

# ValleySpeak Project Server - A Security White Paper

## Introduction

ValleySpeak Project Server includes a range of security features designed to provide reliable and transparent security to the user. These features help ensure that the user data is protected at all times. The best security approach is one which does not rely on the user to take action, but protects the user in a transparent manner. ValleySpeak Project Server is designed to do exactly that.

## Understanding Threats

Understanding the security threats is the first step to understanding the security features in ValleySpeak Project Server. Security threats can be broadly classified into 2 categories, namely data related threats and access related threats. Data related threats deal with protection from data loss, accidental or intentional. Access related threats deal with controlling access to data to ensure that only the right people have access to appropriate data.

### Data Loss Threat

Loss of data can result from accidental causes like hardware failure or from failure to do regular backups. At ValleySpeak we understand that your data is more precious than your software. In order to prevent data loss ValleySpeak Project Server provides automatic backup and restore features. All backups are done automatically at regular intervals without any human intervention.

### Exposure of Confidential Data

Being at the center of all your organization's projects, ValleySpeak Project Server can contain a lot of confidential information. Protecting such information from prying eyes is essential for the success of your company. ValleySpeak Project Server is designed in a way that guarantees that only users with appropriate access get to see only what is relevant to them.

### Attacks by Malicious Code

The Internet can be a very hostile place with widespread and easily available mechanisms for malicious attacks. Some of the most common forms of attack are denial-of-service attacks, network penetrations, and "smash-and-grab" attacks. ValleySpeak Project Server lowers the risk of such attacks by closing all unused ports and tightly controlling the open ports.

### Viruses and Macros

Viruses are programs that take over the functioning of resources of your computer. They then quickly replicate themselves and try to infect other computers. Macro viruses propagate by using the Microsoft Visual Basic® for Applications (VBA) macro language. Being Linux based, ValleySpeak Project Server does not share any DNA with Microsoft Windows family of products. This makes it immune to all Windows borne threats from viruses and macros.

## Security Technologies in ValleySpeak Project Server

ValleySpeak Project Server contains several features that help ensure the safety of your working environment. A basic understanding of how these features work will help create a

secure environment for your users' data. There are six key features that safeguard ValleySpeak Project Server from the risks described earlier in this paper.

- Built in firewall
- 128 Bit Encryption
- Security hardened environment
- Automatic data backup and restore
- No Console Access
- Strong Logging

### **Built in Firewall**

ValleySpeak Project Server includes a built in firewall that protects it from network borne threats. The Iptables based firewall ensures that users can only connect to the server using port 443 for HTTPS and port 3306 for ODBC. All other ports are closed. This drastically reduces the number of network borne threats that can effect Project Server.

### **128 Bit Encryption**

All interaction between the user and ValleySpeak Project Server takes place using a secure browser which is capable of supporting 128 bit encryption. This is the same level of security being used by most financial institutions today. Based on digital certificates, this type of communication using the Hyper Text Transfer Protocol Secure (HTTPS) ensures that data is never intercepted during transit. This helps prevent any "man in the middle" attacks.

### **Security Hardened Environment**

ValleySpeak Project Server is a highly controlled hardened environment which contains only the absolutely necessary parts. This means that there are fewer things to go wrong. There are no daemons allowed that can be used to compromise the system. For example, there is no File Transfer Protocol (FTP) daemon. This ensures that there is no way for a hacker to gain access and download files from ValleySpeak Project Server. The environment is designed to pull data inside from the outside world, rather than the outside world having to push data inside. This leads to very controlled access. The server environment can only be managed from inside. This means that all powerful administration tasks can only be done from the browser interface which is protected by 128 bit encryption.

### **Automatic Data Backup and Restore**

This is the main weapon against accidental or malicious data loss. All data on the server is automatically backed up at regular interval without any intervention by the administrator. This ensures that in case of a data loss there is always a backup around to restore from.

### **Access Control**

There are four possible roles that a user can have when using ValleySpeak Project Server. They are Project Manager, Team Member, Executive and Administrator. It is important to realize that these roles can be overlapping. For example, a project manager in one project can be a team member in another project.

#### Project Manager

A Project Manager has absolute control over his or her project. They decide who has visibility on the project. They also approve/disapprove any changes made to any information within their project. This level of absolute control ensures that unauthorized access is prevented.

## Team Member

Team Members have highly limited access to project data. They can only view and modify task information that is assigned to them by the project manager. This ensures that information is made available to those who have permission to access it.

## Executives

Executives have read only access to a project. While they can see all information within a project they do not have the ability to edit or delete any project related information.

## Administrator

The administrator is a *Super User* who has enormous powers to control the server. However administration is restricted to browser access only which is done through 128 bit encrypted HTTPS access. The administrator has read and write permissions over all project related activities.

## **No Console Access**

ValleySpeak Project Server does not allow any kind of access to the server console. This prevents any potentially malicious use of the server. All interaction between the user and the server must happen using either a secure browser or a password protected ODBC connection.

## **Strong Logging**

All user access via the browser are logged, so that in the unlikely event of a security breach, the cause can be quickly identified.

## **Physical Access**

It is important to realize that adequate physical security is important to ensure that an attacker cannot gain physical access to a computer. Such access can be used to steal and modify data. Since there is no need for any console access to ValleySpeak Project Server, it is strongly advised that it should be kept in a locked environment where the only way to access it would be through the network interface.

## **Conclusion**

ValleySpeak Project Server offers a flexible and powerful set of security controls that help you configure macro and application security as appropriate for your environment. These controls can be individually tailored to help provide the best mix of functionality and security for each user and enterprise.

For more information: <http://www.valleyspeak.com>