Pentest as a Service

Impact Report: 2020

Chenxi Wang

Contents

Pentest as a Service Impact Report: 2020

Commissioned by Cobalt.io and Rain Capital's Dr. Chenxi Wang, this study examines the impact of Pentest as a Service (PtaaS). The goal of this research is to unravel and understand the specific benefits and challenges of deploying a PtaaS solution in a modern software development environment, as well as compare the SaaS model with traditional, legacy pentest services.

We define Pentest as a Service (PtaaS) as a service that utilizes a global talent pool of certified pentesters and a data-centric platform to deliver pentests. The platform delivers actionable results that allow teams to easily pinpoint, track, and remediate software vulnerabilities in an integrated fashion.

About the Author

Dr. Chenxi Wang

An experienced strategist, speaker and technologist in the cybersecurity industry, Wang also is on the board of directors for MDU Resources (NYSE: MDU), and served as a global board member of the Open Web Application Security Project (OWASP) Foundation. Previously, she was Chief Strategy Officer at Twistlock, VP of Strategy at Intel, and VP of Research at Forrester. Wang was named by SC Magazine Women Investor in 2019, Women of Influence in 2016 and is a strong advocate for equality and diversity in the high tech field. Wang's career began as a faculty member of computer engineering at Carnegie Mellon University. She holds a Ph.D. in computer science from the University of Virginia.

Introduction

For this study, we conducted in-depth interviews with five current Cobalt customers. The organizations we interviewed are primarily SaaS and Enterprise software providers and represent a wide swath of different company sizes, including publicly-held, global companies with thousands of employees and privately-held, mid-sized companies with hundreds of employees. More specifically, we interviewed:

1. **A global enterprise software producer** that empowers cloud-based contact center services for organizations to manage communication contacts. Our interviewee is the infosec director, with responsibilities of information security and privacy for the company.

2. **A publicly-held, global cloud communications and business phone service provider.** We interviewed a lead security engineer, who is primarily responsible for both application and infrastructure security.

3. **A software management solution provider.** This global company produces software that helps organizations manage and keep track of the company's software assets, including license management and cost optimization. We interviewed the director of quality and security, who is in charge of application and product security.

4. **A global enterprise SaaS provider on the east coast.** We interviewed two individuals on the security team, whose responsibilities span application security, bug bounty, and threat hunting.

5. **An in-the-cloud recruiting service provider.** We interviewed the senior infosec manager for the company. His team is responsible for a wide variety of security tasks, including vulnerability management, application security, incident response, security training, and infrastructure protection.

One of the questions we seek to answer with this study is the impact of DevOps on the adoption of application security (appsec) measures such as pentesting. DevOps is the "set of practices that combines software development and information-technology operations which aims to shorten the systems development life cycle and provide continuous delivery with high software quality".[1] The practice of DevOps is one of the major disruptive forces, in recent years, in software development and production efficiency.

Of the five companies that we interviewed, four are practicing DevOps extensively. Each of the four companies implemented Continuous Integration (CI) and Continuous Delivery (CD) pipelines and are releasing software multiple times a day. In particular, one company is a sophisticated DevOps shop that has been implementing DevOps for over ten years. This company has a mature DevOps process and runs fast-paced and high-fidelity CI/CD pipelines. The one company that is not practicing DevOps expressed a strong desire to move in that direction, but has many monolithic apps and traditional development practices that present a challenge to adopting DevOps.

Four of the companies we interviewed have dedicated security teams that drove the implementation of pentest services. For the last company, which does not have a separate security team, the engineering organization was responsible for pentests. All but one company had employed traditional pentest services prior to engaging Cobalt.

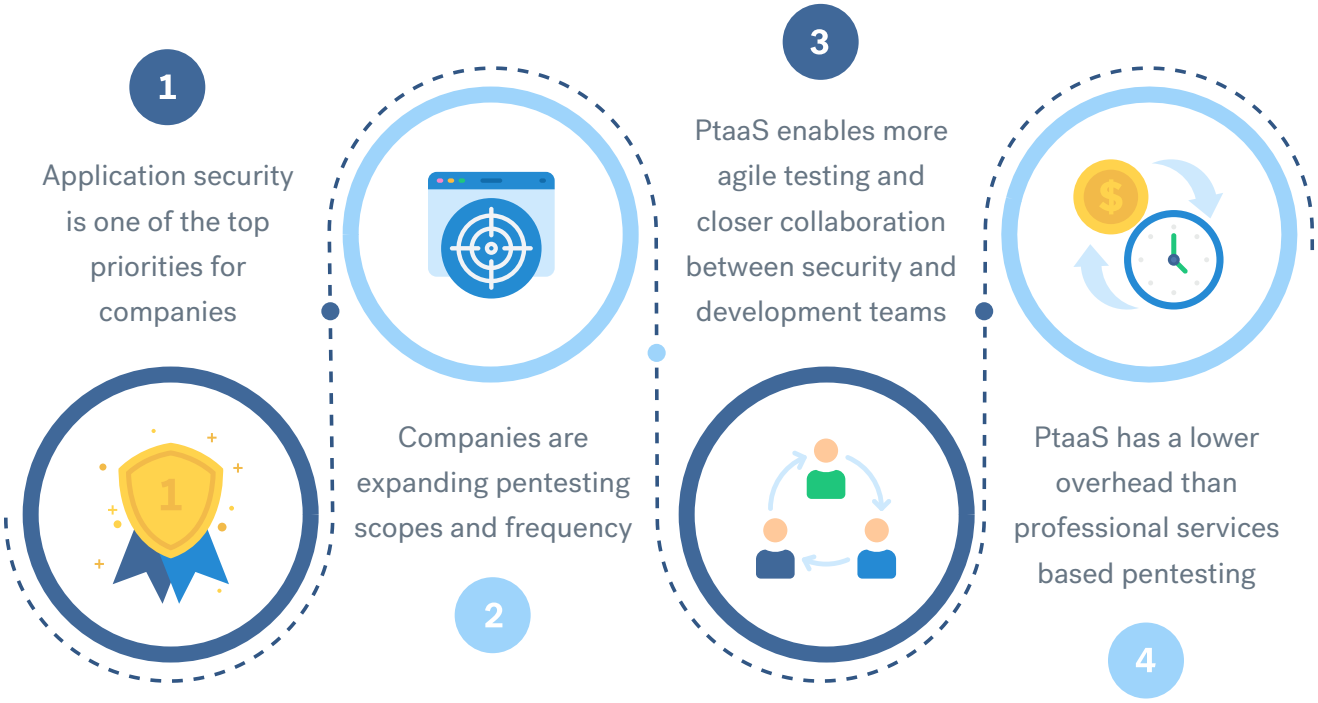
This paper presents our analysis based on the research interviews as well as our own knowledge and understanding of the market. Unless otherwise noted, the information and analysis discussed in this report are aggregated across the organizations we interviewed.

	Number of companies	Software release cadence
Extensively DevOps oriented	3	Multiple times a day
Limited DevOps practices	1	Once
Not really practicing DevOps	1	A few times a year

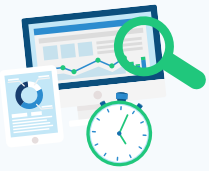
[1] Source: DevOps. Retrieved April 23, 2020, from https://en.wikipedia.org/wiki/DevOps

Key Findings

Our study yielded a number of important findings, which we list in this section first but will explore in more detail in the later parts of the report.



In 2017, we conducted a **similar study**. Even though the objectives of that study were different, we explored some of the same questions. The comparison between the 2017 answers and the ones we received this time around is very telling. More specifically, we see a visible increase in appsec as a company priority from 2017 to 2020. As a result, many have expanded the scope and frequency of pentesting during that same time period.

2017		2020
Drivers for Pentesting		
Largely compliance driven		Driven by increased application security awareness and demand
AppSec Responsibilities		
Largely infosec managed		A shared responsibility model between Info-sec and Dev
Use of Pentesting		
Annual testing of the crown jewel applications		Annual testing of 100% of the company's applications. Higher frequency testing on business critical apps
Pentesting Scopes		
Mostly web apps, a few organizations were testing APIs		Testing includes web applications, APIs, microservices, as well as web and enterprise applications

Summary of key differences between 2017 and 2020 reports

Application Security Is A Top Business Priority

In this section, we explore some of the key findings and the data behind them.

Drivers for Pentesting

Pentesting is a mechanism that tests production apps or infrastructure for vulnerabilities, flaws, or business logic errors. Unlike security scanning services, pentesting is used to discover unknown flaws. meaning, pentesting often requires specific skill sets and knowledge.

Different organizations may have different drivers as to why they employ pentesting. When asked what their company's motivation was for pentesting, our interviewees cited security—the desire to make their apps and services more secure—as the top driver. This is noticeably different from the 2017 study, where compliance and customer requirements were cited as the top drivers for pentesting.

Security is the top driver **for pentesting**

While compliance and customer demand remain drivers for pentesting, all of the companies we interviewed stated that their pentesting initiatives are also driven by a top-down mandate to ensure the security of their apps and services. Some of this is due to heightened awareness among company executives that they need to improve breach resiliency across their digital environments.

This underscores the larger industry trend where security is rapidly becoming a top priority for organizations. It is worth noting that appsec, as an aspect of information security, is now a mainstream concern. Within the five companies we interviewed, four companies have designated appsec teams and personnel.

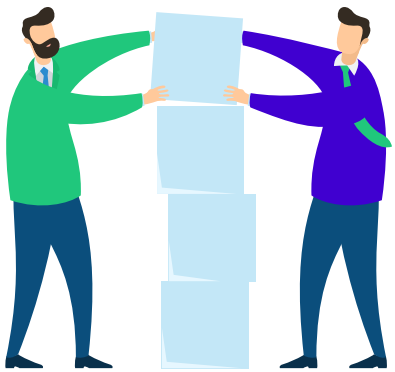
Change of key drivers for pentesting across years	
Largely compliance driven	Driven by increased application security awareness and demand
2017	2020

Shifting Application Security Responsibilities

Appsec, which in some companies is synonymous with product security, is traditionally an information security function. However, in this study we found that appsec responsibility is shifting from an exclusively infosec-managed function to a shared responsibility model between infosec and development teams.

One company we spoke to has over 350 developers and a three-person infosec team, which they're looking to expand with a dedicated appsec engineer. Yet even with that, the infosec manager we interviewed said, "the security team cannot handle all the appsec tasks due to the volume of activity". Instead, the company has identified a few senior developers who are security champions within various development teams to help drive and entrench application security awareness and initiatives into the engineering process.

Another interviewee, a company that runs a SaaS platform, said that their infosec team used to own everything related to appsec. Since that was not scalable, the company established a formal shared responsibility model between engineering and security for closer collaboration. "Strong company leadership is required for implementing a true 'shared responsibility' model," the infosec director said. "Otherwise, the separate silos and organizational barriers will continue to exist between engineering and security."



A shared responsibility model can help alleviate some of the tension between appsec and engineering that exists because of mismatched incentives. Traditionally, developers and engineering teams are incentivised on features to market, whilst appsec (or infosec) is measured on coverage of code analysis or vulnerabilities detected from the code. The two teams have fundamentally different goals, which can lead to friction, mistrust, and ultimately lost productivity. A shared responsibility model seeks to harmonize the goals of the two teams by rewarding development teams with completing appsec tasks and at the same time, rewards appsec teams for helping engineering release features securely.

Shared Responsibility Model

Infosec-managed AppSec responsibility is shifting to a shared responsibility model between engineering and security teams

Engineering Teams

Application Security

Security Teams

Pentesting Is Extensively Used

The population of companies we interviewed is from Cobalt's customer base -- so all of them are using pentesting to a certain degree. We asked them how much of their apps are covered by pentests. Interestingly, every company in this study indicated that they have a policy to pentest 100% of their apps on an annual basis. In addition, some companies are testing business-critical apps on a more frequent basis - either quarterly or two to three times a year.

This is a distinct change since the 2017 study. At that time, most of the organizations were testing only a portion of their apps, typically the crown jewel apps. Almost none were testing everything on an annual basis. The fact that every single company we talked to this time around has a policy to test everything at least once a year is a strong indication that appsec is now a mainstream concern.

More companies are pentesting 100% of their applications on an annual basis

One of the factors that helps to propel the more extensive use of pentesting is DevOps. The security professionals we interviewed agree that it is challenging to adapt traditional application security techniques, such as static analysis and dynamic analysis, to the DevOps environment.

These appsec practices are too heavy weight and too time consuming to be integrated into the DevOps pipeline. As a result, pentesting production apps becomes an appealing solution.

Change of use of pentesting across years	
Annual testing of the crown jewel applications	Annual testing of 100% of the company's applications. Higher frequency testing on business critical apps
2017	**2020**

Pentesting Scopes Expand from Applications to APIs

Four of the five companies we interviewed practice DevOps and utilize microservice apps. All four companies include APIs, as well as their other apps, within the scope of pentesting.

This, again, is a notable change from our last study in 2017, where few organizations were testing APIs. One of the companies we interviewed for this study has been practicing DevOps for nearly a decade. The company runs a fast-paced, high-cadence CI/CD pipeline. “APIs are an increasingly important aspect of an organization’s application portfolio. We have been pentesting our APIs for quite some time now," the head of information security program told us. “It seems recently more and more organizations are catching up to the fact that they need to include APIs in their testing.”

Another company that offers SaaS services told us that their apps are APIs. “We have an API-first development model, which means that we don’t do anything unless it is available through an API.” API testing, therefore, is a central component of pentesting for this company.

Change of pentesting scopes across years

2017	2020
Mostly web apps, a few organizations were testing APIs	Testing includes web applications, APIs, microservices, as well as enterprise applications

Pentest as a Service vs. Traditional Pentesting Services

Another goal of this study is to take a comparative look at Pentest as a Service (PtaaS) versus traditional pentesting that is often delivered as a professional service. To that end, we looked at a number of aspects including access to talent, quality of the results, coverage of the test, and speed and scalability of the tests.

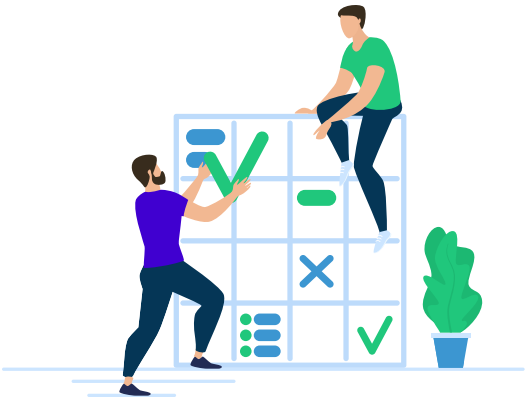
Pentest as a Service Has A Larger and More Agile Talent Pool

When asked if they are happy with the pentester talent with Cobalt's PtaaS platform, our interviewees responded universally in a positive way. "We have been really impressed with the quality of the testers," "We are very happy with the variety of the skillsets of the testers," and "We have always been able to get the type of talent that we want for the tests" are just a few of the comments we received as part of this study.

In particular, our interviews revealed these particularly appealing factors about PtaaS:

- ✓ **A good variety of talent:** The ability to tap different testers, not just for testing of different apps, but for subsequent tests of the same application, is important. Companies we spoke to understand and appreciate the value of having diverse perspectives -- different sets of eyes looking at the same thing may uncover different hidden properties.

- ✓ **Access to a large pool of technical knowledge:** A good pentester needs to understand the underlying makeup of the application. A browser-based app is very different from an application that you interact only with APIs. Thus, the pentesting method should also be very different. The ability to get pentesters who understand the nuances of development frameworks, like mobile architectures, is an important factor to get good results.



A PtaaS solution, because of its nature of being in the cloud, is less constrained by the geographic locations or the physical availability of specific pentesters. As such, it can tap into a large talent pool with a healthy variety of tester backgrounds and knowledge. The customers we interviewed universally indicated that PtaaS provides better skill/knowledge match.

"We want fresh perspectives, but they should come from someone who understands how this type of applications work."

Head of AppSec for a software management company

In contrast, a traditional pentesting consultancy typically only has a limited pool of local pentesters, and they have to cycle the testers through different customer engagements.

Several companies we interviewed had experiences with professional pentesting services. They indicated that it can be challenging to get the right talent mix with pentest consultants. To begin with, the customer may not get the specific talent they want, as the talent may be otherwise engaged. Or, the customer may have no choice but to reuse the same set of pentesters for subsequent tests. "Neither is ideal", as the head of appsec for the software management company told us. "We want fresh perspectives, but they should come from someone who understands how these types of applications work."

	Traditional Pentesting Services	Pentest as a Service
Talent	A limited pool of local pentesters	A large global pool with a variety of tester backgrounds and knowledge
	Cycle/reuse of same set of pentesters for each application	Different pentesters that understand the nuances of diverse applications
	Constrained by the location and physical availability of pentesters -**hard** to get the right talent mix	Less constrained by the location or the physical availability of pentesters-**better** skill/knowledge match

Pentest as a Service Enables Agile Testing

As the number of companies practicing DevOps increases, so does the demand for agile and rapid pentesting. To that end, the companies we interviewed had these things to say about Pentest as a Service:

- **Cloud deployments need SaaS testing:** Many companies develop and deploy cloud apps with workloads distributed across different cloud infrastructure. As such, there is little reason to engage a traditional pentesting consultancy based in a particular geographic location. “As our services have no location bias, we need our service providers to be the same way: agile, location agnostic, and horizontally scalable,” one company told us in the interviews.

- **Easy onboarding of new tests:** Because of its SaaS nature, a PtaaS platform retains knowledge of not only past tests but also tests that are ongoing. Therefore it is far easier to onboard a new test or testers within a PtaaS platform than doing the same thing with a pentesting consultancy, as the latter would need a substantially heavier process of knowledge transfer and set up.

- **PtaaS delivers faster results and more agility:** In addition to easy onboarding, PtaaS allows incremental test results to be delivered through its platform. This enables triage and remediation efforts to be carried out in parallel. In contrast, a traditional pentesting service would only deliver results after the entire test is completed and a report is generated.

	Traditional Pentesting Services	Pentest as a Service
Onboarding of new tests and testers	Limited state carry over from one test to another. Heavier process of knowledge transfer	Ability to leverage prior results within the SaaS platform leads to faster onboarding of new tests
Location-agnostic testing	Geographic location bias results in overhead in delivery	Location agnostic and horizontally scalable testing
Time to result	No information until the final report. Time to result is 2 weeks or longer	Incremental results delivered through the platform. Triage and remediation efforts can start in parallel
Cost of updating test information	Tipically manual means (emails, call, texts) and a long response time to update information such as context, results, or descriptions	Changes can be made in real time. Updates saved and reflected in the PtaaS platform

Pentest as a Service Provides Deep Coverage and High Quality Results

Here's what the organizations had to say about the quality of tests and fiedlity of findings:

✓ **Higher fidelity of findings:** All of our interviewees told us that, when compared with traditional manual testing, the Cobalt PtaaS platform yielded high-fidelity test findings, hich means less false positives and more actionable, impactful outcomes. One company we interviewed indicated that the high-fidelity results also have a qualitative impact—their developers now actively take part in the pentests and engage extensively with the testers, which in turn helps to further improve the quality of the test results.

✓ **Comprehensive documentation:** A traditional pentesting engagement often produces its test findings in a PDF report. The description of tests in those reports is typically terse with little details. In contrast, a PtaaS platform can document detailed information such as the nature of the tests, context, even down to which test inputs were used, observed outputs, and frequency of tests. For our interviewees, the detailed information about a test and the additional context made triage and test validation easier and faster.

✓ **Deeper test coverage:** Because the PtaaS platform documents each test and its associated information, it is relatively easy to verify the coverage of any ongoing tests. For instance, did the tests cover all APIs and core functionality? It is even possible to course correct if coverage becomes a concern. In a traditional pentesting consulting engagement, very little visibility is available for ongoing tests, hence it is often impossible to verify the test coverage.

✓ **More actionable results:** The companies we interviewed agree that a PtaaS platform with its documentation of test scopes, parameters, and context leads to faster triage and more actionable test results. In contrast, many noted that it is challenging to decipher traditional pentesting results that are delivered via static reports and often devoid of appropriate contextual information.

	Traditional Pentesting Services	Pentest as a Service
Fidelity of results	More false positives, more effort needed for triaging and result verification	Less false positives, more accurate results. Faster triage and verification time
Context information	The description of tests and findings lack sufficient contextual details in the report	Detailed information about a test and additional context are saved and can be updated in the PtaaS platform
Test coverage	Difficult to verify or improve coverage	Data is there to enable coverage visibility, which allows coverage improvements
Actionable results	Manual nature of tasks and processes lead to longer triage time and challenging remediation actions	Better documentation of test scopes, parameters and context lead to faster triage and more targeted remediation actions

Pentest as a Service Enables Closer Collaboration Between Security And Engineering

A consistent theme we saw throughout our interviews is that PtaaS brings security and development teams closer together. More specifically:

- ✓ **PtaaS leads to better communications between security and dev:** Because a PtaaS platform documents test scopes, allows easy and early verification of test results, and tracks remediation efforts, companies we interviewed indicated that PtaaS allowed them to improve communication between security and development. In some of the companies, the development team engages directly with the testers throughout the test, which leads to more immediate remediation actions. With traditional pentesting, nearly everything is done manually. Consequently, the communication overhead - the constant back and forth - between security and development is high.

- ✓ **PtaaS delivers better operational efficiency:** In a DevOps environment, where you do multiple code releases and hundreds of builds a day, efficiency is key. PtaaS provides continuous interaction between the testers and the security and engineering teams. In many cases, tasks like opening a ticket and verifying a fix can be triggered directly and automatically from the PtaaS platform. In some cases, this results in tremendous efficiency savings. In contrast, a traditional pentesting engagement relies heavily on manual tasks -- there is little opportunity for automation, integration, or orchestration to improve efficiency.

	Traditional Pentesting Services	Pentest as a Service
Communication models between security and dev	Many back and forth sessions between security and development; high communication overhead	Direct, real-time engagement on the platform improves communication and information sharing between testers, security and development teams
Operational efficiency	Limited optimization or automation opportunities to improve test efficiency	Continuous interaction on the platform and better integration with toolchains allows workkflow efficiency
Transparency	Tests are a blackbox, very little is known about ongoing tests	Ongoing visibility for tests performed, which leads to less friction between security and dev

Summary

As software proliferates and DevOps takes hold, we conducted this study to understand the impact of utilizing Pentest as a Service (PtaaS) vs. traditional pentesting services. Within the backdrop of modern software development practices and rising appsec priorities, our study found that DevOps is a driving force for pushing pentest into the cloud and deploying Pentest as a Service. Furthermore, DevOps demands that appsec measures are delivered in a fashion that favors communication, transparency, and collaboration- PtaaS is exactly the evolution that addresses those aspects.

Traditional Pentesting Services

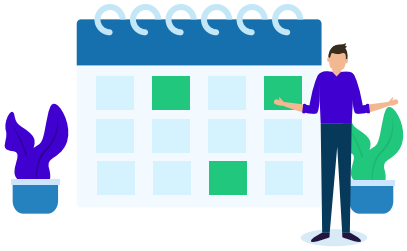
Pentest as a Service

Talent

A limited pool of local pentesters, constrained by the physical availability of pentesters - hard to get the right talent mix for different applications

A large pentester pool with diverse backgrounds, less constrained by the location or the physical availability of pentesters - better skill/knowledge match

Speed and Agility



A heavier process of knowlegde transfer and set up to onboard a new test, limited state carry over from one test to another - hard to scale

Easy onboarding process due to retained knowledge of past and ongoing tests on a centralized platform - agile and horizontally scalable testing

Traditional Pentesting Services

Pentest as a Service

Coverage and Quality of Results

Mixed test results, the description of findings in a PDF report lacks sufficient details and requires manual means (emails, call,texts) to make changes

Fewer false positives, detailed information about a test and additional context on findings are updated and reflected in real-time via the platform

Communication and Efficiency

Limited interaction between pentesters, security and development teams - manual tasks and black box testing results in longer triage time to fix issues

Effective and continuous interaction between pentesters, security and development on the platform - integrations and transparency of findings result in faster triage time


Cobalt