SonarVision Enterprise – Security Primer

Table Of Contents

Section 1: General Policies, Best Practices, and Certifications

OrcaEyes' IT team has an extensive background in network, data, and application security. We remain diligent on a 24/7 basis and take the security of our customers' data extremely personally. Our customers range from health care to explosives manufacturers to government contractors and we have been vetted thoroughly by these organizations as well as third party IT firms.

As a standard we follow both SAS70 and HIPAA regulations. Upon request we can provide a copy of our hosting service's current SAS70 certification documents.

All data transfers are secure. All software is kept patched and up to date. All servers are physically secure. Disaster policies are intact and tested. Servers and applications are tested for security flaws regularly. Documents outlining all of these policies and test results are readily available upon request.

Section 2: Hosting and Physical Location

Part A: General

OrcaEyes' hosting is provided by LiquidWeb (http://www.liquidweb.com). We are hosted on a total of four datacenters. Three at separate locations in Lansing, Michigan, and one in Phoenix, Arizona. The existence of four separate datacenters in two distinct cities and states provides extremely reliable redundancy and failover capability. Should physical disaster befall a datacenter, access to the customer's SonarVision system can be restored in less than four hours (see Section 6: Backups and Disaster Recovery).

The average response time to a phone call to LiquidWeb support is 20 seconds.

LiquidWeb is SAS70 and the certification can be readily provided upon request.

Part B: Physical Security

The OrcaEyes servers hosted at LiquidWeb are protected by top-of-the-line physical security measures.

The datacenters' external walls are made of reinforced poured concrete. Electronic security systems control access to the datacenter itself and all areas. Motion-sensing security cameras monitor the entire facility 24/7/365.

Access to the datacenter is strictly limited to LiquidWeb security staff.

Part C: Power

LiquidWeb's power systems feature extensive fault tolerance and resilience at every layer. Incoming service is routed underground to a dedicated on-site transformer. This system routes to our automatic transfer switch which monitors power quality, and automatically transfers to our emergency generators in the event they are needed. Each facility is also protected by one or more uninterruptible Power Supplies (UPS), featuring redundant battery cabinets and full maintenance bypass cabinets allowing for service and upgrades without interruption of power to our servers.

Liebert Precision power distribution units handle final power transformation and distribution to racks, ensuring clean consistent power to data center equipment.

Each facility has multiple emergency generators waiting on standby, featuring over 24 hours of autonomous runtime before requiring refueling. Each generator is test run at least once a week to ensure they are ready in the event they are needed.

Generator power is activated automatically in the event of a utility failure by the transfer switch. The data center load is maintained by the UPS units with at least 15 minutes of capacity, however this is not necessary as the generator is active and up to speed within 10 seconds of a power failure.

Part D: Environmental

Environmental processing systems include redundant Liebert Precision 22 ton up flow air conditioning units. Temperature and humidity are precisely regulated year round to ensure optimal equipment reliability. Each unit contains independent compressors and cooling loops to

further enhance fault tolerance and reliability. Air filtration systems actively remove foreign particulates from circulation and cycle the entire data center air supply in a matter of minutes.

Section 3: Data Security

Part A: Data Transfers

OrcaEyes supports just about any possible method of file transfer method that is used by commercial organizations. We are sensitive to the private nature of the type of data that we collect, and as such, go above and beyond to protect said data. As a best practice we encourage all clients to use the highest level of transfer security their IT infrastructure allows for. The following transfer methods are supported:

- SFTP (recommended)
- FTPS
- FTP (not recommended)
- HTTPS
- HTTP (not recommended)
- Secure Email
- Email (not recommended)

We can either provide you an OrcaEyes FTP server to send the files to, or our parser can connect to an FTP server the client provides and sweep for new files.

Further, we also are able to hande file encryption methods such as PGP (recommended) or even password protected zip files.

Our IT team will work diligently with you and your IT staff to accommodate whatever security controls and requirements your organization requires.

Part B: Data Retention

The data files collected by OrcaEyes are used to populate our (encrypted) secure databases with the necessary data. Once the data files are collected and parsed into our database, they

are deleted from the server. The raw data files do not get backed up by our automated backup process.

In short, the files are only used as a data transfer method and once the proper data is inserted into our database, the files are removed from the server.

Section 4: Server Security

Part A: Server Hardening

Upon provisioning, all servers undergo a hardening process. This includes security processes and server stress testing.

The server hardening process includes:

- Initial firewall setup
- HTTP intrusion protection
- Setup of daily security audits
- Removal of root FTP access and other unnecessary superuser access
- Rootkit detection and prevention
- Mod_Security setup for detection and prevention of HTTP exploits
- Unnecessary process elimination
- Unnecessary package elimination
- Securing of temporary directories
- Directory permissions check and securing
- Daily security audit setup
- PAM resource hardening
- Sysctl Hardening (Modifies kernel operating values to strengthen TCP/IP stack against various attacks including SYN-floods)
- Initial hardening of Apache based on best-practices

The server stress test process includes:

- Stress/Quality test of CPU, Memory Subsystem, I/O Subsystem, and Hard Drives
- Memory Test

- Operating System update check
- Kernel update check

Part B: Firewall Policies

All OrcaEyes customer servers come with firewall services. As a standard, we use an APF firewall which is an interface to iptables. This is an application-based firewall that resides on the server. Should a physical firewall be required, we can provide one through our hosting services (at additional cost). The hardware firewall option is from the Cisco 5500 series and a range of options are available.

Customer firewall policies are simple. All unnecessary TCP and UDP ports are closed by default. Generally on a customer webserver, the only ports left open are HTTP, HTTPS, and whichever port is used for data transfer (generally port 22 for SFTP).

Open ports can be restricted to customer network IP addresses or subnets for further security.

Part C: Penetration Testing

As part of our standard data security policies, OrcaEyes performs routine monthly penetration tests on all company and customer servers. A range of tests are performed to uncover any potential security flaws, vulnerabilities, or unnecessary pinholes.

Penetration testing includes:

- Port scanning
- Brute force testing
- Dictionary based login/password discovery attempts (our dictionary is over a gigabyte)
- Extensive exploit attempt testing
- DDoS load testing and benchmarking

Should any threats be identified, our IT team works to immediately correct them within 24 hours.

A copy of our monthly penetration test of our central demo server can be provided upon request (customer servers are configured identically to this server). Upon request, customers are provided with penetration test results of their SonarVision server(s).

Customers have license to perform independent penetration tests of their OrcaEyes server, but by doing so void any uptime service level agreements for the month in which the test was performed.

Section 5: Backups and Disaster Recovery

Part A: Backup Policies

OrcaEyes backs up all customer and corporate servers regularly. All OrcaEyes code is backed up on a nightly, weekly, and monthly basis. All customer data existing on customer servers is updated on a nightly, weekly, and monthly basis.

The nightly, weekly, and monthly backups are full backups of all OrcaEyes code, all customer data stored in the database including SonarVision configuration information, and all security, service, and application settings on the server. The most recent of each type (nightly/weekly/monthly) is retained.

All backups are stored in three places for redundancy:

- In a secure directory on the customer server itself (in either Lansing, MI, or Phoenix AZ LiquidWeb datacenter)
- On secure OrcaEyes server in Austin
- On physical media at secure OrcaEyes location in Austin

All backups are encrypted using an extremely secure password that is 20+ characters in length and using uppercase and lowercase letters, numbers, and symbols. Each customer has a different password.

Example password (not an actual Orca password): *rapatru9u5&ha7uHa

Our current backup password for our demo system would take roughly 1.15 thousand trillion centuries to crack.

Part B: Disaster Recovery Policies and Testing

OrcaEyes has very robust disaster recovery policies. Due to the resources available to us through LiquidWeb and via the software that we use for our servers, restoration of customer service is a very fast and simple process. Servers can be nearly instantaneously provisioned

through LiquidWeb. A server image that OrcaEyes backs up monthly is pushed out to the new server rapidly (which avoids almost all configuration tasks). Patches are applied quickly.

Our stated goal is to have service restored within 6 hours of an incident. However, our internal goal is to have service restored within 4 hours.

We are prepared and have scenario plans for various types of scenarios, from basic “oops” incorrect user input/overwrite, to server data loss, to physical server issues, to “total disaster” scenario representing a complete server loss (IE server fire).

Our disaster testing is done on a “total disaster” scenario. Preparing for the worst-case scenario is generally best practice for disaster recovery.

Disaster recovery tests are set up to simulate real world scenarios as closely as possible. The technician performing the test is not notified when the test will be. He or she is given a 120 hour window (12:01am Monday to 12:00pm Friday night), and a server outage simulation (all TCP ports disabled) happens at a fully random (done from cron job and script) hour sometime within the 120 hour window. For a successful test, the SonarVision software must be restored onto a newly-provisioned server, with verified customer data, within four hours.

If the technician does not successfully fully restore the SonarVision software and services within four hours*, the IT staff will analyze why the test failed, make improvements to the process, and re-test until the test comes in under four hours.

* - This has never actually occurred. The longest DR test was finished in 3 hours, 42 minutes.

We will be happy to provide customers with a copy of our most recent disaster recovery test results.

Section 6: Application Security

Part A: Password Policies

OrcaEyes maintains rigid password policies in all areas. Server (root) passwords, service passwords (SQL password, etc), Orca technician passwords, and customer login passwords all have secure policies enforced.

	Minimum Length	Required Character Type	Expiry Period
Root passwords	20	Alpha upper, alpha lower, numeric, symbol	90 days
Service Passwords	20	Alpha upper, alpha lower, numeric, symbol	90 days
Technician Login Passwords	12	3 of the 4 following: Alpha upper, alpha lower, numeric, symbol	30 days
Customer Login Passwords	8	3 of the 4 following: Alpha upper, alpha lower, numeric, symbol	90 days

Part B: Vulnerability Testing

OrcaEyes performs monthly vulnerability on all corporate and customer servers. These vulnerability tests scan all web pages, application files, web directories, and any other outward-facing files accessible to the cloud. The exploit and test database of our application scanning tool is updated prior to all tests, to ensure all tests are current.

Vulnerability testing includes:

- Version Checks
- CGI Testing
- Parameter Manipulation
- MultiRequest Parameter Manipulation
- File and Directory Checks
- Application Checks
- Text Searches
- Weak Password Tests
- Cross Site Scripting Tests
- Exploit Tests (from internal DB and Google hacking database)
- Various Other one-off tests
- And more

Should any vulnerabilities be found, they are rectified by the OrcaEyes IT staff within 24 hours.

Customers have license to perform independent vulnerability tests of their OrcaEyes server(s), but by doing so void any uptime service level agreements for the month in which the test was performed.

Section 7. Patches and Updates

Part A: Initial Setup

As part of initial server provisioning, all applications and services are immediately brought to current. Using yum and rpm, all packages installed on the server are checked for currency, and the most recent stable version of all packages and applications are installed.

The technician then manually checks the versions of Apache, SQL, and PHP to verify that they are up to date. If a new version is found, the technician manually installs it.

Part B: Ongoing

All OrcaEyes servers are configured to check for updates to all installed applications and services over each weekend. If a newer version is found, it is installed automatically. As part of the Monday morning IT process, technicians check the logs of each server to verify completion and successful updates of any applications.

If a new version of a critical app (FTP, Apache, SQL, PHP, etc) is made available, it is installed on all servers within 24 hours. Updates are generally done at night to avoid service interruptions, with the only exception being if failing to update the software presents a major security threat.

Part C: “Zero Day”

The OrcaEyes IT staff is subscribed to several leading news groups, RSS feeds, mailing lists, and even Twitter accounts that post information on newly found exploits and vulnerabilities that could expose our customers.

Upon receiving information about any of these vulnerabilities that might affect any customer or corporate servers or applications, the OrcaEyes IT team works to immediately rectify this flaw. They are under orders not to perform any other IT tasks until the vulnerability is patched on all servers.

On top of our own measures, LiquidWeb also has staff whom monitor for new application and operating system vulnerabilities, and patch appropriately.

Section 8. Customer Exit Policies and Measures

Once an organization is no longer a customer of OrcaEyes, we perform an exit process to clean all customer data and information from our servers.

- All SQL databases wiped
- All backup file on OrcaEyes are deleted
- All physical backup media is destroyed
- 7 cycle full deletion of server hard drive on former customer server

If customer has other requirements, these can be accommodated at an hourly rate.

Section 9. OrcaEyes Internal Controls

Part A: IT Staff Access to Customer Servers

Only members of OrcaEyes IT and technical teams have access to customer servers. Rather than the root password or another global administrator password, each IT member has a unique login to each customer server, to allow for best practices upon employee termination and improved auditing and security. Only three company officers have the root password to servers (Dan Hilbert, Brad Hilbert, Chuck Bardwell).

Part B: OrcaEyes Post-Termination Measures

Upon termination of an employee, a post-termination process will immediately begin. This is a checklist of items to ensure that the employee no longer has access to any sensitive data.

The checklist includes:

- Disabling of employee email and password change
- Disabling of employee accounts on all customer and corporate servers
- Changing of backup file passwords for all servers employee had access to
- Return of all company property (including laptops, computers, sensitive documentation, file storage devices, backup media, etc)
- Notification of OrcaEyes' customers who employee has had contact with or done support/programming for (let the customer know the employee is no longer with us)

Appendix A. Current Versions of Server Software

Operating System: CentOS 5.7

Webserver: Apache v3.7.2

Database: MySQL 5.0.92-community

PHP Version: 5.3.8