Security Overview Whitepaper

Brainshark Security

At Brainshark, we realize that protecting the information you entrust to us is of paramount importance, and we are devoted to meeting your security needs. As the leading sales readiness solution provider, we want you to know that we not only understand what's at stake, but that we have implemented solutions that provide the level of security you demand. Our efforts to protect the integrity, availability, and confidentiality of your data not only ensures compliance with the laws and directives of the United States and European Union, but also forms the basis of a forward-looking information security program designed to ensure proper protection of any and all information you choose to entrust to us.

Many of the security mechanisms that we employ to protect your information, private data, and communications are detailed within this whitepaper, including:

- Independent Audits and Certifications
- Administrative Controls
- Access Controls
- User Permissions and Roles
- Infrastructure Security
- Application Security
- Independent Verification
- Privacy and Confidentiality

Independent Audits and Certifications

Brainshark is independently certified against the ISO 27001:2013 standard, ensuring that it has implemented and maintains an effective system to manage security, respond to threats, and continually improve its controls. Additionally, Brainshark maintains both the Cloud Security Alliance STAR (level 2) attestation and certification, which requires a granular review of security controls in place. Together, the ISO 27001 and CSA STAR audits converge to cover the gamut of information security processes, procedures, and controls to provide the ultimate level of confidence in information protection.

Beyond this, Brainshark also maintains a TrustArc (formerly TRUSTe) privacy certification and is registered with the U.S. Department of Commerce for the EU-US privacy shield framework.

Administrative Controls

Brainshark realizes that security is not only a technology issue and has put in place various administrative controls to ensure a more comprehensive approach to protection of customer data. Included in these are mandatory background checks for all employees as a condition of hire. We also conduct security awareness training for all staff; this training includes defining what information employees may access, what they may do with that data, and how to best respond to social engineering attempts. Additionally, Brainshark maintains policies and procedures regarding acceptable use, incident response, access controls, and data destruction, among others.

Access Controls

On the technical side, access control is the first level of Brainshark security. If your information is sensitive, it is critical that your company allows access only to authorized users.

To accomplish this, Brainshark offers the following user authentication features:

- **User Provisioning:** In the Brainshark system, usernames and initial passwords may only be provisioned by your company's administrators.

- **Password Protection:** User names and passwords are encrypted and authenticated by the system prior to logging in. Only those users with a valid user name and password combination are granted access. Once a user has been authenticated, (s)he is granted functional authority based on the permission levels set by your Brainshark administrator (see *User Permissions and Roles,* below).

- **IP Restrictions:** Company administrators may restrict access to your Brainshark site to a specific IP address or range of addresses. As such, you may restrict the locations from where your site may be accessed.

- **Single Sign-On:** Brainshark also supports multiple single sign-on implementations, allowing you to streamline authentication processes and tie directly into your existing identity management solution.

- **Restricting Public Presentations:** Brainshark authors may designate their presentations as *Public*; however, company administrators may disable their ability to do so. As a result, company administrators may ensure that only authenticated users may view presentations. Note also that these mechanisms are not mutually exclusive. For example, if a presentation is marked as Public, but you have specified an IP restriction, access to that presentation will be restricted to anyone who is in a valid location.

User Permissions and Roles

Brainshark's implementation of security does not end once a user has been authenticated by the system. Your Brainshark administrator can also designate roles and permissions at the user and folder levels:

- **Administration:** You assign your own Company Administrators, who have primary control over access to content through the ability to add and edit new users. They also designate roles and permissions for each user (viewing, authoring, and/or administering content) and control the folder-based directory structure of your site. By controlling these, the administrator is able to limit a user's access to presentations based on groups and folders. Finally, Company Administrators can designate other Company Administrators and give them full or limited permissions (e.g., permission to administer one or many folders, rather than the entire site).

- **Roles and Permissions:** Your administrators may also limit the permissions of registered and authenticated users, thereby limiting their capabilities within the Brainshark system. A user may be designated as a Company Administrator, Folder Administrator, Author, or Viewer – or any combination thereof. Characteristics of each role is as follows:
  - **Company Administrator:** May administer users, passwords, all folders and permissions.
  - **Folder Administrator:** May administer a subset of folders.
  - **Author:** May create content in a subset of folders.
  - **Viewer:** May view a subset of presentations (folder-based).

Infrastructure Security

Brainshark's privately held servers and infrastructure are housed in tier 4 advanced Internet Data Center facilities operated by AT&T, a leading provider of complex Internet hosting for enterprises. Access to our provider's unmarked, locked, and secure facilities is limited to our operations staff, and controlled by state-of-the-art security and monitoring systems.

In addition, we employ the latest state-of-the-art technology for intrusion detection, security, and firewall services (see below). Furthermore, Brainshark has deployed redundancy throughout the physical infrastructure to provide robust data protection and uninterrupted service. The whole system is designed to eliminate single points of failure. Our climate-controlled site includes redundant power with backup generators, fire suppression systems, redundant data storage and servers. We also use redundant load balancing appliances to evenly distribute data and service requests and increase overall reliability and performance.

Brainshark also maintains redundant stateful packet inspection firewalls that protect the application from unwanted internet guests. These firewalls employ the latest features such as deep packet inspection, advanced protocol screening, flood protection, and intrusion detection. All traffic into the Brainshark site is blocked by default, and only the traffic needed for the application to function (or for administration purposes) is explicitly permitted. As an added protection against data leakage, we have also configured our firewalls to (explicitly) deny any outbound traffic that is initiated from within our production environment. We use Transport Layer Security (TLS) to ensure that all information is encrypted in transit at all times.

Brainshark's servers adhere to rigorous lockdown standards stemming from guidelines outlined in the CIS *(Center for Internet Security)* standards. Unnecessary services and protocols are removed from our systems, and privileged access is limited only to those security functions that are required to run and administer the Brainshark application.

Administrative access to the Brainshark systems is provided via a dedicated management network. Only approved Brainshark administrative personnel are granted access to this management network. Administrator access is via temporary VPN connections using strong encryption standards *(IPSEC VPNs with AES-128 /SHA1 with RSA 2-Factor Authentication)* and close and remove the connection when the administrative task is completed. This ensures complete isolation of Brainshark's production site from EVERY other network. In addition, this management network is never used for transfers of customer data, and secure protocols such as TLS are used to access the network equipment for administrative purposes.

Brainshark also subscribes to and monitors security advisories from all its equipment manufacturers as well as SANS, CERT and other security advisory centers. Critical patches are applied as needed. Other patches are applied on a periodic basis, but no less than once per quarter. All patches and upgrades are required to follow Brainshark's standard change management and testing processes.

Application Security

The Brainshark system also has numerous security controls built into the application itself. These include:

- **Presentation Deactivation:** Authors and Administrators can make presentations *Inactive* at any time, hiding the presentation and any link or reference to it for all users.

- **Presentation Passwords**: Authors may assign a password to specific presentations, thereby restricting access to authorized viewers.

- **Comprehensive Reporting**: Brainshark tracks use at a very granular level and provides administrative reporting that reveal when and for how long users view specific presentations, when presentations were created, detailed information regarding use of the Brainshark Interactive Voice Response Unit (IVR), and more. These reports allow you to keep close tabs on access to and use of your Brainshark site.

- **Password Memory**: User credentials may be remembered in a browser to ease the site login process; however, your company administrator may globally disable that function if desired. Once disabled, users must manually log on each time they use the Brainshark application.

- **Telephony Security:** Brainshark's Interactive Voice Response Unit (IVR; the system that allows Authors to add audio narration to their content over the telephone) is also protected from possible intrusion. Each time an author chooses to add audio to a presentation, Brainshark creates a unique eight-digit Presentation Access Code (PAC) and saves it within the IVR system. The PAC provides user and presentation authentication, ensuring that only the author can add (or listen to) audio for that specific presentation. Each time a PAC is used or a session ends, the PAC is disabled and invalidated. The author must start the process over to obtain a new PAC to access the presentation from the telephone –thereby ensuring that a shared or compromised PAC is not a security risk.

Independent Verification

At Brainshark, we recognize that even the best-laid plans can fall short. That's why we have contracted with a pair of external Vulnerability Assessment Services (Nessus and VeraCode) that run weekly network and application security scans to keep us up to date on any of the latest security concerns that may pop up. These scans examine our production environments, as well as our development code base to ensure that any critical vulnerabilities are immediately discovered. We also maintain an in-house quality assurance team to ensure that we are not introducing any new flaws to our application.

Finally, yearly deep penetration testing and vulnerability assessments are performed by an independent third party security auditor, and any concerns are promptly addressed.

Privacy and Confidentiality

The content created by Brainshark's customers using licensed Brainshark software is the sole and proprietary property of each customer. Brainshark maintains the strictest internal policies to protect our customers' right to private and confidential content. Brainshark allows customers to create their own administrator passwords and limit access to those passwords to their creators, Brainshark employees are not granted permissions to access and/or view customer content. If necessary (and *only* if necessary) to perform customer support and/or services, Brainshark may request permission to access a customer's site and/or content. It is only after explicit permission from your designated Brainshark company administrator that any Brainshark employee would attempt to access a customer's site and/or content for any reason.

Note that, in order to maintain billing data and to quantify and analyze Brainshark site traffic, Brainshark, may from time to time use aggregate customer usage information to assist in performing these tasks. This aggregate usage information, collected without requiring direct access to a company's site or content, is limited to authoring and viewing usage statistics and does not include specific information pertaining to registered users or content.

Customer Firewall Support

Brainshark is a web-based system and is compatible with the vast majority of corporate firewalls and other security systems. It uses only standard Web protocols (HTTP and HTTPS) to communicate and can typically be accessed by corporate end-users behind a firewall or proxy server just as they would access any other Web site. There is no need to open an organization's inbound firewall ports or change network firewall policies for Brainshark use, therefore maintaining the integrity of existing enterprise security measures. Brainshark employs no specialized plug-ins that would require adjustments to firewall ports or network policies that might compromise the integrity of your enterprise.

Conclusion

At Brainshark, we recognize that security of your company's content is vital to your enterprise goals – and that makes it vital to *our* goals. As many of the world's leading companies have found, Brainshark provides a highly secure infrastructure for your company's data and communication needs. In addition to this infrastructure, security options are available throughout the Brainshark application to enhance the privacy and integrity of your data and communication of it. We are committed to making the Web a safer place for the communication of corporate intellectual property.

Contact Us

If you have any questions regarding the information in this white paper, please contact security@brainshark.com for more information.

TRUSTe Certified Privacy

Privacy Shield Framework

ISO 27001 CERTIFIED by schellman

CSA STAR CERTIFIED BY schellman