Security Whitepaper for myDynaVox®

myDynaVox® is a cloud-based storage system that provides critical day-to-day backup, storage, restoration and sharing services to users of DynaVox T10 devices, the DynaVox Compass app, and the DynaVox Compass Editor. Learn how myDynaVox has been built to deliver reliable and secure service within existing networks and security infrastructure.

Introduction

myDynaVox is an online, integrated system that allows users to backup, store, share and restore files across multiple platforms, including the DynaVox T10 speech generating device, iPad®, and Windows® tablet PCs. The myDynaVox site fills a pivotal role in the DynaVox communication solution "ecosystem" because it can meet a wide variety of needs for the users of speech generating devices and for those that support them.

myDynaVox functionality includes:

- Online storage and management of communication pagesets and subsets
- Access to print and video resources that aid in the configuration and use of the DynaVox T10 hardware and DynaVox Compass software
- Instructor and caregiver implementation supports
- Software downloads for editing, Windows, and other utilities
- Sharing of communication pages and pagesets between accounts

myDynaVox is hosted entirely by DynaVox. The service is composed of three main components:

- Information about the DynaVox T10, the DynaVox Compass software, and myDynaVox
- The myDynaVox Portal where each customer is provided with a unique login area for access to their account. A user simply visits the secure site, enters a username/password , and then receives access to their particular user account.
- Access to a dedicated area for users to ask question, get answers, file help tickets, and search for existing Knowledgebase articles specific to the DynaVox T10 and DynaVox Compass software.

Protecting the integrity and the privacy of data associated with customers is a high priority. In addition, to ensure low total cost of implementation (TCI), online support systems must integrate smoothly with a variety of customers' existing security infrastructure and require little IT support. myDynaVox, was developed with both of these goals in mind. Secure from the ground up, myDynaVox uses an ASP model designed expressly to ensure robust and secure operation while integrating seamlessly with your district's existing network and security infrastructure.

Secure facility

myDynaVox software, communication and database servers are hosted in a highly secured Tier 1 data center. Physical access to servers is restricted. The entire site sits in a locked cage that is monitored by security cameras to prevent unauthorized access.

Secure platform

myDynaVox runs on hardened Windows servers with the latest security patches installed. Servers are penetration tested using a third-party enterprise-level security service on a daily basis. The myDynaVox servers are configured to watch for denial of service (DoS) attacks and to log denied connections. Multi-layer perimeter security is provided by a pair of firewalls: one between the Internet and Web servers, another between the Web servers and back-end databases. The system is fully PCI compliant.

Scalable and reliable infrastructure

The myDynaVox infrastructure is both robust and secure. Redundant routers, load balancers, server clusters and backup systems are used to ensure high availability. For scalability and reliability, load balancers transparently distribute incoming requests among myDynaVox servers. For optimal performance, the system load balances the client/server sessions across geographically distributed communication servers.

Protecting customer privacy

DynaVox understands that customers are concerned about privacy. We have a strong privacy policy that prohibits unauthorized disclosure of user or enterprise customer information to any third party. This policy identifies the information gathered, how it is used, with whom it is shared and the customer's ability to control the dissemination of information.

Protecting user data

User data on myDynaVox is stored in a proprietary, compressed file format that further protects personal information from being visible to the casual observer.

User email addresses

Each account user must include a valid email address to successfully use the myDynaVox system. Once entered, the email addresses cannot be re-used or changed.

Disclosure of customer information

To deliver the myDynaVox service, DynaVox must collect certain user information, including first/last name, email address and account-level passwords. Unless expressly authorized, DynaVox will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed services. DynaVox may send service update messages to its users at the email addresses they provided when creating an account.

Even when myDynaVox is accessed from a public PC, no personal data is left behind that could pose a privacy threat. myDynaVox uses an optional cookie to remember a user's username if they explicitly request that using the "remember me" option on login. This cookie contains only the username, but does not contain any personally identifiable information or passwords. Users can block this cookie if desired. After a session ends, browser history indicates that myDynaVox was accessed – but information in the history cannot be used to access the account.

Access to customer information

DynaVox staff members are the only individuals with access to DynaVox servers – limited access is granted on a need-to-know basis for the express purpose of customer support. DynaVox developers do not have access to DynaVox's production servers.

DynaVox tracks domain names and browser types for traffic management. However, this data is gathered in the aggregate and is never correlated with an individual user.

Firewall compatibility

myDynaVox is firewall friendly. It generates only outgoing HTTP/TCP to ports 80, 443 and/or 8200. Because most firewalls are already configured to permit outgoing Web traffic, you do not have to bypass or compromise your district or location firewall.

Protecting confidential data

myDynaVox uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. All traffic between the user's browser and the server is protected with end-to-end 128-bit AES encryption.

Advanced encryption

myDynaVox uses 128-bit Advanced Encryption Standard (AES) in Counter Mode (CTR). In early 2001, after an extensive four-year evaluation process, the National Institute of Standards and Technology (NIST) selected AES as a successor to DES. Originally known as Rijndael, AES was selected because of its computational efficiency, modest memory requirements, flexibility, simplicity, and of course, security. AES is now the U.S. government's designated cipher for protecting sensitive information. Through industry-standard encryption methods, myDynaVox can help an organization implement strong security policies and conform to district privacy mandates.

Password Protection

Any system that allows users to login can be compromised by using weak passwords that can easily be guessed, or by sharing passwords. myDynaVox enforces a minimum password length of 6 characters, and it does display password strength when users are creating or changing their passwords.

Password Recovery

If a user forgets their password, the login screen has a "Forgot Password" link that will ask for their email address. If the address matches the one we have in the system, an email will be sent with a link to allow the user to enter a new password.

Inactivity time-outs

If a user walks away from their laptop or desktop computer, or switches away from the myDynaVox site without logging out, myDynaVox addresses this issue by applying inactivity time-outs. Users are automatically logged out of the website or app if their SSL connection is inactive for several minutes.

Conclusion

DynaVox's approach to security and privacy is simple: Start with a secure hosted service and operational practices that preserve customer privacy. Protect data connections with authentication and state-of-the-art encryption to keep traffic safe. Integrate this solution seamlessly with each district's existing network and security infrastructure. Provide flexible administrative controls for user management. The end result: myDynaVox is a robust, secure education management and delivery system with low total cost of implementation (TCI).

DynaVox

Product information: www.mydynavox.com

For more information on DynaVox please visit
www.dynavoxtech.com

About DynaVox Inc.

DynaVox Inc. is a holding Company with its headquarters in Pittsburgh, Pennsylvania, whose primary operating entity is DynaVox Systems LLC. DynaVox provides speech generating solutions and symbol-adapted special education software to assist individuals in overcoming their speech, language and learning challenges. These solutions are designed to help individuals who have complex communication and learning needs participate in the home, classroom and community. Our mission is to enable our customers to realize their full communication and education potential by developing industry-leading devices, software and content and by providing the services to support them. We assist individuals, families, and professionals with an extensive field support organization, as well as centralized technical and reimbursement support. For more information, visit www.dynavoxtech.com.

©2013 DynaVox Technologies, LLC. All rights reserved. myDynaVox® is a registered trademark of DynaVox Systems LLC., in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.