.

SCA is another technology often used in CI/CD pipelines or wherever there is both a focus on speed of delivery, and where there are numerous open-source packages that have been incorporated and need to be tested prior to release.

Platforms

On-Premises. These are desktop solutions where one or more security testing tools are downloaded and used locally by developers, DevOps teams, and security teams. A provider might offer a single technology or provide a suite of technologies to use together. Some industries have regulations requiring on-premises security solutions.

On-Cloud. These security testing tools are available by logging into a cloud server and can be accessed from anywhere. Again, providers may offer one or more technologies that can be used together or separately. On-Cloud platforms often allow the security partner or third-party security teams to monitor the testing and remediation efforts more easily.

The ideal application security solution should complement a development model and working environment.

Additional Features and Strategies

A Simplified User Experience

In some cases, a single technology may handle many specific testing requirements, but since each testing tool scans differently, using two or more often leads to more confidence in the findings. Look for a partner whose platform includes a centralized dashboard and control center where all results can be viewed together so that it is easier to prioritize which issues to fix first.

Oversight and Compliance

A centralized dashboard also helps maintain accurate oversight of all the application security testing an organization is doing by increasing visibility and accountability. It allows security teams to create automated testing guidelines based on both threat modeling and compliance policies.

Scalability

Purchasing a single application security scanning technology may make sense in the short term. But as a business grows and development cycles move faster, there will be more code to scan in shorter amounts of time. It is thus important to consider a partner that can offer what is needed today and anticipate future needs, as well.

Considering Cost

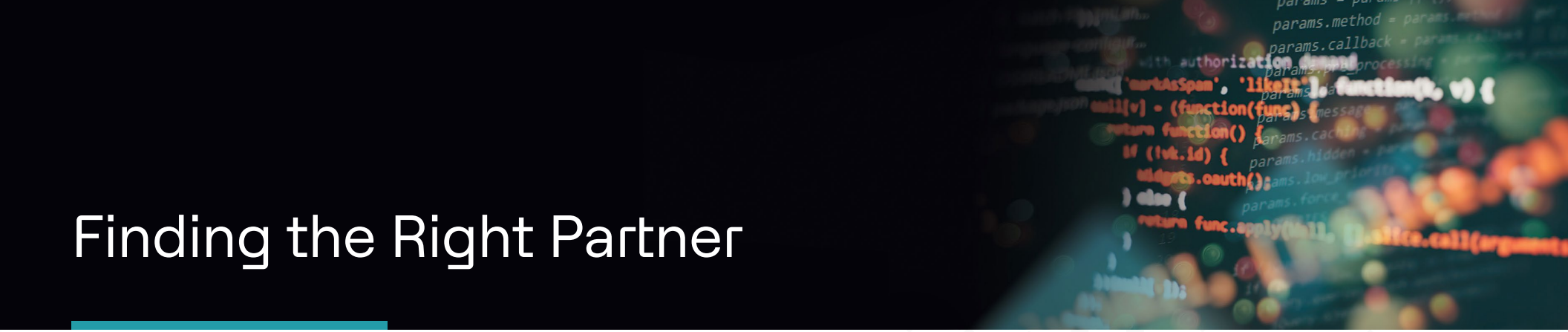
Cost versus Risk

Depending on the size of development needs, the cost of application security can vary greatly. When convincing the CFO of an organization that this type of expense is necessary, it is worth considering the cost of doing nothing from a risk perspective. According to the 2022 Cost of Data Breach Report by IBM and the Ponemon Institute Report, data breaches cost companies on average $4.35 million.

Cost versus Time and Resources

Because much of the application security testing technology today can be used to automatically run tests and correlate results for easier remediation, purchasing these tools can amount to a significant savings in time and resources.

In a recent Forrester Total Economic Impact Report, published in 2022, a Brazilian financial institution saw a 151 percent Return on Investment (ROI) when they switched from manual, third-party application security testing to using an automated software solution. Much of this ROI was based around time savings. Prior to the switch, the company reported that finding and remediating an application vulnerability was taking up to 120 hours (five days).



Finding the Right Partner

An application security testing partner should do more than just sell testing software. There are several additional factors to consider in making a decision:

Technology Ownership

Look for a partner that owns and develops their own proprietary application security software. While some companies have purchased security technologies to sell as their own, companies that develop their own software often provide suites of solutions that work better together and are quicker to release new versions that stay current with security trends and threat models.

Demos, Free Trials, Support

If interested in a technology solution, several companies provide demos and free trials. And, in some cases, there are free versions of the software available for certain segments of the market.

Research Teams and Ongoing Development

Be sure to choose a provider that is actively engaged in ongoing security research. Their commitment to finding vulnerabilities ahead of time and building that knowledge into an organization's tools are critical to staying out in front of threats.

Education and Support

Look for not just a vendor but a partner that offers education, technical support, and potentially customized solutions that address the specific security needs of a business.

Third-party Reviews and Analyst Reports

There are several reputable technology research and consulting firms that publish regular reports on the application security landscape and the companies providing these services. Gartner, Forrester, and IDC are a few examples.

Setting Expectations

Speed versus Security

The more seamlessly application security testing can be added to a development pipeline the less the whole development life cycle is slowed down. Balancing the needs of development speed and application security requires software that can orchestrate testing protocols, correlate results, and help prioritize which issues to fix.

Time and Human Resources

Automatic application security scanning will undoubtedly save an immense amount of time and money but there is some necessary investment up front as things are set up. Establishing policies, determining security roles and responsibilities, and fine-tuning the technology to do what is needed to do, are all necessary parts of the process.

Defining a Security Baseline

It is common for companies to discover an overwhelming backlog of security vulnerabilities once they begin an automatic testing program. Prioritizing fixing all those old issues may not make sense, especially since they have not yet led to a security breach. Often, a better policy is to work to secure all new code going forward and address the backlog as a secondary priority, as time and opportunity allow.

All security stakeholders need to have a shared set of expectations regarding time, speed, and resources to implement application security effectively.

Conclusion

Application security testing software helps organizations that develop their own web applications reduce costs, avoid risk, and avert potentially damaging data breaches. These products, platforms and services assist with scanning and fixing vulnerabilities in application code before web applications reach the market. To choose the right software solutions for a business, focus needs to be on three fundamental areas.

Organizations should develop a comprehensive security picture, the people and culture that make it up, and the application development model that they intend to use. Additionally, they need to decide who will be responsible for application security testing and who benefits most from the use of these tools. Organizations should also determine the policies that need to be followed and whether company growth is anticipated.

Understanding the main types of application security testing technologies available and where each integrates best into the software development life cycle is critical. Each tool has different strengths and there can be benefits of using more than one such as validating vulnerabilities to be fixed.

Organizations need to consider the size, history, and expertise of the vendor as well as their commitment to research and innovation. Ideally, an organization should want an application security partner that not only provides testing software, oversight, reporting, and easy-to-use platforms, but is also committed to onboarding, continuing education and training.

Securing application code before it reaches the market is a crucial step to reducing business risk. Procuring the right application security testing partner for a specific business is a major step in accomplishing this goal.

About this eGuide

HCL AppScan is a scalable suite of security testing platforms and tools including SAST, DAST, IAST, and SCA, available on-premises and on cloud. HCL AppScan technologies detect pervasive application security vulnerabilities during development and facilitate remediation before the software is deployed. Developer-focused advisories and language specific code samples empower developers to remediate vulnerabilities and instill secure coding practices. Comprehensive management capabilities enable security professionals, developers, DevOps, and compliance officers to continuously monitor the security posture of their application and maintain compliance with regulatory requirements.

For more information, visit hclfederal.com or contact info@hclfederal.com