Trustwave®

Trustwave Managed Security Testing

SOLUTION OVERVIEW

Trustwave Managed Security Testing (MST) gives you visibility and insight into vulnerabilities and security weaknesses that need to be addressed to reduce risk. Only Trustwave delivers the full spectrum of vulnerability assessment with a single security testing platform - across databases, networks and applications, from scanning up through penetration testing. Trustwave MST helps you address these critical questions:

- What assets reside on your network?
- Which assets are vulnerable and how?
- Are those vulnerabilities exploitable, and if so, what are the consequences?
- Can you accept the risk introduced by these vulnerabilities?
- How do you spend time and resources most effectively to mitigate and remediate risk?

In this document we will discuss the following aspects of Trustwave Managed Security Testing:

I. Trustwave MST Benefits

Trustwave MST is a one stop shop for all your database, network and application scanning and testing services. Benefits include:

- **Easily scale to keep pace with business demands**
  You gain the flexibility to conduct scans and tests across databases, networks and applications and to go wide or deep to meet your specific needs. You can make adjustments as often or as much as your business needs require. As you detect new assets or your needs change, you can schedule scans or tests quickly thereby keeping pace with business demands and adapting to change without sacrificing security considerations.
- **Make informed decisions around resource allocation**
  Gaining insight into potential targets of attack, the vulnerabilities within them and accurate measures of risk severity empower you to make informed decisions and focus your resources on the most critical vulnerabilities.
- **Simplify security management with a consolidated portal**
  With Trustwave MST you get a unified, holistic view across all your scans and tests with a single, easy-to-use console that simplifies accessing, managing and reporting on scans and tests across all your assets. You can standardize scalable, repeatable scanning and testing with consolidated management and reporting - all on a single platform.
- **Augment internal team and resources quickly and easily**
  We can support your testing and scanning needs as much or as little as you require. Whether you need to augment existing teams and tools with select scans and tests or have us do it all for you – we offer the entire range of services.
- **Allocate funds as needed from your testing budget**
  The Trustwave MST flex-spend model allows you to earmark budget for testing, and then consume your testing funds as needed. This helps eliminate the guesswork in planning for testing needs for the coming year. Security teams can allocate budget for testing and then choose just the right intensity of testing at any time with just a two week lead time.

ll. Trustwave MST Portfolio

Attaining a complete view of all the assets residing on the corporate network is a challenge. You need specialized technology to ensure robust, accurate assessments of your databases and applications and to avoid the risk of missing a critical flaw or drowning in false positives. It is also important to measure the risk presented by a vulnerability in the context of your specific environment, which is done by exploiting it and determining what type of privileged access an attacker can gain or what data is exposed. While vulnerability scanning and penetration testing go hand-in-hand, it is important to understand the differences between the two:

- **Vulnerability scanning** is largely an automated process that evaluates a system for known vulnerabilities or weak configurations and reports on potential exposures. Vulnerabilities scans may be conducted across databases, networks and applications to identify weaknesses. Depending on the expertise of your resources, you have these options:
  - **a. Self-Service Scans** - Users schedule, configure and run scans themselves. Upon completion of a scan, the user receives a list of raw results from our scanning tools that they interpret on their own.
  - **b. Managed Scans** - Trustwave SpiderLabs experts validate and interpret scan results for the user. Upon completion of a scan, the user receives a report of validated results.
- **Penetration testing** is a manual, labor-intensive process. Penetration testers use tools as a part of their work, and apply their ingenuity to exploit vulnerabilities, expose assets to threats and illustrate the severity of risk introduced by identified vulnerabilities.

Types of vulnerability scans and penetration tests offered by Trustwave MST:

<table>
<tr><th></th><th>Managed Scanning</th><th colspan="2">Penetration Testing</th></tr>
<tr><td>Databases</td><td>• Compliance Scanning
• Best Practices Scanning</td><td colspan="2">Some testing may be included as databases are discovered in application and network penetration testing.</td></tr>
<tr><td rowspan="2">Networks</td><td rowspan="2">• Best Practices Scanning</td><td>Internal Network
• Basic
• Opportunistic
• Targeted
• Advanced (including password cracking)</td><td>External Network
• Basic
• Opportunistic
• Targeted (including limited phishing)
• Advanced (including limited phishing and social engineering)</td></tr>
<tr><td colspan="2">Four maintenance tests included with each test. (A total of five tests over a 12-month period).</td></tr>
<tr><td rowspan="2">Applications</td><td rowspan="2">• Compliance Scanning
• Best Practices Scanning</td><td>• Basic
• Opportunistic
• Targeted
• Advanced</td><td></td></tr>
<tr><td colspan="2">Four maintenance tests included with each test. (A total of five tests over a 12-month period).</td></tr>
</table>

A. Vulnerability Scanning

Trustwave MST gives you a holistic view of your security posture and reveals your vulnerabilities by scanning IT assets across databases, networks and applications:

- Database Scans – Protecting Data Where It Resides
- Network Scans – Fortifying Your Infrastructure
- Application Scans – Securing Your Applications

Database Scans – Protecting Data Where It Resides

Trustwave SpiderLabs database security experts conduct managed vulnerability assessments of Microsoft SQL Server, Oracle, Sybase, MySQL, IBM DB2 and Hadoop data stores. An enrollment in Trustwave managed database scanning includes four managed scans over 12 months to provide up-to-date data about the vulnerability of your relational database and big data deployments. Trustwave experts use our technology to spot anomalies such as vulnerabilities, configuration errors, rogue installations and access issues. This information can help a business prevent unauthorized access and help ensure stored data remains confidential.

Managed database scanning identifies discoverable database instances, assesses database(s) against industry best practices, provides actionable information on vulnerabilities and misconfigurations and reviews user privileges.

Network Scans – Fortifying Your Infrastructure

Customers can choose either managed network-host-based vulnerability scanning or in-depth, manual penetration testing from inside or outside the corporate firewall. Trustwave managed network scanning consists of four scans over 12 months where Trustwave SpiderLabs experts configure, execute and interpret results of internal or external vulnerability assessments of your network infrastructure to:

- Discover systems on the network
- Discover services available on the network
- Identify associated vulnerabilities
- Eliminate false positives
- Report on and prioritize only those vulnerabilities that present actual risk (i.e., contribute to a realistic attack chain)

Application Scans– Securing Your Applications

Trustwave delivers Dynamic Application Security Testing (DAST) through Trustwave MST. Patented behavior-based scanning technology provides accurate vulnerability detection for fast, efficient results. With up to 128 categories, our application testing provides some of the highest application vulnerability detection rates in the industry, and our proprietary scores quantify application risk.

Customers may choose either self-serve DAST or managed DAST. Self-serve DAST allows customers unlimited scanning that they can execute immediately from the cloud. Managed DAST consists of Trustwave SpiderLabs application security experts managing application onboarding, scan configuration and execution, validation and reporting. Managed scanning includes four managed scans over a 12-month period (with unlimited scanning options also available).

B. Penetration Testing

A penetration test is an “ethical hack” that evaluates an application’s or network’s ability to withstand attack. During a penetration test, you authorize an expert armed with the same techniques as today’s cybercriminals to hack into your network or application. Such an exercise will open your eyes to vulnerabilities you didn’t know existed and the effects of exploitation.

Trustwave MST provides different levels of penetration testing to meet organizations’ specific business needs. Trustwave MST empowers organizations to model the right threat by selecting the appropriate level of testing based on their testing goals, budget, and the value/criticality of in-scope assets.

Customers choose from four levels of testing aligned with progressive threat severities:

- Tier 1 Basic Threat Test
- Tier 2 Opportunistic Threats Test
- Tier 3 Targeted Threats Test
- Tier 4 Advanced Threats Test

Each tier includes one tier-level scan plus four managed application best practices assessment scans.

Descriptions of Penetration Test Levels

Test Level	Description
Basic Threat	Simulates the most common attacks executed in the wild today. This class of attacker typically uses freely available, automated attack tools.
Opportunistic Threat	Builds upon the basic threat and simulates an opportunistic attack executed by a skilled attacker who does not spend an extensive amount of time executing highly-sophisticated attacks. This type of attacker seeks easy targets and will use a mix of automated tools and manual exploitation to penetrate his/her targets.
Targeted Threat	Simulates a targeted attack executed by a skilled, patient attacker who has targeted a specific organization. This class of attacker will expend significant resources and effort trying to compromise an organization’s systems.
Advanced Threat	Simulates an advanced attack executed by a highly-motivated, well-funded and extremely sophisticated attacker who will exhaust all options for compromise before relenting.

i. Methodology

There are three key steps in the Trustwave MST Methodology. They comprise:

1. Reconnaissance
2. Manual Testing
3. Reporting

1. Reconnaissance

The Process Starts with Reconnaissance. The first step of the process is the discovery process to fully understand what will be tested. This is the information gathering stage when the targets are identified and the scope of the testing is determined - from a particular application to a network range.

When a specific application is tested, the structure of that application must be understood, the level of detail that must be achieved must be determined and the information architecture of the application identified.

When testing a network range, a port scan discovery is conducted to identify all running services that need to be tested. Once the parameters of the testing are well identified and the reconnaissance is complete, rigorous manual testing begins.

2. Manual Testing

The goal of the rigorous manual testing phase is to identify the vulnerabilities that exist in the application or network range being tested and then try to exploit them, also known as ethical hacking. Earlier we saw that vulnerability scanning evaluates a system for potential vulnerabilities or weak configurations. This is followed penetration testing where you authorize your SpiderLabs experts, armed with the same tactics as today's cybercriminals, to hack into your network or application. During manual testing, the SpiderLabs testing experts will:

- Exploit the system
- Identify vulnerabilities
- Confirm vulnerabilities
- Attempt data extraction
- Conduct extensive quality assurance (QA)

If high or critical vulnerabilities are determined, you will be alerted immediately. Once the tester finishes the report, it is submitted to Quality Assurance (QA) to be checked. QA is performed by a senior member of the team.

3. Reporting

All reports are delivered through the TrustKeeper® MST portal. You have dynamic visibility of your test results through the entire testing process. Once reporting is complete, your reports and evidence are also delivered through the MST portal.

ii. Service Levels

Our testers employ several different levels of penetration testing techniques within each tier – basic, opportunistic, targeted and advanced threats penetration tests. We provide the following types of penetration testing:

- External Network Testing
- Internal Network Testing
- Application Testing

External Network Testing

	Basic	Opportunistic	Targeted	Advanced
Most Exploitable Findings	●	●	●	●
Any Exploitable Findings		●	●	●
Vertical Escalation		●	●	●
Horizontal Escalation		●	●	●
Attack Chains			●	●
Escalation to Adjacent Systems			●	●
Client Side Attacks				●
Social Engineering				●

Internal Network Testing

	Basic	Opportunistic	Targeted	Advanced
Most Exploitable Findings	●	●	●	●
Segmentation Testing	●	●	●	●
Attack Chains		●	●	●
Data Exfiltration Testing		●	●	●
Enterprise Escalation			●	●
Testing from Client Subnets			●	●
Advanced Protocol Attacks				●
Client Side/Browser Attacks				●

Application Testing

	Basic	Opportunistic	Targeted	Advanced
Manual Injection Testing	●	●	●	●
Manual Session Management Testing	●	●	●	●
Manual Authentication Testing		●	●	●
Manual Authorization Testing		●	●	●
Manual Testing for Complex Logic Flaws			●	●
Manual Testing for Cryptographic Weaknesses			●	●
Exhaustive Testing				●
Manual Testing of All Input Areas				●

For a complete listing of what's included in each service level for Internal Network Testing, External Network Testing and Application Testing, please refer to the MST Service Level Brief.

III. Getting Started

Trustwave MST's pre-scoped scans and tests, cost transparency and flex-spend consumption model make planning easier and more precise. With quarterly payments, penetration testing becomes a predictable operating expense that can be built into your budgets.

You define your testing budget and allocate it as you see fit. Your account balance depletes with each database, network or application you enroll, and you can replenish your account at any time.

1. An initial balance is credited to your account.
2. You enroll a database, network and/or application target and choose the level of testing.
3. Your account balance is debited according to predefined pricing.
4. You schedule your tests for the enrolled network or application.
5. A SpiderLabs expert conducts the test.
6. Dynamic reporting is made available in the portal.
7. You view and manage reporting within the portal.
8. If desired, you then schedule maintenance testing to re-evaluate findings where possible.

To learn more you can reach a Trustwave solution specialist at **(888) 878-7817** or via email at **infosales@trustwave.com**.

Trustwave®

For more information: www.trustwave.com