



WHITE PAPER



SITECATALYST SECURITY

Ensuring the Security of Client Data

June 6, 2008

Version 2.0



1 Omniture Security

The availability, integrity and confidentiality of client data is of paramount importance to Omniture. To ensure the security of client data, Omniture has identified the network, hosting facility, corporate office, and employee processes as the areas in which to focus security efforts. The SiteCatalyst Security white paper describes the proactive approach and procedures followed by Omniture to maximize the security of each area.

1.1 Network

The security of the SiteCatalyst network is highly important to Omniture because of the data collection and reporting activities taking place. Network security is based on the following items.

- Password protected user access
- Segregated client data
- Secure management
- Firewalls and load balancers
- Intrusion Detection
- Non-routable, private addressing
- Service monitoring
- Data backups
- Notification

1.1.1 Password Protected User Access

In order for a client to access their data, he or she must authenticate with a username and password. All users are required to transmit this information over SSL-encrypted channels to prevent it from being intercepted. SiteCatalyst can restrict the types of passwords users can create to access SiteCatalyst reports. Passwords are created and administered by designated client administrators. When enabled, all system user passwords must meet all of the following criteria.

- Be at least eight characters long
- Contain at least one symbol or number, but may not begin with the symbol or number
- Cannot be found in a dictionary or contain words from an English dictionary
- Not contain three consecutive characters from the login name

1.1.2 Segregating Client Data

Data is placed into separate databases (report suite), and a single client's site reports are grouped together on one or more servers. In some cases, more than one client may share a server, but the data is segmented into separate databases. The only access to these servers and databases is via secure access by the SiteCatalyst application. All other access to the application and data servers is made only by authorized Omniture personnel, and is conducted via SSH over secure management connections.

1.1.3 Secure Management

All management connections to the servers occur over encrypted SSH, SSL, and VPN channels. Omniture has deployed private network connections from our corporate office to our data center facilities to allow secure management of our servers. Management access from the Internet is denied by default unless the connection originates from a list of trusted IP addresses.

1.1.4 Firewalls and Load Balancers

All Internet connections, other than those to allowed ports (80 and 443 for HTTP and HTTPS respectively), are filtered out by the firewalls. The firewalls also perform Network Address Translation (RFC 1631). NAT is a process that masks the true IP address of a server from the client connecting to it. The load balancers proxy incoming HTTP/HTTPS connections and also distributes requests to ensure that momentary load spikes can be handled. Both the firewalls and load balancers are fully redundant, greatly reducing the possibility that a single device failure can disrupt the flow of traffic.

1.1.5 Intrusion Detection

Network Intrusion Detection System (IDS) sensors are placed at critical points in the network to detect and alert on attempts to break into our network. The IDS is monitored and configured to automatically provide real-time notification.

1.1.6 Non-routable, Private Addressing

Omniture maintains all servers containing client data on servers with IP addresses that are not routable across the Internet (RFC 1918). In combination with the firewall and NAT, servers are not directly addressable from the Internet which greatly reduces the vectors of attack that can be tried against them.

1.1.7 Service Monitoring

All servers, routers, switches, load balancers, and other critical network equipment are monitored 24 hours a day. The software responsible for monitoring this system performs over 500,000 health checks per hour probing for data integrity and service interruptions. Temperature probes and power monitoring equipment watch for temperature rises and power spikes to ensure the servers run in an optimal environment without local power interruption. Notifications are monitored by our 24x7 Network Operations Center, who will escalate to the appropriate on-call staff or management until the issue is resolved. Additionally, Omniture employs multiple independent monitoring services to provide several layers of monitoring redundancy.

1.1.8 Data Backups

Every night data backups are taken. These backups are stored and secured in our system on redundant drives on the local network as well as on a tape system. Additionally, backups are rotated weekly to off-site storage for protection from local incidents.

Omniture uses Perpetual Storage, Inc. in Salt Lake City, Utah to store monthly backups of client data. Several characteristics make Perpetual Storage the primary choice for Omniture long-term data storage.

- The vault is centered deep in a granite mountain, protected by its unique location from floods, earthquakes, fires, and man-made disasters.
- By virtue of the vault's location within the granite mountain, temperature and humidity remain constant and meet or exceed all federal requirements for archival storage.
- The vault's unique fire retardant construction is supported by both ionization detectors and the latest fire suppression extinguishers.
- Perpetual Storage has four sources of electric power in case of disaster.

For more information on Perpetual Storage, Inc., go to www.perpetualstorage.com.

1.1.9 Notifications

Notifications are sent to clients for the following types of situations.

- Scheduled maintenance requiring down time

- Outage conditions causing down time
- Security incidents affecting client data

1.2 Hosting Facility

Omniture takes our choice of co-location facilities seriously and requires all facilities to meet the requirements described in the following sections.

1.2.1 Physical Facility Security

All facilities include dedicated 24-hour on-site security personnel who require credentials to gain admittance to the facility. Omniture uses Biometric scanners in combination with a PIN or badge to authorize data center access. Remotely monitored and recorded video cameras provide continuous surveillance. The use of man-traps prevents unauthorized individuals from tailgating into the facility. Additionally, all access to the facility is logged.

1.2.2 Fire Suppression

The facilities employ air-sampling smoke detector systems (such as VESDA) that alert facility personnel at the first sign of a fire, and pre-action, dry-pipe sprinkler systems with double interlock to ensure no water is released into a server area without the activation of a smoke detector and the presence of heat.

1.2.3 Controlled Environment

The facilities are environmentally controlled for temperature, humidity, and fluid detection. The HVAC system is completely redundant and facility teams are available 24 hours a day, every day, to deal with any problems. Environmental monitors alerts the NOC if the environment moves outside of desired parameters.

1.2.4 Backup Power

All facilities provide 100% of the power necessary to run independently of any other power supply. Multiple power feeds from independent power distribution units ensures continuous power delivery. Transition from primary power to backup power is fully automatic and occurs without interruption of service. Redundancy exists at every level, including generators and diesel fuel contracts. Regular testing of the generators under load ensures equipment is ready when needed.

1.3 Corporate Office

Omniture's corporate offices are currently in Orem, Utah (near Salt Lake City). Many companies adequately secure both their hosting facilities and network, but fail to recognize the importance of adequate security at the corporate offices. The following procedures represent the processes Omniture has implemented to protect against security threats:

1.3.1 Virus Protection

Omniture has taken an extremely aggressive position in eliminating virus infections and preventing the introduction of new viruses. All incoming and outgoing email must pass through two independent virus filters. These filters block and quarantine all known viruses as well as any attachments with suspicious extensions. Virus databases are updated automatically. All workstations run real-time virus scanning software to provide yet another layer of protection. The system requires no intervention from Omniture staff or end users.

1.3.2 Facility Access

All employees are issued a key card ID badge for building access. Visitors must enter through the front entrance, sign in and out with the receptionist, have a temporary Visitor ID badge, and be accompanied by an employee at all times.

Server equipment, development machines, phone systems, file and mail servers and other sensitive systems are further kept locked at all times in an environment-controlled server room accessible only to IS staff.

1.3.3 Backups

Each night all data contained on file servers, finance servers and mail servers is backed up to tape. Copies of backup data are periodically taken and stored offsite. Additionally, Omniture retains and archives all employee mail.

1.3.4 Employee Hiring and Termination

Omniture uses a thorough process to hire its employees. A third-party hiring service (HireRight) performs a seven-year background check on the following items:

- National Criminal Database
- Court Records
- SSN History

If the employee will have direct access to customer data, the following additional checks are performed.

- Motor Vehicle Records (MVR/DMV)
- Credit History
- Prohibited Parties (i.e. state/federal registries)

HireRight sends the reports online to Omniture; only two employees from Human Resources are capable of seeing the report. Additionally, Omniture does not keep any copies of the report, but HireRight retains the report for one year.

In the event Omniture must terminate an employee, the employee is notified and removed from the building with their things. Any Omniture property is returned to Omniture. The Human Resources Department immediately contacts the IT Department, which makes the following changes.

- The employee's Blackberry is wiped clean (if applicable)
- The employee's email and VPN access is terminated.
- IT makes an image of the employee's computer, which is retained for two years. The computer is reformatted.
- Their access to Omniture offices and datacenters is terminated.
- If the employee had Live Network Access, all administrative passwords are changed and any access to data centers and internal databases is removed.

1.3.5 Employee Access to Client Data

Access to data is important because it is key to the success of Omniture clients. Omniture has taken measures to ensure that only access to both live data and reporting data is given to the appropriate employees. The following sections contain the Omniture policies and procedures specific to client data access.

Live Network Access

Access to the Omniture Live Network environment is granted only after sufficient justification for such access has been provided, a background check has been conducted, and appropriate written approval has been provided to the respective personnel. A list of those parties approved to have access, including justification for their access, will be maintained and distributed to Omniture's CTO, VP of Network Operations and VP of Engineering.

The following policy is observed.

- Any exceptions to this policy must be approved in advance by Omniture's CTO, or the VP of Network Operations and the VP of Engineering.
- The principle of least privilege is observed, namely only the access necessary to accomplish the required job function shall be granted to the applicable party.
- Each party is responsible to ensure they do not exceed the access needed to perform their work, as defined by Omniture.
- It is the responsibility of parties with access privileges to ensure that unauthorized users are not allowed access to the Omniture Live Network.
- Any system (including personal desktops and laptops) used to gain access to the Omniture Live Network must be verified by the Omniture HelpDesk that it meets the minimum corporate security standard.
- Only approved access methods may be used to access Omniture Live Network resources. The creation of unauthorized tunnels or the addition of any type of access devices is prohibited.
- Use only encrypted communications when accessing the Omniture Live Network from non-live networks.
- The copying or relocation of any client data to non-live networks is strictly prohibited. Exceptions must be approved by Omniture's CTO, VP of Network Operations or VP of Engineering.
- Client data and any information derived from it must be treated as highly confidential, and shall not be disclosed to any third party unless Omniture's CTO, VP of Network Operations or VP of Engineering has specifically authorized such disclosure in writing.
- If any moral, ethical, or legal concern arises, immediately raise such concerns to Omniture's CTO, VP of Network Operations or VP of Engineering.

Reporting Data Access

All access to reporting is logged in SiteCatalyst, including access by support staff, Account Managers, and Implementation Consultants.

1.3.6 Sharing Collected Data

Omniture does not share collected data with any competitors, organizations, or individuals without express written consent of the data owner. Omniture places a high value on the security of data, which will always be treated as confidential.



CALL 1.877.722.7088
1.801.722.0139

www.omniture.com
info@omniture.com

550 East Timpanogos Circle
Orem, Utah 84097

