



McAfee Web Security Service Technical White Paper

Continual Security Auditing	
Vulnerability Knowledge Base	3
Vulnerability Management Portal	3
Secure Portal Architecture and Distributed Scanning Network	3
Daily Audits Keep All the Holes Closed	4
Real-Time Alerting and You	4
Multiphase Vulnerability Audit Technology	
Phase 1 - Port Discovery Scan	4
Phase 2 - Network Services Scan	4
Phase 3 - Web Application Scan	5
Ongoing Auditing	5
The McAfee SECURE Data Security Standard	5
Vulnerability Management Portal	
Interactive Vulnerability Management	5
Devices and Device Groups	6
Configurable Scheduled and Manual Scans	6
Multiple-User Roles	6
Reduced False Positives	6
Device Configuration Editing	6
Reporting	6
McAfee Network Architecture	
Our State-of-the-Art Secure Data Centers	7
Scan Appliances	7
Vulnerability Tests	7
About McAfee	
More Information	7

Most security efforts lose effectiveness over time. Any changes in your web server, web applications, or other infrastructure configuration, can unintentionally open the door to security hazards. With so many new threats identified each day, you need to continually test your security measures and decide which risks are the most important to address. You also need to know which vulnerabilities are the most critical and require your immediate remediation.

The McAfee Web Security Service's accurate vulnerability scanning and reporting technology identifies the presence of security holes, including dangerous web application risks, and then provides the information you need to prioritize and rapidly address risks across business units and IT groups. The service is delivered as Software-as-a-Service, a completely web-based service. It requires no installation, no set-up, no hardware purchases, no software development, no security expertise and no special training to use. We act as your "watchful set of eyes" to monitor your servers' vulnerabilities 24/7 to help ensure your network is protected around the clock.

Key Points

Protection of Entire Infrastructure

- Daily scanning of Internet services, ports, operating systems, servers, key applications, firewalls, addressable switches, load balancers and routers for known vulnerabilities

Safe and Easy to Use

- Remote subscription-based, non-destructive vulnerability scanning and certification to the McAfee SECURE data security standard

Detailed Reporting

- Concise reports provide specific recommendations for remediation.

Comprehensive and Always Up To Date

- Vulnerability data updated from worldwide sources, Tests for over 15,000 individual vulnerabilities.

Continual Security Auditing

More than 80,000 certified McAfee SECURE websites use the same vulnerability scanning technology to help protect themselves from hackers, and benchmark their network security against the McAfee SECURE data security standard. Our advanced vulnerability discovery and management technology provides an easy-to-use, reliable and comprehensive solution with a proven ROI.

Vulnerability Knowledge Base

Our up-to-date knowledge base powers our comprehensive network security audits and vulnerability management technology. We update the knowledge base regularly from sources worldwide with tests for newly discovered vulnerabilities. These updates ensure that McAfee Web Security Service customers are always alerted of the latest vulnerabilities.

Vulnerability Management Portal

Our web-based management portal provides secure access to the latest vulnerability data at any time, from anywhere. Extensive tools allow you to launch scans, examine vulnerability details or trends, access patch information, configure alerts, assign user roles, and generate customized reports.

Secure Portal Architecture and Distributed Scanning Network

The McAfee Web Security Service vulnerability management portal provides secure storage and processing of vulnerability data on an n-tiered architecture of secure load-balanced application servers. All customer data is located in Tier-1 high-availability, continuously monitored data centers. The center is physically and logically secured with biometric access and 7/24 on-site security personnel. Our network of distributed scanning servers allows us to easily and reliably perform daily security audits for tens of thousands of clients located in more than 50 countries around the world.

Daily Audits Keep All the Holes Closed

Active vulnerability analysis and penetration testing is the next generation in security tools. McAfee is leading the way. The McAfee Web Security Service helps customers protect their servers free from dangerous vulnerabilities, including web application vulnerabilities.

Real-Time Alerting and You

Following the daily audit, you will receive an immediate email alert if new vulnerabilities have been found.

After scanning is completed, detailed server fingerprints, open ports and vulnerability data are available in a password-protected account maintained on our secure server. When audits discover vulnerabilities, you receive an email alert, directing you to login to your account. These alerts do not contain any specific security information.

Once logged into your account, vulnerability scan results can be viewed, along with detailed patch recommendations applicable to your specific system configuration. Historical audit data is also available, along with printable audit reports. Should you have any questions or need assistance regarding patching your system, technical support is included in your subscription.

For websites on shared or fully managed servers, a separate account is provided for the web host. The website owner retains full administrative control, but for security reasons, cannot view vulnerability information pertaining to the web host's infrastructure. In this case, only the web host can view vulnerability details and patch information.

Multiphase Vulnerability Audit Technology

Daily security audits are preformed in three phases: Port Scanning, Network Services Testing, and Web Applications Vulnerability Testing. This multi phase approach to vulnerability auditing allows us to perform more accurate audits with lower load on your servers. It also allows us to run any single test phase on a target to detect changes, test specific ports or vulnerabilities, or run web application only tests on multiple websites residing on a single server.

These tests are designed to represent a light-load to the device being tested. Scans are designed to be non-disruptive/non-invasive and will not slow or lock-up the device or service being tested.

The Daily Audit Procedure

Phase 1 - Port Discovery Scan

Phase one is a thorough port scan of the target. Accurately determining which ports on an IP address are open is the crucial first step to a comprehensive security audit. This is often not a simple process, but our advanced dynamic port scanning can handle all targets from desktop PCs to the most aggressive firewalls, IDS and IPS systems.

Phase 2 - Network Services Scan

After determining which ports are alive we begin a network services test on each port. During this phase we thoroughly interrogate the service to determine exactly what software is running and how it is configured. This information is leveraged in order to launch additional service specific and generic tests.

Phase 3 - Web Application Scan

Web application testing is the third phase of our daily security audit. According to industry sources, such as Gartner Group, an estimated 60-75% of all security breaches today are due to vulnerabilities within the web application layer. Traditional security mechanisms such as firewalls provide little or no protection against attacks on your web applications. All HTTP services and virtual domains are tested for the existence of potentially dangerous modules, configurations settings, CGIs and other scripts. The website then is "crawled" to find forms. Forms are exercised in specific ways to disclose all application-level vulnerabilities such as, code revelation, cross-site scripting and SQL injection. Both generic and software specific tests are performed in order to uncover misconfigurations and coding error vulnerabilities.

Ongoing Auditing

In addition to vulnerability scanning, the McAfee Web Security Service also includes technology that helps protect websites (and consumers) against "social engineering" tricks like spyware infections, identity theft scams, and sites which send excessive e-mail. This technology is based on a system of automated testers which continually patrol the Web to browse sites, download files, and enter information on sign-up forms.

The McAfee SECURE Data Security Standard

The McAfee SECURE™ standard is an aggregate of industry best practices, designed to provide a level of security that a business can reasonably achieve with its network perimeter security. When evaluating a network perimeter security (primarily websites and web applications), the McAfee SECURE standard considers both the results of a daily vulnerability assessment as well as a review of the web application's content. When reviewing site content McAfee looks for malicious downloads (adware, spyware, viruses, trojans), malicious affiliations (links), phishing scams, browser exploits, misuse of personal information (spam), annoyances (excessive pop-ups), and other online scams (business practices). Companies in compliance with the McAfee SECURE standard have the option of adding the dynamically-served McAfee SECURE trustmark to their website(s). The McAfee SECURE trustmark has become a widely recognized trust enabler, with extensive testing demonstrating that it reassures visitors, thereby increasing site conversion on average by 11%.

Vulnerability Management Portal

The portal provides a comprehensive and easy-to-use interface for vulnerability management.

Our secure web-based vulnerability management system provides extensive vulnerability data along with complete patch information enabling rapid prioritization and remediation. Configuration of both device (port level) and domain (protocol level) scanning is available. On-demand security audits can be initiated at any time. Multiple user accounts can be created with appropriate roles and privilege levels providing information access and alert levels tailored to your organization. From protecting a single website to auditing a complex network, we provide the appropriate tools for each task.

Interactive Vulnerability Management

McAfee doesn't just provide you with a 100-page list of the vulnerabilities we find like other scan vendors. Instead, we give you an interactive vulnerability management tool. View vulnerabilities by device or device group. Sort and view detailed remediation steps. Create custom alert levels for each user or role. Compare recent audits with data going back up to three years. Configure and generate PDF security management and compliance reports.

Devices and Device Groups

The ability to effectively manage vulnerability data by assigning any network device, group of devices, or IP address to specific groups or individuals is essential to manage your organization's security. Device classification capabilities, individual devices, or entire IP blocks, can be easily grouped by type, business function, geographic location, or other criteria and then assigned to a user or group of user accounts. This flexible, powerful system can then be used to drive audit schedules, alerting, remediation activities and reporting throughout your organization.

Configurable Scheduled and Manual Scans

Scanning time may be scheduled by individual device, device group. Manual scans can be run at any time, while special "denial of service" and "full exploit" scans can only be run in the manual mode. Manual scans of current vulnerabilities only are available to help speed remediation efforts.

Multiple-User Roles

Hierarchical multi-user environment with role-based access, alerting and reporting distributed management capabilities enable delegation of vulnerability assessment and remediation tasks to multiple users with assigned privileges, while maintaining centralized control for the Security Manager. This functionality simplifies delegation of network security maintenance, facilitates compliance reporting, and provides management with up-to-date overview reports.

Reduced False Positives

Our false positive management system greatly reduces the frequency of false positives that plague most vulnerability scanning systems. One of our earliest objectives was creating scanning technology with a low level of false positives. Under some conditions, our system will report the "indication" of a possible threat where none actually exists. This typically occurs when the proper patch cannot be confirmed without invasive action. We always err on the side of caution and will notify you, requesting confirmation of its presence or absence. Potential threats that you have marked as false positive will not influence your certification status.

Device Configuration Editing

All device details, such as the IP address, device type, etc. can be updated at any time. You can add additional devices or domains, create users, initiate on-demand scans, and schedule set scan times.

Reporting

Extensive executive and compliance reporting capabilities include easily customizable report templates. You have the flexibility to create downloadable executive-level summary reports with trend analysis, or detailed technical reports and Reports on Compliance to satisfy various federal and industry requirements

McAfee Network Architecture

Our multi-tier network architecture is fast, highly scalable, fully redundant and secure.

Our State-of-the-Art Secure Data Centers

- Integrated biometric card access control
- 24/7 CCTV video surveillance and recording
- Security staff on patrol 24/7
- Multiple redundant Tier 1 backbone private peering
- Redundant firewalls
- Failover load balancers
- Redundant web server and application server clusters
- Seismically braced racks
- Dual-interlock fire suppression systems
- Uninterruptible Power Supply (UPS with automatic power transfer bridge system)

Scan Appliances

Our scan appliances are distributed in multiple networks. Each appliance is individually protected by its own firewall. All remote administration and reporting is through encrypted connections.

About McAfee

McAfee, Inc., the leading dedicated security technology company, headquartered in Santa Clara, California, delivers proactive and proven solutions and services that secure systems and networks around the world. With its unmatched security expertise and commitment to innovation, McAfee® empowers home users, businesses, the public sector, and service providers with the ability to block attacks, prevent disruptions, and continuously track and improve their security. More information is available at www.mcafee.com.

More Information

Web Security Group
McAfee, Inc.
877-302-9965
info@mcafeesecure.com

Vulnerability Tests

McAfee tests for known vulnerabilities in the following general categories:

- SQL Injection
- Blind SQL Injection
- SQL Database Error Disclosure
- Local File and Remote File Includes
- Directory Traversals
- Improper Error Handling
- Application Source Code Disclosure
- Authentication Bypass
- Insufficient Session
- Expiration Command Injection
- SSI Injection
- Malicious CGI scripts
- Buffer Overflows
- Client Side Vulnerabilities
- Directory Indexing
- Server Misconfigurations
- SSL Encryption
- Malicious Downloads
- Malicious Affiliations (links)
- Phishing Scams
- Browser Exploits
- Misuse of personal information
- Annoyances (excessive pop-ups)
- Scams (business practices)

McAfee®

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and/or additional marks herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2008 McAfee, Inc. All rights reserved.
project code #