Trustwave®

Trustwave Managed Security Testing

PENETRATION TESTING REDEFINED

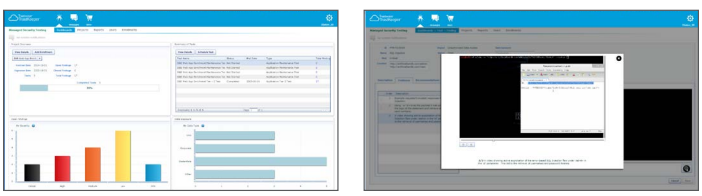
Enlist Trustwave SpiderLabs unparalleled application and network penetration testing services on time, on budget and on demand via Trustwave's award-winning portal.

Gauge Real-World Effectiveness of Your Security Posture

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.

Trustwave Managed Security Testing (MST) 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.

- **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.



Centralized Dashboard and Video Evidence Reporting

Budget and Planning Friendly—Pay As You Go

Within the Trustwave 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 Trustwave 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, Trustwave MST ensures 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. Quarterly maintenance tests fill the gaps and alert you to vulnerabilities that may have materialized from network architecture changes or updates to an application's code base. Trustwave MST not only evaluates 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

Trustwave'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.
- **Web Application Firewall (WAF) Virtual Patches:** Virtual patches custom-built by SpiderLabs block attacks immediately.
- **Data Exposure Charts:** View detailed charts showing what data was exposed during a test.

Network testing may include:

Local Network Segment	Enterprise Infrastructure
VLAN Hopping	Active Directory/LDAP
ARP Cache Poisoning	Source code repositories
Insecure network protocols	Infrastructure Services
Man in the Middle (MITM)	Databases
Network Infrastructure	Mainframes
Routers/Switches/Load Balancers	Middleware
Remote Network Access Devices	SSO
Common Services	Remote Administration
HTTP	Backup
SMTP	File sharing
POP/IMAP	Access Control
FTP	Operating System
Simple Website	OS-Specific Services
XSS	Advanced Tactical
SQL Injection	Non-IP Protocols
Known Command Injection	Multistage Attack Vectors

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.
- **Pre-set 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.

Application testing may include:

Authentication and Authorization	Cryptography
Unlimited Login Attempts	Weak Algorithms
Authentication Bypass	Poor Key Management
Authorization Bypass	Logic Flaws
Default / Weak Passwords	Abuse of Functionality
Session Management	Workflow Bypass
Session Identifier Prediction	Data Protection
Session Hijacking	Transport
Session Replay	Storage
Session Fixation	Information Disclosure
Insufficient Session Expiration	Directory Indexing
Injection	Verbose Error Messages
SQL Injection	HTML Comments
Cross-Site Scripting	Default Content
LDAP Injection	Bounds Checking
HTML Injection	Stack-Based
XML Injection	Heap-Based

Trustwave®

For more information: www.trustwave.com