

## **Legend items on the product comparison chart:**

### ***Scales into secure network applications –***

Whitenoise USB security products are designed to upgrade with a user's security needs. The retail Security Suite is designed to provide personal security features and then to be upgraded so that individuals and small companies have access to affordable networks over the Internet with either managed services or self contained enterprise versions of Secure File Interchange.

Our ultimate target market for our USB based security applications is the small and medium sized enterprise that needs secure network communications but cannot afford the prevalent public key network offerings or do not have the technical expertise to manage these complicated network topologies. The Security Suite contains two personal security applications, products that provide encryption and authentication for personal data access on static storage devices (your computer hard drive or removable medium).

As a user's security needs increase and there is a need for secure network communications, these same USB flash memory drive keys can be upgraded to become Secure File Interchange keys. These keys become part of a topology that creates secure networks over the Internet or IP based digital communications systems. Secure File Interchange is a symmetric distributed key network.

A first step is for these upgraded USB Secure File Interchange keys to be used in a managed service context. For a monthly fee, the enterprise has access to a secure Internet portal from their host service provider for secure file/content exchange. A monthly fee for secure network capabilities is affordable to all enterprises.

The next step when the security needs of an enterprise increase is the purchase of a self managed, self administered Secure File Interchange network. Trusted Third Parties are eliminated altogether and the enterprise is self reliant.

This requires just the easy installation of server software and then the enterprise simply manages their keys and their key distribution.

Here we are competing against extra-ordinarily expensive public key networks. Versign estimates a cost of \$400,000 and 12 weeks just to set an enterprise network up. Please read the cost of implementing a Versign network: <http://www.verisign.com/static/005321.pdf>

The vast majority of companies can't afford those networks but all enterprises can afford a secure enterprise network for an average of \$1,000 per user. This scales the cost of secure digital networks in a manner that all companies can afford. A secure network for a 10 person company is \$10,000; a 20 person Secure File Interchange network is \$20,000 etc,

A secure network can easily be set up and training completed in a day or less.

Because of the unique characteristics of Whitenoise keys, these keys provide for ongoing authentication throughout a network session, inherent intrusion detection, and automatic denial of network access to criminal behavior without human intervention. Please read:

[Critical Insights and Differentiators of Whitenoise](#)

***I.O.Data USB drives*** are designed for network authentication (identification of user) but their authentication can likely be circumvented. This authentication additionally only occurs at login, so if it is circumvented there is complete network access to the criminal. Their application does not address the encryption of data or the network ability to securely exchange files.

Sandisk has limited network capability but it is addressed to a different function. Sandisk Cruiser utilities are designed to facilitate the safe mobility of data by carrying encrypted files on the USB drive itself and not by network communications. Its network capability, in its limited state, is designed to try to be able to monitor all the USB drives that are in use by a company. In that capacity the server will store passwords associated with each USB drive in use by company employees and in that capacity can replace passwords in order to be able to recover the encrypted files that are being carried around. This utility still has a security weakness in that access to the encrypted files on the USB drive is still dependent on a password and it is the password that acts as a seed to create unique encryption of the files on the USB drive. Password dependent encryption keys are not considered to be the highest security. It appears that the physical key itself can be copied.

Sandisk is designed to monitor files that are physically being transported by company employees. It is NOT designed to create a secure network to facilitate secure electronic communications over the Internet or IP based networks and as such is limited in its capacity.

## ***Key Recovery***

Key recovery is a critical component for individuals and enterprises. All the competing products appear to create unique encryption keys on the USB drive by using a password that then perturbs a generic device encryption key. This means if the password is lost then the data is lost.

Only Sandisk has a password recovery capability which means that they can recover lost data. However, the encrypted data being transported is protected with a password dependent key, and the key is being carried along with the data, which means it is more vulnerable to being broken or circumvented.

## ***Encrypt files on computers***

This is to distinguish whether files can be encrypted on other computers or storage devices.

## ***Encrypt files on the USB drives***

This is to distinguish whether the utility is designed to encrypt files that are being stored on the USB drive itself. Whitenoise does not ever recommend carrying encrypted files on a USB device since the key to encrypt these files is on the USB device. This means that the encryption is only as strong as the password and passwords are notoriously easy to break. There are many publicly available password breaking utilities on the Internet.

The only way this could be considered secure is to have the encrypted files on one USB drive and the encryption key on a separate USB drive to keep the key away from the encrypted data.

## ***Encryption Algorithm***

This identifies which encryption algorithm is available for use on the product. Sandisk offers AES and other algorithms. Whitenoise Computer File Security offers AES and Whitenoise.

## ***Encryption Strength***

This indicates how secure the encryption algorithm itself is. The higher the bit strength of the encryption, the more secure the data is. As an example, a 256 bit encryption key is 32 characters long. This means that in order to encrypt a 32 –kilo byte file that the key repeats itself 1000 times. The instant a key repeats itself once it is possible to attack the key.

Whitenoise offers AES on all of its applications. However, a user can choose to secure their data with Whitenoise in which case they are using encryption where the keys are a minimum of 240,000 bits in strength and it generates random key streams on the order of  $10^{60}$  in length. With offset management, a key segment is never repeated which means that it retains the characteristics of a one-time pad which is the only encryption that can mathematically be proven to be unbreakable.

## ***Encryption Password or Finger Print Dependent***

Encryption that is dependent on passwords to generate the key are only as strong as the password and NOT as strong as the encryption algorithm being used. For example, if you have a 256 bit strong encryption algorithm, but the key is generated from a 5 letter (5 bytes X 8 bits/byte) password then the strength of the resulting encryption is 40 bits.

Finger Print dependent encryption is a terrible idea from a security stand point. The finger print biometrics we have seen to date are not reliable and the USB keys having finger print dependent authentication or encryption generally offer the ability to turn off the biometric altogether. Because of this, it appears that on all the competitive products that the finger print biometric is for authentication only (logging onto the USB drive or network with the biometric being an authentication factor).

Besides the security of finger print biometrics being debunked in myth busters, see [http://en.wikipedia.org/wiki/MythBusters\\_\(season\\_4\)#Fingerprint\\_Lock](http://en.wikipedia.org/wiki/MythBusters_(season_4)#Fingerprint_Lock) , there is a security nightmare waiting. If you had a company where each employee is encrypting files based on their own finger print, when they leave, the enterprise has no way of recovering these files unless they have taken the fingerprints of all their employees previously or they are backing them up by some means on a server. This raises all kinds of legal and ethical questions and liabilities for enterprises.

If the finger print biometric is used simply for authentication, or identifying the person, then this still can be circumvented and does not provide authentication beyond the network login and does not provide data encryption, intrusion detection or automatic denial of network access to criminals. Once they are in the network the entire network is vulnerable.

## ***Authentication***

Authentication is the electronic identification of a person by a password, finger print, or device specific key. Whitenoise use a password as just one factor of the multi-factor authentication of a person logging on to a specific USB key, but the person is electronically identified by their own unique key which is used as an additional factor for the authentication and securing of data. That key is specifically intended for the securing of data on other storage media and NOT on the USB device itself. This ensures the highest level of security for both personal and secure networked communications because the key is separate from the encrypted data.

## ***Authentication Login Only***

This means the person is authenticated only at logging into the key or network. This is not secure as it can be bypassed by hacking into the network by other means. The authentication technique of just passwords or biometrics by themselves can be circumvented.

## ***Authentication Through-out Session SFI***

This is a distinct feature of Secure File Interchange which is designed for secure network communications. This is accomplished by the use of DIVA. See: [Critical Insights and Differentiators of Whitenoise](#)

## ***Save Passwords for the Internet***

Only Sanwa offers the ability for a user to store multiple passwords for accessing Internet sites. It is a convenient place to store passwords but the USB drive can be broken into, and if it is lost, presumably the person won't remember the passwords they were saving. It is simply an electronic wallet to store passwords and automatically populate login screens when accessing Internet sites. It is a convenience feature and not a security feature as it addresses none of the other issues involved in the proper use of passwords.

## ***Can the key be copied***

This addresses whether a physical copy of the key (all the files on the USB drive) can be copied and used by a hacker.

The following presentation shows why the keys are so strong and why the key streams are so long. It shows how the keys are protected are protected from theft or duplication.

<http://www.wnlabs.com/Presentations/ISC2%20ver%203%20AB%20AES%20DDKI%20narrated.pps>

## ***Password replacement or recovery***

This is critical in order to recover company data that has been encrypted.

Encrypting files to a USB drive to carry around and being password or fingerprint dependent is a bad idea.

## ***Buffalo –***

The following quotes are taken from Buffalo marketing material "buffalo security.pdf".

"Security you control - Data only you can access but be aware **lose your password; lose your data.**"

"Same method as the previous solution. Once received by mail, the attached file must be decrypted for viewing. In order to be able to decrypt the file the recipient must have Secure Lock Ware installed on their PC and they also must be informed by the sender of the password which was set to the file when it was encrypted."

Whitenoise offers the same email utility in its Security Suite application. However, because it is recognized that this technique does not offer the highest level of security, Whitenoise Email Attachment Encryptor utilizes two pass phrases in order to increase the strength of the encryption and to exponentially make more difficult the ability for interlopers to break the password. This

technique is as secure as the ability to safely share the passwords or pass phrases with another user. (See PGP for this class of security.)

256 BIT ENCRYPTION is only supported on a Buffalo work station. Their USB drives only offer 128-bit encryption because of overhead issues presumably.

## ***I.O.Data***

I.O.Data utilities are only designed to manage secure network access with a physical key. It provides no encryption and network communication capacity. It retains the same security issues as the other competitive products.

## ***Elecom***

Elecom appears to be primarily a product distributor. It is likely that their USB offering is white branded from another company. Its finger print biometric USB device faces the same issues as the others.

## ***Sanwa Supply***

<http://www.sanwa.co.jp/product/syohin.asp?code=FP-FL128&cate=9>

[http://www.datafab.com/chinese/product/fingerprint\\_ufd\\_fin010.htm](http://www.datafab.com/chinese/product/fingerprint_ufd_fin010.htm)

Chinese Sanwa distributor of the Sanwa USB disk on key. Uses finger print for authentication and access to the USB drive. I did not see any ability for key recovery.

## ***Sandisk***

USB flash drives offer an inexpensive and convenient way to **carry large amounts of digital information in a pocket or purse**, yet without proper security these benefits become a huge threat to businesses of all sizes,” said Yariv Fishman, product manager for enterprise solutions in the USB business unit at SanDisk. “Cruzer Professional and Cruzer Enterprise are business tools, from a trusted leader in USB flash drives, which help ensure confidential data remains confidential – even if the drives themselves are lost or stolen.”

Cruzer Professional lets the owner establish a secure, **password-protected** “Privacy Zone” that can occupy anywhere from one percent to 100 percent of the drive’s total capacity. The area outside the Privacy Zone is unprotected and is therefore open to any user. Here’s how this can work: A sales executive heading out for a trip puts confidential business plans in the Privacy Zone of a Cruzer Professional, and a product presentation in the public area. Arriving at a client’s office, the executive hands the Cruzer Professional to the client and allows the client to transfer the presentation – without worrying the client might accidentally or deliberately copy confidential files.

For larger organizations seeking more functionality, as well as more efficient management of secure USB flash drives, SanDisk is introducing Cruzer Enterprise CMC (Central Management & Control) server software. Cruzer Enterprise CMC **supports password recovery** and renewal through the network, remote termination of lost drives, **central back-up and restore**, as well as central usage tracking and auditing. CMC is available now, with pricing information provided on request to enterprise clients.

Sandisk has nice capabilities but it is targeted for the maintenance of monitoring the movement of corporate data on removable devices. It is not designed to serve as an architecture to create

secure networks over the Internet for secure communications and secure electronic file/content transfer.

## Whitenoise

Whitenoise™ is patented in the United States of America ([US Patent Number 7,190,791](#)) and in 27 countries who are participants to the European Patent Cooperation Treaty ([European Patent Number EP1566009](#)). It is patent pending in 12 additional countries.

	A	B	C	D	E	F	G
1	<b>USB AUTHENTICATION AND</b>	<b>Whitenoise Computer</b>	<b>BUFFALO</b>	<b>ELECOM</b>	<b>I.O.DATA</b>	<b>SANWA</b>	<b>SANDISK - CRUISER</b>
2	<b>ENCRYPTION PRODUCTS</b>	<b>File Security</b>					
3							
4	<b>SCALES INTO</b>	<b>Yes</b>	<b>NO</b>	<b>NO</b>	<b>AUTHENTICATION</b>	<b>NO</b>	<b>SEE NOTES</b>
5	<b>SECURE NETWORKS</b>				<b>LOG ON ONLY</b>		
6							
7	<b>Key Recovery</b>	<b>YES</b>	<b>NO</b>	<b>NO</b>	<b>NO</b>	<b>NO</b>	<b>YES</b>
8							
9	<b>Encrypt files</b>	<b>YES</b>	<b>YES</b>	<b>YES</b>	<b>NO</b>	<b>YES</b>	<b>NO</b>
10	<b>on computers</b>						
11							
12	<b>Encrypt files</b>	<b>YES</b>	<b>YES</b>	<b>YES</b>	<b>NO</b>	<b>YES</b>	<b>YES</b>
13	<b>on USB drive</b>						
14							
15	<b>Encryption</b>	<b>AES OR</b>	<b>AES</b>	<b>AES</b>	<b>AES</b>	<b>AES</b>	<b>AES</b>
16	<b>Algorith</b>	<b>WHITENOISE</b>					
17							
18	<b>Encryption</b>	<b>AES 256 BITS</b>	<b>128 BIT</b>	<b>128 BIT</b>	<b>N/A</b>	<b>128 BIT</b>	<b>256 BIT</b>
19	<b>Strength</b>	<b>WN 240,000 BITS</b>					
20							
21	<b>ENCRYPTION is Password</b>	<b>NO</b>	<b>YES</b>	<b>YES</b>	<b>N/A</b>	<b>YES</b>	<b>YES</b>
22	<b>or Finger Print dependent</b>	<b>NO</b>					
23							
24	<b>Authentication</b>	<b>YES</b>	<b>NO</b>	<b>YES</b>	<b>YES</b>	<b>YES</b>	<b>YES</b>
25							
26	<b>Authentication Login only</b>	<b>NO</b>	<b>NO</b>	<b>YES</b>	<b>YES</b>	<b>YES</b>	<b>YES</b>
27							
28	<b>Authentication Throughout</b>	<b>YES</b>	<b>NO</b>	<b>NO</b>	<b>NO</b>	<b>NO</b>	<b>NO</b>
29	<b>network session SFI</b>						
30							
31	<b>Save Passwords for the Internet</b>	<b>NO</b>	<b>NO</b>	<b>NO</b>	<b>NO</b>	<b>YES</b>	<b>NO</b>
32							
33	<b>Key can be copied</b>	<b>NO</b>	<b>YES</b>	<b>YES</b>	<b>YES</b>	<b>YES</b>	<b>YES</b>
34							
35	<b>Password Recovery</b>	<b>YES</b>	<b>NO</b>	<b>NO</b>	<b>YES</b>	<b>NO</b>	<b>YES</b>
36	<b>or replacement</b>						