Trustwave®
Smart security on demand

TRUSTWAVE MANAGED SECURITY TESTING

DON'T GUESS. TEST.

Trustwave Managed Security Testing reveals your vulnerabilities and alerts you to the consequences of exploitation.

If you're concerned about cyberattacks and how they might affect your business, Trustwave Managed Security Testing gives you visibility and insight into the vulnerabilities and security weaknesses you need to address to reduce risk. Only Trustwave offers the full spectrum of vulnerability assessment from scanning up through penetration testing and across databases, networks, and applications—through a single security testing platform.

To make the most impact, you need to know what you're protecting and what you're protecting it from:

- 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 severe is the associated risk?
- How do you spend time and resources most effectively to mitigate and remediate risk?

A FULL, CLEAR VIEW IS HARD TO COME BY

Attaining a complete view of all the assets residing on the corporate network is a challenge. Even if you're confident in the quality of your inventory; assessing vulnerabilities across your databases, network infrastructure and applications can't be done thoroughly with general vulnerability assessment tools.

You need specialized technology to ensure robust, accurate assessment of your databases and applications. Otherwise you risk missing a critical flaw or drowning in false positives.

Because general purpose tools won't cut it, you face managing a hodgepodge of technologies. Trying to correlate the results from each is painful and time-consuming (if it's even possible). Disjointed assessments and reporting gives you only a fragmented view of your risk.

Even then, while a list of missing patches or misconfigurations is a start, resource-strapped IT and security teams need to know what to fix first. A vulnerability may only receive a rating of five from the Common Vulnerability Scoring System (CVSS), however, in the context of your operations it could supply the footing for the compromise of a critical asset. One of the only practical ways to measure the risk presented by a vulnerability in the context of your specific environment is to exploit it and determine what sorts of privileged access an attacker can achieve or what data is exposed as a result.

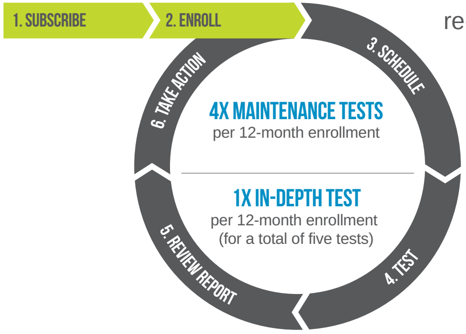
Scanning is largely an automated activity. Penetration testing, on the other hand, is a manual, typically labor-intensive process. Penetration testers will use tools as a part of their work, but they apply their ingenuity to exploit vulnerabilities, expose assets to threats, and illustrate the severity of risk introduced by any particular vulnerability.

Trustwave data breach investigations, malware reverse-engineering projects, millions of scans, thousands of penetration tests, leadership of open-source security projects and contributions to the security community have established the SpiderLabs team at Trustwave as world-renowned experts on the past, present and future of security threats.

VULNERABILITY DATA IS ONLY AS ACCURATE AS IT IS CURRENT

A report of test findings gathering dust in a manager's drawer does nothing to fortify IT infrastructure against attacks. New threats develop by the day and the next big vulnerability lurks just around the corner.

Too much can change between assessments. To keep pace with business demands, IT departments need more than point-in-time testing. They need regular assessment and testing to minimize exposure introduced by changes in the environment and to curtail cybercriminals' window of opportunity. Maintenance testing included as part of Managed Security Testing allows businesses to meet re-testing requirements in compliance regimes such as PCI DSS and provide proof that they've fixed any issues.



A COHESIVE, PROGRAMMATIC APPROACH

Trustwave Managed Security Testing is a full suite of vulnerability scanning and penetration testing services for visibility across all asset types. The integration of our precision database, network and application vulnerability scanning with our industry-leading, manual penetration testing give users a complete view of risk across their entire environment through a single-pane-of-glass while simplifying and consolidating toolsets. In addition, Trustwave Managed Security Testing's flexible consumption model empowers IT and security teams to take a programmatic approach to vulnerability management and operationalize scanning and testing expenses to avoid unexpected balloon payments during the year.

Many businesses realize the need for pro-active security testing and budgets are increasing as a result. Still, planning for and procuring security testing presents a number of challenges:

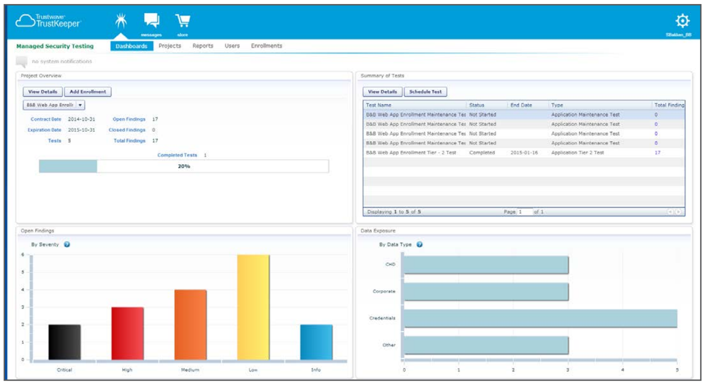
- Anticipating future testing needs
- Conducting testing in a timely manner
- Making testing an efficient, business-as-usual initiative rather than an obstacle
- Getting high quality testing across asset types
- Standardizing repeatable testing/reporting
- Fulfilling compliance requirements
- Effectively managing multiple tests, and re-testing, over the course of the year.

Trustwave Managed Security Testing helps eliminate the guess-work in planning for testing needs in the coming year. Security teams can allocate budget for testing and then choose just the right intensity of testing at any time with just two weeks' lead time. Trustwave provides IT and security teams with detailed visibility of potential targets of attack, awareness of vulnerabilities within them, and accurate measure of the associated risk severity. With this information, managers can make quick, informed decisions about where to focus their resources and fix the most dangerous vulnerabilities first.

MODELING THE RIGHT THREAT

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:

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

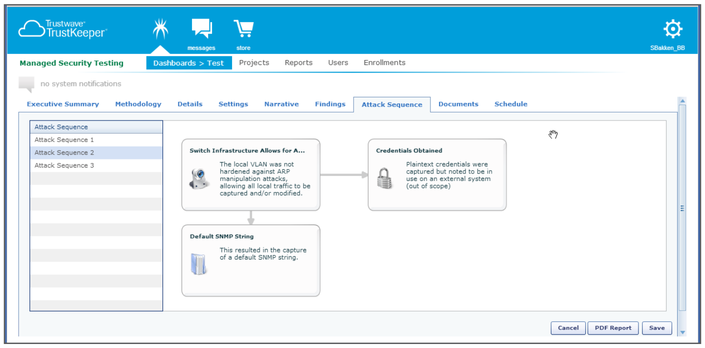


no system notifications

Contract Date 2014-10-31
Expiration Date 2015-10-31
Tests 5
Open Findings 17
Closed Findings 0
Total Findings 17
Completed Tests 1
20%

Test Name	Status	End Date	Type	Total Finding
B&B Web App Enrollment Maintenance Tes	Not Started		Application Maintenance Test	0
B&B Web App Enrollment Maintenance Tes	Not Started		Application Maintenance Test	0
B&B Web App Enrollment Maintenance Tes	Not Started		Application Maintenance Test	0
B&B Web App Enrollment Maintenance Tes	Not Started		Application Maintenance Test	0
B&B Web App Enrollment Tier - 2 Test	Completed	2015-01-16	Application Tier 2 Test	17

Displaying 1 to 5 of 5 Page 1 of 1



no system notifications

Switch Infrastructure Allows for A...
The local VLAN was not hardened against ARP manipulation attacks, allowing all local traffic to be captured and/or modified.

Credentials Obtained
Plaintext credentials were captured but noted to be in use on an external system (out of scope)

Default SNMP String
This resulted in the capture of a default SNMP string.

PROTECT DATA WHERE IT LIVES: DATABASE ASSESSMENT

Through Trustwave Managed Security Testing, Trustwave SpiderLabs' database security experts conduct managed vulnerability assessment 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 will 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 can: identify discoverable database instances, assess database(s) against industry best practices, provide actionable information on vulnerabilities and misconfigurations, and review user privileges.

Depending on the level of scanning selected, test classes covered during managed database scanning may include, but not be limited to, the following tests and checks:

Authentication and Authorization	Vulnerabilities
Weak authentication modes	Missing patches
Dangerous privilege grants	Privilege escalation
PUBLIC privileges and guest accounts	Denial of service
	Buffer overflow
Weak Passwords	**Misconfigurations**
Default account/password	Disabled security settings
Password based on username	Non-encrypted communications
Easily-guessed passwords	
	Inadequate audit trail
	Operating System
	File permissions
	Registry permissions

STORMING THE NETWORK: EVALUATING INFRASTRUCTURE

Through Trustwave Managed Security Testing, 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 wherein Trustwave SpiderLabs experts configure, execute and interpret results of internal or external vulnerability assessments of your network infrastructure to:

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

Network security testing goes beyond vulnerability assessment to exploit vulnerabilities and evaluate the target network's resilience to attack. Trustwave SpiderLabs experts will model and explore actual attack vectors with the goal of circumventing security controls and gaining unauthorized access to systems and data.

Trustwave network security testing includes one in-depth tiered penetration test along with four maintenance tests over 12 months for use as ongoing validation.

Depending on the level of testing selected, test classes covered during a network penetration test may include (but are not limited to):

Local Network Segment	Password Cracking Enterprise Infrastructure
VLAN hopping	LDAP/Active directory
ARP cache poisoning	Source code repositories
Insecure network protocols	**Infrastructure Services**
Man-in-the-middle	Databases
Credential capture	Mainframes
Network Infrastructure	Middleware
Routers/switches/load balancers	Single sign-on
Remote network access devices	Remote administration
Name/allocation services	Backup
Common Services	File sharing
HTTP	Access control
SMTP	**Operating System**
POP/IMAP	OS-specific services
FTP	**Advanced Tactical**
Simple Website	Non-IP protocols
XSS	Non-standard network services
SQL injection	
Arbitrary redirection	Multistage attack vectors
Known command injection	**Social Engineering**
	Phishing
	Client-side attacks

EVALUATING APPLICATION SECURITY

Analysts estimate that 75 percent of attacks occur at the application layer. Add to that the fact that 98 percent of the applications assessed by Trustwave SpiderLabs in 2014 included at least one vulnerability. These statistics prove that attackers have applications in their sights and why.

Trustwave delivers Dynamic Application Security Testing (DAST) through Trustwave Managed Security Testing. 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 they can execute immediately from the cloud. Managed DAST consists of Trustwave SpiderLabs application security experts managing app 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).

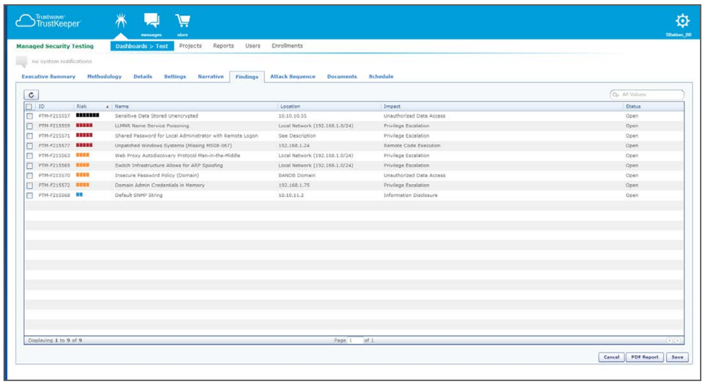
Customers may also choose in-depth, manual application penetration testing for deeper evaluation than provided by DAST. Depending on the level of testing selected, test classes covered during an application penetration may include (but are not limited to):

Authentication and Authorization	**Application Resource Handling**
Unlimited login attempts	Path traversal
Authentication bypass	Predictable object identifiers
Authorization bypass	XML entity expansion
Default / weak passwords	Local & remote file inclusion
Session Management	**Cryptography**
Session identifier prediction	Weak algorithms
Session hijacking	Poor key management
Session replay	**Logic Flaws**
Session fixation	Abuse of functionality
Insufficient session expiration	Workflow bypass
Injection	**Data Protection**
SQL injection	Transport
Cross-site scripting	Storage
LDAP injection	**Information Disclosure**
HTML injection	Directory indexing
XML injection	Verbose error messages
OS command injection	HTML comments
	Default content
	Bounds Checking
	Stack-Based

NO-HASSLE, SCALABLE TESTING AT THE RIGHT TIME FROM A SINGLE VENDOR

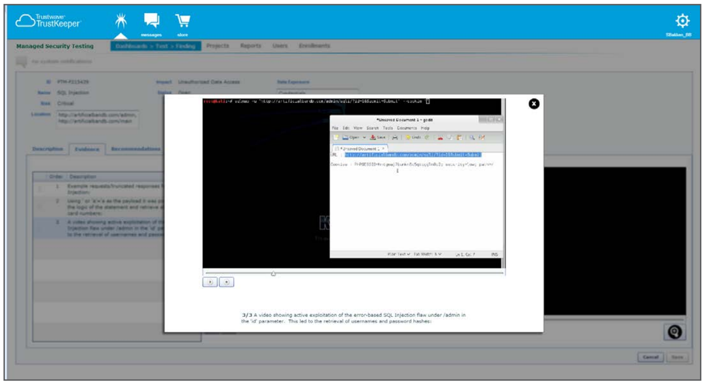
Trustwave Managed Security Testing provides you a programmatic, holistic approach to vulnerability management and a single, consolidated view of risk across your entire IT environment—spanning databases, network infrastructure, and applications. Trustwave customers also get just the right test at just the right time through a single platform and without the hassle.

1. **The right test** Testing as wide or deep as needed across databases, networks and apps
2. **At the right time** Quickly schedule testing online with only two weeks' lead time
3. **Through one vendor** Maximize budget, standardize and consolidate reporting through a single view
4. **Without the hassle** Earmark budget then allocate as needed with flex-spending and cost transparency.



ID	Risk	Name	Location	Impact	Status
PTM-F215557	■■■■■■■	Sensitive Data Stored Unencrypted	10.10.10.55	Unauthorized Data Access	Open
PTM-F215559	■■■■■	LLMNR Name Service Poisoning	Local Network (192.168.1.0/24)	Privilege Escalation	Open
PTM-F215571	■■■■■	Shared Password for Local Administrator with Remote Logon	See Description	Privilege Escalation	Open
PTM-F215577	■■■■■	Unpatched Windows Systems (Missing MS08-067)	192.168.1.24	Remote Code Execution	Open
PTM-F215563	■■■■	Web Proxy Autodiscovery Protocol Man-in-the-Middle	Local Network (192.168.1.0/24)	Privilege Escalation	Open
PTM-F215565	■■■■	Switch Infrastructure Allows for ARP Spoofing	Local Network (192.168.1.0/24)	Privilege Escalation	Open
PTM-F215570	■■■■	Insecure Password Policy (Domain)	BANDB Domain	Unauthorized Data Access	Open
PTM-F215572	■■■■	Domain Admin Credentials in Memory	192.168.1.75	Privilege Escalation	Open
PTM-F215568	■■	Default SNMP String	10.10.11.2	Information Disclosure	Open

Displaying 1 to 9 of 9 Page 1 of 1



ID PTM-F215429
Name SQL Injection
Risk Critical
Impact Unauthorized Data Access
Status Open

3/3 A video showing active exploitation of the error-based SQL Injection flaw under /admin in the 'id' parameter. This led to the retrieval of usernames and password hashes.

THE TRUSTWAVE MANAGED SECURITY TESTING PORTFOLIO

This chart outlines the scanning and testing services available to Trustwave Managed Security Testing subscribers.

	Managed Scanning	Penetration Testing	
Databases	• Compliance Scanning • Best Practices Scanning	*Some testing may be included as databases are discovered in application and network penetration testing*	
Networks	• Best Practices Scanning	Internal Network • Basic • Opportunistic • Targeted • Advanced (including password cracking)	External Network • Basic • Opportunistic • Targeted (including limited phishing) • Advanced (including limited phishing and social engineering)
		Four maintenance tests included with each test (five total tests over a 12-month period)	
Applications	• Compliance Scanning • Best Practices Scanning	• Basic • Opportunistic • Targeted • Advanced	
		Four maintenance tests included with each test (five total tests over a 12-month period)	

Trustwave®

Smart security on demand

For more information: https://www.trustwave.com