Rhinoback Online Backup Security Measures

Overview

This document describes the security measures used to protect data in the Rhinoback system. Rhino USA, LLC. Considers data security a top priority and takes all necessary precautions to protect customer backup data from known and unknown security threats.

Contents

Physical Site Security

Rhinoback servers and backup data are located in a secure internet data center with controlled access and 24 hour surveillance. A second data center, also with controlled access and 24 hour surveillance, is utilized as a backup site to protect against a disaster at the primary location. Only a limited number of trusted senior level engineers have physical access to the data centers.

Data Encryption

All customer data stored on the Rhinoback system is strongly encrypted. Customer data is never transmitted or stored in unencrypted form. This includes transmission between the Rhinoback software that is installed on client computers and the Rhinoback storage servers, as well as the data transmission between data centers. The Rhinoback website uses SSL encryption to secure all pages that display or transmit customer data or account information.

Encryption Algorithms

By default, the Rhinoback software encrypts backup data using the Advanced Encryption Standard (AES). AES was adopted in 2001 by the US Government as the encryption standard for data classified as top secret after a 5-year testing and standardization process. AES has been analyzed extensively and is now widely used worldwide. Rhinoback customers can choose Twofish or Triple DES as an alternative to AES if they desire.

Encrypting Key Protection

All encryption and decryption of backup data takes place on the client computer. Data is encrypted before it is transmitted to the Rhinoback servers for storage. When data is restored; the data is decrypted on the client computer after it is retrieved from the Rhinoback storage system. During the setup of the client software on the customer's computer, the user is prompted to enter an encryption key for each backup set. The encrypting key is stored on the customer's computer and is never transmitted over the wire to Rhinoback or any other location. Backup files cannot be decrypted without the encrypting key. Since the encrypting key is never transmitted to the Rhinoback servers, there is no way for any administrator, technician, engineer, or other person at Rhinoback to gain access to your data in useable form. Even in the event of a security breach at the data center; there is virtually no risk of customer files being exposed to unauthorized viewing, assuming that a sufficiently secure encrypting key was selected by the customer.

While customers can allow their encryption key to default to their password, this does not pose a serious security threat. Rhinoback does not store passwords in unencrypted form. Only a hashed version of the password is stored for each customer account. The hashed password cannot be used to decrypt data, even if the customer allowed the encrypting key to default to their password.

Seed Load Encryption

Rhinoback offers users with large storage requirements the ability to seed load their backup data onto portable hard drives and physically ship the data to be loaded on the servers. The seed load data is encrypted and loaded onto the portable drives using the same backup software that is used to transmit the data to the datacenter.

Emergency Restore Encryption

In the event that a customer experiences an emergency and needs to restore a large amount of data; Rhino USA will load the data onto portable hard drives or DVD's and express ship the data to the customer site. Since Rhinoback does not store any data in unencrypted form, the data that is loaded onto the media to be sent to the customer site is already encrypted with the customer's encrypting key. The Rhinoback software can be used to restore and decrypt the data from the media. Note: there is a charge for emergency restore services. Once the drives are returned to Rhino USA, the drives are wiped clean before they are reused for any purpose.

Network Security

Rhinoback servers are isolated within the data centers behind dedicated firewalls. Minimal ports are open and accessible from outside of the physical network segments where the servers reside. Administrative access is tightly controlled and only available to a few selected IP address.

Media Retirement

Rhino USA, is continuously upgrading equipment and expanding storage. During normal maintenance and upgrade operations certain drives are retired. These drives contain strongly encrypted data and they are also members of RAID sets making them virtually impossible to decipher. As an extra security measure, the drives are wiped clean using a multi-pass data wiping technology before the drives are recycled or discarded.

Threat Assessment

Due to the strong encryption of the backup data and customer information, the only known threats that would expose customer data involve the selection and protection of passwords and encryption keys by the customers. Use of weak or easily guessed passwords may allow an unauthorized person to gain access to the contents of your data. See http://kb.rhinoback.com/Article.aspx?id=10073 for more information about setting strong passwords and encryption keys.

Threats involving denial of service attacks are addressed with firewall technology that is configured for maximum protection and stealth.   Physical threats to the data center facilities and severe denial of service attacks are addressed by our secondary data center.   Physical data center addresses are not published in an effort to make a simultaneous attack on multiple data centers more difficult and less likely to affect the availability of Rhinoback backup data. In addition, the Rhinoback network segments at the secondary facilities are completely blocked from public access during normal operation.

Certain detailed information such as network configuration, firewall configuration, router information, data center locations, security procedures, and other security related configuration information is kept confidential to avoid giving potential attackers information that can be used to plan an attack.