

SecureTrust™ Penetration Testing

GAUGE REAL-WORLD EFFECTIVENESS OF YOUR SECURITY POSTURE

Benefits

- Gain the ability to conduct scanning and testing across databases, networks and applications with a single solution.
- Implement a risk-based approach to security to make the most impact with resources.
- Simplify security management with a consolidated portal that lets you access, manage and report on scans and tests conducted across all your assets.
- Augment internal team and resources quickly and easily. We can support your testing and scanning needs to any extent you need.
- Keep pace with business demands and adapt quickly to change while meeting security needs with a flex-spend model that lets you allocate budget and then consume funds as needed.

Defensive controls alone cannot secure your applications or networks. Even highly automated, sophisticated and advanced security tools and technologies are often vulnerable to attacks and are no match for the determination and creativity of the human mind. Penetration testing employs the ingenuity of the human intellect to expose the effectiveness of an organization's security controls in real world situations against skilled hackers. Penetration testing ensures holistic defense against attacks by exploring multiple attack vectors and combining vulnerabilities across different systems.

Through SecureTrust's long-standing relationship with our sister company, Trustwave, we're able to offer industry-leading penetration testing services known as Managed Security Testing (MST). Our penetration testing service puts a Trustwave SpiderLabs® expert on your team. You administer penetration testing projects through Trustwave's award-winning portal putting you in control to make sure testing occurs on your schedule, within your budget and on an on-going basis. Enlist Trustwave SpiderLabs unparalleled application and network penetration testing services on time, on budget and on demand via Trustwave's award-winning portal.

- **On Time.** You enroll your target networks or applications and select testing dates on demand.
- **On Budget.** As a subscription service, you define your annual (or multi-year) testing budget, pay a quarterly subscription fee and utilize your account balance as you see fit.
- **On Going.** Depending on the tier you select, MST consists of one in-depth, manual network or application penetration test and four maintenance tests each year.

Budget and Planning Friendly—Pay as You Go

Within the MST portal you will enroll a target based on tier. Each tier includes a different degree of testing which you will select based on the target network's or application's risk level and any relevant data that traverses or is stored by it. The online tier menu clearly explains the level of the associated testing and its price. Each enrollment deducts from your account balance automatically.

The MST subscription model prevents balloon payments and helps you forecast annual budgets and allocate your spend efficiently without the hassles of multiple contract negotiations.

Mind the Gaps—Quarterly Maintenance

Once you enroll a network segment or application, MST helps you ensure that the target is tested on a regular basis. The time between in-depth penetration tests can result in a window-of-opportunity for cyber criminals. With MST you have the ability to schedule quarterly maintenance tests or validated vulnerability scans to fill the gaps and alert you to vulnerabilities that may have materialized from network architecture changes or updates to an application's code base. MST gives you the ability to not only evaluate an application or network today, but on a continual basis to maintain a secure environment, even as it changes and evolves to meet business demands.

Unmatched Expertise

SecureTrust's penetration testing services are delivered by SpiderLabs — an advanced security team within Trustwave focused on forensics, ethical hacking and application security testing. The team has performed more than 1,500 forensic investigations and thousands of ethical hacking exercises and application security tests globally. Our manual process transcends the generic responses, false positive findings and other limitations of automated application assessment tools.

The SpiderLabs team comprises some of the top information security professionals in the world, with experience ranging from Corporate Information Security and Security Research to Federal and Local Law Enforcement. Members of Trustwave SpiderLabs are regularly invited to speak at security conferences around the world.

Portal-Based, On-Demand Security Testing

- **Schedule Tests with Ease:** Simply enroll your target and select a convenient date and time period for the test to occur.
- **Budget At-A-Glance:** View remaining account balance and purchase history.
- **Centralized Dashboard:** Simplify the management of penetration tests, with at-a-glance views of project and test status and findings.
- **Project and Test Drill Down:** Display the relationship between projects and tests to easily organize enterprise security programs.
- **Detailed Findings:** Evidence including images and videos offers detailed walkthroughs of vulnerabilities. Slideshow presentation views explain security risks to key personnel in the organization.
- **Attack Sequence Reporting:** Graphically displays the relationships between multiple vulnerabilities and simplifies attack scenarios for easy understanding.
- **Real-time Notification:** E-mail alerts are sent instantly when tests change status and findings are identified or remediated.

- **Secure Document Transfer:** Securely share sensitive files such as code, network diagrams, media, etc.
- **Self-managed Accounts:** Create new users and delegate permissions.
- **Data Exposure Charts:** View detailed charts showing what data was exposed during a test.

Powerful Reporting Features

The Trustwave SpiderLabs portal offers a variety of reporting functions to help meet internal reporting, audit, compliance and other needs, including:

- **Online Reporting and Metrics:** Vulnerability data is captured through the portal, including risk, remediation status, data compromised and status across projects or for individual tests. Complete historical access to test results for trend analysis, providing insight into an organization's security posture over time.
- **Preset Reports:** Online reporting includes executive summary, summary recommendations, detailed test methodology and findings. PDF exports are also available.
- **Custom Reporting:** Users can build custom reports in a number of different ways such as by risk, by finding status, across a mix of projects, by custom fields, individual tests and test types.
- **Common Vulnerability Scoring System (CVSSv2) Values for All Vulnerabilities:** CVSS provides a standard method for risk ranking and prioritizing security vulnerabilities to streamline the remediation process..
- **Multi-format Reports:** Export report data in PDF, Excel, XML, CSV and HTML.