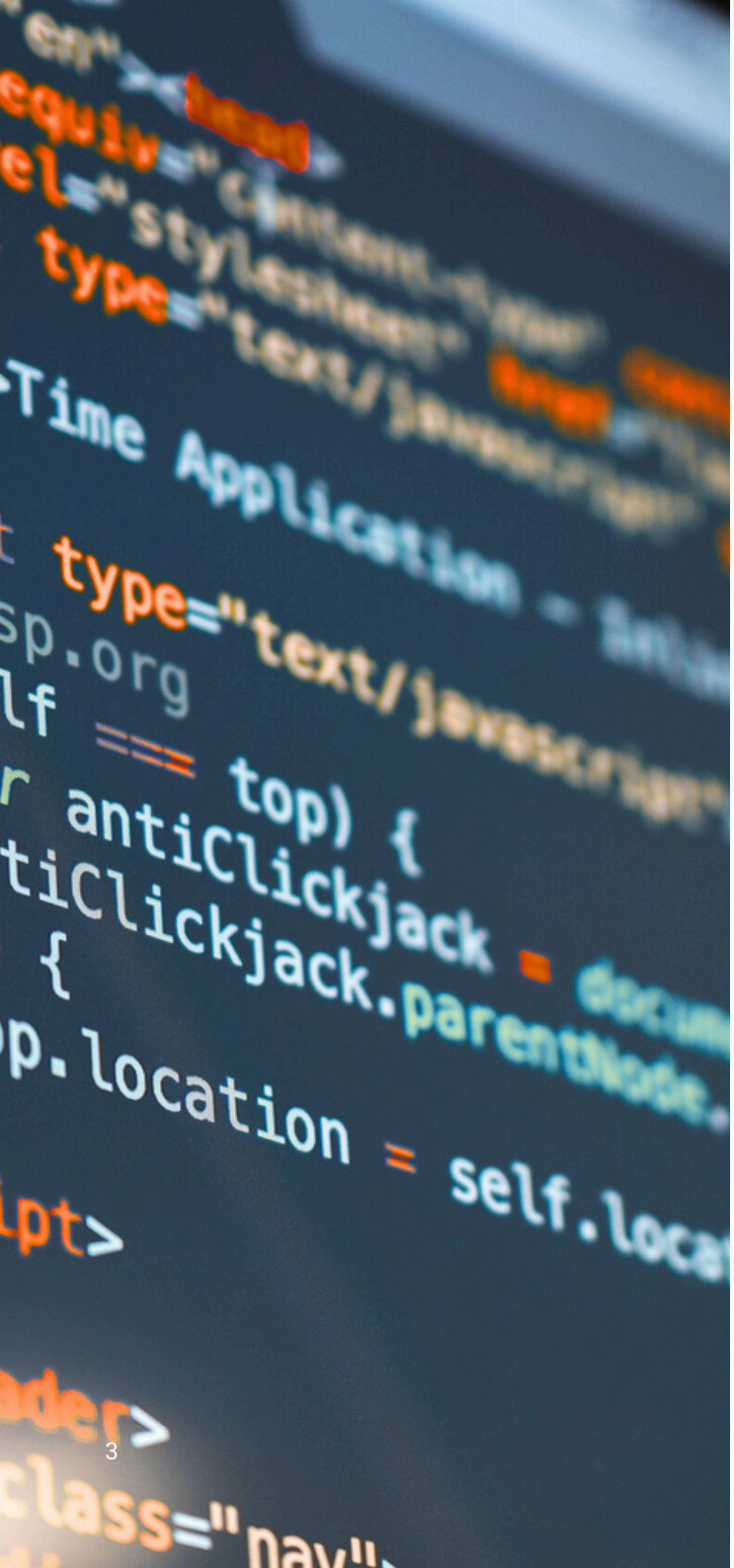
Securify

The power of Continuous Pentesting

Why the annual pentest is no longer sufficient

WHITEPAPER

Content



Introduction

Over the past decade, the way organisations develop software and applications has completely transformed. Teams now work in an agile way and release new features almost continuously. Yet most security processes have barely kept pace with this speed. The classic model is based on a single penetration test per year, followed by a report and a remediation round. This is a relic from the days when software development was predictable and easy to oversee.

Those days are gone. For many organisations, the annual pen test is still seen as the standard proof that an application is secure. But a snapshot in time, no matter how thorough, cannot guarantee that an application remains secure. The reality is that new releases, updates, and integrations create fresh risks almost every day.

If you want to continue meeting customer expectations and keep innovating, you cannot rely on a process that is months behind reality. Security must be just as flexible, fast, and iterative as software development itself. On top of that, you must now comply with the latest security standards and regulations, such as NIS2 or DORA.

In this whitepaper, you will discover why annual testing and static PDF reports are no longer sufficient, and how Continuous Penetration Testing enables you to move towards a continuous, data-driven process. You will see how a real-time security dashboard can detect vulnerabilities, identify which risks are urgent for each new release, and automatically relay that information to your development team. With a direct security feedback loop, security naturally follows in the slipstream of development.

"If you want to continue meeting **customer expectations and driving innovation**, you cannot simply rely on a process that is months behind reality."

Why the annual pentest is no longer sufficient

Testing is essential for maintaining control over the security of digital systems. Vulnerabilities in applications can lead to data breaches, service disruptions, or reputational damage, all of which result in dissatisfied customers and financial losses. This is especially critical in sectors where software is vital to operations, or in applications that handle personal, medical, or other sensitive data. In such cases, organisations need to be able to demonstrate that they understand the risks, have them under control, and can take timely action where necessary.

The traditional pentesting process supports this need. It typically involves an intake phase to identify risks and scenarios, the test phase itself, and a report outlining the findings. Many organisations have embedded this process in their policies or included it within their compliance frameworks. However, this approach is increasingly showing its limitations. The development cycle has shifted from a handful of releases per year to a continuous stream of new functionality. Software is now highly dynamic and can change on a daily basis. A test report from just a few months ago, however thorough, may say little about the current version.

On top of that, applications have become more complex. Many modern applications are made up of dozens of individual components, often developed by different teams or suppliers. Any change to one of these components can introduce new vulnerabilities.

An annual pentest can create a false sense of security. A release that has passed testing is no guarantee of what happens afterwards. The process is much like ‘trying to hit a moving target’. By the time the report is delivered, it is often already out of date.

At the same time, attacks are becoming increasingly sophisticated. Hackers and cybercriminals are better organised, have greater resources, and make extensive use of automated tools. Even less experienced attackers can cause serious damage using off-the-shelf software. This means vulnerabilities can be found and exploited more quickly than ever before. The time between a code change and an actual attack is now shorter than ever. Security measures that are months out of date simply do not provide adequate protection.

Regulators, auditors, and customers are also asking more probing questions. How can you be sure that new functionality is secure? How do you ensure that risks are detected in time? How quickly can you demonstrate that you have taken action? Many organisations struggle to answer these questions in full. For years, the annual pentest was considered the minimum standard, but it is no longer enough.

Speed as a competitive advantage

Digital innovation is never optional. In almost every sector, the speed at which you develop new services determines whether you remain relevant. Banks, insurers, healthcare organisations, and technology companies compete not only on price and quality, but increasingly on how quickly they can respond to changing customer needs.

With Agile development and DevOps, it is now possible to deliver new functionality at a rapid pace. But this speed is at odds with traditional security approaches. The classic testing process demands repeated coordination, planning, waiting times, and reporting. This slows down development and fails to provide an up-to-date picture. Development teams do not want to wait weeks for a test result. They want real-time insight so they can fix vulnerabilities in the very next sprint.

As long as security remains a separate process, it will slow innovation. And as long as a PDF document is the only proof, you can never be certain your application is truly secure.

By checking application changes immediately, potential problems can be nipped in the bud. This prevents unpleasant last-minute surprises and costly remedial work. In short, embedding security tests within the development process enables you to respond and innovate more quickly. It also reduces the cost of remediation. Discovering and fixing a bug early can be up to 30 times cheaper than applying a fix just before, or worse, after go-live.

"Development teams want **real-time insight** so they can fix vulnerabilities immediately in the next sprint."

Continuous Pentesting: the new standard

Security is not a barrier. On the contrary, it can be a driver of innovation when organised in the same way as development. When testing is applied flexibly, iteratively, and continuously, it becomes an accelerator of innovation.

That's why Continuous Pentesting is not just a collection of standalone tools or an extra layer of documentation, but a fundamentally different way of working. Instead of relying on annual checkpoints, security becomes an integral process for monitoring new releases in real time and continuously assessing risks.

In addition, the development team receives direct feedback to resolve issues. The strength of this approach lies in the combination of automation, human expertise, and a central dashboard where everything comes together.

From PDFs to real-time insight

A major difference is that the dashboard tracks the development cycle closely. All changes and new features are validated immediately, creating a continuous view rather than a periodic snapshot. For CISOs, Product Owners, C-level executives, and auditors, this is a goldmine.

An important feature for development teams is that it connects directly to the development tools they use every day. Findings automatically appear in the backlog. Development teams can immediately see which new vulnerabilities have been identified, how severe they are, and where they are located within the application.

Each finding contains all the details needed for teams to start assessing and addressing it straight away. In this way, security is not an extra step but an integral part of the normal development process.

The benefits of Continuous Pentesting

- Always a central and up-to-date view of risks
- Rapid detection of what matters and where action is required
- No high remediation costs afterwards
- Less manual handover
- Faster response time for fixing vulnerabilities
- Direct collaboration with developers on security matters
- Developers write more secure code through continuous feedback
- Based on standards and demonstrably secure

Machine learning as an accelerator

With software development moving faster than ever, security can no longer rely solely on manual checks. There is simply too much code, and systems and applications change too quickly. Leveraging technologies such as machine learning is therefore essential to help security keep pace with the speed of software development.

For example, a self-developed risk engine can be used to automatically predict which specific code changes carry the greatest risk of containing vulnerabilities. The engine recognises patterns in the changes that have been made and determines which components are potentially most susceptible to security issues.

A change to the colour of a button, for instance, will require little attention, whereas a modification to login functionality or a public API carries far greater risk.

Typically, only around 10 to 20% of an application is directly relevant to security. By mapping this critical portion and thoroughly inspecting all changes to it in real time, the security foundation remains solid without incurring unnecessary testing work.

Highlighting these security hotspots is immensely valuable for security specialists, allowing them to focus immediately on the areas that matter most. And because the engine continuously learns from the feedback provided by security specialists, its predictive accuracy improves over time.

This unique approach is essential for organising security efficiently and at scale, while making the smartest possible use of expensive specialists. The motto “Test less, secure more” is key to conducting security reviews intelligently and at speed.

"The use of technologies such as **machine learning** is essential to help security keep pace with the speed of software developmen."

An integrated workflow

In traditional models, security is separate from the development process. Continuous Pentesting removes that separation. The dashboard, the forecasting engine, and the expertise of security specialists form an integral part of the development workflow.

As soon as a team creates a new release, an analysis begins automatically. Findings are immediately visible, allowing the team to address vulnerabilities straight away. This also reduces the risk of errors spreading to other parts of the system.

The dashboard serves as a central hub of information. Developers, security officers, and managers each have their own access, receiving a clear, tailored view. From individual findings to long-term trends, everything is continuously available and up to date. And because security specialists work closely with development teams, there is a constant transfer of knowledge. This directly contributes to smarter and stronger security within development teams: application and security quality improve, while the number of findings declines.

Demonstrably better prepared

More and more organisations recognise that compliance does not end with an audit or an annual check. Regulators increasingly want to know not just whether you have conducted a pentest, but more importantly how you can demonstrate that risks are being effectively managed. The security dashboard makes this proof far easier. Every finding is traceable, and every fix is logged. In addition, each change is linked to a standard such as the OWASP Top 10 or the OWASP Application Security Verification Standard (ASVS). The result is a complete and reliable view of security status, available at any moment.

New legislation, such as NIS2, DORA, and the upcoming Cyber Resilience Act (CRA), makes having control over the process even more critical. These regulations impose stricter requirements for demonstrable security. Organisations must be able to prove that they are actively managing risks — not only in advance, but also during and after every release. Whereas an annual pentest was once sufficient for frameworks like ISO 27001, these laws now raise the bar.

Continuous Pentesting helps meet these standards by making a product's security quality measurable and demonstrable. At any time, for example, a report can be generated showing the current security status and the activities being carried out to ensure security on an ongoing basis.

The result is reduced audit pressure, stronger evidence, and better preparation for future requirements. Customers and regulators increasingly expect security to be structurally embedded. Continuous Pentesting not only makes this possible, but also demonstrable.

"More and more organisations realise that **compliance** does not end with an **audit** or an annual check".

Quick and secure innovation

For a long time, the annual pentest was the minimum standard. But the minimum is no longer enough. In a world where software changes continuously, security must keep pace.

Continuous Pentesting turns security into an ongoing process, fully integrated into the way organisations develop, release, and improve their software. It's time to move on from the traditional pentest and adopt an approach that matches the speed of modern software development, enabling you to innovate quickly and demonstrably securely.

With real-time visibility of risks from every release security becomes a continuous stream rather than an occasional snapshot.

Want to know how to make your security process faster and smarter?

Discover how Continuous Pentesting works in practice. Get in touch for a no-obligation demo.

See for yourself where your organisation stands today, and where it can be smarter, faster, and more secure.

+31(0)20 820 4516

info@securify.nl

Securify

Securify B.V.
Naritaweg 132
1143 CA Amsterdam

T +31(0)20 820 4516
E info@securify.nl
www.securify.nl/en

Securify helps organisations identify, resolve, and prevent technical security risks through penetration tests, red teaming engagements, and security code reviews. The focus is on providing effective protection against the most significant business risks. Based on security roadmaps, we ensure that code, (mobile) applications, infrastructure, and the organisation as a whole are optimally secured. For many years, companies ranging from start-ups to major banks have relied on Securify to safeguard their systems and (mobile) applications. With hundreds of penetration tests and security code reviews carried out each year, the Securify team helps protect the data of millions of people in the Netherlands.

Securify also brings an innovative vision to application security for (business) critical systems. Our unique approach enables development teams to deliver software continuously, demonstrably, faster, and more securely. This way security is no longer a blocker to progress. Securify is part of the Solvinity Group. For more information, visit Securify.nl/en.