SYNOPSYS®

Solving FSI Challenges with the Synopsys Solution Suite

The financial services industry must balance transformation and security

In the dynamic and ever-changing technology landscape, financial services industry (FSI) organizations are rushing to adopt new technologies aimed at automating internal processes, improving margins, and modernizing online and mobile experiences for customers. At the same time, these organizations must quickly transform their AppSec practices and streamline their DevSecOps strategies in response to the rapid increase in development velocity.

As FSI firms prioritize modernization efforts and adapt to competitive pressures, they struggle to implement the AppSec tools and processes critical to securing their applications at the necessary speed and scale. Misalignment between transformation and security efforts results in increased risk to both the business as a whole and to clients' sensitive data.

Synopsys confirmed this reality via a recent study commissioned by the Synopsys Cybersecurity Research Center (CyRC), "The State of Software Security in the Financial Services Industry." The Ponemon Institute conducted an independent survey of 404 FSI firms in order to understand how they are tackling application security (AppSec), and it found that a shocking 56% of respondents had experienced an attack that resulted in system failure and downtime. Further, 51% had sensitive customer information stolen from their organization at some point, and 38% had been a victim of ransomware or some other form of extortion.[1] More concerning still was the discovery that a meager 34% of FSI software included in the study had been tested for vulnerabilities, and much of that testing occurred after the software was released.[2] Clearly, application security remains a very real problem for FSI organizations.

Synopsys has identified the top six application security challenges that plague the FSI, and this paper offers an in-depth examination of how the Synopsys solution suite is specially equipped to support and resolve these challenges in alignment with your specific business needs, objectives, and risks.

The Six Challenges of the FSI

As the complexity of modern software increases, so does the challenge of securing it, including proprietary code, open source code, APIs, protocols, business logic, and more. Each of these elements comes from various sources and is then assembled into release pipelines, making for an intricate and complex environment with ties to numerous points of origin.

In the financial services industry, the implications of mismanaging application security are especially dire; opportunities for exploit abound, and the sensitive data that FSI firms are trusted to manage offers a high-profile opportunity for attack. A recent Synopsys report on the security of popular mobile applications, "Peril in a Pandemic: The State of Mobile Application Security," found that banking, budgeting, and payment apps had the most discovered vulnerabilities.3 More concerning still, according to the Ponemon report, 56% of the FSI firms surveyed had experienced system failure and associated downtime due to security issues, and 51% had their customers' sensitive data stolen.[4] Without proper application security strategies, tools, and processes, you expose yourself, your customers, and your organization as a whole to undue risk.

Challenge 1: Supply Chain Security

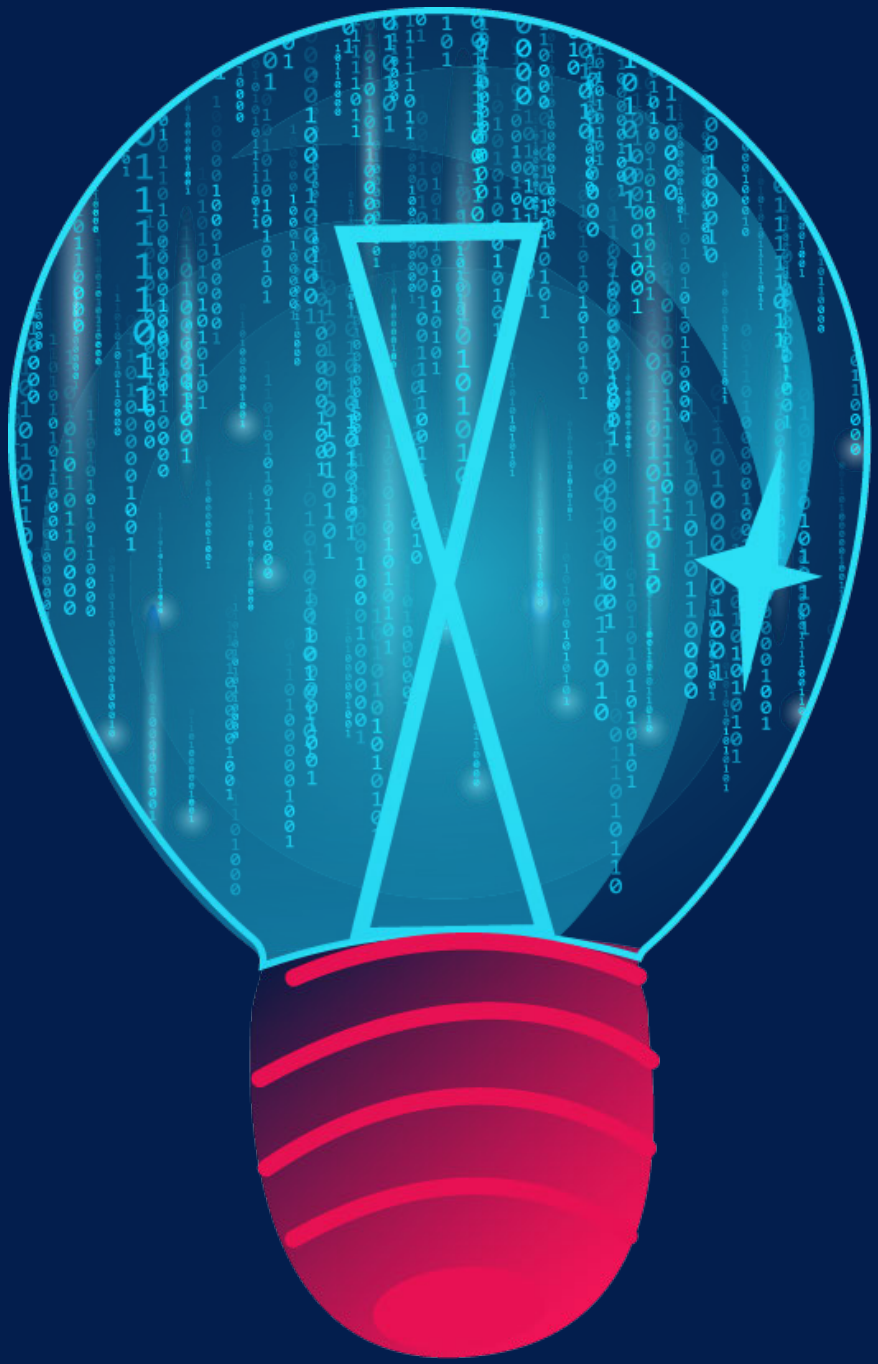
Knowing what's in the code

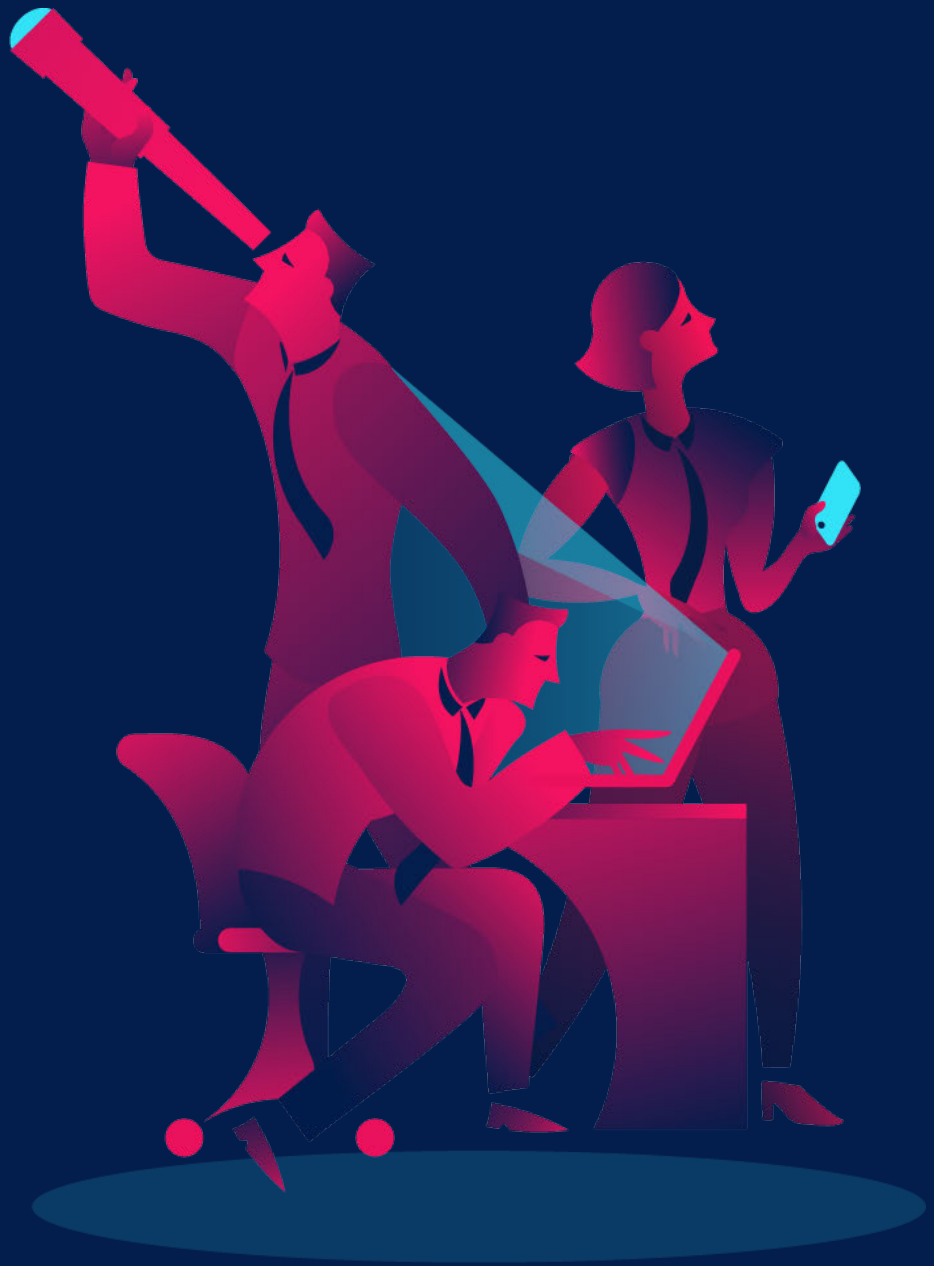
When tackling software supply chain security, it's important to acknowledge that there is no single conclusive method or strategy for guaranteeing absolute security. The supply chain is a massive expanse of items and factors, including who wrote the code, how they wrote it, who reviewed it, how it was reviewed, licensing information, binaries, package managers, and much more. It is every single activity, practice, and tool that touched the code at any point in time, from development to the CI/CD pipeline, all the way through to deployment. So security will look very different for every organization.

Synopsys believes supply chain security can be approached through three key activities.

- Securing the open source your developers build with
- Identifying and securing open source in third-party software you use
- Finding and fixing security vulnerabilities in your proprietary code

Successfully addressing security in these three areas is critical to overall supply chain health.





Securing the open source your teams build with

Today, open source is everywhere. Your developers undoubtedly use open source in nearly everything they create—meaning that large portions of your applications consist of code that you didn't write. Addressing security at every single point in your supply chain is imperative, but one of the greatest threats to your overall security is the mismanagement of open source. Open source finds its way into your supply chain via two channels: from your internal developers using open source to build, and from inherited third-party software.

The "2021 Open Source Security Risk and Analysis" (OSSRA) report from Synopsys confirms this fact: 98% of the codebases scanned in the study contained open source. Of those, 84% had at least one vulnerability, with an average of 158 vulnerabilities per codebase. This data indicates that organizations are not appropriately managing open source. When inheriting code someone else wrote, you inherit its vulnerabilities, its countless transitive dependencies, and its license obligations. Without proper practices to manage this, you expose your organization to significant security risk. Unpatched vulnerabilities, whether they are a mistake or a malicious attack, can severely affect your supply chain.

Identifying and securing open source in your third-party software

In addition to using open source in your builds, your organization may rely on commercial third-party software to deliver your products and service offerings. In doing so, you inherit this software's vulnerabilities, dependencies, and license obligations as well, and they must all be addressed. In the Ponemon report, nearly half the organizations surveyed had no policies in place that dictated how third-party vendors should address AppSec. Additionally, the same percentage had no policy requiring any level of verification from third parties to prove that any AppSec was performed at all. Put bluntly, this means 50% of respondents had no application security strategy at all for third-party or open source code.[5]

When FSI firms don't have third-party policies in place, they are unnecessarily exposing their entire supply chain to high levels of risk. A single vulnerability making its way into the supply chain via untested third-party code can have devastating consequences on the entire operation.

Securing proprietary code

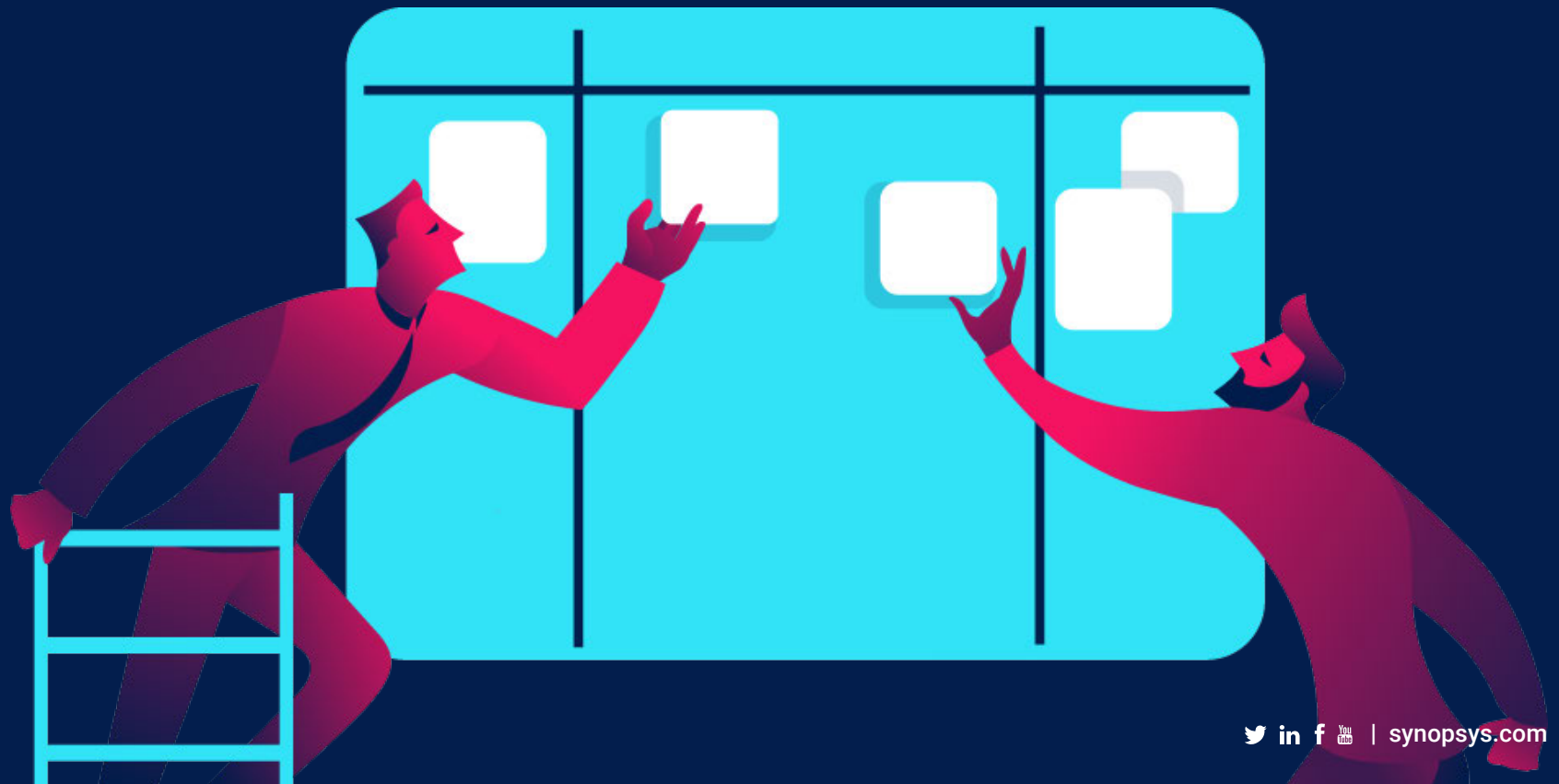
If you develop applications internally, supply chain security must be holistic and complete. Your supply chain encompasses everything from the security tools you use to the training and education of your developers. This demands comprehensive AppSec solutions; you need to manage and secure every single thing that goes on in your supply chain.

Adding a layer of difficulty, developers often lack the knowledge to practice secure coding techniques, or they haven't been trained in the best practices that are crucial to the overall health of your supply chain. And with new data privacy laws and increasing cybersecurity attacks, you need tools and solutions that prevent sensitive data leakage and ensure compliance to standards including PCI DSS, OWASP, CWE security, and more.

Organizations often must balance development velocity and security. It is crucial to incorporate solutions that let developers get started quickly and receive analysis results and remediation advice they can actually trust while they code. Without solutions capable of performing at this level, security inevitably hinders development speeds.

Facing the overarching challenge

Setting up the proper processes, policies, and tools to help effectively manage security throughout the development life cycle is a challenge. To adequately address supply chain security, you need to adopt an ongoing and constant security stance. This means you need to know about the weaknesses, vulnerabilities, and dependencies in the code, as well as the vulnerabilities in those dependencies. You also need a way to easily patch them and ensure constant monitoring. You need a clear picture of what's in your development environment, a way to manage your dependencies (maintain updates, version control, code change review), and a means for monitoring your overall supply chain strategy—making sure what you're doing is working and staying relevant. This is not an easy task without the right tools.



Challenge 2: Vulnerability Overload

Sorting through so many tools and findings

As organizations work to adopt DevOps and DevSecOps methodologies, the market continues to deliver more tools and solutions to help build out these security strategies. But more tools can lead to vulnerability overload.

With tools including static application security testing (SAST), dynamic application security testing (DAST), penetration testing, and fuzz testers, you can end up with a deluge of information from a multitude of sources. You are responsible for identifying and evaluating vulnerabilities across the entire supply chain environment, and across platforms including mobile, tablet, the cloud, and more. This can be overwhelming.

Most AppSec tools all find the same vulnerabilities and offer overlapping and redundant information. Although it's important to find all vulnerabilities across your applications, you still need to appropriately handle your findings. How do you find the true signals in all this noise? How do you know what vulnerabilities really need attention, which should be prioritized, and which can be addressed later? Even more importantly, how do you know which vulnerabilities pose real and probable threats to your development environment and business as a whole?

You need a solution that can correlate all this information and synthesize it into clearly prioritized results, so you know what you need to do and when you need to do it.

Challenge 3: Data Privacy and Protection

Ensuring your data is secure

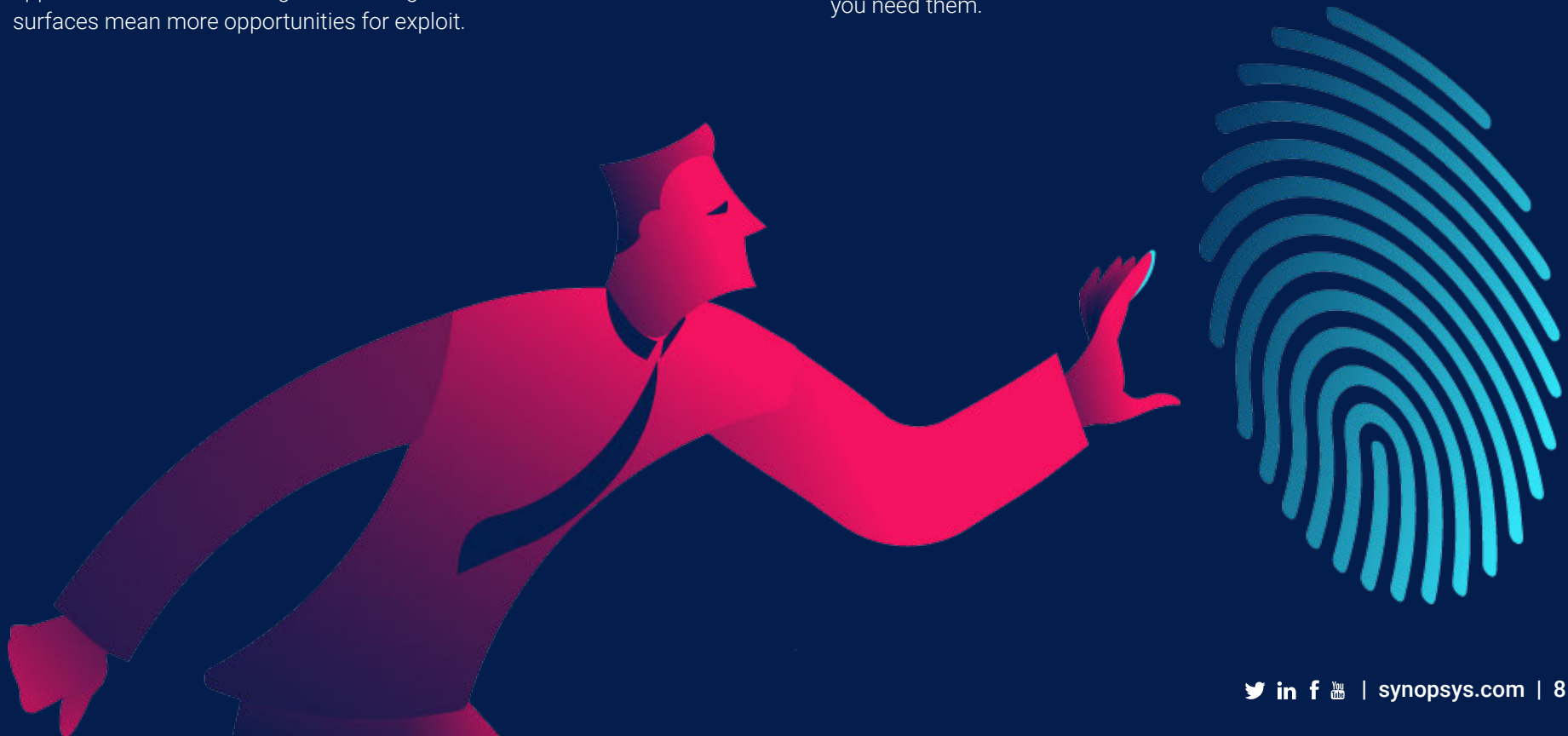
Today, new data privacy standards are driving a fundamental shift in how organizations manage risk across their applications and systems, and the processes and people building them. These standards define how user data can be used and stored, and as a result FSI firms are under increased pressure to protect user data both internally and with the third-party vendors they so often rely on to deliver their service offerings. The implications for security measures are great, and security leadership must grapple with data protection and privacy, compliance, and the overall development and security practices within their organization. FSI firms need a way to easily and reliably understand their risk, and they need to respond quickly with effective security measures.

An added layer of difficulty is the current climate; FSI firms are hurrying to transform their offerings, often at the expense of their security efforts. This rush to modernize and accommodate the increased use of mobile and web applications is also causing enormous growth of the attack vector—more surfaces mean more opportunities for exploit.

The Payment Card Industry Data Security Standard (PCI DSS) is another major concern for FSI firms. PCI DSS demands that any entity responsible for storing, processing, or transmitting cardholder data must do so in certain ways. There are specific requirements for developers about how application security is performed during the development process. FSI firms must continue to develop at high speeds while maintaining constant compliance.

Ensuring compliance with the General Data Privacy Regulation (GDPR) is also a key struggle for FSI firms. The GDPR defines how personal data can and should be transferred outside of the European Union, and it provides guidelines for data transparency, purpose limitation, accuracy, storage time limits, and much more. The GDPR also specifies how privacy should be considered during application development. Essentially, it provides a broad framework of requirements for building and using applications that touch sensitive data in any way.[6]

The challenge for FSI firms is finding tools and solutions that make compliance easy, automated, and robust. You need a clear picture of your risk, in real time, and prioritized remediation guidance and capabilities when you need them.



Challenge 4: Sensitive Data Leakage

Protecting against data leakage

Information leakage happens when developers accidentally (or rarely, intentionally) leave sensitive data within the source code or configuration files of applications. This information could be tokens, keys and passwords, or IP addresses and email addresses left behind in code. This data can allow a hacker to access your servers, systems, or property, and then access your IP, plant malware, or launch compute resources that attribute costs to you, the application owner.

In the Ponemon report's findings, over 50% of the financial institutions surveyed had experienced data theft due to sensitive data leakage. As the gatekeepers of highly sensitive personal and financial data, FSI firms must ensure that their applications are free from data leakage. Tools with effective discovery capabilities allow organizations to find instances of data leakage before they can be exploited.

Challenge 5: DevSecOps

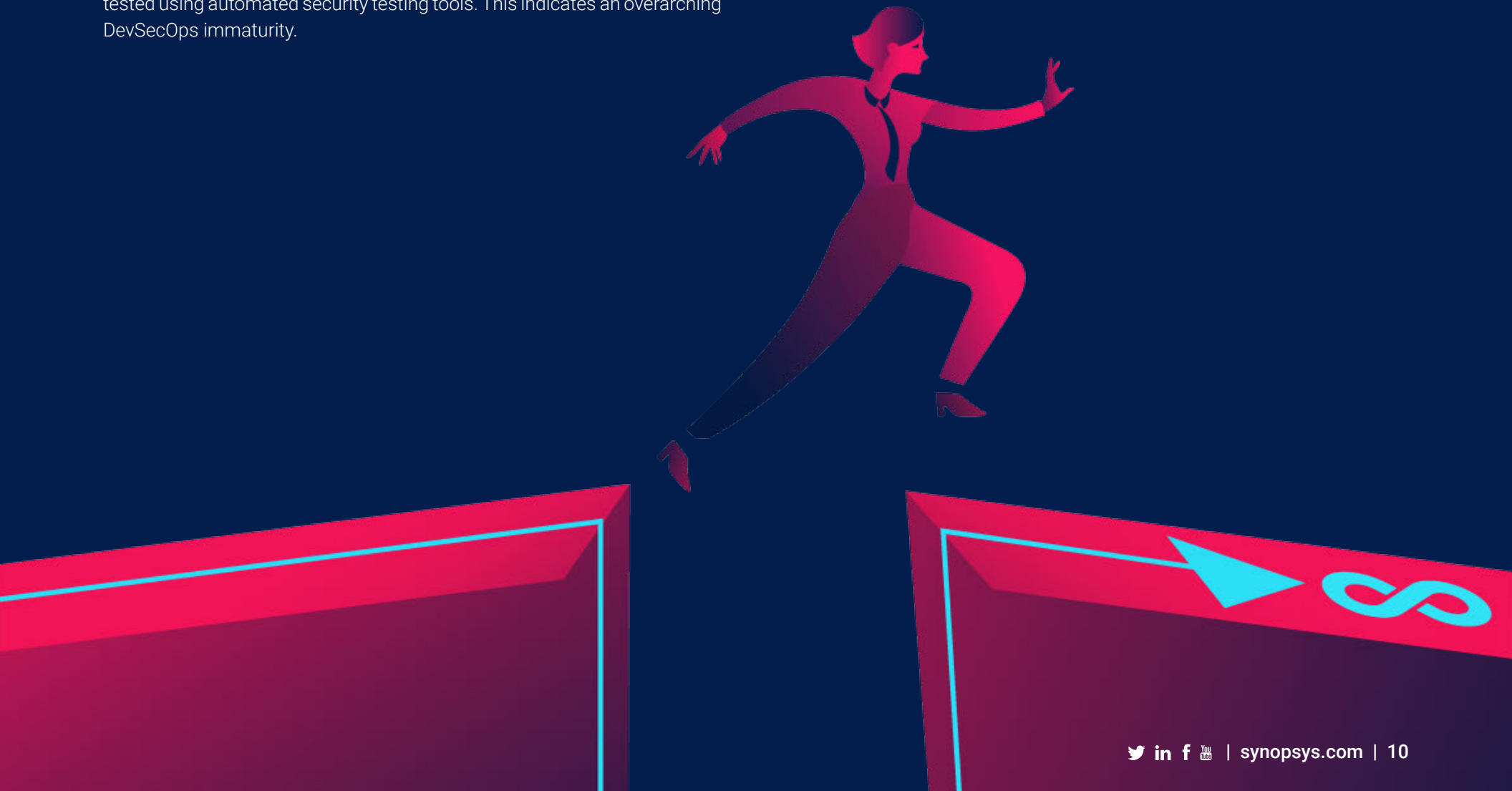
Achieving DevSecOps

If your organization develops its own applications in-house, you likely are somewhere on the journey toward adopting DevSecOps. Whether just starting or well on your way to automating and streamlining your development and security practices, achieving a successful and thriving DevSecOps environment is a never-ending effort.

Automation is a key pillar of DevSecOps and it must be central to any security initiative. The Ponemon report noted that only a third of the software produced or consumed by financial services industry organizations is tested using automated security testing tools. This indicates an overarching DevSecOps immaturity.

The goal of DevSecOps is to bridge the gaps between teams (IT, security, development) to ensure the delivery of safe and secure code, quickly. Without tools and solutions that enable the automation necessary for this effort, an organization is likely to struggle with DevSecOps adoption.

Customers are relying more heavily on digital (mobile) offerings, and FSI firms are under great pressure to deliver new products and services that keep up with this demand. Legacy infrastructure and growing compliance and security challenges compound an already-challenging security landscape. By arming your security teams with DevSecOps solutions and tooling, you can aid in delivering superior products, faster.



Challenge 6: Scarcity of Resources

Finding more security experts

As an FSI firm, you are in the business of serving your customers—so security training is not always the top priority. But without security experts, or at least security-aware individuals, application security becomes a major weakness. In fact, most FSI organizations report budget and resource constraints as hindrances to their application security.

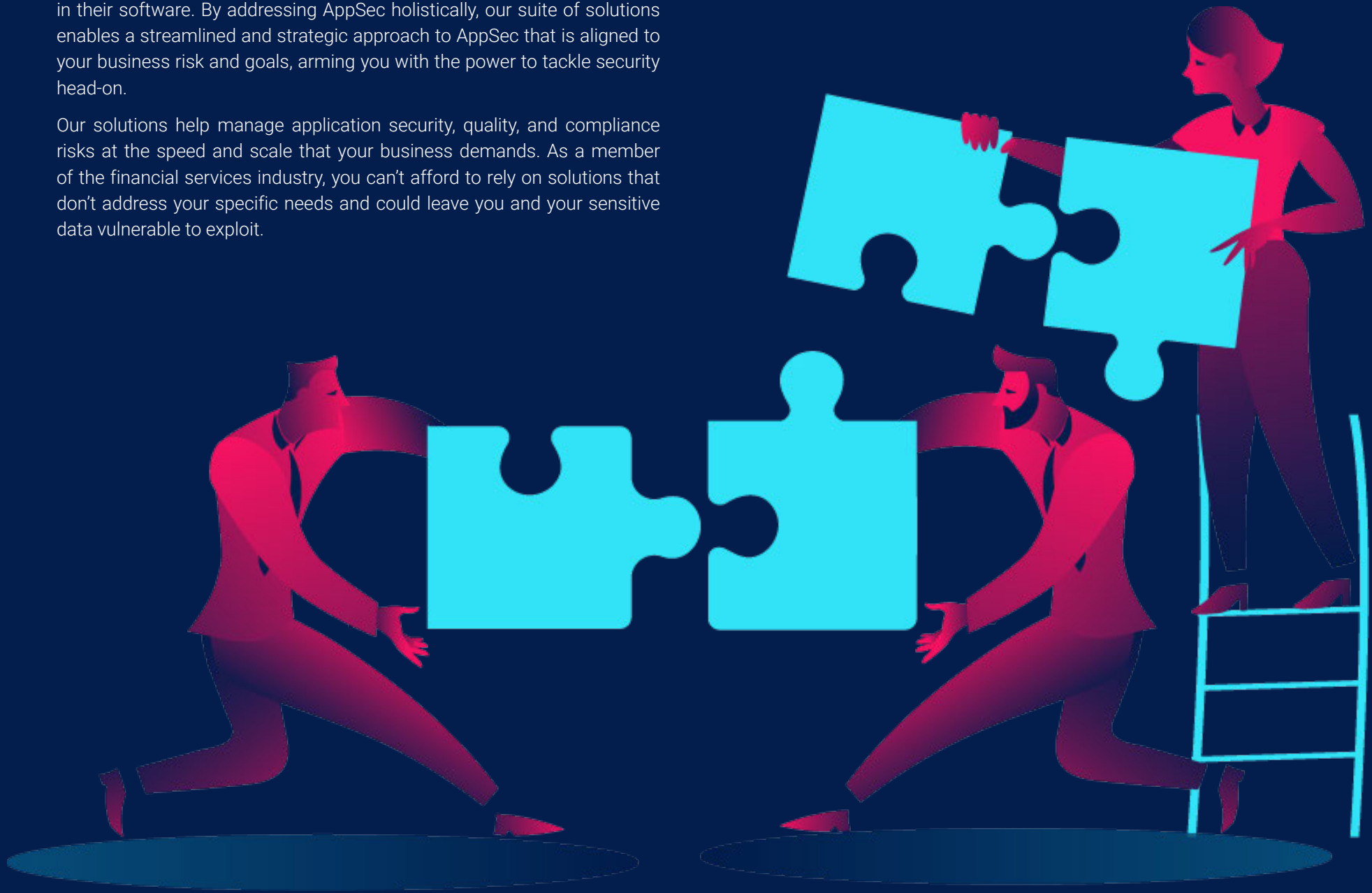
The Ponemon report noted that respondents "felt their organizations need more resources and in-house expertise to mitigate cybersecurity risks." Only 45% of respondents believed their organization had adequate budget in place to address cybersecurity risks, and only 38% believed they had the necessary cybersecurity skills.[7]

This reality is alarming and indicates the need for increased emphasis on training, security experts, and overall spend on application security initiatives within the financial services industry.

The Synopsys Solution Suite: Modern Solutions for Modern Challenges

As a global AppSec leader, Synopsys empowers organizations to build trust in their software. By addressing AppSec holistically, our suite of solutions enables a streamlined and strategic approach to AppSec that is aligned to your business risk and goals, arming you with the power to tackle security head-on.

Our solutions help manage application security, quality, and compliance risks at the speed and scale that your business demands. As a member of the financial services industry, you can't afford to rely on solutions that don't address your specific needs and could leave you and your sensitive data vulnerable to exploit.



Solution 1: Black Duck and Coverity to Secure the Supply Chain

Perhaps the most important step toward securing your supply chain is knowing what's in your software.

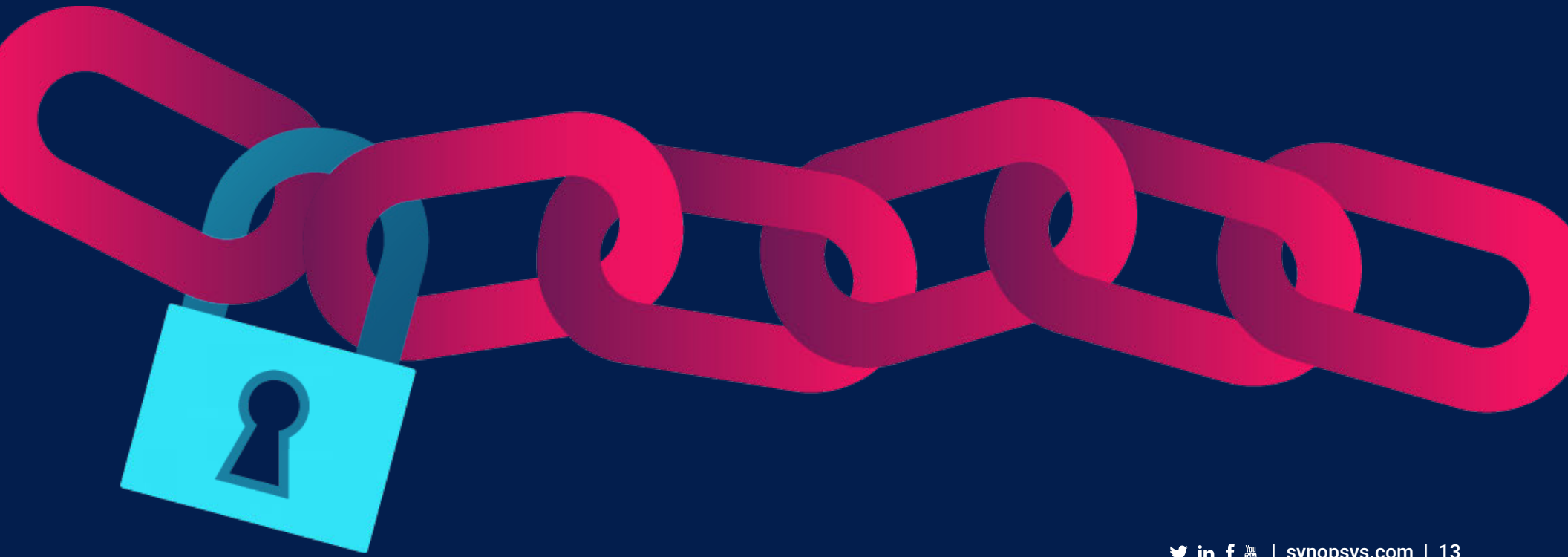
Securing the supply chain means securing all components, activities, and policies across your organization, and finding and fixing quality and security issues. The code you develop internally, the open source your developers use, and the third-party software you rely on—everything must be secured. Beyond simply securing your supply chain, you need to build trust in it: You and your customers must be able to trust the integrity of your software. No matter what your supply chain looks like, Synopsys has the solutions to secure your entire development environment and build this trust.

Securing the open source your teams use

The prevalence of open source necessitates that you view it differently. It's no longer a question of if your developers use it in your development environment, it's how much they use and how trustworthy it is. Without a complete picture of your open source, you can't protect yourself from risk.

The Ponemon report found that a troubling 57% of respondents don't have an established process for inventorying it or managing the use of open source.[8] This means over half of the FSI firms surveyed don't have a proper grasp of their open source usage, its implications for their supply chain security, and the risk to their business as a whole. The need here is not simply to establish reactive policies and practices that help secure open source—it is to create a proactive security program that helps avoid future security concerns, identifies problematic components, and saves time and resources to further reduce your risk. You need a program that inspires trust in the software you're developing and provides demonstrable evidence of your trustworthiness to your customers.

Black Duck® software composition analysis (SCA) from Synopsys helps your teams manage the security, quality, and license compliance risks that stem from the use of open source code. Black Duck integrates easily into your existing development environment, and automated policy management allows you to define policies for open source use, security risk, and license compliance up front. It also automates enforcement across the software development life cycle (SDLC) with the tools your developers already use.



Black Duck's key functionalities support critical open source usage needs.

- **Black Duck helps you see into your supply chain.** Black Duck provides visibility into your software supply chain and helps you track what open source components are going into your software. With multifactor open source detection, Black Duck goes beyond relying solely on declared dependencies. This means that all open source is discovered, and a complete inventory is compiled for your developers.
- **Black Duck helps you establish trust with your customers.** Black Duck makes it easy to effectively communicate the makeup of your software to your customers and comply with emerging regulations. Black Duck also provides reports that detail what and who built your applications. It does this by exporting to Software Package Data Exchange (SPDX), an open standard for software Bills of Materials. SPDX is a recognized format as defined in the supply chain security executive order (EO 14028).
- **Black Duck gives you control over supply chain risks.** Black Duck makes it easy to proactively manage the security and quality of your supply chain. It delivers operational risk metrics like contributors, new versions, commit activity, and activity trends over time, empowering you to take action early and proactively. With Black Duck you get insight into the quality of your components and an understanding of how actively your open source is maintained.
- **Black Duck helps you stay informed when new vulnerabilities are found.** Black Duck Security Advisories provide detailed open source vulnerability records that are sourced, curated, and analyzed by the Synopsys CyRC. They deliver timely, thorough, and actionable vulnerability research directly to your Bill of Materials (BOM), so you can effectively prioritize and remediate vulnerabilities before a breach. Black Duck further ensures your open source license compliance, tracking over 2,500 open source licenses, helping you avoid license violations and protecting you from costly litigation loss of your valuable IP.
- **Black Duck helps maintain development velocity.** Black Duck enables you to set up precise and customizable policies that are automatically enforced. With multiple scan types fine-tuned for specific roles across the SDLC, you can easily enforce open source governance without slowing your developers down. Black Duck helps you align your actions and priorities with your unique risk tolerance with minimal input and action needed from your development teams.

"When we built our business case for bringing in Black Duck, our internal information security group was a cosponsor of the effort. This group now has a significantly easier way to determine which artifacts and versions are affected by any security vulnerability and which applications are impacted as a result. This capability did not exist before, so this is huge."

—Kostas Gaitanos, senior director of development services at FINRA

See the full success story here.

Identifying and securing open source in your third-party software

When an FSI company relies on outside providers for third-party software and then integrates this software within their own applications or through the firmware of devices embedded in their products, they open the business up to risk. The only way to truly protect your organization from this potential risk is to implement your own security practices around the treatment of third-party code and software.

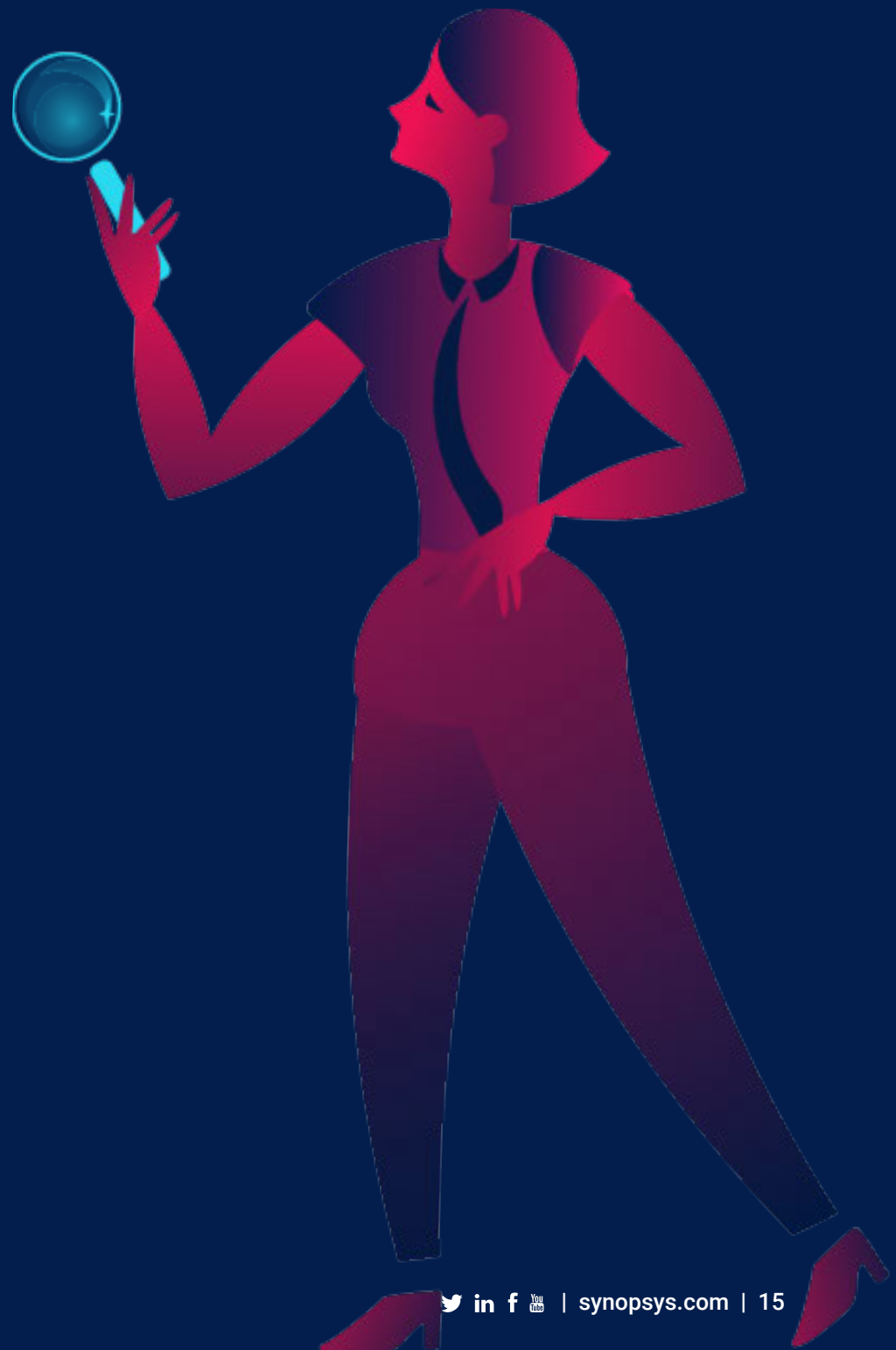
The Ponemon report found that most organizations don't have any established process for inventorying or managing their use of open source. Only 43% had any concrete process in place.[9] Black Duck Binary Analysis (BDBA) is a powerful SCA tool that helps easily generate a software BOM that tracks third-party and open source components in your applications' binary files. You quickly get a snapshot of vulnerabilities, dependencies, and license obligations and violations in your code. BDBA effortlessly identifies known security vulnerabilities without requiring access to source code, which makes it ideal for screening third-party software that are procured from external vendors.

BDBA can also scan almost anything—from desktop and mobile applications to embedded system firmware and more—for information leakage secrets such as clear text passwords, active AWS keys, developers' credentials, and IP addresses. With complete visibility into the composition of all your code, your procurement, operations, and development teams can make decisions that align with your security strategy. And BDBA's binary file identification capability adds a layer of open source discovery that is absolutely essential to the security of your software supply chain.

BDBA gives you the ability to

- See into the software supply chain
- Establish trust with customers and the consumers of your applications
- Control your supply chain risks, proactively
- Provide consistent controls and governance without slowing down development

Visit our website to learn more about Black Duck and how it can help secure your supply chain.



Securing proprietary code

As data privacy laws multiply and the number of cyberattacks continues to grow, organizations need to protect their web applications from sensitive data leakage and ensure regulatory compliance. In the context of supply chain security, securing the code you develop internally should be a high priority. The challenge of implementing adequate security solutions and practices was noted in the Ponemon report, in which 76% of respondents affirmed that it was difficult to detect security vulnerabilities in financial software and systems before going to market.[10] This indicates a deficiency in processes and tooling.

Synopsys Coverity® static application security testing (SAST) is a fast, accurate, and highly scalable solution that helps development and security teams address security and quality defects early in the SDLC, track and manage risks across the application portfolio, and ensure compliance with security and coding standards.

Coverity's key functionalities support proprietary code security.

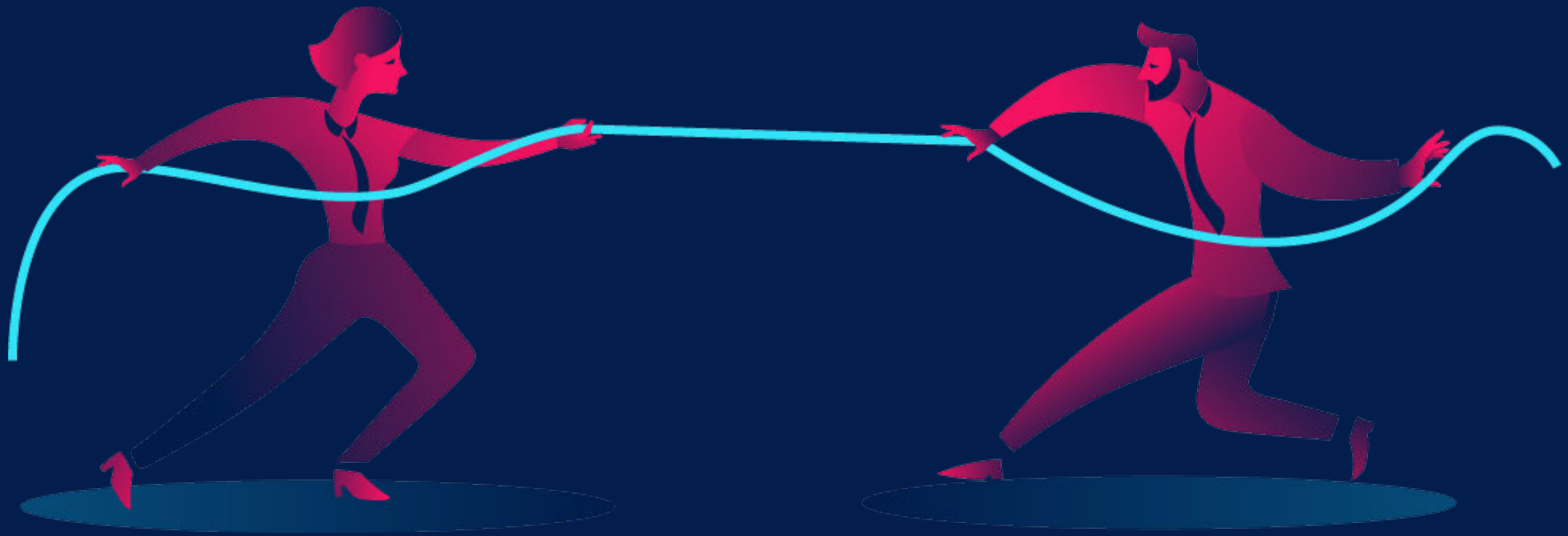
- **Coverity is a comprehensive solution that can identify multiple types of software risk.** Coverity helps identify sensitive data and unencrypted credentials in source code, enabling quick remediation. Coverity is the only solution with strong support for CWE Top 25, OWASP Top 10, and PCI DSS security standards.
- **Coverity delivers a wide range of development technology support.** Coverity supports 22 coding languages, 70+ frameworks, and infrastructure-as-code platforms and data formats, and it includes key integrations and plugin support. Coverity supports analysis on premises, in the cloud, and within the major IDEs via Code Sight™. It supports the languages, frameworks, and development tools your teams use today.
- **Coverity drives and enhances developer productivity and security adoption.** Coverity is easy for your teams to use, doesn't distract them with false positives, and provides the guidance they need to fix issues quickly. With one of the highest OWASP benchmark scores on the market, Coverity gives developers blazing fast analysis results, as they code, using Rapid Scan. And the actionable remediation advice provides detailed, real-time feedback to improve quality and security.

Solution 2: Code Dx for Vulnerability Overload

Code Dx® by Synopsys is an automation platform that helps you manage vulnerability overload. According to the NIST SATE V report, 66% of all AppSec findings are noise. This translates to a lot of time wasted on unnecessary and redundant triage activities.[11]

With Code Dx, you can effortlessly correlate your results, prioritize your vulnerabilities, and get a centralized view of your business risk. Code Dx's powerful capabilities include

- **Result correlation.** At its core, Code Dx is a powerful correlator. The Code Dx Correlation Engine dramatically reduces the time you spend combining and correlating the results from all your AppSec tools to eliminate redundant findings. By combining results from dynamic, commercial, and open source tooling into a single console, you can easily cut through the noise and rely on a single location to view and manage your vulnerabilities.
- **Vulnerability prioritization.** Code Dx Triage Assistant uses machine learning to intelligently predict which vulnerabilities are most critical and pose the greatest threat to your organization. Vulnerability findings are automatically prioritized based on compliance standards such as NIST, PCI, HIPAA, DISA, OWASP Top 10, and more, along with your unique business rules.
- **Centralized risk visibility.** Code Dx provides a 360-degreee view of risk for all your applications. From custom code to third-party components and networks, you get a clear picture of your risk so you can make informed security decisions based on data.



Solution 3: Synopsys for Data Privacy/Protection

Protecting data has never been more imperative for the financial services industry. Having the right tools helps you understand your risks and makes it easy to address them. Synopsys solutions help organizations eliminate attack vectors, preventing hackers from exploiting weaknesses in application security practices and gaining access to personal data. It can also help keep you compliant.

Synopsys solutions provide three key functionalities to help you avoid noncompliance.

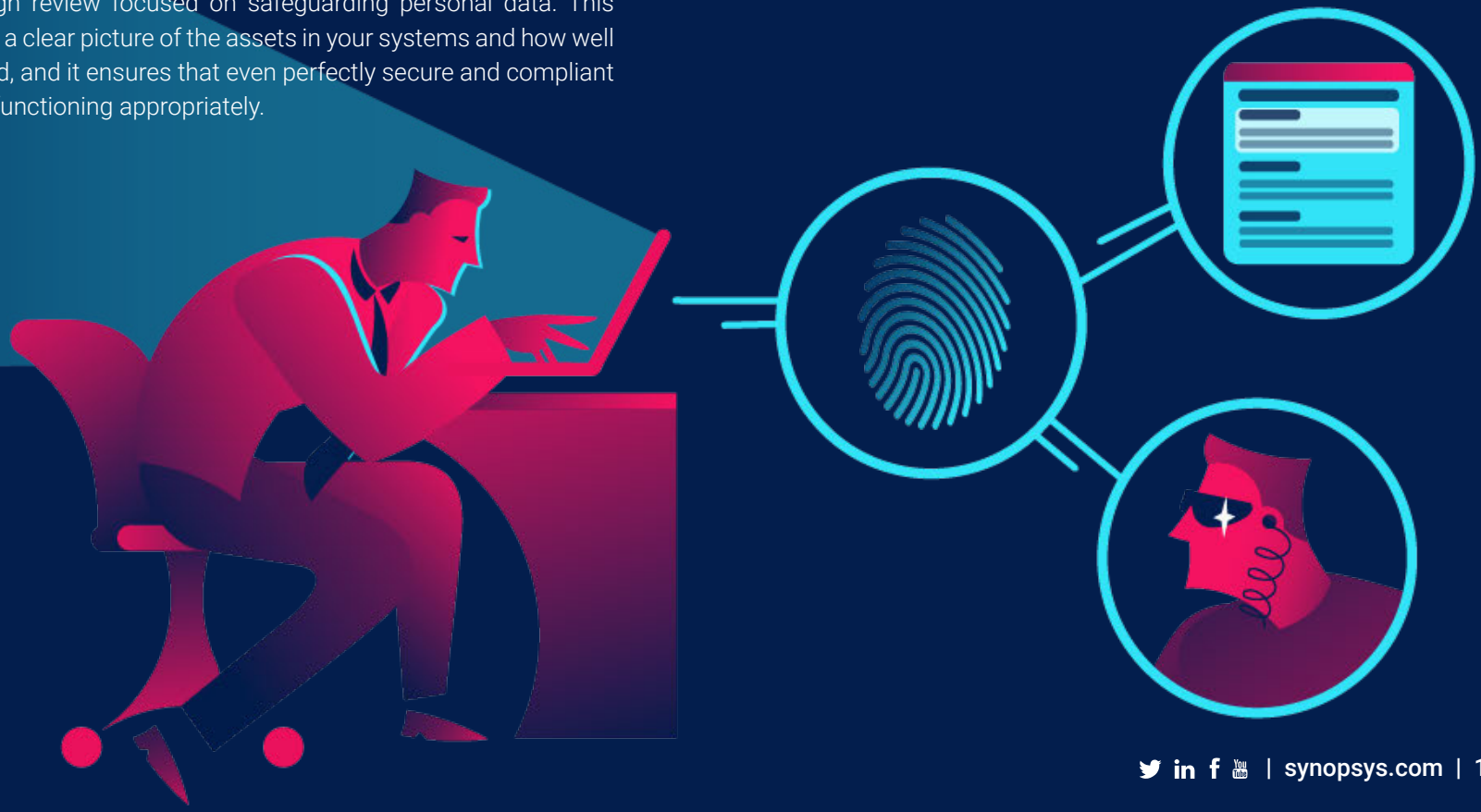
- They can audit your applications for security issues that could result in a data breach.
- They can track and manage vulnerabilities throughout the SDLC.
- They can monitor for new vulnerabilities affecting applications, including internal and open source code.

Threat modeling. Architecture risk analysis evaluates your applications and systems through the lens of relevant GDPR articles. Synopsys also performs a design review focused on safeguarding personal data. This analysis provides a clear picture of the assets in your systems and how well they are protected, and it ensures that even perfectly secure and compliant applications are functioning appropriately.

Policies and standards development. Synopsys works with you to create policies and standards that define the scope of software security in your organization, establish roles and responsibilities, and provide a common definition of terms to facilitate communication. Synopsys also helps you define your rules of governance and compliance so you can

- Measure the effectiveness of your security program
- Ensure consistent development and application testing
- Establish acceptable security minimums for building and deploying applications

Maturity Action Plan. A Synopsys Maturity Action Plan (MAP) helps you address your specific application security challenges and objectives by providing an actionable roadmap for your security and development teams. With a MAP, Synopsys will build a detailed, step-by-step process to move you toward compliance.



Solution 4: Coverity, Seeker, and BDBA for Sensitive Data Leakage

As new data protection and privacy laws continue to be passed, FSI firms must quickly develop strategies and practices that tackle compliance and governance requirements. As guardians of highly sensitive data, this effort is critical. Synopsys solutions provide automated data leakage detection, allowing you to make appropriate fixes before exploits can occur.

Coverity® SAST has a built-in security checker that enables you to scan your own repositories and web applications for sensitive data you need to protect. Coverity helps you identify secrets or data leakage that has been accidentally left behind in your code to help ensure compliance with OWASP Top 10 (web and mobile) and CWE Top 25 vulnerabilities, as well as PCI DSS and other standards. By offering automated scan capabilities, Coverity allows you to identify these security issues early in development, before they can be exploited.[12]

Seeker® IAST provides sensitive-data tracking that identifies where the most critical information is stored within your applications and finds instances where your encryption is insufficient. This helps you ensure compliance with key industry standards and regulations, including PCI DSS, CWE Top 25, and GDPR. It also detects when user-designated sensitive data is exposed, unencrypted, or inadequately encrypted in logs, databases, and files. Seeker helps monitor and track any type of sensitive user data, including national ID, cardholder data, account data, transaction information, medical information, biometric data, and geographical data. Mishandling of this type of information is a significant contributor to information leakage and the most common cause of failed audits. With Seeker, this process is automated and easily integrates into your existing build environments.

BDBA helps address information leakage in any type of software, including if sensitive information like email addresses, authorization tokens, compiler switches, and passwords are exposed. It also identifies when mobile applications request excessive permissions—all of which puts your organization and users' personal data at risk.

Solution 5: Code Dx, Intelligent Orchestration, Coverity, Black Duck, and Seeker to Support DevSecOps

Successful DevSecOps is a hefty undertaking and one that will not look the same across organizations. The guiding principle of DevSecOps is harmonizing development, security, and operations through the use of tools, practices, and policies that streamline the delivery of secure software, quickly. The Synopsys solution suite was designed to support this goal, automating your security efforts across the SDLC and empowering teams to tackle security confidently.

Intelligent Orchestration is a powerful tool that makes development at the speed of DevOps possible. Intelligent Orchestration allows teams to integrate AppSec analysis into their DevOps pipelines, without slowing down development efforts. It helps you automatically perform the right security tests at the right time, based on user-defined policies, risk profiles, and severity/context-specific code changes. And its risk-based vulnerability reporting ensures that developers can remediate the most pressing vulnerability issues first. Intelligent Orchestration takes in the entire picture of your existing AppSec tooling, policies, and practices, synthesizes them, and then provides a tactical and automated approach to security.

"The net benefit we've found is less extraneous testing, which translates into less data to manage, less confusion trying to reconcile data from duplicate tests, [and] ultimately less stress on our resources. Intelligent Orchestration has allowed us to focus on higher-value tasks."

—Senior technical lead, Synopsys FSI client

See the full success story here.

Code Dx delivers automated AppSec at the speed of DevOps. It enables you to implement DevSecOps in your organization by automating application security processes throughout the entire SDLC. It automatically determines the appropriate tests to execute at scale (SAST, DAST, SCA, etc.), and then automatically prioritizes your most exploitable vulnerabilities by correlating thousands of results from multiple AppSec tools. You get a complete picture of risk visibility for your organization's entire software portfolio from one centralized hub.

Coverity SAST helps you effortlessly integrate and automate application security in your CI/CD pipelines. Coverity allows you to automate SAST at scale, with the tools your teams are already using. Much like Black Duck helps secure open source, Coverity helps you secure your proprietary code in your supply chain.

With Coverity, you can

- Integrate. Build SAST into your DevOps pipeline with CI, SCM, and issue-tracking integrations and REST APIs.
- Automate. Get fast, accurate results out-of-the-box, without the need for tuning.
- Scale. Confidently support large applications and teams with Coverity's comprehensive analysis.

"The Synopsys application security validation program provides rigorous software security assessments, including Coverity static application security testing, Black Duck software composition analysis, penetration testing, and code reviews. The net result is a win/win for both FinTech providers and their financial services customers. FinTech app providers get third-party validation from an industry-leading application security company, and their customers can rely on the applications with confidence."

—Paul Andrusyshyn, GM, financial services, Finastra

See the full success story here.

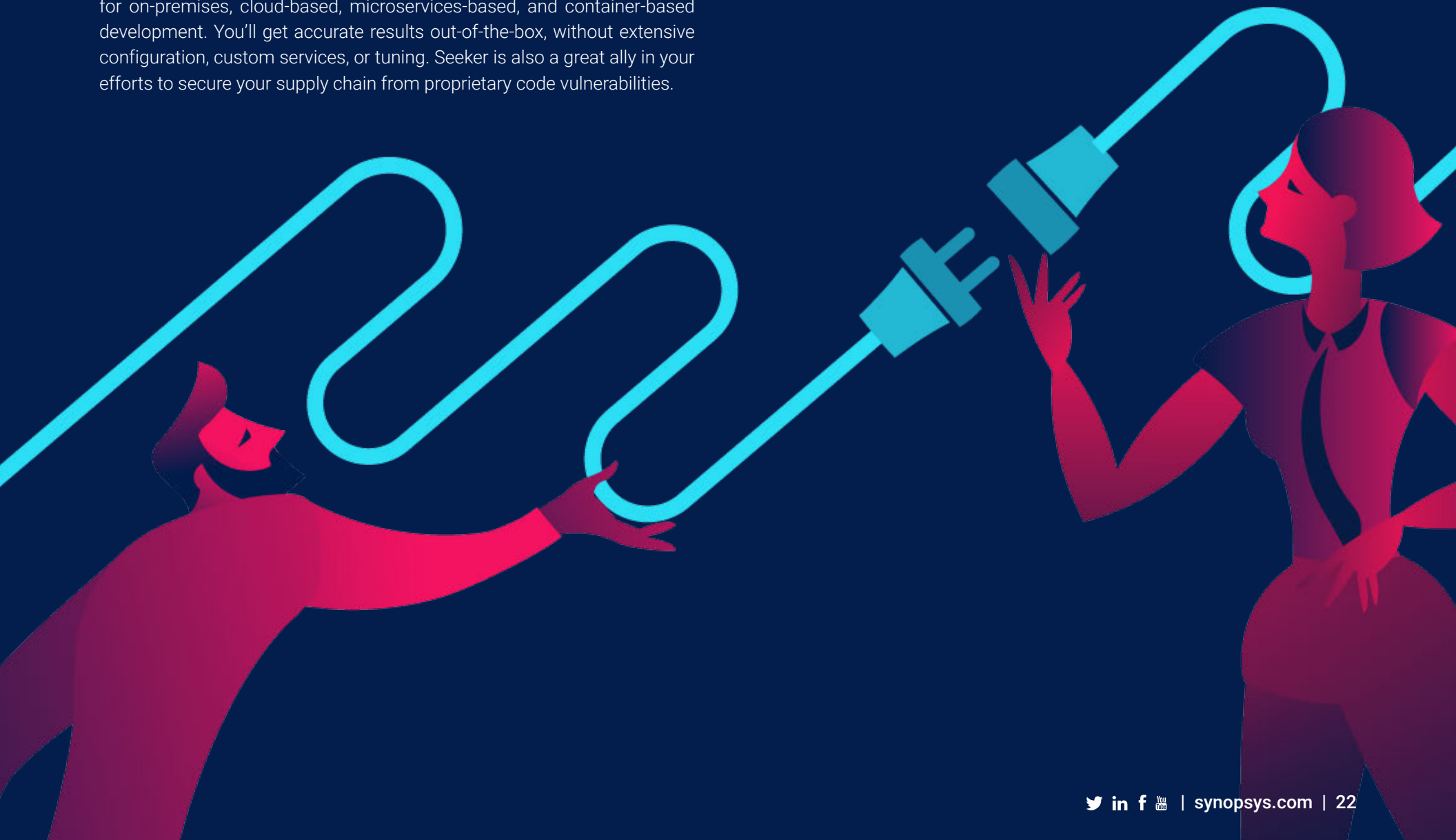
Black Duck SCA helps you easily integrate and automate open source governance into your DevSecOps environment. Black Duck's automated policy management allows you to define policies for open source use, security risk, and license compliance, and automate enforcement across the SDLC with the tools your developers already use.

Seeker IAST automates web security testing within your DevOps pipelines, and it's easy to deploy and scale in your CI/CD workflows. Native integrations, web APIs, and plugins provide seamless integration with the tools you use for on-premises, cloud-based, microservices-based, and container-based development. You'll get accurate results out-of-the-box, without extensive configuration, custom services, or tuning. Seeker is also a great ally in your efforts to secure your supply chain from proprietary code vulnerabilities.

"Seeker answered our integration and automation needs. It provides training and knowledge to its users. Seeker is the perfect tool to help us improve our security practice to build excellent software."

—L. Porcheon, Parkeon, payment solution application provider

See full success story here.



Solution 6: Managed Security Testing and Training to Resolve Resource Constraints

Synopsys recommends that FSI firms leverage both managed services and Synopsys eLearning to help bring security efforts up-to-speed. Research from Ponemon uncovered the reality that FSI firms are severely lacking in talent and resources, and that groups across these organizations see this shortcoming as something that should be addressed expeditiously. When asked whether their organization provides secure development training for its software developers, 32% of respondents said that training was optional, 25% said they did not, and only 19% have mandatory training.

If your security efforts are represented somewhere in that range of answers, Synopsys offers a variety of solutions that can help supplement and bolster your existing in-house security efforts to quickly get you back on track.

Synopsys application security training and product education

Synopsys security training provides interactive courseware designed to help development teams learn and implement best practices for securing code. Using our training program, you can equip your development teams with the skills they need to produce more-secure software, quickly.

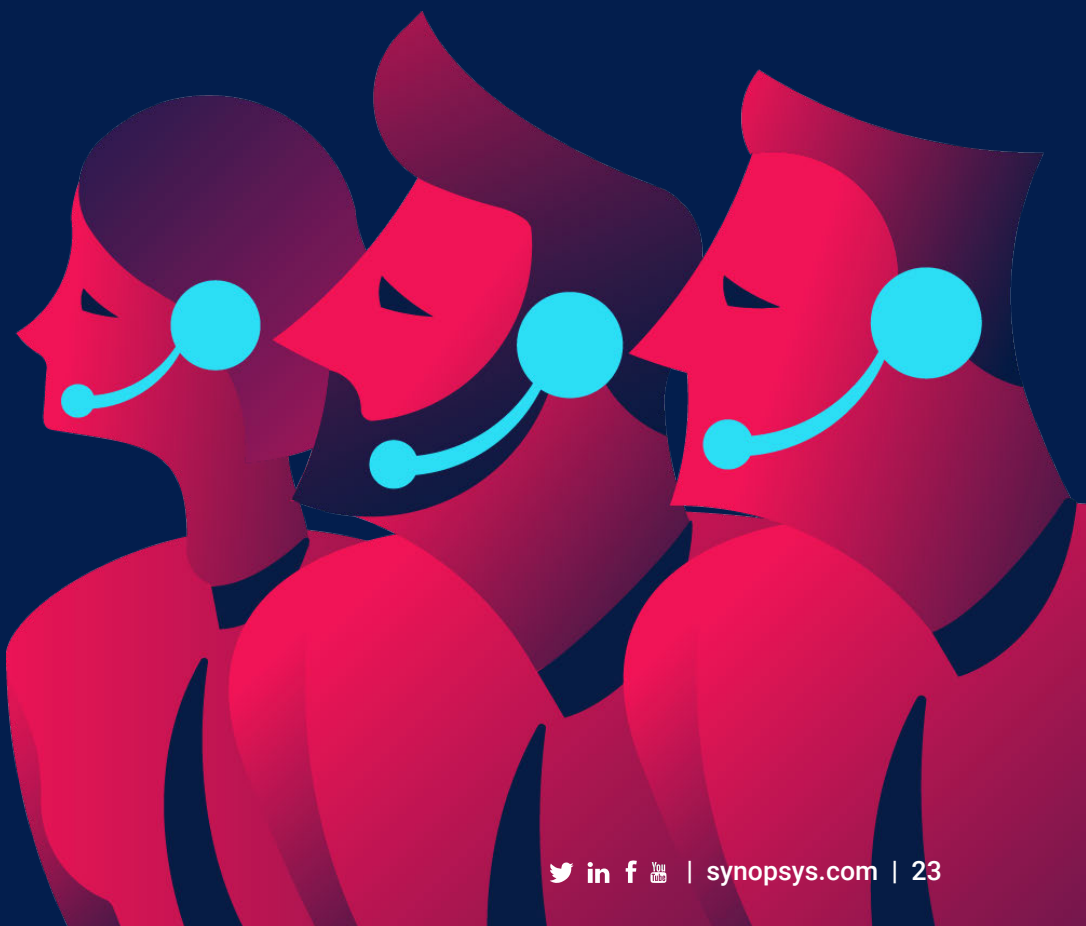
We make security training easy, relevant, and accessible. We know the world of AppSec can be daunting, so we offer outcome-driven, learner-centric solutions, and courseware that fits the skill levels, roles, and responsibilities of your team.

You can easily build a security training program that can integrate into your existing SDLC and address security challenges both broad and narrow. With Synopsys security training, developers can get contextual, easy-to-consume training, directly in their IDE, while they code.

"The format that Citi and Synopsys developed offers a great opportunity for team training—dynamic collaboration among the attendees to apply knowledge to common situations and problems faced by the team. One of the proof points that the format works is that the virtual classes have had much higher attendee rates than our traditional onsite training. And of course, we've seen a big reduction in wasted time due to travel logistics."

—Peigi Maides, training program manager of Citi's chief information security office, Citi Group

See the full success story here.



Synopsys security testing services

Synopsys managed services help you accelerate and scale your application security testing strategy using on-demand resources and expertise.

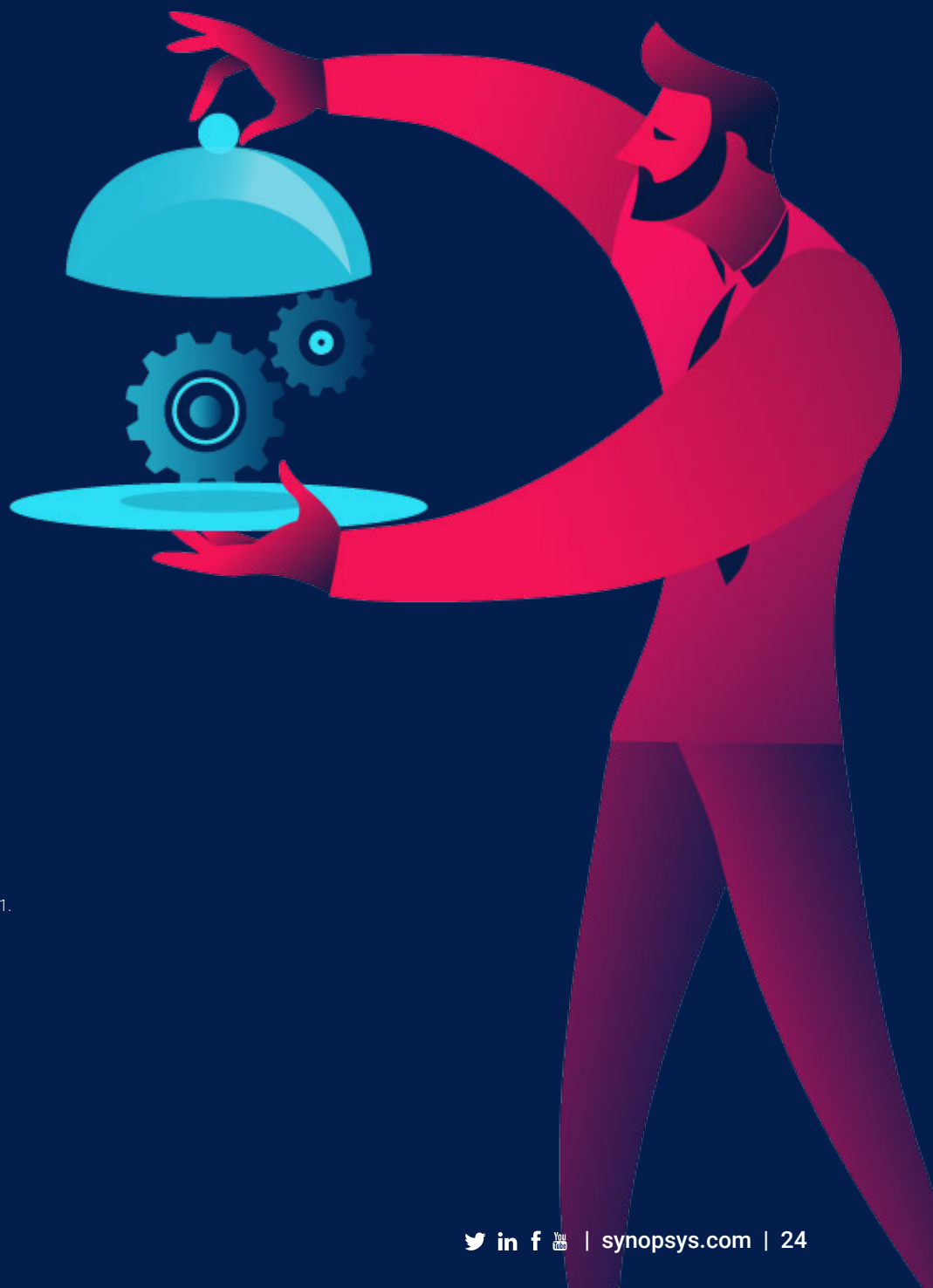
If your organization develops software internally, you're doing so faster than ever before. It's likely that your team lacks sufficient application security skills and resources to sufficiently test your proprietary and third-party code. Synopsys security testing services provide on-demand access to security testing experts who have the skills, tools, and discipline needed to cost-effectively analyze any application, at any depth, at any time.

You can use managed services to strengthen your AppSec stance and fill in any existing gaps in your security initiatives. Managed services provide a shortcut to security, so you can protect yourself today.

Learn more about Synopsys managed testing services.

- Penetration testing. Find vulnerabilities in your applications and services before hackers do.
- Dynamic application security testing. Expert DAST, delivered on demand.
- Static application security testing. Respond to changing testing requirements and evolving threats with on-demand SAST expertise.
- Mobile application security testing. On-demand security testing, optimized for the unique risks of mobile applications.

To explore the complete Synopsys solution suite, visit our website to learn more.



Resources

1. Ponemon Institute, The State of Software Security in the Financial Services Industry, Synopsys, 2019.
2. Ibid.
3. Synopsys Cybersecurity research Center, Peril in a Pandemic: The State of Mobile Application Security, 2021.
4. Ponemon Institute, The State of Software Security in the Financial Services Industry, Synopsys, 2019.
5. Ibid.
6. Chiang, Anna, CISO's Guide to Sensitive Data Protection, Synopsys, 2021.
7. Ponemon Institute, The State of Software Security in the Financial Services Industry, Synopsys, 2019.
8. Ibid.
9. Ibid.
10. Ibid.
11. National Institute of Standards and Technology, Static Analysis Tool Exposition (SATE) V, 2021.
12. Chiang, Anna, CISO's Guide to Sensitive Data Protection, Synopsys, 2021.

The Synopsys difference

Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

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