PLEXTRAC EBOOK

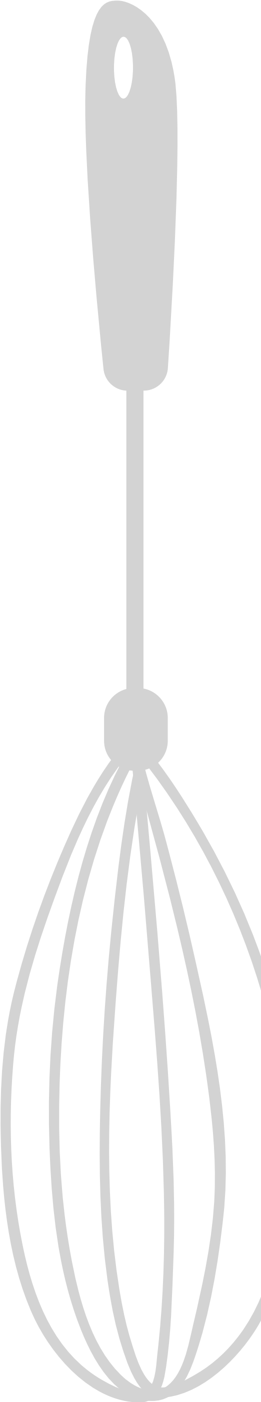
How to Select a Pentest Management and Reporting Automation Tool

The recipe for success

PlexTrac®

The Recipe for Success: How to Select a Pentest Management and Reporting Automation Tool

Whether you're a pentester or managing a pentesting/offensive security team, you understand the pain that accompanies pentest reporting. For service providers looking to take on additional clients, the pain might be around speed and quality. Manual pentest reports can take, on average, 35 – 50% of the overall assessment time. Trying to custom-tailor reports to meet the specific needs of individual clients can add to that time suck.



For enterprise security teams, pentest reporting pains might look a little different. Speed will likely still come into play to ensure that vulnerabilities are remediated in a timely manner. However, the handoff from offensive security teams to development teams and the ability to continuously validate and retest findings might be of greater concern.

So how do you properly address these pain points?

Well, if you're reading this guide, you've likely already established that an automated pentesting management and reporting solution is vital. But how do you know what platform to pick?

We've cooked up some tips to help you compare platforms.

Bon Appétit

Table of Contents

Pieces of the Pie: What to Look For When Comparing Platforms

10 must-have ingredients:

Aggregates data from multiple sources:

Manually managing information from disparate sources is time-consuming and can lead to missed detail or errors. Look for a reporting automation platform that serves as a central location to easily upload results from all standard pentesting tools and analyze the raw data files.

Offers a reusable content repository:

Technical snippets are a critical component of the report writeup and findings analysis. However, they often are repetitive as similar findings come up in many different engagements. A reporting automation solution that includes a powerful content management module can transform the quality and consistency of finding writeups. It enables you to store QAed writeups in organized repositories directly in the reporting platform for single-click, permission-based access. Being able to archive and reuse other forms of content, like bios, boilerplates, etc., is also important.

Captures artifacts:

A quality report includes visual evidence that supports the findings and recommendations, like screenshots, code snippets, photos, or even video artifacts. Look for a reporting automation solution that facilitates the capture and storage of all the artifacts and evidence needed for the final report.

Facilitates collaboration and QA processes:

Many inefficiencies in the report creation process happen during collaboration. An effective pentest reporting automation platform should facilitate collaboration and QA processes to save time and improve the final product. Commenting and change tracking in the same place where reusable content is housed and the report is produced greatly reduces context shifting and version-control issues.

Formats report templates:

The ability to create the template once and automate the inclusion of content and formatting is a game changer for ensuring quality and consistency with every deliverable. Whether you need a fully customized template to represent your service provider's unique perspective or are seeking multiple standardized templates for different types of security reports, look for a reporting automation platform that will keep branding and content consistent with company standards every time — with much less effort for everyone involved.

Supports secure dynamic findings delivery:

It's essential to find a pentest reporting automation platform that enables you to scale an engagement and a report without expending more resources. A reporting automation platform that can support secure dynamic findings delivery gives clients or internal stakeholders access to in-depth information — and even raw data findings — without making the report cumbersome or unreadable.

Ensures secure delivery of reports:

A reporting automation platform with a permission-based portal ensures simple secure delivery of the report along with more efficient communication throughout the engagement. It also enables you to communicate scoping questionnaires, provide results throughout the engagement, and deliver the final recommendations securely — all without added tools, steps, or processes.

Creates actionable insights:

Completing annual testing and finding the same issues engagement after engagement, for example, is frustrating for testers. Look for a platform that supports dynamic findings delivery. When all stakeholders use a reporting automation platform, recommendations can be immediately turned into remediation tickets and assigned and tracked.

Promotes stakeholder differentiation:

To truly be effective, a pentest report must communicate to several different stakeholders. Look for a reporting automation platform that makes the differentiation of content for various stakeholders more of a science.

For example, the platform should offer reusable standard narrative content, the ability to create analytics and data visualizations, and access to raw data and all the findings via a portal.

Passes the customer vibe check:

When comparing pentest reporting automation platforms, be sure to ask for customer references. Hearing or reading testimonials from existing customers can help you determine if the platform has the necessary features to meet your needs.

Prosciutto or Pepperoni? Identifying the Differences Between PlexTrac and Its Competitors

We gave you a list of the basic “must have” ingredients for a pentest management and reporting platform, but it’s important to dive a bit deeper into specific pros and cons of competitor platforms versus the PlexTrac platform.

You will find that although some competitor platforms seemingly have the right mix of ingredients, they may lack the depth and breadth of PlexTrac. In other words, a competitor platform might have all of the ingredients needed to make a basic pizza dough, but PlexTrac has higher-quality ingredients and more toppings for the pizza.

Feature	Competitor	PlexTrac
Large array of integrations (including vulnerability scanners, adversary emulation tools, automated pentesting tools, bug bounty tools, and ticketing systems)	★ Most competitors only offer a handful of integrations (less than 10), largely comprised of vulnerability scanners or ticketing systems.	★★★ PlexTrac offers close to 30 integrations, enabling you to easily aggregate data from multiple sources and feed remediation needs to your preferred ticketing system. PlexTrac also has an open API to aggregate data from key sources and provide a complete view of activity and progress.

Feature	Competitor	PlexTrac
Customizable Jira field mapping (for remediation workflows)	★ When evaluating a competitor, ask what data is needed to support the existing remediation workflow and how it needs to flow back and forth. You'll likely find that they're lacking the necessary fields to support existing remediation workflows without process disruption.	★★★ PlexTrac makes the process of remediation tracking seamless with Jira. The integration is customizable and won't require time-consuming changes to your existing workflow.
Commenting and change tracking (to support peer review workflows)	★ Many competitor platforms make QA a challenge or lack this functionality entirely. Not having the ability to leave comments referencing specific text or track changes within your findings and narratives may require you to execute this process outside of the platform experience.	★★★ With PlexTrac, comments clearly highlight the text they are referencing and change tracking allows for multiple review levels to take place, streamlining and driving collaboration in the QA process.
Report formatting (Out-of-the-box templates and low-code customization options)	★★ You want your reports to be easily customizable to fit your stakeholders' requirements. Unfortunately, some competitors make customization a challenge by requiring extensive coding or significant upcharges for report tailoring.	★★ PlexTrac helps you deliver customized reports at scale without coding knowledge. Choose from multiple pre-built export templates, update colors, fonts, etc. using our in-app style guides feature, and set custom findings layouts per report.

Feature	Competitor	PlexTrac
Report delivery (sending the report to your stakeholder)	⯨ Most competitors do not offer a solution for the report handoff process. They assume that you will print or email a PDF or Word document. While this might satisfy a pentest shop strictly focused on cranking out reports, it won’t develop a more strategic partnership with the client the way a portal can. And for enterprise teams, a poor handoff can increase MTTR.	★★★ PlexTrac aims to solve for the report handoff by offering a client portal that can be shared with your internal or external stakeholders. If your stakeholders are internal security folks, you can send the findings from the report to ticketing systems. If your stakeholders are external clients, you can share historical data via the portal and build a case for a continuous assessment strategy.
Custom questionnaires	★ The majority of competitors offer pre-built scoping questionnaires that cannot be customized.	★★★ PlexTrac offers fully customizable questionnaires that can be used as pentest scoping questionnaires, framework-based assessments, onboarding checklists, etc., to support multiple use cases while keeping sensitive data secure.

Feature	Competitor	PlexTrac
Narratives library	⯪ Competitors often lack the ability to save individual narratives sections into a library to pull into your report.	★★★ Write and save as many custom narratives sections as you would like to your library. Pull and customize these individual sections into your final report.
Findings writeups	★ Many competitors offer findings writeups, but not nearly as many as PlexTrac. Searching for or manually creating a CWE, CVE, and KEV writeup is tedious and error prone. Incomplete writeups can result in missed remediation steps or, worse, threat recurrence.	★★★ We offer the industry's largest repository of findings writeups (over 25,000 CWEs, CVEs, and CISA KEVs) enabling you to enrich findings with guidance on vulnerabilities or flaws, the level of exposure, and remediation steps.

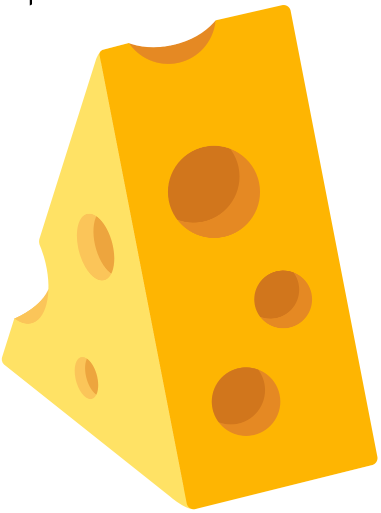
The Big Cheese: Why PlexTrac Is the Premier Platform for Automating Pentest Planning, Reporting, and Delivery

PlexTrac is so much more than a pentest management and reporting automation platform. It supports all of the front-end use cases related to assessments (both offensive security assessments and pentesting assessments) and integrates with many commonly used vendors to bring in data from your other systems and tools (like Snyk, Qualys, Veracode, etc.) for a single source of truth.

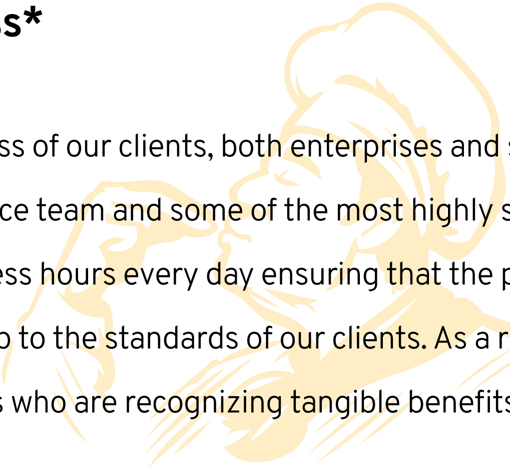
PlexTrac was designed to make your job easier, enabling you to hack more and report less. In the spirit of ease, we offer one of the most extensive content libraries, which enables you to reuse types of findings and even the narrative sections. Findings can be sent to different areas of your organization, or stakeholders' organizations, to address remediation. You can use PlexTrac to track fixes, send tickets via tools like Jira, and leverage the analytics.

Since PlexTrac was designed to meet the needs of both service providers and enterprise teams, labels can be changed in your dashboard to align with your team setup. For example, if you're a service provider, you can label your reports by client. If you're part of an enterprise, you can label your reports by department.

The platform has robust access control, so you can limit who has access to different departments or client reports. Data doesn't carry over between clients or departments. And for added convenience, you can share the report findings with stakeholders using our portal.



PlexTrac is *chef’s kiss*



We are dedicated to the success of our clients, both enterprises and service providers. We have a top-tier customer service team and some of the most highly sought after product developers who spend countless hours every day ensuring that the product addresses current market needs and is up to the standards of our clients. As a result, we have a growing list of loyal customers who are recognizing tangible benefits from PlexTrac.

> **“PlexTrac enables our Proactive Assessment Team with a platform to streamline the assessment reporting process. This helps our services team provide our customers with a better experience by delivering better reports in less time than we could before we had PlexTrac in place.”**
>
> – Evan Peña, Director of Professional Services, Mandiant

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

> **“PlexTrac enables the team to produce higher quality findings to our stakeholders faster. Our internal processes have been changed to take advantage of this capability.”**
>
> –Security Assessment Team Lead, Fortune 100 Apparel Company

“

We had an opportunity to further enhance our reporting, and PlexTrac was the solution to make it possible. PlexTrac helped us standardize our template and automate the report building process, and it has enabled us to produce reports with a few clicks. We create over 60 reports a year, so the savings in time and resources is significant.”

– Alex Boyle, Senior Manager, Offensive Security,
Early Warning

“

PlexTrac has helped me create better pentest reports with greater speed. I love that I can create my own custom database of findings and insert them quickly into any report. My clients appreciate having a Web-based portal to work on findings together. Executives especially like PlexTrac’s ability to measure remediation efforts over time.”

– Brian Johnson, CEO and President, 7 Minute Security

Dig in!

Ready to learn more about PlexTrac?

REQUEST A 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®