



Infrastructure and Security Overview

This document was last updated January 26th, 2009.

Physical Security

Decipher's production servers run in three different locations: two in the U.S. and one in the UK. We have a total of six (6) production servers among these three different locations. The operational security of our data-center partner employs ISO17799-based policies and procedures, regularly reviewed as part of their SAS70 Type II audit process.

All of these locations have industry-leading physical access controls, including biometric scanning. Decipher staff does not have physical access to these machines; only certified staff at each facility have access using keycards and relying on monitored electronic security. The facilities are not only physically secure but also fireproof, with modern, redundant backup power and network. In each case, backup media are stored offsite from the production servers themselves, in another secure facility. It is not a coincidence that both of our hosting providers have such similar physical security; being security-conscious ourselves, we sought out providers with modern best-practice solutions.

Transport-Layer Network Security

Decipher has set up a secure network environment, both for our clients and for respondents. We have SSLv3/TLS encryption available on every web page, although it is still the client's option whether respondents will see an encrypted or unencrypted survey page. We also provide a secure upload page, to allow clients with sensitive data to transfer files to us through the web.

For projects requiring non-web-based file transfers, we have experience providing PGP file encryption in both directions, AES-encrypted zip files and a variety of secure transport methods such as FTPS, SFTP, and HTTPS uploads.

Application Security and Maintenance

In our data collection application, we deploy application patches to two separate levels of testing environments, beta and gamma. Only after application patches have been tested by developers and relevant internal staff will we deploy any changes to the production environment, ensuring our high availability and code quality. We currently stand at 99.99% availability accounting for application-level and ISP/network outages.

Where it comes to security in our application, we employ a software scanning firewall that checks for several categories of web-based HTTP attacks, such as XSS (cross-site scripting) and SQL injection. We also ensure that the underlying platform is secure.

Our servers run Redhat Enterprise Linux Advanced Platform, a highly secure UNIX variant. Our support contract with Redhat gives us access to their expert staff and automatically installed security patches. Our staff also follow a number of general technology mailing lists to keep up with security threats at all levels of the enterprise.

Decipher mitigates known web threats through a multi-layered approach: parameterised SQL queries stop SQL injection vulnerabilities; proper quoting of untrusted user parameters stops XSS vulnerabilities as do "httpOnly" cookies. A form security token mitigates XSRF attacks. Finally an application-level firewall (mod_security) stops any other vulnerability we might not have covered and logs possible attack vectors.

Survey Security

Respondents are prevented from re-taking the survey through several mechanisms: the most security requires a unique ID for each respondent to be provided in the survey link. However we can also stop multiple completes by tracking respondent cookies and if desired, IP address.

Email Security

Emails are sent using opportunistic encryption when available. All email servers are secured against relaying (i.e. a third party trying to send emails through them pretending to be us). Authentication systems like SPF and DomainKeys / DKIM are used to digitally sign outgoing email, to prove it originates from Decipher.

Image Security

Decipher's image protection system disables the right click and print screen features as well as watermarks images with a visible or invisible ID (e.g. user email address or unique ID in lower right corner). The watermarked ID can be retrieved from the image if it's lifted. Images can also be presented in a protected state such that they can't be copied by right-clicking on them, even with Javascript disabled.

Note: Right click functionality can be disabled if desired, however, disabling is not effective in all browsers (e.g. Firefox lets one disallow the disabling, but if Javascript is disabled by the user the disable functionality won't work).

Print screen cannot be reliably disabled. Some firms have developed scripts to disable print screen functionality (which work by constantly clearing the clipboard), however, disabling process is only compatible with Internet Explorer v6.

Video Security

Decipher's technology incorporates a streaming video solution with its propriety Digital Rights Management (DRM) security wrapper, a superior security technology endorsed by the Yankee Group. In addition, Decipher's ad testing technology increases compression efficiency by 30% compared to Windows Media Player 9. In other words, respondents see full screen content in noticeably less time.

Media can only be streamed from authorized domains

- Permitted URLs (or FQDNs) are encrypted into video file metadata during the encode process
- The player decrypts the FQDN in the video file, then checks that the server is on that FQDN, if not no decryption and no playback.

In addition, the DRM solution limits the number to number of plays within any time period:

- Permission server delivers a unique user key, which is formatted into a post string and delivered to the user
- User attempts playback, if the key and business rules are valid, playback begins
- At intervals the player sends an updated post string back to the server which tracks each user on the timeline
- If the user exits or loses connection, reconnection via the original URL will cause playback to resume at the exit point.
- If user forwards URL to another user, playback will occur if the business rules return valid parameters via the permissions server

Flash Video

Our Flash formatted videos stream securely, in real time, via the internet. The SWF file sources a FLV file that is hosted on our Playstream server. Pulling the direct link of the SWF will not allow video replay.

NOTE: Although Decipher takes every technical measure to secure media content online, there is no solution that will guarantee 100% security in an online environment. Any content posted online is at risk for pirating. Decipher's security solutions are designed prevent the majority of online pirating practices.

Staff Expertise and Safe Procedures

Our staff with access to the data is required to select strong passwords and handle data with care. We do not keep data on personal machines; all data must be stored only on the secure production servers. Staff computers are secured against viruses and malware with eTrust antivirus software, updated automatically.

Staff with the ability to log into the production machines are Unix-trained and trained on safe data access procedures. All access to these machines is handled via secure encrypted connections (HTTPS, OpenSSH), the most secure encrypted remote access methods available. Staff members with server access are required to change their passwords every 3 months. Clients that create accounts have a wide array of security options such as requiring passwords of certain length or strength, expiring accounts, or removing access to a specific project automatically after a while. Data downloads and invalid access are logged per project. Passwords are stored encrypted on the server.

Only two staff members have administrative access to these machines, each of whom have over 10 years of experience in the fields of secure systems programming and secure IT infrastructure. In addition, there's a documented process in place for staff arrival and departure that ensures Decipher staff that leave the company will no longer have any access.

There is a flexible system in place to determine project access via the portal (e.g. access data? edit survey?). Folders allow granting access to many surveys at once for a particular user, but access can also be controlled individually (e.g. give a vendor access to all projects in a folder --except a particular one). Users can see exactly who has been given access to projects, directly or indirectly.

Audits and Alerts

Decipher runs an internal security audit every three months. In addition, we have been audited by numerous security-conscious clients. These audits have variously checked everything from our application's vulnerability to common HTTP exploits, to ensuring that our staff email connections are encrypted. We have satisfied our clients' need for high security each time.

Clients that create accounts have a wide array of security options such as requiring passwords of certain length or strength, expiring accounts or access to a specific project automatically after a while. Data download and invalid access are logged per-project. Passwords are stored encrypted on the server.

We monitor suspicious activity with an array of protection mechanisms, including the aforementioned vulnerability scanner, and a kernel-level port-filtering firewall. We employ an IDS, which automatically logs exceptions. Alert-level events are mailed to the system administrators at our ISPs as well as to our staff, at the same time.

In addition to this monitoring activity, Qualys regularly scans each Decipher server for known security vulnerabilities.

Contact Information

Decipher Inc welcomes your comments regarding this security statement; please contact us at:

Decipher Inc

5250 N Palm Avenue

Suite 220

Fresno, CA 93704

559-436-6940

www.decipherinc.com