



Nirix Hosted Backup Data Security White Paper

Technology Today Utility Tomorrow

ABSTRACT

This document describes the security measures available in Nirix's Remote Backup Agent (RBA) software from a user's perspective. It serves as a reference for customer queries regarding security related questions.

NIRIX CONFIDENTIAL

Explicit written consent of Nirix Technology is required prior to any form of distribution of this document outside the intended recipient.

TRADEMARKS

Nirix Technology and the Nirix Technology logo are registered trademarks of Nirix Inc.

STATEMENT OF CONFIDENTIALITY AND VALIDITY

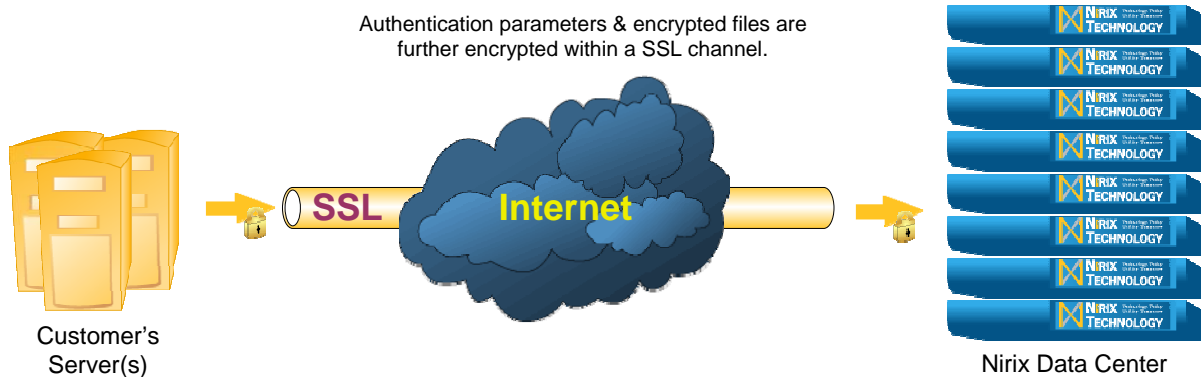
Nirix Technology has prepared this outline for the sole purpose and exclusive use of the intended recipient. Due to the confidential nature of the material in this outline, Nirix Technology requests that this document and its contents not be discussed, disclosed or divulged without prior explicit written consent of Nirix Technology.

© NIRIX TECHNOLOGY, 2001 – 2009. All rights reserved

Secure, Robust and Reliable

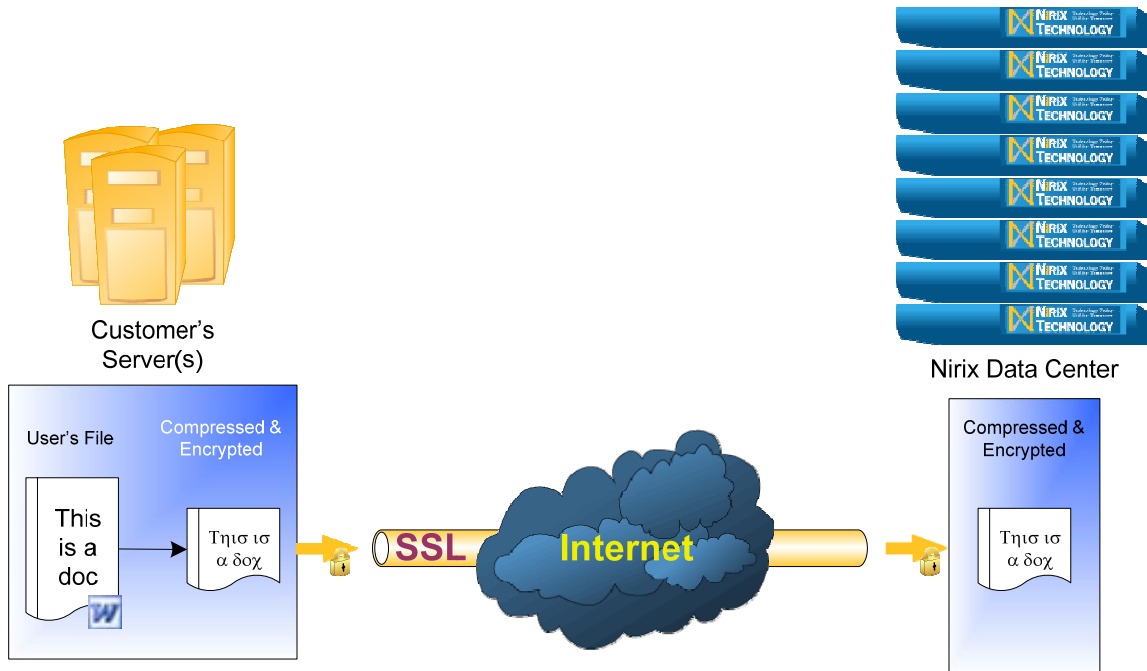
This document describes the security measures available in Nirix's Remote Backup Agent (RBA) software from a user's perspective. It serves as a reference for customer queries regarding security related questions.

Secure 128-bit SSL Communications



All communications between Nirix's Remote Backup Server (RBS) and your computer / server are transported in a 128-bit SSL (Secure Socket Layer) channel. Although all your backup files travel through a public network (the Internet), eavesdroppers have no knowledge of what has been exchanged as all traffic is encrypted.

Backup Data are Securely Encrypted



All of your files are first compressed and encrypted with your defined encrypting key before they are sent to Nirix's Remote Backup Server (RBS). To any one but you, your files stored on Nirix's Remote Backup Server (RBS) are no more than garbage files with random content.

We Don't Keep Your Encrypting Key

The encryption key used to encrypt your files resides only on your computer and is known only to you. It is never transmitted anywhere across the network. If this key is lost, all backup files can never be recovered. Therefore, although we have access to all files you stored on our backup server, we have no knowledge of the content of the files you stored.

NOTE: Please make sure you write down you encryption key in a safe place where it will never be forgotten. Otherwise, you will never be able to recover your backup files if you ever lose this information!

Industrial Strength Encryption Algorithm Used

Currently, the algorithm that we are using to encrypt your files is 128-bit Twofish. It is a block cipher designed by Counterpane Labs. It was also one of the five Advanced Encryption Standard (AES) finalists chosen by the National Institute of Standard and Technology (NIST). It is subject to frequent public reviews and currently no known attacks against this algorithm have ever been reported.

8.77 x 10¹⁷ Years Required to Crack the 128-bit Encryption

A 128-bit key size has 2¹²⁸ or around 3.4 x 10³⁸ possible combinations. Even if you have the world's best super computer, ASCI White, SP Power3 375 MHz manufactured by IBM as of November 2000, it would take 8.77 x 10¹⁷ years to test all of the combinations. Assuming you have the super computer, ASCI White, SP Power3 375 MHz, it has 8192 processors which totals a capability of 12.3 teraflops (trillions of operations/second), available to you. Also it just needs one computer operation to test a possible combination (which is already faster than what it can do). To use a brute force attack (checking all combinations) on this encryption algorithm, it would take:

$$\frac{3.4 \times 10^{38}}{12.3 \times 10^{12}} \text{ seconds} \sim 2.76 \times 10^{25} \text{ sec}$$

i.e. 876530835323573935 years or 8.77 x 10¹⁷ years

to successfully try all combinations. Let alone, the ASCI White can not process as fast as what described here. You can be sure that your data stored on our server is 100% secured.

Restrict Data Access by IP Address

You can also restrict access to your backup files from a set of IP addresses you define. If someone tries to access your data from an IP address that is not on the defined authorized IP list, their access will be denied. This additional security ensures backup files are not open to all locations, even if the web portal username and passwords are known.

If you require more information regarding the Nirix Hosted Backup service, you can always visit our web site @ <http://www.nirix.com> 24 hours a day, 7 days a week or call our customer service line at 1-780-414-1556 to speak to one of our knowledgeable account executives today.