SOFTWARE SECURED

When Penetration Testing Meets DevOps

The Value of Penetration Testing as a Service (PTaaS)

2021

When Penetration Testing Meets DevOps

The Value of Penetration Testing as a Service (PTaaS)

YOUR APPSEC MANDATE

As the CTO of a fast-growing Software as a Service (SaaS) business, you're under tremendous pressure to continuously ship secure software to stay competitive.

You should have a mandate and a responsibility to build out partial or full application security (AppSec) and/or web security (WebSec) programs. **Penetration testing** is an important part of any security program as it has the potential to uncover blind spots and vulnerabilities that an administrator can't see.

PENETRATION TESTING AS A SERVICE (PTaaS)

Penetration testing (also known as pentesting) is the ultimate test of your application's resilience against attacks. Also called ethical hacking, it involves hiring a third party vendor to attempt breaking in and exploiting vulnerabilities in your application(s).

Regular penetration testing is normally done once a year, as a practice inherited from the times of waterfall methodologies when it was normal for release cycles to last 18-months. As development teams adopt more agile software development processes today, pushing code daily or multiple times a day is becoming the new norm (The Phoenix Project, 2013). These faster processes now need new testing capabilities. The table below shows the deploy frequency of the world's top SaaS companies versus that of a typical enterprise.

Penetration Testing as a Service (PTaaS) is a more continuous type of manual pentesting. It evolves regular pentesting from an isolated yearly exercise into a more integrated, application-aware manual pentest. PTaaS works at the speed of DevOps, ensuring that their deployed code is secure.

COMPANY	DEPLOY FREQ.	DEPLOY LEAD TIME	RELIABILITY
AMAZON	23,000/DAY	MINUTES	HIGH
GOOGLE	5,500/DAY	MINUTES	HIGH
TWITTER	3/WEEK	HOURS	HIGH
TYPICAL ENTERPRISE	1 EVERY 9 MONTHS	MONTHS+	LOW/MEDIUM

Which of these is your security picture missing?

- ☐ Corporate Application Security Training
- ☐ Security Champion(s)
- ☐ Integrated Analyses
  - ○ SAST
  - ○ DAST
  - ○ IAST
- ☐ Threat Modeling
- ☐ Dependency Checking
- ☐ Container Security
- ☐ Penetration Testing
- ☐ Service Level Agreements
  - ○ Internal
  - ○ External
- ☐ Risk Acceptance & Exception Process

SOFTWARE SECURED

We help development teams build confidence in their application security.

softwaresecured.com
1-800-611-5741
info@softwaresecured.com

When Penetration Testing Meets DevOps

The Value of Penetration Testing as a Service (PTaaS)

The Benefits of PTaaS

THE BENEFIT	THE REASON	THE PROOF
INCREASED AGILITY	As SaaS companies prepare to deploy code more frequently (or more automatically), companies need to integrate agile security assessments that align with faster deployment schedules. PTaaS aligns to do comprehensive penetration testing during major launches and continuous reporting and re-testing on new features and patches all-year long.	**81%** of companies have already adopted or are soon implementing CI/CD methods (Mabl, 2021)
DevOps INTEGRATION = DevSecOps	PTaaS works alongside the DevOps process, reinforcing the role of security in development. Together, they create DevSecOps, where security is prioritized in the SDLC. When applications are secure by design, developers can spend more time building applications and less time mitigating risk.	**61%** of tested apps that had at least one high- or critical-severity vulnerability not listed in the OWASP Top 10 (Flexera, 2020)
CONSTANT ACCESS TO SECURITY EXPERTISE	PTaaS is year-round, which means a client's access to their security advisory services is year-round too. Pentesters are always available to answer your developer's questions for any stage of the SDLC or provide expert insights on your organization's security policies.	**38%** of businesses didn't even know if they experienced a breach or not in 2019 (CIRA, 2020)
EMPOWERS A SECURITY CULTURE	A sustainable security culture is organization-wide and provides long-term security returns. Working side by side, development teams can learn current security best practices in the SDLC from their PTaaS team. Then, these practices can be shared and implemented throughout the entire organization.	**$3.3M** the cost of cybersecurity attacks due to employee or contractor negligence (IBM, 2020)
MIX OF MANUAL & AUTOMATIC TESTING	Combining both methods of penetration testing allows for the most deep insights on an application. With their security experience and tools, pentesters are creative, innovative and strategic. They will build attack scenarios, triage results from an automatic tool, know where to dig deeper and find hidden vulnerabilities that other methods can't find alone.	**77 days** the average time it takes to contain an incident (IBM, 2020)

SOFTWARE SECURED

We help development teams build confidence in their application security.

softwaresecured.com
1-800-611-5741
info@softwaresecured.com

When Penetration Testing Meets DevOps

The Value of Penetration Testing as a Service (PTaaS)

THE RISE OF CITIZEN DEVELOPMENT IN DIGITAL TRANSFORMATION

Digital transformation is the digitization of business, bringing all areas of the organization into more automated, organized and accessible processes. Through new or modified technologies, digital transformation allows companies of any size to be more agile in today's rapidly changing markets.

89%

of all companies have already adopted a digital-first business strategy or plan to do so (IDG, 2018)

41%

of enterprises have active citizen development initiatives (Gartner, 2021)

Agile methodologies are critical in digital transformations. As such, more businesses are turning to low-code, no-code or citizen development to develop applications and integrations more quickly, even in SaaS based businesses with established DevOps teams. This is usually used in areas like marketing, sales or customer service.

Although more efficient, citizen developers tend to have less security training and it can be risky to allow them to develop on their own. However, with PTaaS, the entire organization benefits from comprehensive security coverage. A security engineer will be able to work with your DevOps team to cover both traditional and low-code applications. Through security testing and corporate application training opportunities, there are many ways to safely allow your organization to adopt low-code or no-code digital transformation efforts.

SECURITY PROOF

A penetration test certification is proof of an application's security and is provided with each completed pentest. The certification could be needed for closing a business transaction, moving to the next funding round, or in assuring end-users.

Fast-growing organizations need to be proactive in their security efforts and choose to use PTaaS so that they can access an updated pentesting certification at any time. As PTaaS clients always have new releases and fixes monitored, their software can always be trusted as secure.

External Sources

1. https://www.amazon.ca/Phoenix-Project-DevOps-Helping-Business/dp/0988262592
2. https://www.netsolutions.com/insights/why-do-great-product-companies-release-software-to-production-multiple-times-a-day/
3. https://www.mabl.com/devtestops/landscape-survey-2020
4. https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020
5. https://www.cira.ca/cybersecurity-report-2020
6. https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/
7. https://research.aimultiple.com/digital-transformation-stats/
8. https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/

Empower Your Team's Security Champion(s)

Your security champion(s) will act as the reminder to be conscious about security in team meetings and design sessions.

You need to seek out, identify, and empower someone who can act as your team's security champion. Find at least one champion to start, and add more if they are available. As you grow, you may even consider assembling a Security Champions team.

Your security champion will promote the best practices in application security. With their knowledge of security threats and remediation methods, champions are qualified to consult with developers and contribute meaningful recommendations for practices and tools. They also provide support in preventing and eliminating security problems earlier in the software development lifecycle.

SOFTWARE SECURED

We help development teams build confidence in their application security.

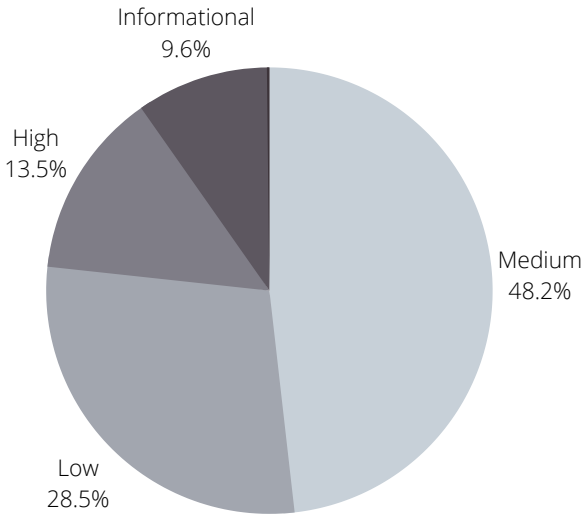
softwaresecured.com
1-800-611-5741
info@softwaresecured.com

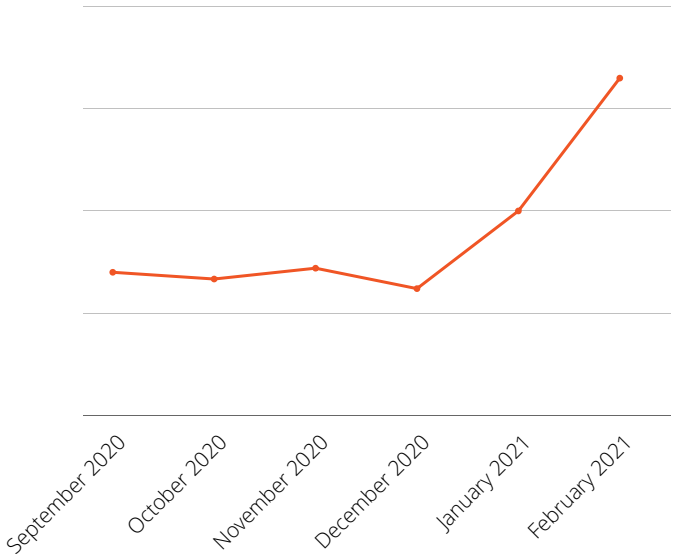
When Penetration Testing Meets DevOps

The Value of Penetration Testing as a Service (PTaaS)

SOFTWARE SECURED IN NUMBERS

Since we were founded in 2009, we've tested over 500 applications. That's over 100 million lines of code. See how we performed for our clients in the middle of the COVID-19 pandemic.



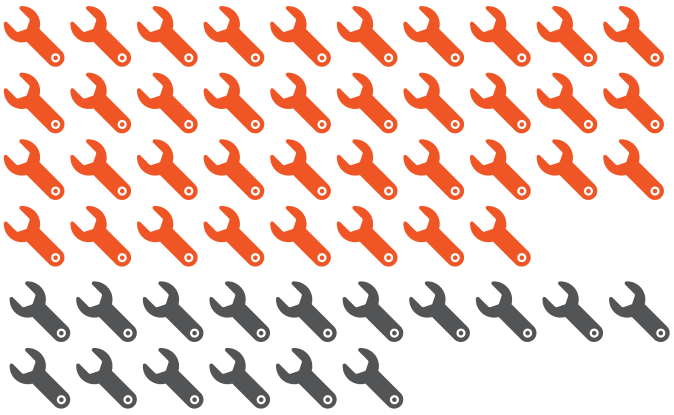


13.6% of our findings were high severity vulnerabilities. These security bugs could have caused serious loss of data or downtime if exploited. Each high severity vulnerability found saved a company from huge potential losses in time, legal fees and/or remediation efforts.

Our security engineers are finding more bugs per test than ever. As teams work from home and DevOps teams are speeding up development processes again, we saw an increase in client testing requirements and discovered vulnerabilities.

Twice as many bugs are found in PTaaS

Within a year, our clients who use Penetration Testing as a Service find on average more than twice as many bugs than our one-time penetration testing clients. This is a result of more frequent testing, ability to do source code review and constant access to security expertise. We're able to dive deeper into a PTaaS client's application after every update and major launch. Consequently, PTaaS clients are more likely to have secure applications all-year long.



Our team is ready to help fast-moving SaaS companies ship more secure software.

Contact us today to see what Penetration Testing can do for you.

Book a Demo

https://bit.ly/valueofptaas

Learn More

https://bit.ly/ptaas

SOFTWARE SECURED

We help development teams build confidence in their application security.

softwaresecured.com
1-800-611-5741
info@softwaresecured.com