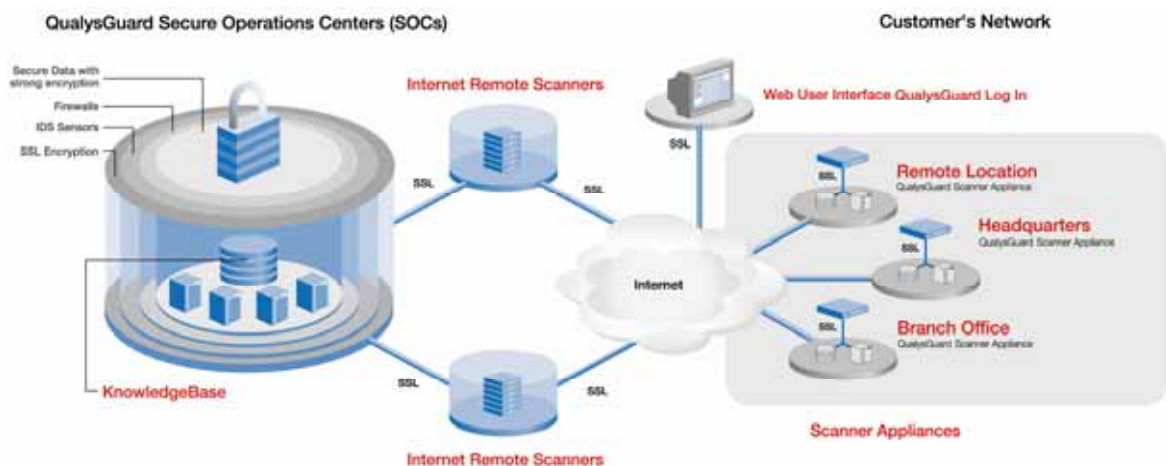




Published April 2004

## Summary

The QualysGuard Secure Operations Center is designed with multiple layers of data and physical security to secure customers' vulnerability information. This document summarizes the security architecture and report data security mechanisms built into the QualysGuard On-Demand Platform for Network Security Audits, Vulnerability Management and Remediation.



QualysGuard is designed to provide end-to-end security for sensitive vulnerability data, considering industry best practices at all layers of the application:

- The Secure Operations Center (SOC)
- User Authentication and Communication Security
- Vulnerability Data Encryption and Protection
- Monitoring and Availability
- Intranet Scanner Appliance Security

From an infrastructure perspective, the report database is layered within our n-tier architecture behind a set of load-balanced Web application servers. The QualysGuard Web servers, which are configured in a multi-homed configuration, connect to the report database server via private (non-routable) IP addresses. Additional layers of protection are provided by dedicated firewall and IDS systems, as well as specific procedures for hardening the operating systems of all systems involved. All communication with our worldwide distributed scanning servers employs SSHv2 to protect sensitive information.

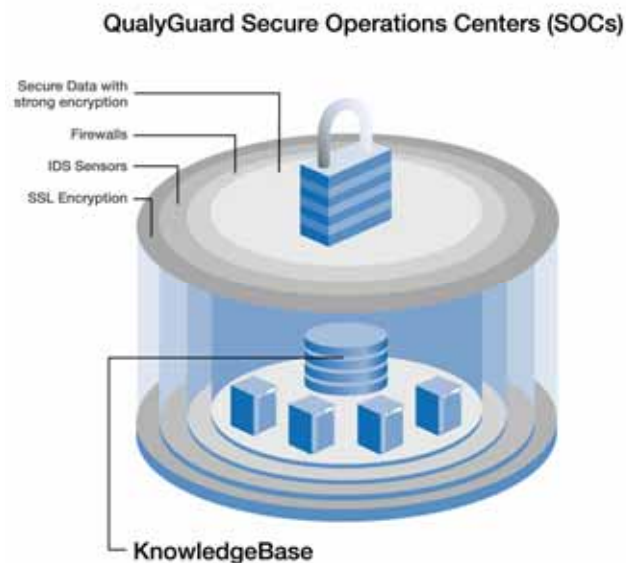
Our team of dedicated security experts monitors the QualysGuard datacenter for any potential vulnerabilities and exposures.

Individual report data within the report database is protected via strong encryption, where the key material is derived via the individual customer's username and password. QualysGuard also leverages password salting techniques, designed to defend against password guessing attacks. There is no centralized password database or key escrow, and Qualys provides the password information required to decrypt the individual report data only to the applicable customer. Qualys and its employees do not have customers' password information, and therefore have no access to customers' vulnerability report data.

All network traffic in transit between the QualysGuard datacenter and the end user is encrypted through SSL. At no point does Qualys save or transmit any report data in clear-text. Only when report data reaches the end user via SSL is it displayed within the end user's browser for viewing.

## The QualysGuard Secure Operations Center (SOC)

The primary Qualys Secure Operations Center is located in Santa Clara, CA at a Cable & Wireless secure datacenter facility. This datacenter successfully completed a SAS-70 audit on their access methods and controls. All Qualys machines and racks are in a locked, private vault that requires the use of a badge and biometric authentication for access. Only designated Qualys employees are allowed access to these racks.



The QualysGuard service infrastructure is isolated from other systems within Qualys and only designated employees have access to this infrastructure. All critical systems are configured with a host-based firewall, a policy-driven file system and an integrity checking system. Additionally, critical systems require two-factor authentication technology to obtain logged access.

Qualys uses a monitoring application designed to assure that all certificates in use are renewed in a timely manner. Also, Qualys' trusted certificate authority, VeriSign, uses a

management system that provides alerting and generates a record in a Qualys internal ticketing system when a certificate renewal is pending.

## QualysGuard User Authentication and Communication Security

All user interaction with QualysGuard requires HTTPS (SSLv3) connections from the user's Web Browser (strong crypto only) to the QualysGuard Secure Operations Center. QualysGuard does not support any clear text communication to navigate the user interface, launch scans or run reports.

QualysGuard currently supports username/password and two-factor authentication (SecurID) for login through an HTTPS connection. The user password is not stored anywhere on the QualysGuard servers. Neither Qualys nor its employees have access to user passwords. The QualysGuard database contains the MD5 hash of the user's password, which is created during account setup and is used for user authentication. Additionally, the MD5 hash contains a salting value designed to defend password brute forcing.

At login, the MD5 hash of the user password is compared to the hashed (MD5+random salt) value stored in the database. Once the username and password have been authenticated, a user session is initiated and the session-id is sent and maintained via a browser cookie with automatic session timeout. The browser cookie does not contain any session information other than a unique session-id.

If a user does not remember the QualysGuard password, Qualys cannot recreate the user's password. QualysGuard passwords are unique to every user and are randomly generated by the application. Machine-generated passwords are initially used as a security mechanism to avoid weak passwords. Customers can configure expiration and lockout policy for account passwords. In addition, account managers can allow users to define their own password. If this is enabled managers can also enforce password minimum length and complexity requirements in addition to expiration and account lockout settings. Passwords can be changed as often as necessary. When users request a new machine-generated password, they are sent a link to the QualysGuard application. This is a one time, one use link which is accessed via SSL/HTTPS. Only when the link is activated by the user will the password be generated in memory, hashed and then stored as a reference for login. Passwords are never sent in clear-text via email or stored in clear-text on disk. If the password is forgotten or lost, Qualys cannot recover the password or the customer's vulnerability results. Consequently, the vulnerability result information is lost.

## QualysGuard Vulnerability Data Encryption and Protection

Customer vulnerability data is encrypted on a per-customer basis and then stored in the QualysGuard database. The encryption algorithm used is Blowfish-CBC without IV. The vulnerability report key is 96 bits long and is randomly generated per customer account. This vulnerability report key, which is used to decrypt vulnerability information, is unlocked with the information provided by the user during login. Qualys never writes this key to the disk in clear text, nor stores it anywhere other than memory. Therefore the vulnerability results data is encrypted before it is stored in the database on a per-customer basis. Not even a Qualys Administrator, with full privileges, is able to read the

customer-related vulnerability data. An example of such an encrypted database record (base64 encoded) is shown below.

```
SELECT report
FROM scan
WHERE reportref='scan/1042582990.24379';

/4wvKKJLT0/8IGP0nizrBn8FC8EwCjv5lpD2NRK/B1fe0cJjKERW5XcJ86F6ulpzHDx33ELkgPd
u+/1cPttAPX0vALUwVirjWDjdXcEu8A5Ga9qmsEK5CaI7xvKegJZcinTPLAiZ3QYsETPcMzGOqx
rsMIsQ5QzU4IA9xP6MnixB/bcDcfsR4zOK+ikau3uBg3s30sknOg70z5brMpqgW6ps+7jupuFvW
PoB5ERFq60UrPZZycdJ3c75K0xmaWIJnWGkTH42TZQm5zRx7n4KvQnmzbOs/FBVjiSw7JUHDcno
X2VeGw/+t6BSOouuD/vGjbtLFxH0iN7ZJvvXMi+ErY7e/fS3OQnm12bb7tTuz3xWRXgVm1D02Nz
3A6AzdB5eDVytSs/tLQz7parkw+j1zrix8qhVlG5uSDvR5sBJJuQiXipa4ZhfMcvlRqmZS0lCpv
li3qr//GCTez+aLtvk+6nYJ49+QY1IMVwu9TDFs+IX7QFSRMBDExnaEwQc6xTwLXDq+aIRtUujJ
ZOKwk8fI29fI3Wfzmxtp+w89QPEeSWdBnRJEDUC3ST7+8jTlsgDpdBCX1aWshzC/1XN8kVCZmL
UMLW0a9cnYvx/3uCrOpaoJaehj6N3EfhAbdOyqMnbTyrsovKh7V74OCRvIKBhejgvNpUy1pF9U
A9emPf3GGAMvERUtTtQtOPxMbAxopj2sky2mx7uGw3BparAeL/5P2xvT/zLCw4kbrjqrlXx5PCA
vNRormQ8HCzmxHly7DytXKvCelJGbdYm4PDFn+LliBFlyiHC867M+qaWVWs0JIBY/Tx/aFVzDPs
8cNUl/7aQ/7eNbupKYSq8gr9FMtW91IOa9lySd9zXnKQcvaM7TdeJBXzKKQE9auJgLVz4WUijz
ahq9FSilxrfm+8uBlaxBjWXnmNYgjubQe/kPKMb+UO09Ork3ZqQBdEidgLM4dF44YXPKr4rakjo
eWmkmBaFGu0csb3QWueaMj75K0fun7Br92cEomUhdPtJNJ0U0J0aDzsxj2vPO8kLPbTM2lpUf7
22sVA5wzHRTH/u37uom3BzxbOkW5hsDBcDmoy547Q0i0A7h9BDD/EOjWvTbKR+EJZo7Uph19k85
lqOd3GnxhXg34Cl76fqRVF2egx+HYs3b6Cd93g++hdYXrllCyU4I5esq5+WW9TRVmLQM0HT5DY3
7Tcz3QFSK0wqtoHtJpU8mFIK92r05fH5kQc/9sluTQh4viDZRsvrrQGLBP5IHfphY/FdKLU3ivy
6UwmWrPia8IPb1O4dbwEgLJxJdXsJNRSdReB2dLGHr9msk1j9vCixpmhGJXLXfaMQSn7BKuzqf5
JuUBfqRQz17cab2KiPP8JtVgnpWxfzJYxBmMsGfjb60zbUisrl/mAo3l3xL6s9z7o2o5mw77z7S
kkFgd0CG6qxGj25ox5E9AFGeD3zZsGeVLnv548ZpMri+rDMS9CBAxp6URKAKBFybc4FVpw0B2b6
nUN5ssuFk//2GSFAC5PjJ3/d3sB7aUPY3wajjc9zbOXuj85Die5ut6qtKYLHAdBWDLRB0QJ97JR
Sg5vgd2NPFuMkFDKZPZCcea0SbYMsA9GC0A19Tp7q/22YH2faRrSByZs8Jk7JSp8jiPCymB2lJh
awgnVfnKHGpk2H9NDiDiX+hiB46J5kuri7DUec/SI2/xN1IT1LZEIpyZLobEmBVJzn9nxyzBiGs
.....
```

The QualysGuard security architecture has been reviewed by independent third parties. Most recently @stake performed a security architecture review as well as a penetration test, and found the security of QualysGuard exceptional. The @stake assessment report is available upon request from Qualys. Additionally, Qualys' data storage model has undergone a SAS-70 audit by E&Y. This report is also available from Qualys upon request.

## Qualys SOC: Monitoring and Availability

QualysGuard is a fully automated Web service that is available to customers 24x7x365. The QualysGuard Secure Operations Center is built upon a redundant and load-balanced architecture for its critical systems.

Qualys has a dedicated staff of qualified security engineers to monitor and maintain the QualysGuard infrastructure. As part of the hiring process, these employees undergo third-party reference and background checks, and sign confidentiality agreements. Additionally, Qualys employees are required to use two-factor authentication technology to obtain logged access to critical servers.

New vulnerabilities are immediately assessed and respective remedies are applied. Additionally, a robust firewall, integrity checking and IDS architecture is implemented to protect against and monitor any attacks. Qualys also maintains log files from its Web servers. As they are created by the Web server, they do not contain any vulnerability-related information. Web logs store the connecting IP of the customer, but do not store

information about the IP addresses being scanned. A sample from the Web server log (requesting IP address replaced by xxx) is enclosed:

```
xxx.xxx.xxx.xxx - - [14/Jan/2003: 14:22:57 -0800] "GET /fo HTTP/1.1" 301 234 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" SSLv3 RC4-MD5
B5A85AE75F1D4354F86BE623C48CA42DEC895333CDE5A21FF830DA28C747A78
xxx.xxx.xxx.xxx - - [14/Jan/2003: 14:22:58 -0800] "GET /fo/ HTTP/1.1" 200 202 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" SSLv3 RC4-MD5
B5A85AE75F1D4354F86BE623C48CA42DEC895333CDE5A21FF830DA28C747A78
xxx.xxx.xxx.xxx - - [14/Jan/2003: 14:22:58 -0800] "GET /fo/user_login.php HTTP/1.1" 200 985 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" SSLv3 RC4-MD5
B5A85AE75F1D4354F86BE623C48CA42DEC895333CDE5A21FF830DA28C747A78
xxx.xxx.xxx.xxx - - [14/Jan/2003: 14:22:58 -0800] "GET /fo/menu.php?noauth=true HTTP/1.1" 200 602
"https://qualysguard.qualys.com/fo/user_login.php" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
SSLv3 RC4-MD5 B5A85AE75F1D4354F86BE623C48CA42DEC895333CDE5A21FF830DA28C747A78
xxx.xxx.xxx.xxx - - [14/Jan/2003: 14:22:59 -0800] "GET /images/q_menu_bg.gif HTTP/1.1" 304 -
"https://qualysguard.qualys.com/fo/menu.php?noauth=true" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1)" SSLv3 RC4-MD5 B5A85AE75F1D4354F86BE623C48CA42DEC895333CDE5A21FF830DA28C747A78
xxx.xxx.xxx.xxx - - [14/Jan/2003: 14:22:59 -0800] "GET /images/q_menu_top.gif HTTP/1.1" 304 -
"https://qualysguard.qualys.com/fo/menu.php?noauth=true" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1)" SSLv3 RC4-MD5 B5A85AE75F1D4354F86BE623C48CA42DEC895333CDE5A21FF830DA28C747A78
xxx.xxx.xxx.xxx - - [14/Jan/2003: 14:22:59 -0800] "GET /fo/footer.php?noauth=true HTTP/1.1" 200 762
"https://qualysguard.qualys.com/fo/user_login.php" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
SSLv3 RC4-MD5 B5A85AE75F1D4354F86BE623C48CA42DEC895333CDE5A21FF830DA28C747A78
.....
```

## QualysGuard Scanner Appliance Security

The QualysGuard Scanner Appliance is designed as a client-only device, with no services or daemons exposed to the network, and with a specifically hardened operating system kernel designed to prevent shell-code and buffer overflow attacks. In fact, the most recent review by Federal Computer Week (<http://www.fcw.com/fcw/articles/2003/0609/tec-scan-06-09-03.asp>) concluded that the QualysGuard Scanner Appliance is masterfully hardened against intrusions.

All communication between the QualysGuard Scanner Appliance and the Qualys Secure Operations Center is encrypted (strong crypto), leveraging SSLv3 outbound connectivity via port 443. The QualysGuard appliance communicates with the Qualys SOC for downloading updates and new vulnerability signatures as well as job requests for network discovery and scanning. The QualysGuard appliance does not keep any scan results; instead, all data is transmitted using encryption and then stored encrypted at the Qualys SOC. Update packages are digitally signed by Qualys during the release process and validated before installation at the appliance.

Initial configuration (IP address, DNS, Proxy, ...) of the appliance is accomplished via the built-in LCD panel and keys. This includes the QualysGuard username/password used to authenticate the appliance with the Qualys SOC through the established SSL connection. After initial installation, the appliance does not require any user interaction, as all application management is done via the QualysGuard Web-based user interface.