BLACKDUCK®

GUIDE

Managed Services Buying Guide

Managing security risk can feel like climbing a mountain. The terrain is rocky and the grade is uneven. Conditions can change suddenly, making it difficult to reach your goal.

Even the most experienced climbers travel together to share the burden.

It's more challenging than ever to keep your sensitive information and assets safe from cyber threats. Some experts expect the number of unfilled cyber security positions to exceed 1.8 million by 2022.[1] But staffing an internal security team is expensive, particularly when you need experts that understand a range of potential threats and security strategies.

Don't climb a mountain without a team to support you

Managed security services partners support a variety of cyber security functions, including identity and access management (IAM), incident response (IR), and security information and event management (SIEM). These efforts are essential in an overall security plan for companies that can't afford to purchase tools or build out a security operations center.

That said, these types of managed services activities are typically passive. They involve monitoring and responding, not proactively working to lower the risk of a cyber attack. They also tend to ignore one of the most critical areas of security risk: applications.

Why seek support from managed services?

While application security has improved in the past five years, 82% of reported security vulnerabilities still lurk in application code, not in networks.[2] Yet most companies do not have the deep skill set or the appropriate tools to address application security risk.

What's more, testing demands ebb and flow. When new threats emerge or business changes invite new risk, your internal team has only a fixed capacity to address vulnerabilities. You might have to delay launches if your team can't keep up. On the other hand, if you staff up to meet immediate needs, you may be overspending when demand decreases.

A managed services partner that specializes in application security can offer proactive security testing for web and mobile applications, including static (SAST) and dynamic (DAST) assessments, as well as manual business logic testing. In addition, a partner can provide remediation guidance to fix software security bugs or flaws so you can prevent attacks before they happen.

If you're considering using managed services to address your cyber risk, you're in good company: 99% of C-level executives surveyed in 2019 said they had outsourced at least some of their cyber security functions.[3]

How to choose the right partner for your security journey

Shifting from an in-house application security solution to a managed services model is a big decision. The assumptions you use to compare costs and benefits depend in great part on the partner you select. Use this Buying Guide to make sure the vendor you choose helps you reach the mountaintop—and realize the return you expect.

Before you select a vendor, there are a host of questions to answer, requirements to define, and options to consider. Use the following as a framework for your discussions.

1. How do you test for vulnerabilities?

Why it's important to ask: Finding a managed services partner that has deep expertise in application security is vital. The right partner will combine tools and expert-driven manual analysis based on business context to identify and qualify vulnerabilities in ways automated tests alone cannot. With this approach, results are true positives and remediation guidance is actionable.

What to look for: A managed application security services partner should offer security testing for web and mobile applications, including static (SAST) and dynamic (DAST) assessments, as well as manual business logic testing for multistep attacks.

A managed services provider with broad responsibility for your application security shouldn't just test individual apps. Instead, they should investigate your system architecture to flag vulnerabilities that occur when applications share information or rely on the same controls.

Hybrid application and network testing is becoming more important for security, particularly as the Internet of Things (IoT) affects how applications are accessed. Look for a managed services provider that also offers network-level assessment services. They should search for vulnerabilities in areas such as router filtering, firewall filtering, visible network services, operating system software flaws, server application software flaws, known configuration errors, access management, and authentication controls.

2. What is your pricing structure?

Why it's important to ask: Pricing for application security services should be transparent. Pricing against a standard set of requirements will help you make an apples-to-apples comparison of any managed services proposal you receive. The clearer the requirements are between you and a vendor, the more likely you are to receive the value you expect.

What to look for: The amount you pay a managed services provider can depend on a variety of factors, such as:

- Number of applications to test
- Mix of web and mobile applications
- Number of applications that require in-depth manual testing and business logic testing
- Time period over which to conduct testing
- Turnaround time to receive testing results
- Type and quality of findings reports
- Whether read-out calls with developers are included
- Whether retests are included
- How often business or product changes, such as release schedules, will affect application security
- Location, which may affect compliance considerations or legal concerns regarding data storage
- Whether you require services other than application testing and remediation, such as threat modeling or network penetration testing

Once you have a common set of requirements, you can choose a partner based on expertise and approach. A partner that provides true positives and actionable advice may be more expensive than one who hands you a report of bugs and flaws with little guidance. However, with the right vendor, your overall costs should decrease, as the time and effort needed to find and fix vulnerabilities will go down.

3. How predictable will the budget be?

Why it's important to ask: Once you and your managed services partner agree on a price for services, you should be able to structure an agreement with a predictable price. You should not have to pay extra for customized reports and remediation of bugs and flaws or other hidden fees that catch you by surprise.

What to look for: Your managed services provider should work with you to set up an agreement that incorporates diverse applications at varying levels of testing depth, covering multiple testing cycles. If you have unanticipated testing needs, you should be able to add a la carte services easily at a predetermined price. Some vendors may also offer packages that provide unlimited testing at any depth so that you don't need to worry about costs increasing if your needs change.

4. How will you help us determine our priorities?

Why it's important to ask: Without prioritization, your team may spend countless hours trying to fix vulnerabilities that have little impact on your business, while ignoring others that introduce greater risk.

What to look for: Findings from security assessments should have a standard severity rating scale and consistent read-outs so your team knows where to start remediation efforts.

5. How do you address varying levels of criticality across an application portfolio?

Why it's important to ask: Not all applications require the same level of testing. If your partner tests all applications in the same way, you could be overspending. It's far better to focus your resources on testing applications at an appropriate level.

What to look for: Your partner should provide multiple levels of application security testing, from automated scanning that identifies common vulnerabilities to in-depth manual testing that focuses on business logic testing and exploiting application functionality. They should apply the appropriate level to each application.

6. Who will be on my account's team?

Why it's important to ask: You rely on your managed services partner to stay up to date on the latest cyber threats and risk management strategies. The quality of service you receive depends on both the staff's expertise and their ability to apply that knowledge to your business and applications.

What to look for: Your managed services partner should have engagement management and technical delivery staff with deep technical expertise, covering a breadth of technologies and business domains. They should take the time to build a relationship with your team to transfer knowledge most effectively. Your partner should offer an option to set up a credentialed pool of staff who will be the only staff accessing your data.

7. What types of assessment tools do you use?

Why it's important to ask: Some vendors use only tools they sell, or apply a simplistic approach to tool-based scans. The truth is no single tool offers complete coverage. Even for a single application, different tools may catch different vulnerabilities. Eliminating false positives requires tuning tools to your situation and comparing the results of various tools against each other.

What to look for: Look for a managed services provider that employs a combination of commercial, internally developed, and open source tools so that they can serve the most appropriate testing techniques for the application under test.

Your managed services partner should be able to customize rule sets to get the most out of a tool for your situation. Don't let a managed services partner lock you into using a tool that they sell. If you have a tool you prefer, make sure they can use that as well.

8. What is your process to schedule or change requests for tests?

Why it's important to ask: You shouldn't have to give up visibility or control over application security testing just because you're using a third party to help with execution.

What to look for: Managed service providers should make it easy for you to control the assessment schedule and see the status of tests you've requested. Providers often offer a web-based portal where you can make changes at any time. Ask for a demonstration so you can test it out before making a decision.

9. How quickly will you provide results?

Why it's important to ask: You should expect a reliable, consistent time frame so that you can plan ahead and not slow down development.

What to look for: The answer will likely depend on the test depth you require, but you should expect results within three to five business days after test completion. To accomplish this, your managed service provider should integrate the testing process with your development flow, regardless of your development methodology. For production tests, your provider should notify you immediately after qualifying the findings.

10. What deliverables are included with the results?

Why it's important to ask: Clarify with any potential partner that test results will not simply offer a list of issues and generalized advice. Results will be much more valuable and save time in the long run if they help developers understand issues and, more importantly, how to fix them.

What to look for: Ask potential providers for sample assessment reports. Reports should point out specific areas of risk and include detailed and relevant remediation guidance that goes beyond a list of findings. They should include an analysis of aggregate issues to identify trends and systemic problems.

The most effective results require an active discussion between assessors and developers in the form of read-out calls. Your partner should provide ongoing, on-demand remediation support.

A proactive managed services provider will also deliver reports that help you compare the performance of different business units and demonstrate improvement over time.

11. How will your remote team access our confidential information?

Why it's important to ask: Your customers and employees trust you to keep their information secure. Any partner you choose must take confidentiality and data privacy as seriously as you do.

What to look for: Your managed services partner should be able to provide options for accessing applications, whether via the cloud or with a pool of staff provisioned with your laptop and VPN credentials for remote access.

12. What solutions do you provide that will help us reach our goals in the future?

Why it's important to ask: Not all managed services providers offer solutions to help your developers become more proficient at building security into their process. The more effectively you can help developers build secure software, the less time and money it will take to fix issues.

What to look for: Your managed services partner should offer many options for remediation advice, from read-out calls to an on-demand help desk. They may also have additional consulting or training services to help you grow your software security initiative.

References:

1. William Crumpler and James A. Lewis, The Cybersecurity Workforce Gap, Center for Strategic & International Studies, Jan. 29, 2019.
2. Positive Technologies, Web Applications Vulnerabilities and Threats: Statistics for 2019, Feb. 13, 2020.
3. Deloitte, 2019 Future of Cyber Survey, March 2019.

The team braving the security mountain includes multiple climbing parties, including different functions and business units inside your organization. A vital part of the buying process is sharing a vision of success and gaining acceptance from your security staff, the development team, and executive leadership.

Include stakeholders from different departments in the vendor selection process to make sure they're comfortable that you've addressed their needs. The more involved they are in the early stages, the better prepared they'll be to work together with a new partner. To ensure you get the budget and executive support you need, make sure you can demonstrate to company leadership that you'll get the most return on your investment with the vendor you choose.

As a result, you'll pave the way for a successful transition that reduces risk and elevates security in the culture of your organization. You'll be well on your way to the security mountaintop.

Next steps

Once you've decided to move forward with a managed services partner, you'll need to gain the support of your leadership team.

Demonstrate return on investment for managed services and have a productive conversation with your board of directors about your application security needs.

.

Learn more

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.