ESG Economic Validation

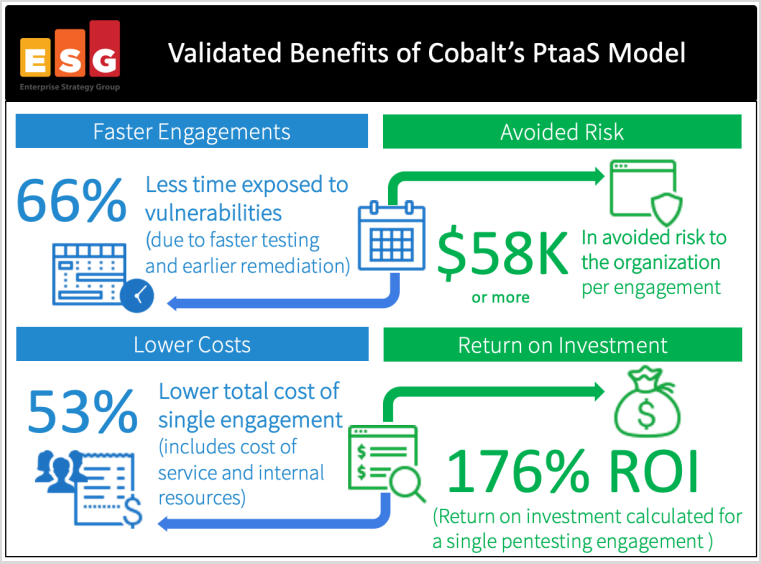
Analyzing the Economic Benefits of Cobalt's Pentest as a Service (PtaaS) Model

By Aviv Kaufmann, Principal Validation Analyst; and Jen Duey and Justin Boyer, Validation Analysts

July 2022

Executive Summary

Data breaches cost businesses millions of dollars and can cripple an organization. Penetration testing business applications is one of the most effective ways to prevent data breaches due to application coding or configuration errors. However, many organizations struggle to pentest their applications effectively and frequently enough to make a difference. Some struggle to find the right talent to perform the test. Others find it difficult to work proper testing into their development lifecycle. Often, companies feel like the only option is to pay expensive consultants to do the work for them.



Through customer interviews and case studies, ESG validated that Cobalt's Pentest as a Service (PtaaS) model provides a cost-effective way to reduce risk and accelerate results. Cobalt provides skilled testers who collaborate with development teams during the test and help them fix vulnerabilities before they become an expensive data breach. Organizations no longer need to engage with expensive consultants that disappear for weeks to test their applications before dumping a cryptic list of vulnerabilities on their doorstep. ESG models found that customers using Cobalt's services reduce the time that vulnerabilities stay exposed by 66%, while lowering the total cost of the pentest by 53%, resulting in an expected return on investment (ROI) of 176% per engagement. With Cobalt, collaboration and highly skilled testers lead to excellent results and a massive reduction in risk exposure for companies of all sizes.

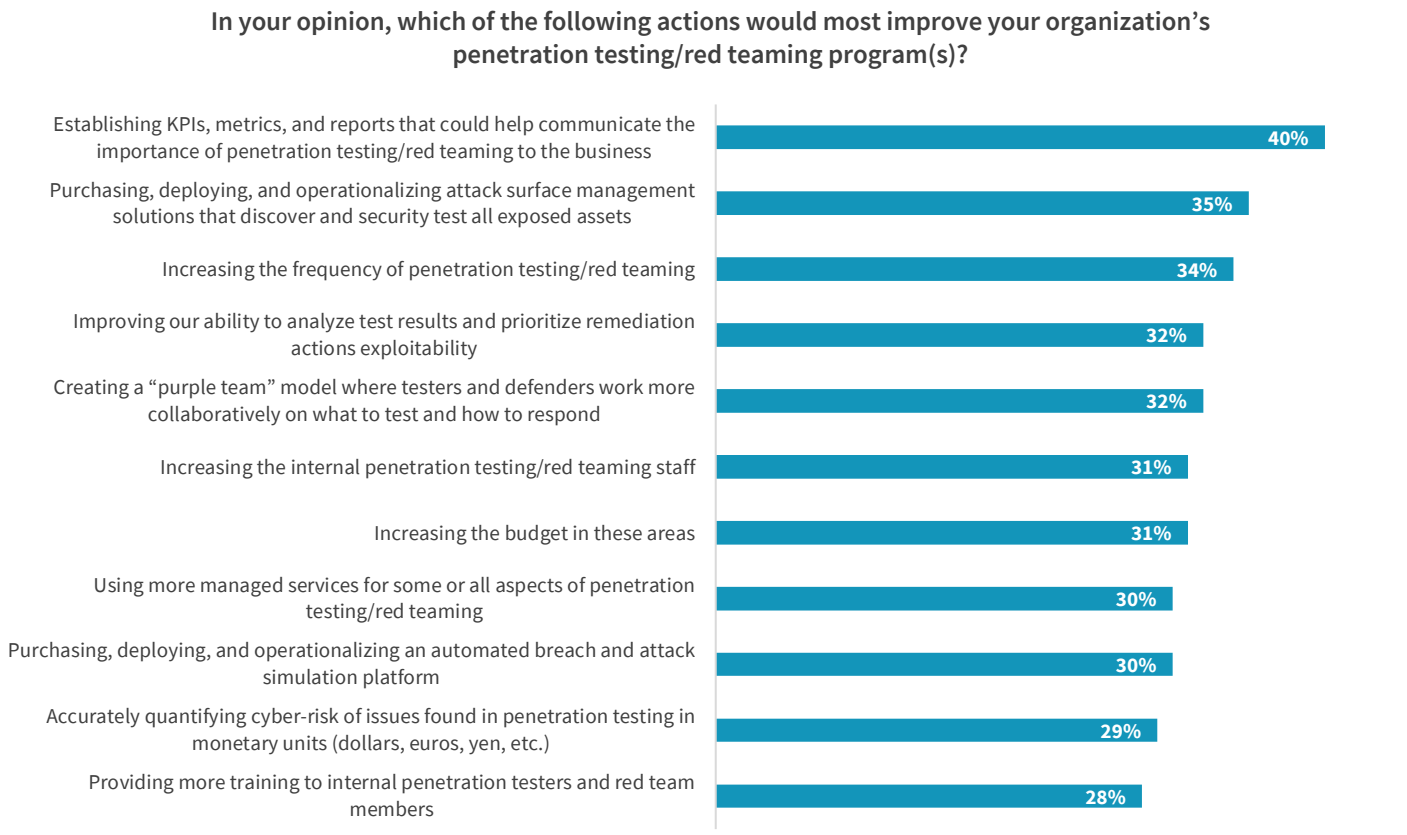
Introduction

This ESG Economic Validation focused on the quantitative and qualitative benefits, such as faster time to results and remediation, operational savings, and reduced costs and risk, that organizations can expect from using Cobalt's Pentest (also referred to as "penetration testing") as a Service (PtaaS) Model.

Challenges

Without thorough pentesting to identify potential vulnerabilities, organizations leave themselves open to a possible data breach. Data breaches cost organizations millions of dollars to address and are often crippling to business integrity, operations, and brand reputation. However, organizations often lack the resources to execute pentesting. Often, the experienced resources they do have that can complete a proper pentest are needed for higher priority development and security projects. According to ESG research, less than half of organizations feel that their pentesting capabilities are adequate in any area.[1] Our research also identifies that better communication around the importance of testing, more frequent pentesting, improving the ability to analyze test results and prioritize remediation, and better collaboration between testers and defenders are four of the top five actions that would improve pentesting for organizations.[2]

Figure 1. Actions to Improve Pentesting for Organizations



Source: ESG, a division of TechTarget, Inc.

In an effort to augment internal resources, many organizations have turned to contractors, security vendors, or pentesting providers and specialists to complete penetration testing. Even so, internal staffing is required to prepare for, manage, and perform triage and remediation after these engagements. Timelines are lengthy and serialized, and organizations must often pay for additional retesting after remediation. Whether using internal resources or contractors, organizations will

[1] Source: ESG Research Report, *Security Hygiene and Posture Management*, January 2022.
[2] Source: ESG Complete Survey Results, *Security Hygiene and Posture Management*, January 2022.

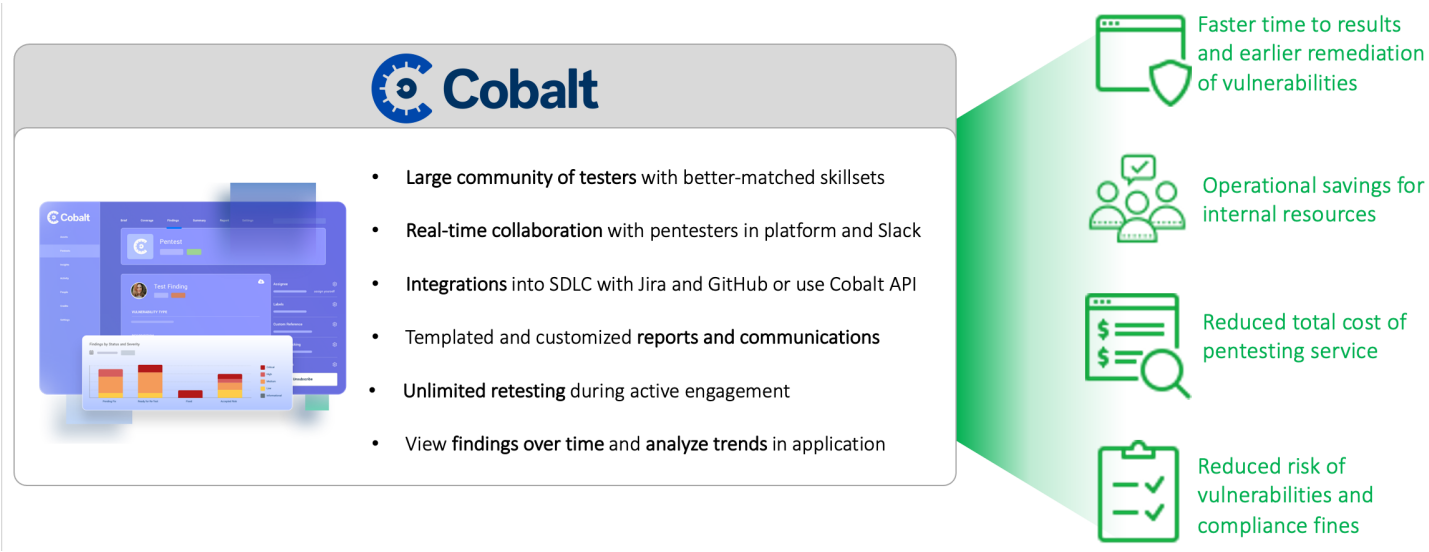
operate more slowly and pull resources from daily tasks. Organizations continue to struggle to meet the evolving industry standards and regulations, protect themselves and customers from vulnerabilities, and deliver agile services and applications without impacting timelines.

One other method that bears mention is bug bounty. These are open-ended programs in which anyone can search for vulnerabilities in an application or asset. Customers pay testers on perceived "quality" of each finding. Bug bounty offers sparse coverage in comparison with pentesting because participants focus primarily on incentivized vulnerabilities. In addition, bug bounty researchers often vary in quality and are fueled by competition with each other, which differs from collaborative approaches like PtaaS, which we will explore in the next section.

The Solution: Cobalt's Pentest as a Service Model

Cobalt aims to reinvent how organizations pentest their assets with a new approach: Pentest as a Service. Instead of offering long, quiet engagements with consultants, Cobalt's testers become part of your team from day one. Cobalt's philosophy of open collaboration, interactive pentests, and agile delivery gives organizations quick access to a pool of 400 experienced pentesters. During the engagement, businesses get a front-row seat to pentesting operations, always knowing what is being tested and receiving vulnerabilities in real time.

Figure 2. Cobalt's Pentest as a Service Model



Source: ESG, a division of TechTarget, Inc.

Cobalt provides a comprehensive testing platform to foster communication and operational efficiency. The platform features the following capabilities:

Integration Capabilities:

- Streamline remediation and reporting workflows by integrating with customers' existing tech stack.
- Streamline communication between security and development.
- Create a single pane of glass for all pentest findings.

Automation Capabilities:

- Feed internal security dashboard with custom pentest data.

- Automatically push pentest findings to internal system(s).
- Accelerate remediation cycle by automating workflows and communication.

Analysis Capabilities:

- Use data to calculate internal performance metrics and track historical progress.
- Get comprehensive information about assets, associated findings, and events.
- Define filters to include criteria and make queries more specific.

ESG Economic Validation

ESG's Economic Validation process is a proven method for understanding, validating, quantifying, and modeling the economic value propositions of a product or solution. The process leverages ESG's core competencies in market and industry analysis, forward-looking research, and technical/economic validation. For this validation, ESG interviewed Cobalt customers and reviewed existing analysis and customer case studies to better understand and quantify how PtaaS has impacted organizations, particularly in comparison to traditional pentesting methods.

Cobalt PtaaS Economic Overview

ESG's economic analysis revealed that PtaaS provided Cobalt's customers with significant savings and benefits in the following categories:

- Faster Time to Results and Remediation – Begin remediating critical vulnerabilities within days of starting a test.
- Operational Savings – Reduced organizational overhead to manage the pentest.
- Reduced Cost and Risk to the Organization – Cost flexibility and a reduced chance of a data breach.

Faster Time to Results and Remediation

Finding and fixing vulnerabilities quickly reduces risk to the organization and saves money. Customers reported that Cobalt PtaaS successfully condensed the testing window while keeping communication open and service quality high. ESG found that customers enjoyed the following benefits:

- Accelerated Start to Engagement – ESG found that planning and onboarding are significantly faster when using Cobalt's PtaaS model. Customers reported the engagement beginning as quickly as 48 hours after signing the contract. To help accelerate the start of the engagement, Cobalt pre-scans the applications under test before the experts begin testing to help show possible areas of concern as early as possible. Cobalt provides a dedicated customer success manager to help new clients get underway.

"Traditional consultancy lead times can be between four and eight weeks depending on the time of year and the resources available. With Cobalt, the lead time to begin testing was inside 48 hours."

- Faster Time to First Results – Cobalt's pentesters remain in constant contact with customers during the testing process through Cobalt's platform or through a dedicated

"One of the best things was being able to collaborate with the testers through the platform as well as through Slack. We got on-the-fly updates to the dashboard and were able to work on fixing issues as they were still testing."

Slack channel. Vulnerabilities are reported immediately after being found instead of waiting until the end of the engagement. Customers reported receiving their first findings within 48 hours of the start of the engagement—93% faster than traditional consulting models.

- Faster Time to Test Completion – Customers reported that Cobalt engagements were completed in 10-14 days, resulting in up to a 50% reduction in time to results compared to traditional engagements. Cobalt matches customers with expertise from their Cobalt Core Pentesters, ensuring applications are tested by those with the most experience in the business domain or technology. Cobalt's credit-based pricing allows them to assign more resources when necessary to fit demand and stay within that 14-day window.

- Faster Time to Remediation – Due to the constant two-way communication with experienced pentesters who shared guidance on potential remediation, customers were able to start earlier and triage, remediate, and retest faster. Customers reported between 80% to 100% of their retesting for the most critical vulnerabilities was complete by the time the engagement was over. For any that remained, Cobalt provided free and unlimited re-testing until the issues were fixed. One customer reported that communication with Cobalt "allowed us to come up with solutions in almost real time."

- Faster Subsequent Testing – Companies requiring regular security testing of their assets found that using Cobalt's PtaaS model scales well over time. Cobalt's platform stores data about the environment and assets and carries it over to the next engagement. Pentesters get to know applications over time, using trends to make testing more efficient with each engagement. Pentesters can use their knowledge to identify difficult-to-find vulnerabilities that require deeper understanding of in-scope assets.

"80% of our retesting was finished before the engagement was over."

Operational Savings and Efficiency

The cost of pentesting doesn't only include the price paid to a consultant. There are many steps to prepare and run a successful pentest, and customers typically have to allocate resources and hours to help the test run smoothly. Cobalt customers found that PtaaS required fewer resources due to the strong collaboration with Cobalt's pentesters and the help from a dedicated customer success manager. The operational savings include:

- Less Time Spent Managing Testing – ESG investigated how Cobalt helps to reduce the required resources for organizations to run a pentest. Cobalt becomes an extension to the team, working with customers every day through the application and Slack channel. A dedicated customer success manager helps to manage the engagement. Customers who purchase the Premium and Enterprise tiers also receive technical help with the Cobalt platform from dedicated sales engineers.

"The engagement came with a customer success manager who is your partner from day one. The support you get from the platform and guided experience saves you a lot of time."

- More Efficient Triage – Customers reported that the collaboration with Cobalt, coupled with the guidance provided on discovered vulnerabilities, helped to make triage and remediation easier. At the end of the engagement, Cobalt provides a remediation plan and prioritized list of vulnerabilities so customers can focus on fixing what was found instead of investigating further.

"We had to achieve compliance for two standards, and we just don't have the experience or resources in-house to dedicate to pentesting. There is no way we could have done it that timeframe without Cobalt ."

- Fewer Internal Resources Required (versus DIY or in-house testing) – Customers commented on the difficulty in staffing security expertise. One customer mentioned they only had a handful of developers when they needed to pentest their solution. Even larger organizations don't always have the resources to build internal red teams to test their applications. Cobalt Core Pentesters supplement customers' businesses and allow greater focus on core business activities. Startups and established companies alike benefit from on-demand security expertise, saving time and money necessary to hire cybersecurity talent. In addition, using Cobalt's experts frees up development talent to continue delivering core business features instead of switching to pentesting for several weeks.

- Consistent System of Pentesting Record – Cobalt's platform saves pertinent information for each application under test. When an application requires a new pentest, Cobalt will already have the necessary information, along with a history of vulnerabilities found and trends over time. This leads to fewer resources required for subsequent testing, historical information, and trending as people come and go and other tests need to get done.

"Data is stored for subsequent testing, allowing you to go through the pentest wizard and test the same asset you've already collected within the platform, so to spin up the next test is so much faster."

- Integration with Existing Processes – ESG found that Cobalt fits in with a customer's existing DevSecOps ecosystem. Cobalt integrates with existing tools such as Jira and GitHub with the ability to create tickets or issues for the vulnerabilities found. This functionality allows customers to focus on fixing vulnerabilities instead of spending hours manually entering tickets into various systems.

Reduced Cost and Risk to the Organization

Pentests aren't effective unless they reduce risk. However, not all companies have the resources available to spend large amounts of money to hire consultants. Cobalt's credit-based pricing model, proprietary tools, two-way collaboration, and free retesting after the engagement help customers significantly reduce risk without breaking the bank.

"You have to pick the best choice between price, quality, and other elements related to the end result. We interviewed four or five different companies. Cobalt's value was awesome as opposed to other providers."

- Reduced Cost of Engagement – Cobalt's credit-based pricing allows organizations to pay only for the resources they need. In addition, Cobalt offers retesting of discovered vulnerabilities for free, instead of forcing customers to pay for a second pentest.
- Lower Risk of Data Breach – Customers reported that the greater speed with which Cobalt tested their applications led to a faster remediation time. When organizations fix vulnerabilities right away, their exposure to the risk of data breach is reduced. ESG found that the time Cobalt customers are exposed to risk is reduced by 66% versus traditional pentesting methods.

"With Cobalt we were able to address all of the critical vulnerabilites before the end of the engagement – with other testers we would not have even had a report of what was found by then."

- Greater Depth and Frequency of Testing – The Cobalt Core Pentesters give customers access to a specialized experience that may not be found in-house or with pentesting consultants. This experience translates to a greater depth of testing since experienced pentesters can use advanced attacks others may not think to try. Cobalt's speed of engagement (50% faster than traditional pentests) allows for greater agility and frequency of testing. Customers can engage with Cobalt more frequently to support rapid feedback and release cycles.
- Historical Vulnerabilities – Cobalt's platform stores previous vulnerabilities found within each application under test. This database allows organizations to discover trends and adjust to prevent similar coding errors in the future.

ESG Analysis

ESG leveraged the information collected through vendor-provided material, public and industry knowledge of pentesting and security practices, and the results of customer interviews to create a modeled scenario that compares the expected time and cost for a traditional pentest engagement versus using Cobalt's Pentest as a Service model to satisfy the same testing criteria. ESG's interviews with Cobalt subject matter experts and Cobalt customers, combined with our own research and technical validation of penetration testing products, helped to form the basis for our modeled scenario.

ESG's modeled scenario was based on a small to mid-sized organization looking to satisfy pentesting requirements for their online SaaS applications. ESG leveraged information provided by previous Cobalt pentesting ROI studies, ESG research, publicly available information, and blended averages across our interviews with Cobalt customers as the basis for our assumptions used in our modeled scenario.

ESG assumed that the traditional pentesting engagement would take a total of four weeks to complete based on previous studies. ESG's validation concluded that a Cobalt engagement took roughly half of the time of traditional engagements, or a total of two weeks. This proved credible, as a two-week engagement time was also reported by several Cobalt customers in our interviews. While the traditional pentesting service would not provide a list of found vulnerabilities until the conclusion of the engagement, Cobalt customers agreed that the first vulnerability was identified and reported to them by Cobalt in the first 48 hours of testing.

Why This Matters

Pentesting is a critical step in identifying potential vulnerabilities in applications and infrastructure or regulatory compliance violations. Few organizations have the appropriate internal resources, and traditional pentesting services can be lengthy and costly.

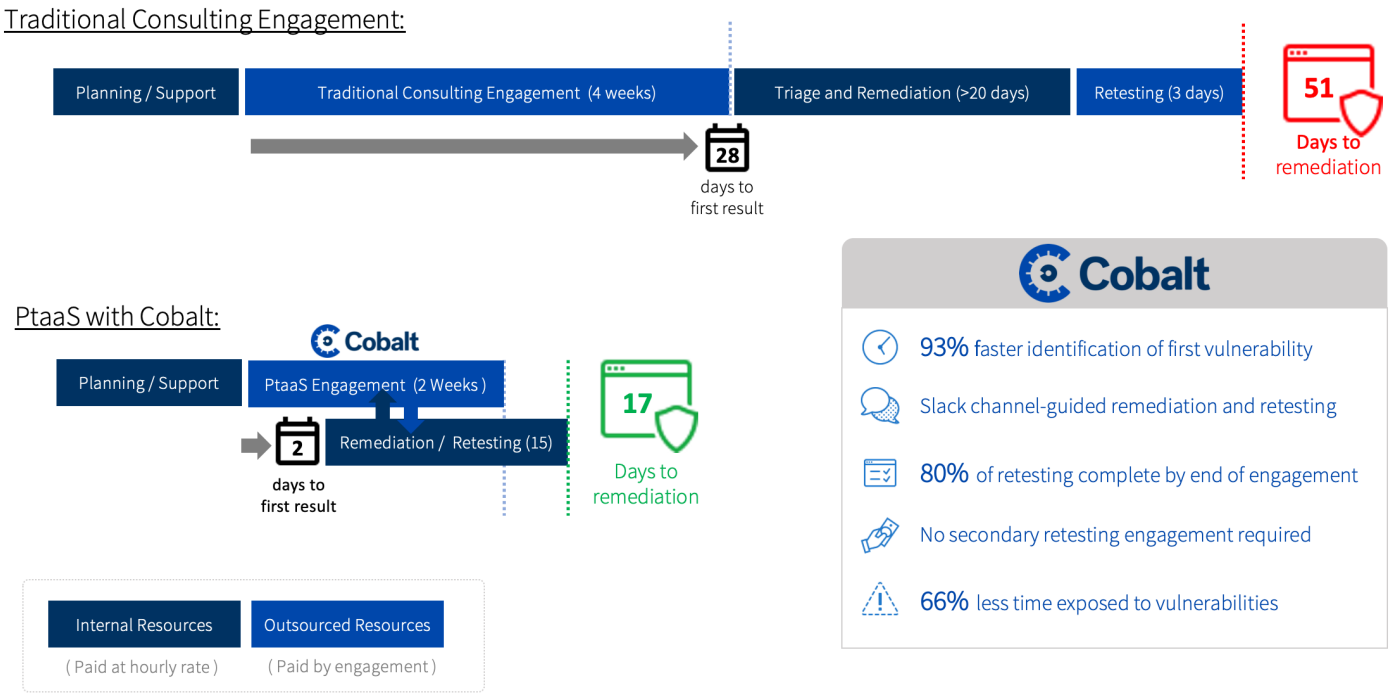
Cobalt's PtaaS model can reduce the total cost of a pentesting engagement by 53%, while reducing the time exposed to vulnerabilities by 66%.

From this point forward, customers were able to begin remediation with constant two-way communication with the Cobalt tester within the PtaaS platform and via Slack channels. During the engagement, Cobalt was not only reporting more vulnerabilities, but was also helping to prioritize them, offering experienced guidance on remediation steps and performing retesting to ensure that the issue was fixed. Based on customer feedback, ESG assumed that 80% of critical remediation and retesting was complete before the end of the Cobalt engagement, and that the remaining 20% of vulnerabilities were of lower severity and could quickly and easily be remediated and retested on their own following the engagement.

In contrast, remediation did not start for the traditional pentesting service until 28 days later, at the end of the engagement. At this time, many organizations would feed the reports into a ticketing system for triage and would need to further interpret and research the results, spending even longer to get started (sometimes as long as a month). Our model conservatively assumed that customers started triage and remediation of vulnerabilities right away and took only 20 days to remediate the most critical ones. At this time, they would then re-engage the pentesting service at a cost to perform a secondary engagement to retest only the known severe vulnerabilities. ESG assumed that this engagement would take only 3 days and that no additional critical vulnerabilities would be reported.

Our models predicted that Cobalt's PtaaS model provides a 93% faster time to identification of the first vulnerability and a 66% faster time to remediation of critical vulnerabilities, meaning that the service was exposed to vulnerabilities for a total of 34 fewer days per engagement. Our results are shown in Figure 3.

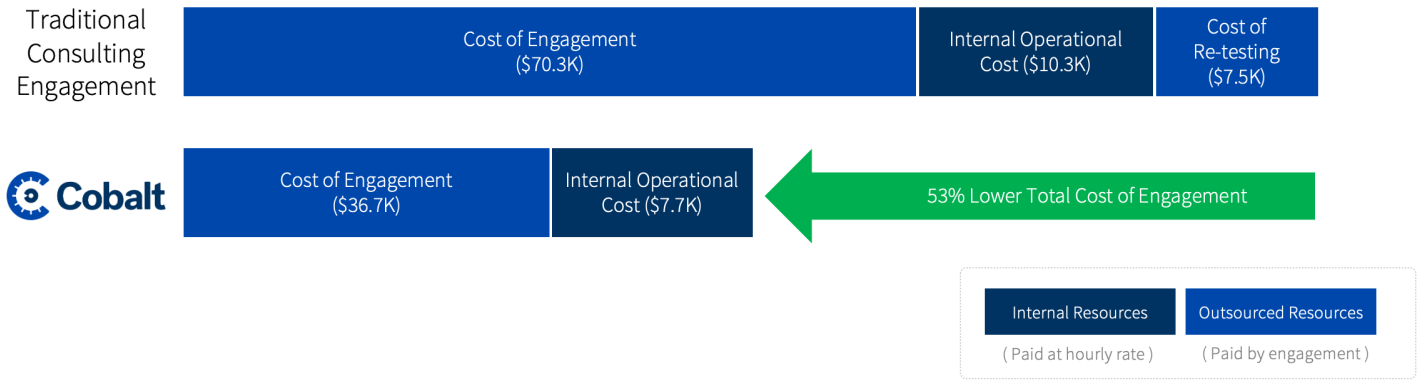
Figure 3. Cobalt Provides Faster Pentesting Engagement and Remediation of Critical Vulnerabilities



Source: ESG, a division of TechTarget, Inc.

Next, ESG calculated the total expected cost of engagement and the expected internal operational costs required to support pentesting and remediation. Our analysis shows that Cobalt's PtaaS model resulted in a 53% lower cost when compared to a traditional consulting engagement, based mainly on the reduced time required. It should be noted that, unlike traditional testing, if faster engagements are required, Cobalt can provide additional resources (even working weekends and around the clock) to meet testing deadlines. Internal operational costs were expected to be lower with Cobalt based on the advantages of a dedicated project manager, built-in capabilities of the application, two-way communication with testers, prioritization and visualization of vulnerabilities, and added guidance during remediation. These resulted in a total expected internal operational cost that was 25% lower. Figure 4 summarizes our findings on the total cost of engagement and remediation.

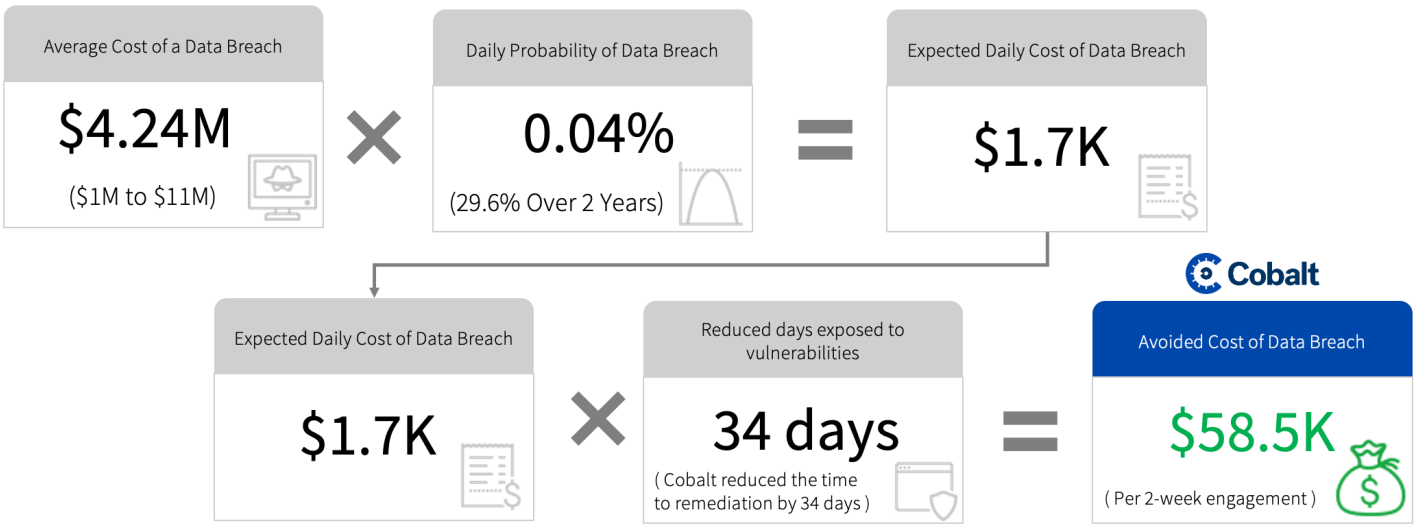
Figure 4. Cobalt Provides Lower Total Cost of Engagement and Remediation of Critical Vulnerabilities



Source: ESG, a division of TechTarget, Inc.

The Ponemon Institute reports that the average cost per data breach is $4.24M per attack worldwide[3] (this is as high as $9M for North America). Further, the probability of a data breach occurring over a two-year period has been reported at 29.6%,[4] resulting in a 0.04% average daily probability of a successful data attack. Since we previously predicted that Cobalt's PtaaS model reduces the average time exposed to vulnerabilities by 34 days when compared to a traditional consulting engagement, the result is an avoided risk cost of $58.5K per pentesting engagement (see Figure 5).

Figure 5. Expected Avoided Cost of Data Breach Due to Earlier Remediation of Critical Issues



Source: ESG, a division of TechTarget, Inc.

Using the expected savings (cost of engagement and internal operational costs) and benefits (risk avoidance) provided over traditional pentesting services, ESG calculated a **176% expected return on investment** per PtaaS engagement with Cobalt.

Issues to Consider

While ESG's models are built in good faith upon conservative, credible, and validated assumptions, no single modeled scenario will ever represent every potential environment or engagement. The benefits and risk avoidance provided by Cobalt could possibly be higher for some organizations engaging in more frequent retesting or with a larger potential risk

[3] Source: IBM, *How much does a data breach cost?*
[4] Source: UpGuard, *What is the Cost of a Data Breach in 2022?*

profile or stricter compliance regulations. In addition, the faster time of engagements and remediation provided by Cobalt could result in businesses being able to engage in opportunities that they otherwise could not have met the testing timelines for. ESG recommends that you perform your own analysis of your pentesting requirements and consult with your Cobalt representative to understand and discuss the differences between the solutions proven through your own proof-of-concept testing.

The Bigger Truth

Enforcement of comprehensive security testing practices and acceleration of agile development efforts are, by nature, conflicting initiatives but are equally critical to the success of modern businesses. Many organizations struggle to deliver continuous features and value to customers while keeping the applications secure from attack. Security often is bolted on because it takes too long to find and fix vulnerabilities using traditional pentesting methods. Traditional pentests can take up to a month to complete, and an organization is left the job of triage and remediation. After that, many consultants require a new SOW for retesting an application.

ESG validated that Cobalt's PtaaS model is built with modern development in mind. Cobalt's testing fits into an agile development environment and doesn't slow things down. Customers reported that their engagements with Cobalt started only 48 hours after signing the contract. The testing was complete in 10-14 days, with a majority of remediation and retesting completed during the engagement. Customers found the Cobalt Core Pentesters easy to work with, knowledgeable, and professional. Pentesters become an extension of the development team, openly collaborating through the application and dedicated Slack channels.

ESG found that Cobalt's PtaaS model will benefit organizations in three ways. First, it gives organizations results faster and in real time. Second, it reduces an organization's need to spend expensive internal resources to manage the pentest engagement. Third, Cobalt finds and fixes vulnerabilities more quickly, reducing the risk of exposure. Our models show a 93% reduction in time to first result and a 66% reduction in risk exposure due to the speed with which remediation can begin. Customers reported that 80% or more of remediation and retesting was completed by the end of the engagement. When considering the average cost of a data breach, our conservative models predict a $58K savings in avoided cost of a data breach per two-week engagement with Cobalt. If your organization is looking to reduce risk without slowing delivery down, ESG recommends that you give Cobalt's PtaaS model serious consideration.