ScanAlert™ *Making the web HACKER SAFE®*

ScanAlert™
HACKER SAFE
TESTED DAILY 01-JAN

ScanAlert Technology White Paper

ScanAlert
Technology White Paper
May 2005

ScanAlert, Inc.
860 Napa Valley Corporate Way, Suite R
Napa, CA 94558
(877) 302-9965
support@scanalert.com

www.scanalert.com

CONTINUOUS SECURITY AUDITING

Most security efforts lose effectiveness over time. Any changes in your web server, or other infrastructure configuration, can unintentionally open the door to security hazards. Add to this the many new threats identified each day and you have a situation where security measures need to be continuously tested.

ScanAlert provides automated network security audits combined with an interactive, highly customizable vulnerability management portal. ScanAlert's service is completely web-based and runs entirely from our network. 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.

Tens of thousands of web sites use ScanAlert for protection from hackers and third-party security certification to the highest government and industry standards. ScanAlert's advanced vulnerability discovery and management technology provides an easy-to-use, reliable and comprehensive solution with a proven ROI.

Vulnerability Knowledge Base

ScanAlert's up-to-date knowledge base powers our comprehensive network security audits and vulnerability management technology. We update the knowledge base every 15 minutes with tests for newly discovered vulnerabilities and validated fixes from hundreds of sources worldwide. These continuous updates ensure ScanAlert 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 rolls, and generate customized reports.

Secure Portal Architecture and Distributed Scanning Network

ScanAlert's vulnerability management portal provides highly secure storage and processing of vulnerability data on an n-tiered architecture of secure load-balanced application servers. All customer data is located in our Tier-1 high-availability, continuously monitored data center. 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 thousands of clients located in more than 20 countries around the world.

Key Features

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

Safe and Easy-to-Use
Remote subscription-based, non-invasive, non-destructive vulnerability scanning and certification

Tracks System Configuration
Identifies unauthorized server applications and tracks system configuration changes

Detailed Reporting
Concise reports provide specific recommendations for remediation. Reports results of over 6,000 individual vulnerability tests plus port scans

Continuous 24/7 coverage
Seamless protection due to continual comparisons between scans of your most-current system configuration against new threats

Always Up-To-Date
Vulnerability data updated on-the-fly from hundreds of worldwide sources

Certified Customer Support
Service includes unlimited email or telephone customer support from CISSP certified security professionals.

Compliance with Legislative Acts
HACKER SAFE sites meet the web site security vulnerabilities audit requirements mandated by HIPAA, GRAMM-LEACH-BLILEY, SARBANES-OXLEY, and other federal legislation

Daily Audits Keep All the Holes Closed

Proactive vulnerability analysis and penetration testing is the next generation in security tools, and ScanAlert is leading the way. HACKER SAFE certification means that all accessible services hosted on your servers are free from all vulnerabilities that can be scanned for, including web application vulnerabilities. While the Internet worms and credit card thefts that make headlines in the news cannot be prevented by firewalls or SSL, they are stopped by systems we certify as HACKER SAFE.

Real-Time Alerting

Following the daily audit, you will receive an immediate email alert if any 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, unlimited telephone technical support from our CISSP certified security staff is included in your subscription.

For web sites on shared or fully managed servers, a separate account is provided for the web host. The web site 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.

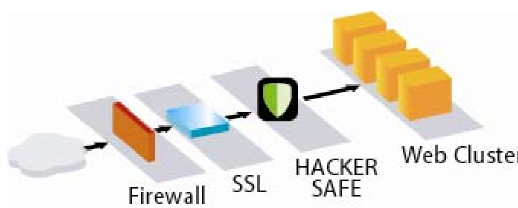
More Features

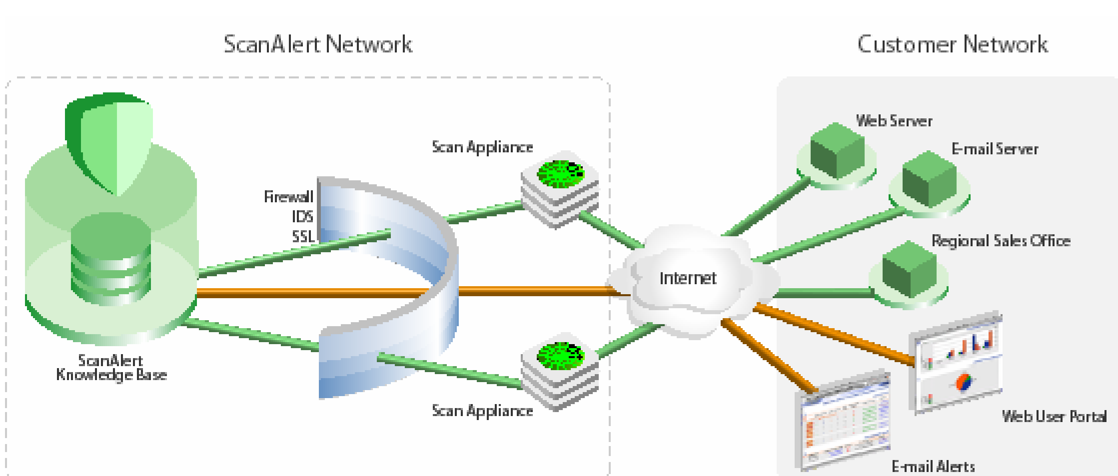
Compliance with Credit Card Issuers

HACKER SAFE certification meets the vulnerability scanning requirements of the Payment Card Industry (PCI) data security standard.

SANS Top 20 Internet Vulnerabilities

HACKER SAFE sites are tested daily against the SANS Top 20 Internet Security Vulnerabilities list.





MULTIPHASE VULNERABILITY AUDIT TECHNOLOGY

Daily security audits are preformed in three phases: Port Scanning, Network Services Penetration Testing, and Web Applications Vulnerability Testing. This multi phased approach to vulnerability auditing allows us to perform more accurate audits with less 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 web sites residing on a single server.

Scans typically take between 60-90 minutes and transfer approximately 10 megabytes of data. These tests are designed to represent a light-load to the device being tested. Scans are non-disruptive and will not slow or lockup 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. Once this information is acquired it is matched to our knowledge base of vulnerabilities in order to launch additional service specific and generic tests.

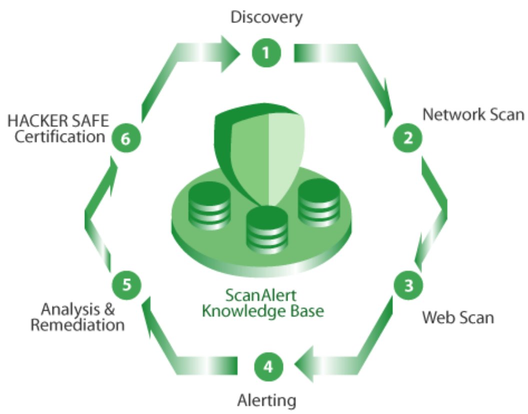
Phase 3 - Web Application Scan

Web application testing is the third phase of ScanAlert's daily security audit. According to industry analyst firm Gartner Group, an estimated 70% of all security breaches today are due to vulnerabilities within the web application layer. Traditional security mechanisms such as firewalls and IDSes 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 web site 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

Continuous Protection

Between each daily audit, you will receive an immediate email alert if any new vulnerabilities are added to our system that target your exact device configuration as we recorded it during the most recent scan.

This unique 24-hour continuous alert system protects you around the clock by comparing any newly announced vulnerabilities against your most recent device profile. Whenever new vulnerabilities are relevant to your most recent device profile, you will be notified immediately via email, minimizing your possible risk exposure between daily scans. We do all the research and testing for you, making it easy for you to keep your servers secure. Alerts do not contain any specific security information; they only direct you to login to your account.



VULNERABILITY MANAGEMENT PORTAL

The portal provides a comprehensive and easy-to-use suite of network security management tools.

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 web site to auditing a complex network, we provide the appropriate tools for each task.

Interactive Vulnerability Management

ScanAlert doesn't just provide you with a 10 page list of the vulnerabilities we find, 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. Using ScanAlert's 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, or separate schedules for web application and port-level scans. 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 maintained, facilitates compliance reporting, and provides management with up-to-date overview reports.

Reduced False Positives

Our patent pending False Positive Management System greatly reduces the frequency of false positives that plague most vulnerability scanning systems. The low level of false positives from Scan Alert's audit technology is something we are very proud of.

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 detected 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

SCANALERT NETWORK ARCHITECTURE

ScanAlert's multi-tier network architecture is designed to be fast, highly scalable, fully redundant and secure.

Our State-of-the-Art Secure Data Center

- 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 and active IDS
- Failover load balancers
- Redundant web server and application server clusters
- Seismically braced racks
- Redundant heating, ventilation, and air conditioning
- 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 and active IDS. All remote administration and reporting is through encrypted VPN connections.

> *"So here's the question, if you're running an ecommerce site, you have vulnerability detection software, don't you? I'm sure you do. So how much revenue is the security software making for you? I have to confess I like what ScanAlert is doing. It's such a neat business model and for the ecommerce businesses that need vulnerability detection software, it has to be a no-brainer."*
>
> Robin Bloor
> Analyst
> IT-Director.com

Vulnerability Tests

ScanAlert tests for all known vulnerabilities in the following general categories:

- Backdoors, Remote Controls and Trojan Horse Programs
- Brute Force Attacks
- CGI and Form Processing Vulnerabilities (incl. SQL injection)
- Default Passwords
- All Database Servers
- All Microsoft Versions
- All UNIX and Linux Versions
- E-mail Services
- News and Chat Services
- Remote Administration Access
- Remote Database Access
- Remote File Access
- All TCP Ports
- RPC
- SMB/NetBIOS
- ICMP
- All HTTP services (incl. XSS)
- SNMP
- SMTP
- UDP
- FTP and Telnet
- SOAP and other XML services
- Routers and Load Balancers
- Firewalls and Addressable Switches

About ScanAlert

Headquartered in Napa, CA, ScanAlert makes web sites secure from hackers and certifies it to their customers with a HACKER SAFE certification mark. HACKER SAFE certification protects millions of visitors every day to tens of thousands of web sites. The certification mark indicates that these sites are compliant with the highest federal and industry web site security standards.

For More Information

Web: www.scanalert.com
Tel: 877-302-9965
Email: info@scanalert.com