SYNOPSYS®

Top 6 Application Security Hurdles and the Secret to Overcoming Them

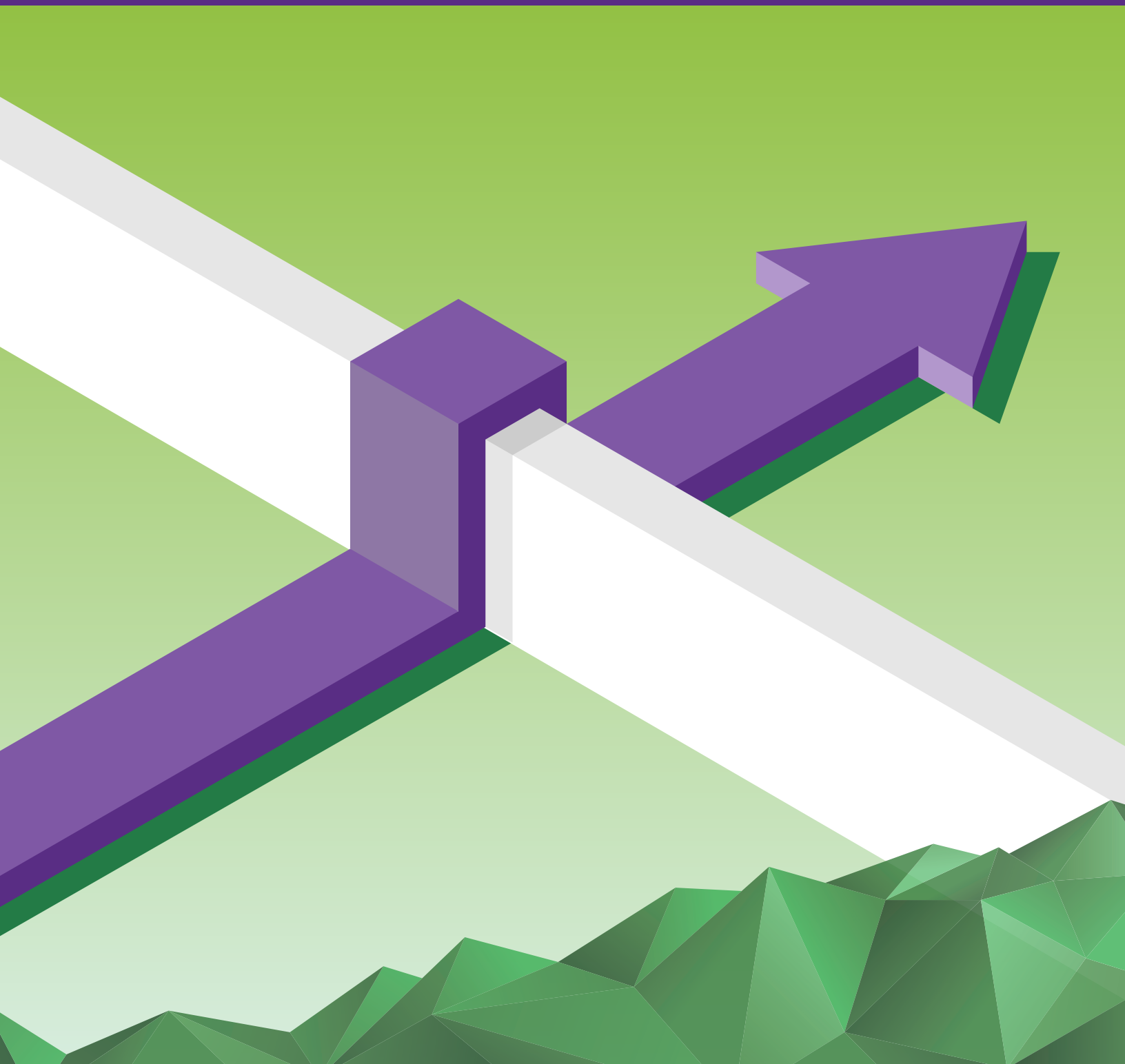


Table of contents

Are you stuck at the application security starting gate?

Applications support organizations' most strategic business processes and access their most sensitive data. Yet application security continues to receive less budget and attention than network security.

Why? It can't be for lack of awareness. Weekly headlines remind security experts and business leaders alike that hackers seeking to break into organizations target applications.

As Forrester's The State of Application Security, 2019 reports, "Application weaknesses and software vulnerabilities continue to be the most common means by which cybercriminals carry out external attacks."[1]

So when a company hesitates to implement or expand its application security program, what are its leaders really thinking?

We don't have the time.

We don't have the expertise.

We don't have the money.

We can't afford to slow things down.

Lack of time, skill shortages, limited budget, and the mandate to deliver as fast as possible are indeed hurdles—more on that shortly. But the irony is that if your organization suffers a breach, you'll spend more time and money on response and recovery than you would have spent on improving security to avoid the breach. And that doesn't even count the possibly catastrophic cost of brand damage.

So the reasons above are not so much reasons as **they are excuses**—risky excuses.

While application security has improved in the past five years, 82% of reported security vulnerabilities still lurk in application code,[2] not in networks. The conclusion is obvious: To lower risk, you must address application security.

So the question is this: How can you lower application-related security risk while keeping costs in line and maintaining high productivity?

The answer is managed services. With managed services, you can outsource security activities to a team of skilled experts, armed with the latest methods and tools, who will perform the testing services you need as soon as you need them.

According to a 2019 survey by Continuum, 77% of small businesses expect to outsource at least half of their cyber security needs within the next five years.[3]

82% of reported security vulnerabilities lurk in application code, not in networks.

What do those companies know about the path to proactive application security? Let's find out. Here are six common hurdles you might encounter on the way to better application security and how managed services can solve them.

Hurdle 1: Hiring and retaining security experts is difficult and costly.

If you've attempted to hire security experts lately, you know it's not easy. Consider the following:

314K+

Number of unfilled cyber security jobs in the U.S. today

(Center for Strategic & International Studies)

1.8M

Number of unfilled cyber security jobs worldwide by 2022

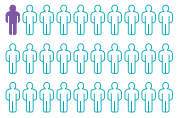
(CSIS)

32%

Expected demand growth for information security analysts through 2028

(Bureau of Labor Statistics)

1:30



Ratio of top-level cyber security experts available to experts needed globally

(RAND Corp.)

Beyond those depressing statistics, your new expert will need to have deep knowledge in multiple domains, with more to learn as your software security program evolves. Here are just the basics:

Authentication, data protection, and encryption

Static analysis and dynamic testing

Design flaws and coding bugs

Client-side applications, web apps, and mobile apps

Depending on your environment, you might need someone with expertise in areas ranging from malware to threat mitigation, cryptography, forensics, advanced analytics, network virtualization, cloud security, and mobile security, as well as industry-specific knowledge.

Plus, your new expert must have the soft skills needed to perform a demanding, time-sensitive, highly cooperative job: communication, management, reporting, and so on.

That's a lot to ask of any person. Given all that, you'll probably have better luck finding a unicorn. And if you do find an expert, it'll cost you.

The shortage of available talent for cyber security positions has caused their salaries to skyrocket. In 2018, information security analyst salaries averaged $98,350, and the top 25% made nearly $127,000.[4] Add the cost of benefits and overhead (about 43% of wages and salary in the private sector[5]), and you're looking at a major investment for a very specific skill set.

You'll also need to invest in training to make sure your new security expert stays up to speed. Roughly half of organizations plan to increase cyber security training for staff in 2020.[6]

And after all that, the risk remains that this rare creature will be lured away by a job with even better pay and benefits. More than half of companies report that it takes three to six months, or even longer, to fill open cyber security positions.[7] Furthermore, research suggests that the conservative cost of replacing an employee is 34% of their annual salary ($15,000 at the median U.S. wage of $44,564).[8]

Why managed services is your best solution

A managed services partner provides the expertise you need when you need it, from secure architecture to business logic testing, threat modeling, and mobile security. Rather than hire full-time specialists in each of these areas, you can simply draw on them as needed.

Besides that, a managed services team doesn't require that you pay them benefits, and they come with their own workspace and set of tools. Most importantly, the team can work on multiple tests and projects at once.

Finally, bringing in a managed services team frees up your employees to work on other high-priority projects even when emergencies arise. Again, you pay only for the people and tools you need when you need them.

Hurdle 2: Your legacy or third-party applications might carry security risks.

Hackers look for the easiest way into your organization. Unfortunately, your limited internal resources might not have the time, skills, or tools to identify all the paths hackers have access to, even if you've been testing your applications regularly.

Attackers also like to exploit vulnerabilities in legacy code. When your developers reuse code that has been in circulation for decades, they may unwittingly inherit its technical debt, which includes security bugs and flaws.

Consequently, your testing policy must cover your full portfolio. You need to investigate both existing applications and those currently under development, including web, mobile, and client-server applications that your team developed, as well as those you license from third parties, such as middleware or software-as-a-service (SaaS) tools.

Why managed services is your best solution

Don't let a lack of capacity dictate your software security policy. Managed services can help you eliminate testing gaps by covering the breadth of your portfolio, while adapting testing depth to match the technical and business risk of each application.

Beware of technical debt lurking in your third-party applications.

Hurdle 3: Lumpy demand requires elastic capacity.

Your testing demand is always the same, right?

Of course not. If you're like most companies, you struggle with "lumpy" demand for testing. It rises, it falls.

The most common cause of lumpy demand is an uneven rate of new applications coming out of your development group. Most companies no longer follow a fixed-release schedule. Instead, continuous integration and continuous delivery (CI/CD) has essentially become mandatory for organizations to stay competitive and meet customer demands. And each of these continual feature releases carries a different level of technical risk and business impact, which an application security program must be able to accommodate.

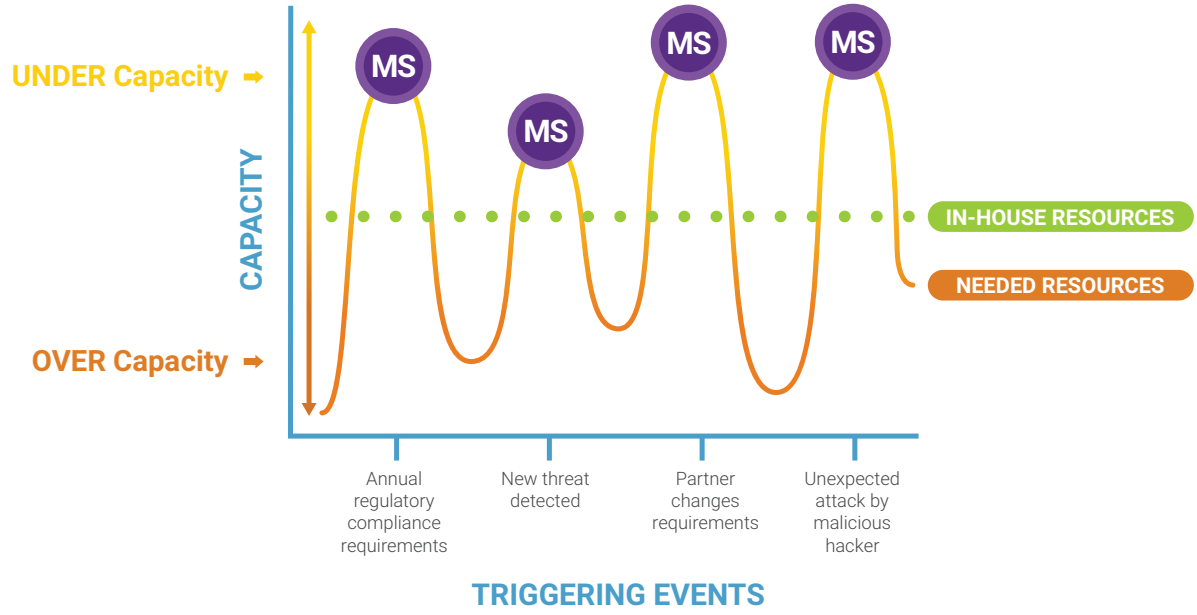
But using internal-only application security testing to meet lumpy demand can be difficult and costly. Many organizations find they have too few staff during busy times or too many skilled (and well-paid) employees sitting around during slow times—or both.

Why managed services is your best solution

Managed services can be a lifeline for companies with uneven testing demand. Once again, it provides what you need when you need it—the flexibility to call in the cavalry and then, depending on demand, call it off again.

How to stretch your testing capacity with managed services

With managed services' elastic capacity, you pay only for the resources you need when you need them.



Hurdle 4: You need to respond to changes on a dime.

Not only are you dealing with a lumpy release schedule, but your business is also evolving quickly. Your security team needs to keep pace.

Are you prepared to respond if any of these things happens?

- New threats come to light that you must investigate and address.
- You enter a new market or industry that has different regulatory requirements.
- The business starts rolling out mobile apps.
- Your organization engages in a merger or acquisition that places new apps under your umbrella.

If demand spikes without your having a full application security team on hand, you'll be scrambling to test and clean up code—or worse, to deploy patches to software that's already in the hands of users.

Why managed services is your best solution

An established managed services partner can help you respond quickly to new types of business or technical challenges. That partner will already know your systems and priorities and can hit the ground running. There'll be no need to waste time hiring, onboarding, or training.

Hurdle 5: No single testing tool can catch every vulnerability.

Over the past few years, the dynamic and static analysis testing space has become crowded, and automated testing tools have become more sophisticated. Their ability to identify common coding errors at scale has never been better.

But there's still a problem: A software testing tool is not a guarantee of reduced risk.

The reality is that each security testing tool has different strengths, and no tool catches everything. If budget and resource limits restrict you to using only one or two security testing tools, you might miss critical vulnerabilities. What's more, without the capacity to replicate and confirm findings, you might spend countless hours chasing false positives.

But the same testing tool in the hands of a security expert with decades of experience might yield more accurate results than your internal team could. It's well worth finding out if that's true.

Why managed services is your best solution

External testing partners have access to a myriad of best-of-breed testing tools. So not only can they choose the best testing approach for a specific type of application and risk scenario, but they can also compare results across tests, combine findings, and reduce false positives.

Because they work at scale, managed services providers follow a consistent process that is repeatable, test after test. Therefore, their results are more accurate and predictable.

One caveat: Some managed service providers also sell their own testing tools, which might mean they'll lock you into using that tool, regardless of its limitations.

So if you want to use a specific tool for consistency, make sure that your managed services partner can incorporate that tool into their execution plan, and that they plan to use multiple tools to get the best results.

Watch out for service providers who are in love with their own tool.

Hurdle 6: Tools alone are not enough to keep you safe.

To protect applications that manage business-critical functions or access sensitive data, running a standard set of automated scans is not sufficient. You need expertise to execute in-depth manual tests and interpret results.

Application security changes constantly. New threats and attack vectors emerge, and new regulations ramp up compliance requirements. Your testing and prevention strategies need to keep up with those changes.

Why managed services is your best solution

An expert managed services partner is versed in the latest compliance requirements and emerging threats, as well as the most effective remediation strategies.

That partner will go beyond automated scans to perform in-depth manual tests, including multistep penetration scenarios and targeted explorations with your business logic in mind.

Most importantly, expert managed services providers will interpret both automated and manual test results and help you fix the vulnerabilities they find. By providing detailed reports and read-outs, they can transfer their knowledge to your team so that you can keep learning and improving.

You've cleared your application security hurdles. Now what?

Once you find a managed services partner that can help you overcome the hurdles of fixed capacity and limited skills, you can reclaim your staff and reinvest their time.

What could you do if you and your staff could stop being so reactive?

You could leave run-of-the-mill testing of your broad portfolio to your partner and focus your internal team on more specialized tests or high-profile applications.

Or you could let your partner handle all application security testing, while you focus on high-level management: improving internal processes, motivating stakeholders, communication, education, and long-term planning.

Either way, choosing a managed services partner will allow you to be more agile in creating a flexible, forward-looking software security strategy and responding to the unpredictable, ever-evolving security threat landscape.

References

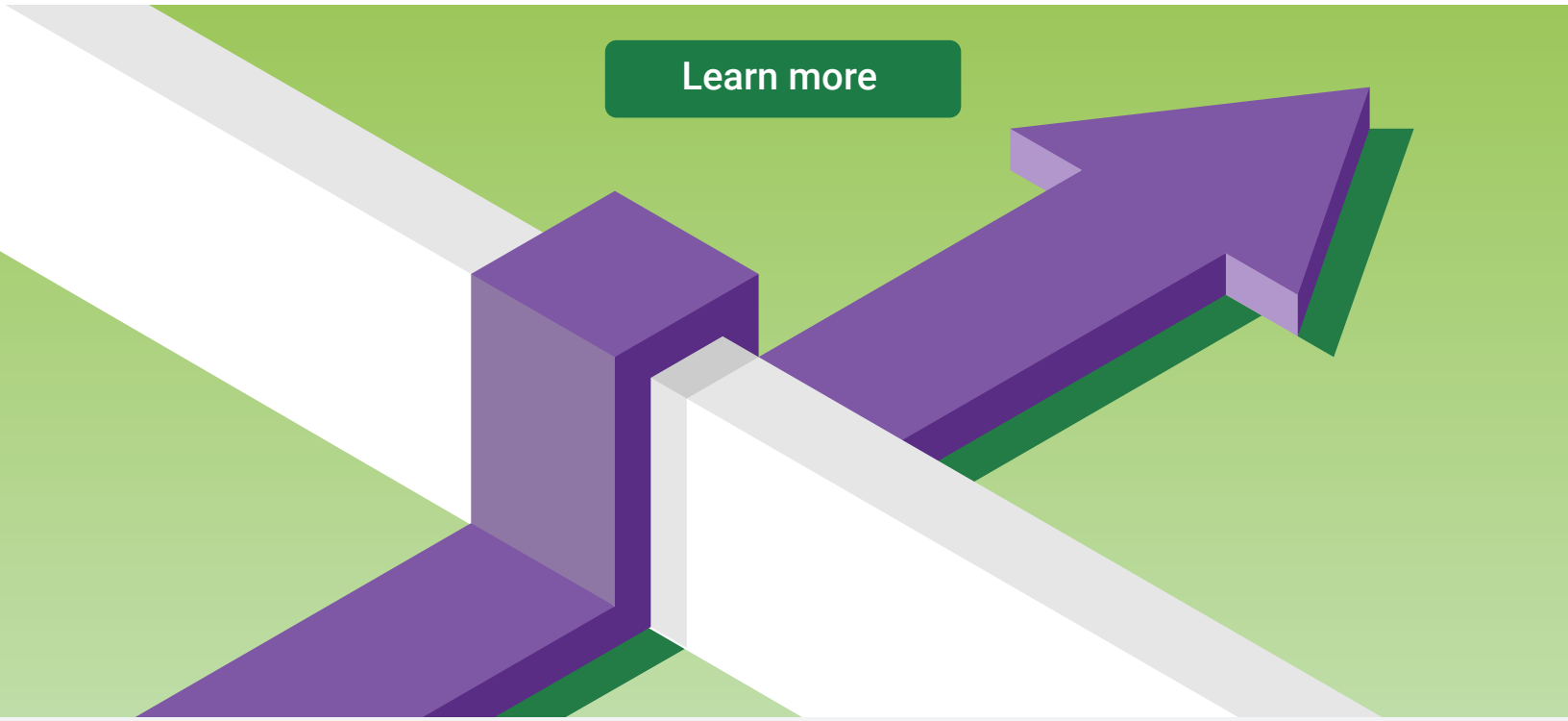
1. Amy DeMartine, with Stephanie Balaouras, et al., The State of Application Security, 2019, Forrester, Feb. 27, 2019.
2. Positive Technologies, Web Applications Vulnerabilities and Threats: Statistics for 2019, Feb. 13, 2020.
3. Continuum, Underserved and Unprepared: The State of SMB Cybersecurity in 2019, 2019.
4. U.S. News and World Report, Information Security Analyst, Salary, accessed April 27, 2020.
5. U.S. Bureau of Labor Statistics, Employer Costs for Employee Compensation Summary, March 19, 2020.
6. (ICS)^2, Cybersecurity Workforce Study 2019: Strategies for Building and Growing Strong Cybersecurity Teams, 2019.
7. ISACA, State of Cybersecurity 2020, Part 1: Global Update on Workforce Efforts and Resources, 2020.
8. Work Institute, 2019 Retention Report: Trends, Reasons & a Call to Action, 2019.

4 reasons to choose Synopsys Managed Services

1. **On-demand testing.** The Synopsys portal makes it easy to schedule tests and update existing schedules to address changing business requirements, adapt to agile development cycles, and respond to evolving threats.
2. **Elastic capacity.** Synopsys has the capacity to handle high-demand periods and eliminates the need for you to pay idle employees during low-demand periods.
3. **Higher fidelity.** Our clients tell us that they get much higher fidelity testing from Synopsys—even when they use the same testing tools we use.
4. **Access to security experts.** Synopsys believes that it is our security experts—our people—who make us different from other vendors. Every test we execute is reviewed by a security expert who analyzes the results, reduces false positives, and provides remediation guidance.

Are you ready to move to a proactive model for application security?

Now that you've determined that managed services is the best solution for your application security needs, it's critical to find the right partner.



The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com