ROI of Pen Testing as a Service

Research Conducted by Dr. Chenxi Wang, industry thought leader and analyst

Return on Investment of Cobalt's Pen Testing as a Service

Cobalt commissioned Dr. Chenxi Wang of the Jane Bond Project to examine the Return on Investment (ROI) that organizations may realize by using Cobalt's Pen Testing as a Service (PTaaS) platform. This study took a detailed look at the benefits and costs of deploying Cobalt's services in comparison with using traditional penetration testing consultancies.

For this study, we conducted in-depth interviews with current Cobalt customers. The organizations we interviewed represent a wide swath of different industry segments, including SaaS, enterprise software, healthcare, and FinTech. Some of the example customers we interviewed include:

• An enterprise SaaS provider on the east coast of the US. We interviewed the product security lead, who manages application security for over 1,000 customer-facing applications.

• An enterprise software solution provider in the San Francisco Bay Area. We interviewed the Director of Engineering, who manages over 20 engineers across two distinct product lines.

• An in-the-cloud research service provider. We interviewed the VP of Engineering of this company that has 4 different applications across mobile platforms, web, and APIs.

• A consumer-facing cloud service located on the west coast of the US. We interviewed the Product Security Engineer, who works in a dedicated 3-person security team responsible for information, infrastructure and application security.

• A healthcare service provider. We interviewed the Director of Trust for the company. The company has 50 developers across approximately 30 applications, with a 6-person security team.

• A financial services technology company. We interviewed the CISO of the company, whose responsibilities include managing information security and application security across the 30-some different applications.

Figure 1: 2/3 of the Interviewees are Security Professionals while the other 1/3 are Engineers

Two out of three companies we interviewed had dedicated security teams while the remaining ⅓ lacked such a function. For the companies in the latter category, the engineering team typically drove the implementation of pen testing services. None of the companies that we interviewed had a dedicated application security function. All but one company had employed pen testing services prior to engaging Cobalt.

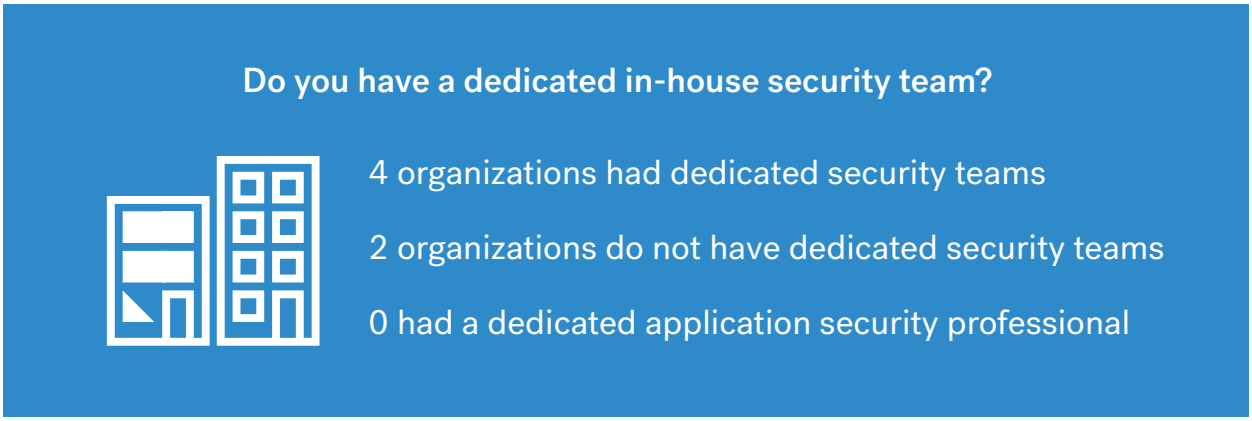


Figure 2: 2/3 Of Organizations We Interviewed Have Dedicated Security Teams

This paper presents the aggregate findings derived from the research interviews as well as our independent research. Whenever meaningful, we took the average data across all the customers we interviewed.

Key Findings

The study found that Cobalt's Pen Testing as a Service (PTaaS) approach brings a significant higher Return On Investment (ROI) than traditional pen tests -- organizations see approximately 103% higher return on investment when they use Cobalt. Other interesting metrics include:

• Interviewees considered Cobalt's crowd-sourced testers more knowledgeable than traditional pen testers; they rated Cobalt testers **4.6 out of 5 in terms of knowledgeableness vs. 3.4 out of 5** for traditional testers. This difference is attributed primarily to Cobalt's crowdsourcing model that allows better matching of tester skills to targeted applications.

• Cobalt takes slightly longer in the initial planning and set up stage - **3.2 hours vs. 2.4 hours** in traditional pen tests. Interviewees attributed this to Cobalt's extensive information gathering and planning process.

• During the test, Cobalt required **62% fewer overhead hours** to manage than traditional pen tests

• Time-to-complete-results with Cobalt is **24.7% shorter** than traditional pen tests

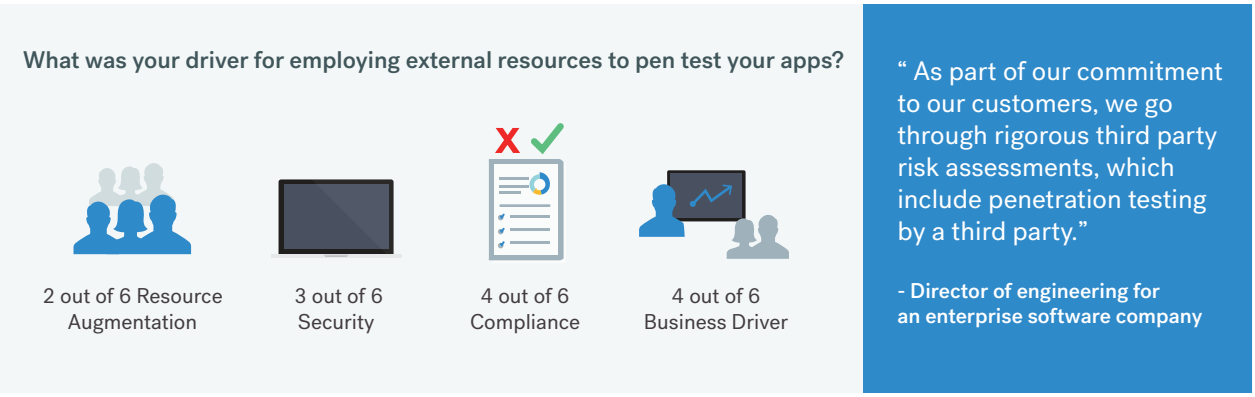
• On average, Cobalt effects **78% reduction in triage time**, compared to traditional pen tests

Note: This data is based on the six in-depth interviews

Figure 3: Users rate Cobalt testers more knowledgeable than traditional testers

Drivers for Penetration Testing Services

When asked what their motivation was for employing external pen testing services, interviewees cited compliance and business reasons, in particular customer demand, as the top drivers, followed by security and the need to augment internal resources.



Note: This data is based on the six in-depth interviews

Figure 4: Business Drivers And Compliance Are Top Reasons Why Companies Pen Test Their Apps Via External Services

Cobalt's Pen Testing as a Service (PTaaS) Platform - An Overview

To kick off a Cobalt pen test, an organization provides information about its application's technology stack and a team of certified pen testers with matching skill sets are selected to do the project. A typical team consists of one lead supported by two technical domain experts. The pen testers work together to explore the complete application over a fixed time period. They work together to perform manual security testing related to topics like input validation, authentication, and access controls in order to identify flaws in the application's implementation.

As the team discovers issues in the application, they submit reports to the organization through the Cobalt platform. The lead researcher is responsible for reviewing each report before it is submitted to ensure the report is valid. He or she also assigns a criticality rating to each finding, based on likelihood and impact.

The organization receives reports as soon as they're discovered and reviewed by the pen test lead. Security and developers can interact directly with pen testers using the platform to discuss issues as needed. The platform also integrates with developer bug tracking systems like JIRA and GitHub.

When the project is complete, the organization can also download a PDF summary report to share with internal and external stakeholders, such as development team leads or customers requiring proof of a technical security test.

Comparison Between Cobalt And Traditional Pen Test Consulting Services

In order to understand ROI comparisons between Cobalt Pen Testing as a Service (PTaaS) and traditional pen testing, we asked our interviewees detailed questions on service cost, the quality of test outcomes, accuracy, depth and coverage of findings, etc. The aggregated interview results are captured in Table 1 below.

Table 1: Comparison of cost and quality metrics

	Traditional Pen Test Consulting	Pen Test as a Service (PTaaS)
Remediation Validation	**Limited:** Not all consulting firms include remediation validation as part of the service package. When they do, the grace period is usually limited.	**Full coverage:** Remediation validation is included as part of the package. The same testers are bound to the project until all issues are resolved.
Knowledgeableness of pen testers	**Gaps in knowledge:** On average, Interviewees thought the pen testers were "good, but with some gaps in knowledge", especially in areas such as IoT, micro-services, and cloud applications.	**Extensive Knowledge:** The PTaaS model allows Cobalt to tap into a more extensive pool of potential pen testers for better skill/knowledge match.
Cost	**Moderate to high**	**Moderate:** On average, a Cobalt test is 31% less expensive than traditional pen testing services
Transparency	**Limited visibility:** "You have little information as to which tests were actually conducted."	**Extensive visibility:** "Using Cobalt's platform, you can see in real-time what the testers are doing."
Depth of Findings	**Shallow findings:** Tests are typically conducted in a black box, which often focused on config errors and a set script for attacks.	**Deep Coverage:** With the collaborative platform, dev and security can have real-time Q&A with the pen testers, which helped guide the tests to produce deep probe and discoveries.
Accuracy of results	**Certain Issues Missed:** Interviewees gave traditional pen testing services 3.4 out of 5 for accuracy. "They found configuration errors but no deep flaws"	**Very accurate:** Interviewees ranked Cobalt's results 4.7 out of 5 for accuracy. "The testers were creative; they crafted unique ways to attack the code as well as the business logic"
Coverage of tests	**Mixed coverage:** Depending on the application, interviewees reported mixed results in terms of how extensive the applications are covered by the tests.	**Extensive coverage:** "A noticeable benefit of Cobalt is the coverage of the applications. They cover a larger part of the application and produced a larger volume of findings."

We also explored specific efficiency metrics in our interviews to understand the overhead of testing, the level of effort required to deal with test findings, communication between teams, and the organization's ability to leverage or access results.

Table 2: Comparison of efficiency metrics with Cobalt and traditional pen testing services

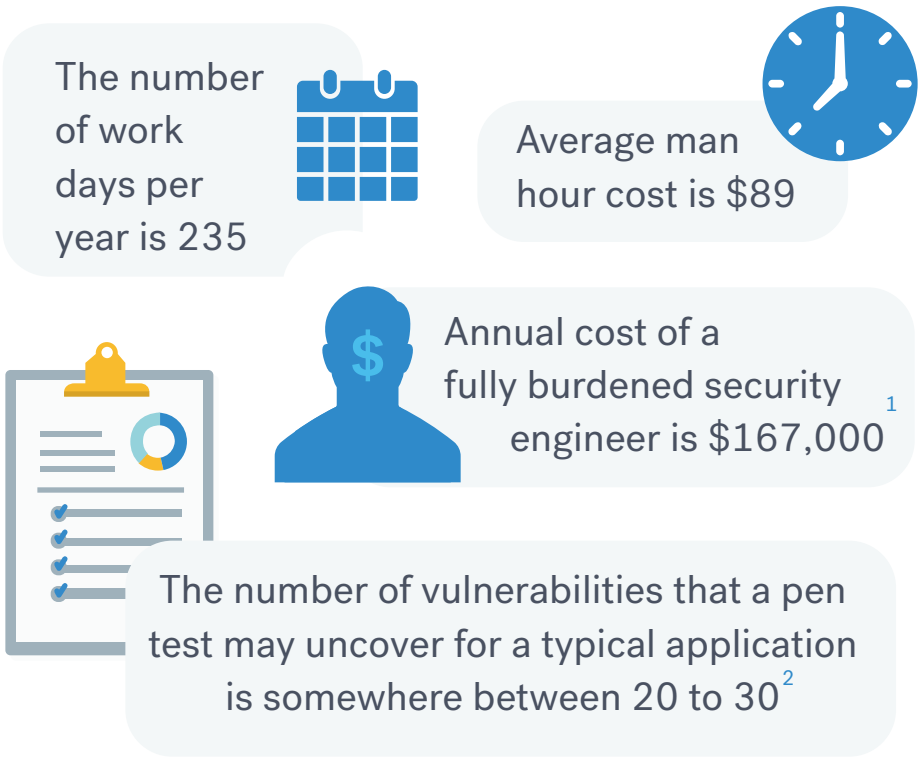
	Traditional Pen Test Consulting	Pen Test as a Service (PTaaS)
Test prep time (this does not include purchasing & procurement)	**Minimum:** On average companies reported spending 2.4 hours preparing the environment for testing and provisioning necessary accounts).	**Minimum +:** On average Cobalt customers reported spending 3.2 hours for pre-test tasks, including the kick off call, platform set up, and filling out a detailed questionnaire, etc.
Time to results	**Longer:** Little is available before the final report, which typically takes a week or two after the end of the test.	**Immediate:** Findings are visible immediately via the Cobalt platform.
Triage time	**Lost in translation:** Back and forth between dev, security, and pen testers are done via manual means (emails, call, texts), which are labor intensive and error prone.	**Collaborative triage:** The platform allows collaborative triage, which the interviewees credited for shortening triage time and facilitating effective communication between testers,
Communication effort	**Manual:** Companies typically use email and phone calls to ask a question or resolve dispute with the pen testers.	**Collaborative:** Both security and engineering leads can use the Cobalt platform to communicate and discuss with pen testers. This cuts many hours of back and forth.
Management of overhead during testing	**Minimum:** Interviewees reported an average of 7.5 man hours needed to manage a test with traditional pen testing.	**Minimum:** Interviewees reported an average of 2.8 man hours needed to manage a test with Cobalt.
Ability to leverage prior results	**Certain Issues Missed:** Interviewees gave traditional pen testing services 3.4 out of 5 for accuracy. "They found configuration errors but no deep flaws"	**Very accurate:** Interviewees ranked Cobalt's results 4.7 out of 5 for accuracy. "The testers were creative; they crafted unique ways to attack the code as well as the business logic"

Analysis and ROI Calculation

Our analysis is built on an ROI calculation that includes these aspects:[1]

- Cost of services
- Benefits and efficiency saving analysis

In this analysis, we use the following assumptions:



[1] Using Glassdoor data of average salary for security engineers as $128,500, and a fully burdened rate is 30%.

[2] It's very difficult to characterize what a typical application is. We simply used the average number of bugs found from the interviews.

Cost Analysis

With the exception of one, the customers we interviewed have all deployed other penetration testing services before. Many used traditional penetration testing consultancies that employ a specific testing team.

Cobalt uses a different approach: it uses crowdsourcing to identify pen testers for its clients. As such, Cobalt has access to a larger pool of talents from which you can often find exact skill/talent fit for the target application. One interviewee, the Product Security Lead for an enterprise SaaS service, remarked that "It's easy to find pen testing services that are proficient in vulnerability scanning or even in exploitation. But when it comes to micro-services or APIs, it was challenging to find good testers. Cobalt succeeded because of their crowd-sourced model. We were impressed that Cobalt testers found multi-API dependency bugs that are typically very difficult to ping down."

In terms of the cost for services, we found that, on average, the price tag of Cobalt's services is 31% lower than those of traditional pen testing consultancies. This number is a bit skewed as one customer we interviewed paid a higher-than-market rate for a pen testing consultancy.

Benefits and Efficiency Savings Analysis

Cost Savings Benefits Of the Cobalt platform on Triage Time — $2,573

The Cobalt platform, along with the slack channel Cobalt sets up between the testers and the client, have reduced the number of time-consuming triage tasks that used to require many back and forth meetings and calls between security engineers and engineering (or between engineering and testers). On average, this helped organizations reduce triage time to approximately 20 minutes per vulnerability.

With traditional pen testing services, the triage time is approaching 89 minutes per vulnerability. This translates to an average saving of approximately 29 man hour per test, assuming on average a test uncovers 20 to 30 vulnerabilities in the high or medium category. This is a saving of $2,573 per test for the organization. For a company that conducts semi-annual tests on a large application portfolio, the saving can be significant.

Cost Savings Benefits From Increased Test Depth and Coverage by Cobalt — $2,225

80% of the companies that deployed traditional pen testing services prior to Cobalt reported shallow findings and limited test coverage by those testers. To compensate, some of these companies resorted to retest themselves prior to deploying Cobalt.

With Cobalt, customers reported an increased test depth and more extensive test coverage. Director of Engineering of the enterprise software company said: "Cobalt testers crafted some inventive attacks. One test involved abusing of the business logic in a way that none of us had seen before. It was educational even for my developers."

To augment a shallow test, companies might spend 20-30 man hours of in-house time for further testing. At this rate, Cobalt enables a saving of roughly $2,225 per test so that companies do not have to spend in-house resources to retest and ensure coverage.

Cost Savings Benefits From Decreased Management Overhead — $415 per test

With a pen testing consultancy, sometimes the customer needs to do daily calls with the testers in order to keep on top of the progress. One of our interviewees, the InfoSec Officer for a financial technology company, said that "waiting for a daily call to occur and dealing with the added overhead of a call every day is challenging". With Cobalt, managing the test and keeping up with the testers simply involves responding to notifications from the portal and checking them as soon as they occur.

On average, the interviewees said that they were spending 7.5 man hours managing the tests with traditional pen testers. With Cobalt, that number drops to 2.8 man hours. The saving is $415 per test.

Figure 5: Cobalt Requires Less Time To Manage Testing

Cost Savings Benefits From Shortened Time To Results — Unquantified

With a traditional pen testing consultancy, the testers conduct their tasks in a "blackbox" -- the customer has little visibility to what is going on until he or she receives a pen-testing report that describes the findings.

With Cobalt, the tests performed are documented in the platform. Security or development teams can log into the platform and see real-time information of the ongoing tests. Results of the tests are visible in the platform as soon as they become available - no need to wait for a final report.

The interviewees called this out as a significant benefit. While Cobalt required a bit longer in the beginning to set up and gather information, the time-to-first-result is shortened from a minimum of 2 weeks with a pen testing consultancy to a day, or sometimes hours with Cobalt. On average, time-to-complete-results is shortened from 3.1 weeks with the consultancies to 2.25 weeks with Cobalt.

The biggest impact of reducing time to results is the reduced window of exposure for vulnerabilities. Since there is no industry-standard number to calculate cost of exposure, we left this item unquantified. We note that this makes our model more conservative.

Table 3: Time-to-result and Time-to-complete-result

	Initial prep time	Time to first result	Time to complete result
Traditional Pen Test Services	2.4 hours	2 weeks (minimum)	3.1 weeks
Cobalt	3.2 hours	Hours or days	2.25 weeks

Cost Savings Benefits From Increased Accuracy — $10,000

Our interviewees also pointed out that the Cobalt services render more accurate results. Compared to traditional pen testing services, which the interviewees ranked 3.4 out of 5 in terms of accuracy, Cobalt received a 4.6 accuracy out of 5 accuracy rating.

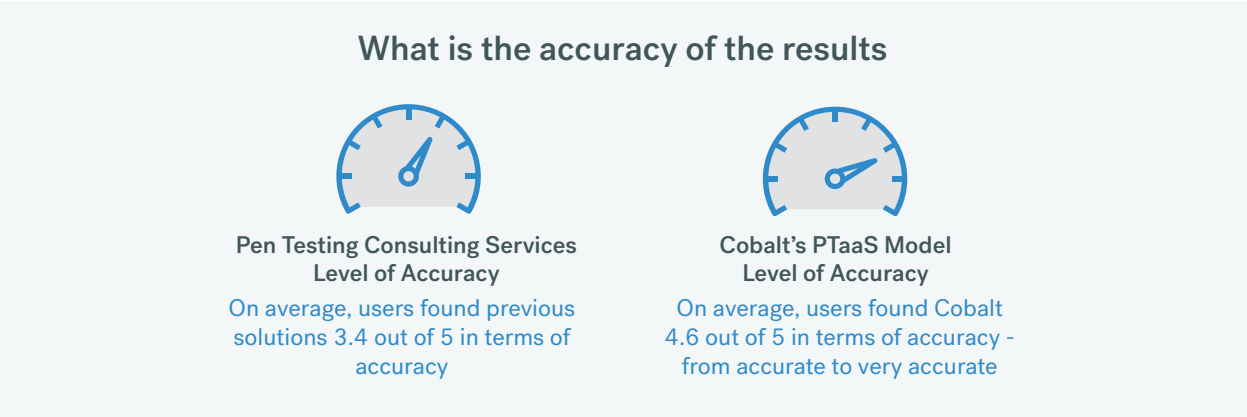


Figure 6: Users Reported Cobalt's Tests More Accurate Than Traditional Pen Tests

Assuming there are 25 meaningful vulnerabilities per application, each point reduction, on a 5 point accuracy scale, would miss approximately 6 such vulnerabilities. Therefore, by using Cobalt, customers on average discover 7 more vulnerabilities per test.[3]

We assume that 30% of the vulnerabilities found would be critical or high vulnerabilities (P1), which may lead to remote exploitation or security breaches. This means that Cobalt's increased accuracy allows organizations to discover two critical vulnerabilities on average. It is impossible to quantify the exact economic impact of missing critical vulnerabilities because it depends heavily on the nature of the application and the vulnerability.

We note that the going price for zero-day vulnerabilities in the underground market is in the range of thousands, with the high reaching $50,000. To approximate the risk, we used $5,000 as a crude cost approximation for each missed critical vulnerability.[4]

[3] Note that the accuracy number is an average derived from the interviews. There are some customers who observed equal accuracy between Cobalt and other testers.

[4] Note that $5,000 doesn't even begin to describe the cost experienced after a breach the scale of Equifax, Target, or Sony. However, since we cannot adequately assess the potential scale of a breach here, we took a conservative approach, using the cost of vulnerabilities on the underground market to approximate the impact to the organization.

Table 4 shows the summary of the cost saving benefits using Cobalt's Pen Testing As A Service (PTaaS) model, as compared to traditional pen testing consultancies. The numbers shown here are per test.

Table 4: Cost Saving Benefits of Cobalt over Traditional Pen Testing

	Increased test depth and coverage	Decreased triage time	Decreased management overhead	Increased accuracy	Total cost savings
Cost saving benefits over traditional testing	$2,225	$2,573	$415	$10,000	$15,203

Summary

Here we use the financial calculation in the Benefits and Costs sections to determine the comparative ROI between Cobalt's Pen Testing as a Service (PTaaS) and the more traditional form of Pen Testing Consulting Services. We assume a price tag of $20,000 per penetration test with traditional pen testers. Table 5 shows the risk-adjusted ROI. We assume a 10% risk adjusted ratio.

Table 5: Cobalt's ROI Analysis Over Traditional Pen Testing

	Raw	Risk Adjusted
Total Cost Over traditional testing (assuming a price tag of $20,000 per test)	- $6,200	- $5,580
Total Benefits over traditional testing	$15,203	$13,682
ROI over traditional testing	107%	96%

Cobalt's Pen Testing as a Service model has a **96% higher ROI** than traditional pen testing

In summary, we found that Cobalt's Pen Testing as a Service (PTaaS) ROI is 96% higher than traditional pen testing, primarily due to Cobalt's increased accuracy, lower cost, and improved efficiency.

The benefits and cost savings illustrated here can be even more significant for companies that have a large application portfolio.

Table 6: ROI Analysis Over Large Application Portfolios

	4 tests a year (2 applications)	**10 tests a year** (5 applications)	**20 tests a year** (10 applications)
Risk-adjusted cost savings over traditional penetration testing services	$77,048	$192,620	$385,240