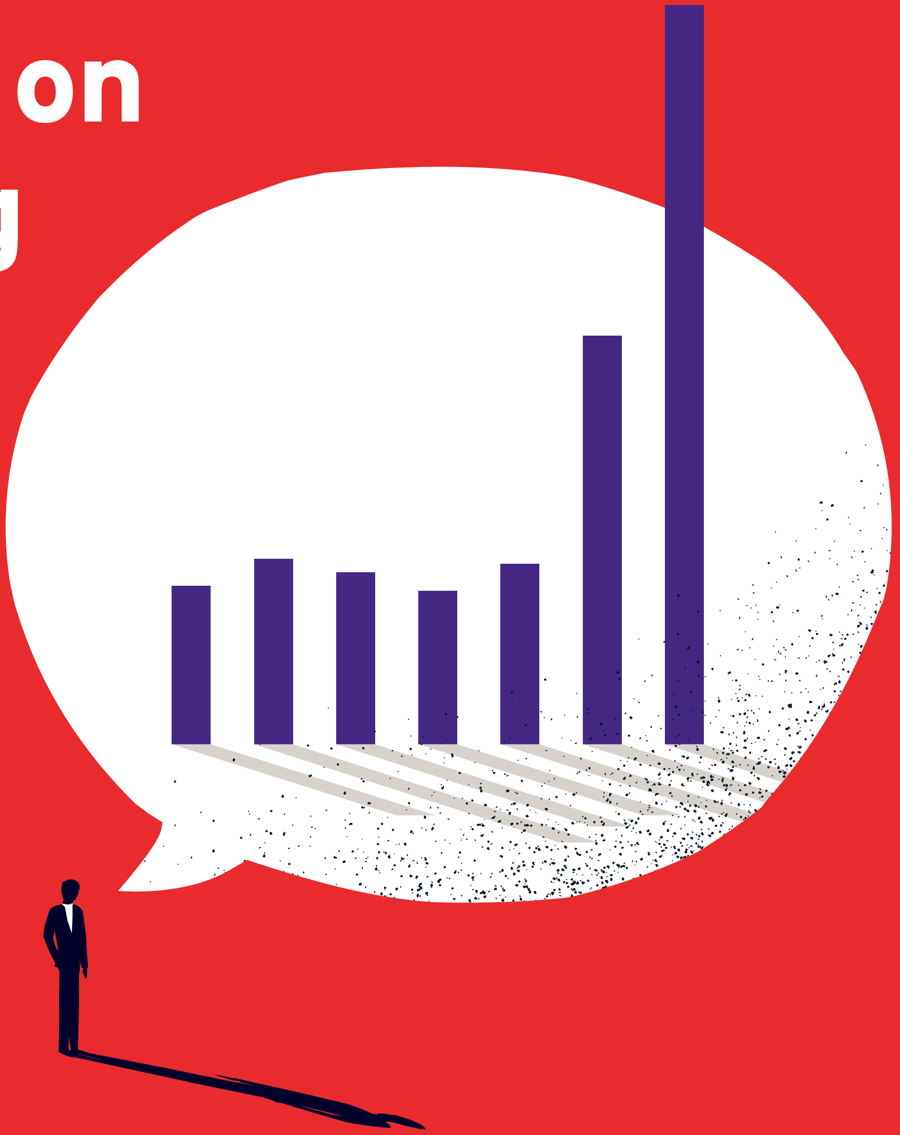
PLEXTRAC EBOOK

Selling Your Boss on Pentest Reporting Automation

A Practitioner's Guide to Making a Winning Business Case at Your Service Provider



PlexTrac®

Contents

The role of a **penetration tester at a security service provider** goes beyond conducting security assessments. It is equally important to effectively communicate the results of these assessments to clients in a thorough penetration test report. Although typically not the favorite task of a skilled tester, creating a quality report and effectively communicating results to the client are the payload of your work. The report is the concrete deliverable your client is paying for and relying upon to improve their security posture … but does getting there have to be so painful?

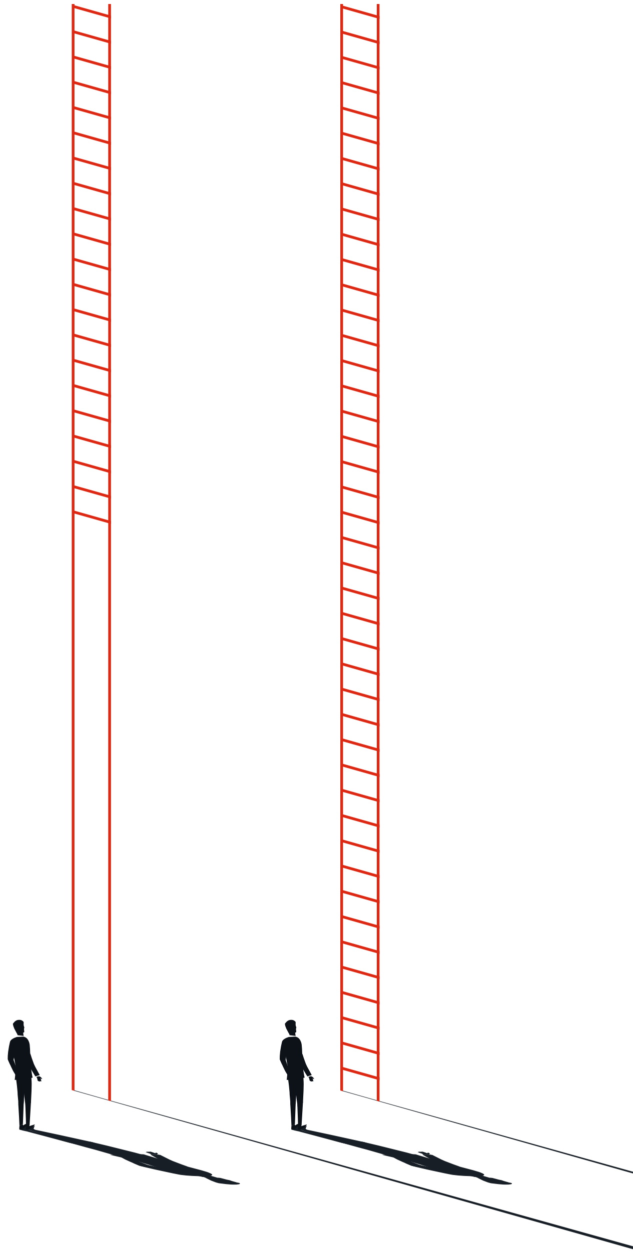
You've likely experienced late nights after finishing an engagement triaging data, copy and pasting bits and pieces of content from past reports, searching for or recreating artifacts, and formatting — so much formatting. When you are done, the tome you have created is quite impressive but you're pretty sure the client won't even read most of it, let alone actually fix the issues you've uncovered.

Since most pentesters are not trained communicators or graphic designers, time spent writing up and applying templates to the culminated data from your exploits is typically more time consuming than necessary — if not painfully inefficient. What if there was a better way? Pentest reporting automation is the solution to take the repetitive and menial work out of this critical task. The less time you spend preparing the report, the more time available to do what you are really good at — hacking.

> **"Our big problem was time. As a professional services organization, everything is centered around billable hours."**
>
> *JT Gaietto, Chief Security Officer, Digital Silence*

But practice managers, owners, and other leadership in a security service provider have different concerns than the individual tester. They are responsible not only for the report, but also how the report drives value for the client and, ultimately, ensures the organization is profitable and growing. In a service-based industry, profit margins are everything, and managers are faced with many choices on how to deploy their often very tight budgets.

Not only does a pentester have a responsibility to conduct assessments and communicate results to clients, they should also contribute to the success of the organization as a whole by expressing the value of their work and solutions for improving it to internal stakeholders and decision-makers. Pentest reporting automation can add value to the individual tester making them more efficient and effective, but it can also provide tremendous value to the team and the organization by allowing for increased testing capacity and higher quality deliverables.



Win, win! Right?

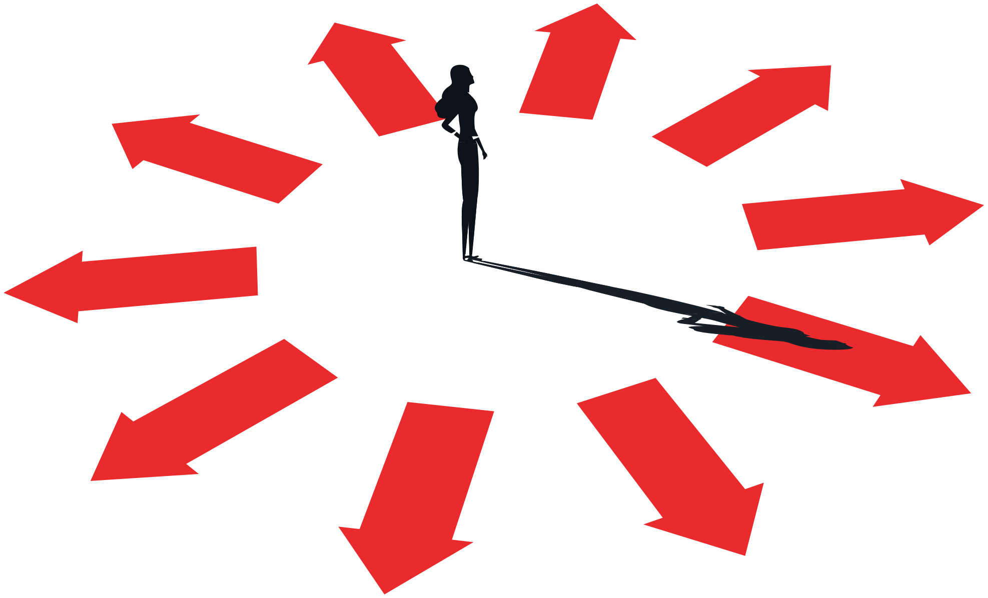
But how do you assess how much value reporting automation is actually adding? How do you evaluate a solution from both the practitioner and the business perspectives? And how do you speak to the greater business concerns of those with purchasing power and many competing budgetary demands? The following ebook details five steps to successfully pitching a reporting automation solution to your leadership.

1. **Articulate the problem** — Consider the pain points in the pentesting and reporting life cycle and identify where an automation solution can help.

2. **Understand management's priorities** — Align the benefits of reporting automation with the business objectives of the organization.
3. **Research your chosen solution** — Use criteria relevant to your organization to make a case for the solution you'd like to pitch.
4. **Gather the data to support your pitch** — Calculate the business benefits and potential ROI possible with pentest reporting automation.
5. **Make your pitch** — Communicate your proposal with confidence that you are serving the goals of your organization.

Armed with the right approach, a clear understanding of the business value, and the arguments and data to back you up, you'll make adopting pentest reporting automation an easy choice for your organization. Read on for step-by-step information for preparing your pitch — we want to make it easy for you, too.

Now that's a win, win, win!



STEP 1 Articulate the Pain Points in the Pentesting and Reporting Workflow

The first step to making a strong case for reporting automation is to clearly understand and quantify the inefficiencies and issues in your workflow and those of the larger team. Chances are, if you spend an excessive amount of time on tasks that are more administrative than specialized, others are doing the same. Inefficiencies and manual, tedious work performed by highly skilled professionals are a business liability as well as an individual annoyance. Assessing these pain points and their severity is a good foundation on which to build a case for automation and workflow management solutions.

Some area that are common time sucks in the pentesting workflow ripe for automation include

- **Managing automated and manual data produced in the testing process** – Pentesters use a number of essential tools to find low hanging fruit and scope their projects, in addition to manually testing security vectors. Capturing and aggregating the data needed to inform the report produced from these efforts and from disparate sources can be unnecessarily challenging and is typically inefficient.

- **Collaborating and editing content consistently** – Achieving quality and consistency across a team of pentesters, and perhaps technical editors or QA support staff, is another common pain point. Many teams manage these processes using software ill designed for collaboration, let alone the specific data and relationships in the cybersecurity workflow.

- **Building the report itself to the organization’s specifications** – Even after the testing is done and the content has been triaged, testers can spend a significant amount of time building out the report in the required template of their organization and the requirements of the project or client. Changing customer information, locating boilerplate elements, and adjusting styles are tedious tasks solvable with automation.

These pain points of the pentesting practitioner may not be of great concern to a practice manager on the surface. However, when inefficiency and ineffective processes cost enough in lost time for highly paid practitioners and reduced quality in deliverables to clients, they become extremely relevant to the business as a whole. Documenting not only bottlenecks and time sucks that annoy pentesters, but also critically examining how much time is spent on them and places where quality is sacrificed for speed – to meet an SLA deadline, for example – will provide a strong basis to measure potential business ROI.

> **“With PlexTrac we have definitely seen our reporting time drop significantly. We used to measure it in days, and now we measure in hours.”**
>
> *Director of Offensive Security, Security Vendor in Vermont*

STEP 2 Examine the Business Priorities for Adopting New Technology Solutions

So what are the priorities of the manager and the broader organization? And how can reporting automation serve those priorities as well as relieve practitioner pain points?

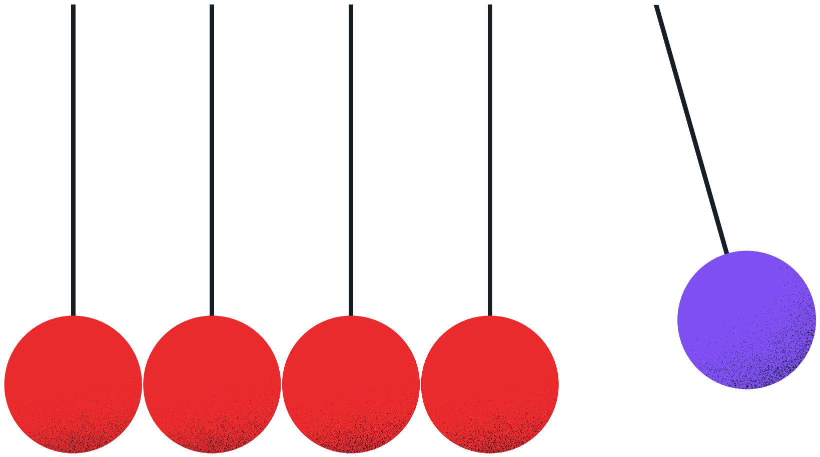
Once you've articulated the areas for improvement and assessed the costs of not addressing them in time and quality, the next step is relating them to the priorities of the practice manager and the goals of the organization as a whole. While adopting all the latest tech as soon as it comes out would be amazing, managers have budgetary and change management constraints to consider. They have to weigh the value add of a given solution against other technology requests, needs, and desires. They have to prudently build a tech stack that properly resources the team while maintaining profit margins.

Manager priorities to consider when presenting a reporting solution include

1. **Value**
2. **Integration**
3. **Scalability**
4. **Personnel**
5. **Customer Satisfaction**

Value

The top concern any manager has to take into account with any change or addition is the cost to benefit ratio. It isn't just about the price but also if the price is justified. Managers understand that tools and people are absolutely necessary to operations, but how many and which ones are important questions. In tight economic times, especially, any purchase must enhance the overall profitability of the team to be considered.



Integration

Managers are also interested in how a new product will fit into the existing ecosystem. What will onboarding and training look like? How much maintenance will it take? They will want to know if the solution solves problems at one point in the process or at many, and if it will be useful for the full team or just a few specific roles.

Scalability

Another purchasing consideration is scalability: Can a solution grow with the organization over time? Or more so, can a solution help the business itself scale? Products, like personnel, can be a long-term commitment. A manager will want to know that solutions will add value over time, not become obsolete or burdensome. When a product introduces efficiencies that allow the business to take on more work or provide new services, a manager will be truly interested.

Personnel

In a service-based industry like cybersecurity, people are the most important asset of an organization, and they are also the most expensive. Managers are always interested in opportunities to help their people be more productive, the team to be more collaborative, and the results produced more valuable to the client. If a tool or service can help with these personnel goals in a significant way, it will be well worth considering. Managers are also interested in retaining talent, so if a solution will boost morale and relieve pain points, it's a bonus.

Customer Satisfaction

Finally, managers will want to know not only if a solution will solve internal issues, but also if it can improve the deliverable in a way that will positively impact clients directly or indirectly. If the clients will derive more value from existing offerings or, even better, engage in services more often or in new ways, it will make a powerful argument in favor of purchasing a solution.

Orienting a proposal for a reporting automation solution to the larger concerns of the business will increase likelihood of acceptance. Successfully pitching to a manager in a security service provider, like in any business, requires adopting their viewpoint of the business as a whole.

> **"We offer clients free access to the PlexTrac client facing portal if they subscribe to a recurring service so it's generated more revenue and stickier clients because the instant access to information is so valuable to clients."**
>
> *Billy Steeghs, CISO & Director of Consulting Operations, OnDefend*

STEP 3 Research Your Chosen Solution Using Relevant Criteria

Tailoring a proposal for a pentest reporting automation solution should include doing the appropriate research. You may have experience with a particular product from a previous role or heard an impressive pitch from a vendor at a conference, but your manager will want more than your personal experience to recommend the product. Do the work to collect data about your chosen product including a wide set of criteria to show that the solution is a strong fit, and you will decrease decision time exponentially.

Rank criteria for evaluating your chosen solution first around your team's specific pain points and your manager's concerns. After that research key information about the product itself and the company producing the solution. Use the following checklists of relevant questions to guide your information gathering.

Product Criteria

Of course, evaluating a product should involve understanding the features and benefits it offers. But when researching a pentest reporting solution to pitch to a manager, be sure to evaluate the functionality with their primary objectives in mind: grow revenue, scale service offerings, increase client satisfaction and retention.

Product Checklist

- □ Where does the product fit in the workflow?
- □ What features does it offer (i.e. integrations, templating, QA collaboration, reusable content)?
- □ Is it customizable?
- □ How is it deployed (cloud, on-premise)?
- □ Can it work with and complement your existing tech stack?
- □ Can customers interact with it (i.e. a client portal)?
- □ What are the report outputs available?
- □ Can it support or improve your existing templates?
- □ What does the interface look like?
- □ Does it offer functionality beyond reporting?

Company Criteria

Understanding the company that creates a solution can help provide information about how robust it is, long-term viability, and if it will be scalable. For example, if you are looking at an open source product, it will be cheap but will not likely have support or a product roadmap for growth. Companies that have been around a while or startups with funding are good bets for scalability as they are actively investing in ongoing updates to the product. Understanding the company probably isn't your manager's first concern, but it can definitely help measure potential value and long term viability, and justify pricing.

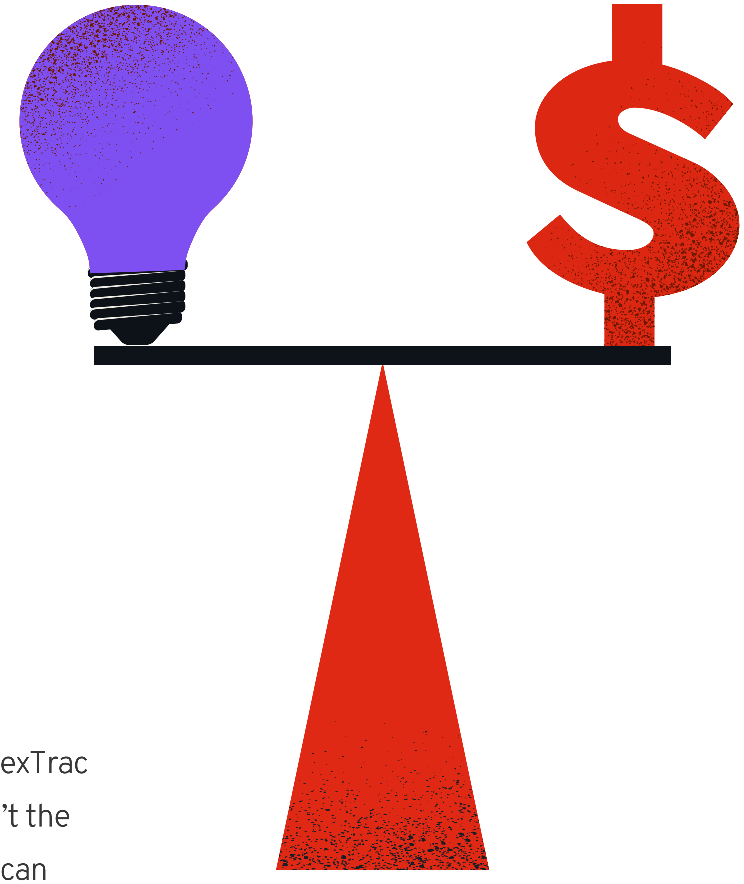
Company Checklist

- □ How old is the company?
- □ Where are they in their growth? Are they funded?
- □ Who are some of their customers?
  Do organizations like yours use the product?
- □ How many employees do they have?
- □ What is their customer support like?
- □ Do they release updates regularly?
- □ How robust is their product documentation?
- □ How do they handle security issues?
- □ Are they interactive with their customers after the purchase?
- □ Do they have a product roadmap that complements your goals?

> **"The industry is constantly changing and evolving. The PlexTrac Customer Success team has been a real value add for us because they are so responsive to our ideas and feedback on the product. Having a partner in PlexTrac that can run as fast as the industry is a real game changer for us."**
>
> *JT Gaietto, Chief Security Officer, Digital Silence*

STEP 4 Calculate the Potential Financial Benefits

Once the problem is fully assessed, managers' priorities considered, and your preferred solution assessed against relevant criteria, it's time to get to the most persuasive argument — potential return on investment (ROI). Managers of security service providers need to know that an automated pentest solution will do more than make the pentesters happy; it must add significant value to the organization as a whole, particularly providing benefit to the bottom line.



The best pentest reporting automation solution can and should increase service margins by significantly driving efficiency, scale revenue opportunities with existing resources, and produce better client outcomes with more actionable findings. Present the following areas to your manager as ripe for significant direct and indirect ROI.

Drive Efficiency to Increase Service Margins

Reporting automation most obviously brings ROI in time savings. For example, PlexTrac can reduce time spent reporting by fifty percent or more. But just saving time isn't the full ROI story with efficiency. It is also important to consider how that saved time can be reallocated to conduct more engagements. This is the real value to the manager, the potential for larger service margins.

To illustrate the value in concrete terms, consider the following scenario:

- We have 10 pentesters on the team at our security service provider
- We complete an average of 30 annual pentests per pentester (approximately 600 total)
- Creating each report takes around 20 hours to complete
- The average salary of a pentester is $150,000
- We charge clients around $10,000 per new engagement/pentest

Apply a 50 percent time saving on report creation per engagement with PlexTrac to double your revenue potential.

COMPARISON	without PlexTrac	with PlexTrac
Est # of Total Pentests Per Year	**300**	**600**
Hours Per Report	20	10
Total Hours Spent on Report Creation	6,000	6,000
Revenue	$3,000,000	$6,000,000
Labor Cost	$1,500,000	$1,500,000
Profit	$1,500,000	$4,500,000
Gross Margin %	**50%**	**75%**

Try the Live Calculator

> “Deploying PlexTrac allowed our team to cut the reporting cycle by sixty five percent.”
>
> *— Matthew Puckett, Vulnerability Management Team Lead, Jacobs Engineering*

> “Overall, we’ve seen at least a 50 percent time saving on our reporting processes.”
>
> *— JT Gaietto, Chief Security Officer, Digital Silence*

Increase Revenue with New Value-added Proactive Security Services

Ultimately, significant time saving from automation can be reallocated to complete more and deeper work with the existing team. Your business has the opportunity to serve more clients based on additional testing capacity without increasing headcount. The pentest automation solution becomes a force multiplier.

But not only are testers freed up to perform more engagements, the organization can open up new revenue streams with specialized services to upsell to existing clients and attract new ones. Those services could include targeted testing around specific attack vectors or threat intelligence, for example, or purple teaming and tabletop exercises. Or the practice can advise clients and offer framework-based assessments tailored to OWASP Top 10, NIST, or other specific areas of concern for customers. The greatest potential of automation isn't about the pentesting itself but the opportunity to sell more services to more clients without adding more team members or resources.

> **"With PlexTrac, we've increased the efficiency and consistency of our report writing process. Our engineers are relieved of some tedious and repeated tasks so they can spend more time interacting with and bringing value to the client, all while maintaining a leaner team."**
>
> *Brandon Potter, Chief Technology Officer, Procircular*

Become a Trusted Partner by Delivering More Value

Finally, consider the ROI potential of pentest reporting automation in client satisfaction and potential for business growth. Consistently meeting service level agreement requirements due to improved efficiency and effectiveness is just the beginning. The real value of automation comes in delivering measurable results to clients and the potential that creates for new and consistent revenue streams.

Reporting automation value adds for the client include

1. **Better quality and consistency in the report they receive**
2. **Findings delivered in a more dynamic and actionable form**
3. **Insights that more clearly guide risk prioritization and remediation**
4. **Enablement of continuous testing and validation strategy**
5. **Progress metrics to attest to leadership**

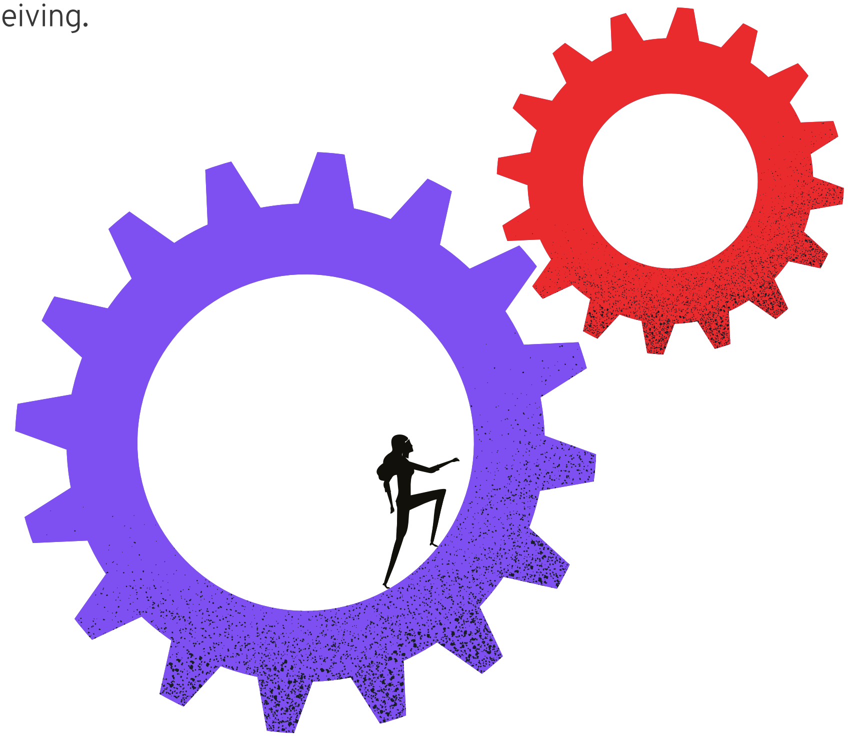
When a client begins making measurable improvement to their security posture due to the quality and actionability of your recommendations — made possible by your automation solution — your organization will become an essential part of that client's larger security strategy. Developing long-term and deep relationships with clients as a strategic advisor ensures consistent, recurring revenue sources with added potential through service expansion.

Providing more actionable insights in the form of dynamic delivery of findings, prioritizing those findings according to frameworks like OWASP Top 10 or NIST, and reducing clients' mean time to remediation (MTTR) will create an opportunity for continuous service delivery.

> "We were looking for a way to streamline and expedite our own reporting process while also giving our clients a better reporting product and new way to interact with our findings and recommendations. We found that in PlexTrac."
>
> *Will Keppler, Security Specialist, CyZen*

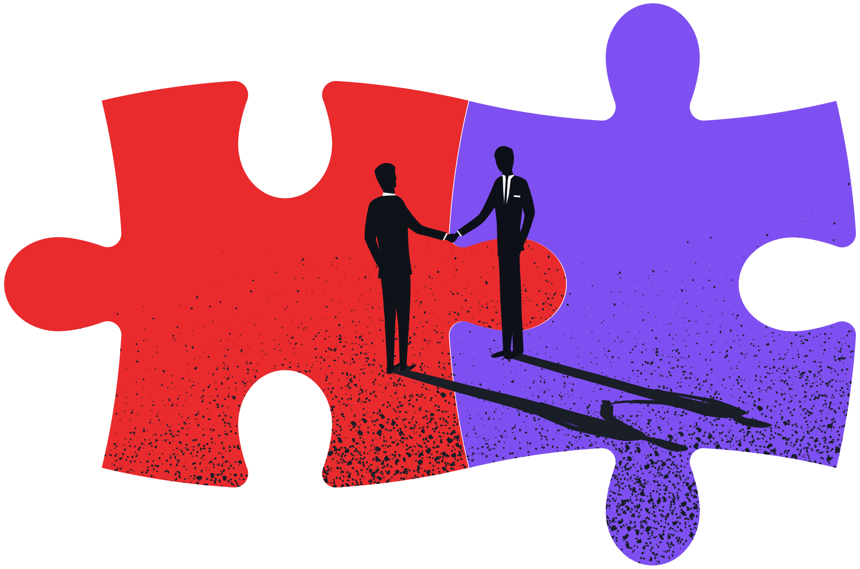
Pentest reporting automation not only enables a continuous assessment strategy, but also a way to continuously validate and demonstrate progress of those efforts well beyond the internal team manager. Your organization can become a trusted partner by enabling and demonstrating your contributions to clients' improved security posture, relative to the concerns of their C-suite.

Your manager wants to know their technology and partnerships provide good business value and so do your clients' managers. A pentest reporting automation solution can accomplish both: delivering business value to your practice and helping better demonstrate to clients the value of the service they are receiving.



STEP 5 Communicate to Your Manager and Overcome Objections

Armed with a concrete ROI estimate, case studies and testimonials, and clear rationale for the product you are recommending, it's time to make the pitch. Whether formally or informally, you must present your case. Effective proposals are clear, compelling, direct, and time-oriented. They also anticipate objections and address them in advance. Possible objections to adopting a pentest reporting solution may include



1. **Limited resources** — This isn't just an excuse; managers never have sufficient resources to have all the tools they would like. Overcoming this objection comes down to demonstrating potential ROI, cost savings, and new growth opportunities. It also requires appropriate timing of the request, persistence, and patience.

2. **Product capabilities** — A manager may question if a product is worth the investment based on its functionality or fit in the ecosystem. No solution is perfect, but once you've found a product that ticks the majority of boxes, highlight a strong product roadmap and responsive customer success team. An open API adds flexibility as well.

3. **Maintenance requirements** – Evaluating the resources required to use, maintain, and derive full value from a product is certainly a valid consideration. To overcome this potential objection, a proof of concept to understand the product in your environment may be necessary or simply a conversation with a product sales engineer to get questions answered. Choosing a commercial, off-the-shelf product rather than an open-source or custom-built solution will typically mean fewer resource requirements to keep it functioning well.

> "One of our challenges was not having a centralized tool to capture results and create consistent reporting to manage our growth. Now [with PlexTrac] we aren't constrained by our tooling but rather empowered by it."
>
> *Jeremy Pierson, Secure Enterprise Program Architect, CompuNet*

Scale Up Your Offensive Security Practice with PlexTrac

PlexTrac offers a robust automation platform for pentest reporting and collaboration to serve the needs of the pentester and the offensive security practice as a whole. PlexTrac streamlines planning, reporting, and findings delivery so security service providers can scale revenue while delivering premium value and diversifying their offerings to their clients.

Request a personalized product demonstration with a PlexTrac expert who will help you calculate the potential business value for your organization and use cases.

PLEXTRAC.COM/DEMO

PlexTrac is the premier penetration test reporting, collaboration, and management platform designed to automate planning, documentation, communication, and remediation tracking, allowing service providers to enhance margins and client outcomes and enterprises to demonstrate the value of internal pentesting efforts and improved security posture.

www.plextrac.com

PlexTrac®