Relevant Technologies, Inc.

Product Review

The CyberAngel: Laptop Recovery and File Encryption All-In-One

By Laura Taylor
November 14, 2003

Executive Summary

Relevant Technologies took the CyberAngel into our labs to test it for our acceptability rating. It worked as advertised, and had more features than expected.

Background

According to the Computer Security Institute's *2003 Computer Crime and Security Survey*, theft of private or proprietary information created the greatest financial losses for the survey respondents. If you are a medical institution, U.S. government agency, or financial institution, information theft can result in violation of patient privacy regulations, loss of customer credit card numbers, unauthorized financial transactions, or disclosure of national security secrets.

While all computers are vulnerable to information theft, laptops are particularly vulnerable due to their portability and ease of theft. Most servers are locked in racks in data centers, however laptops are typically left out on desks where access is easy. If an office visitor walked out of the office with a laptop under their arm, an unknowing receptionist would likely expect that it was the visitor's own laptop and not question it. If you're laptop was stolen, you'd want it back. The CyberAngel®, made by CyberAngel Security Solutions (CSS), is a product that claims to locate stolen laptops and return them to you. Their recovery rate on returning stolen and lost laptops to folks who have licensed their software is 88%. Relevant Technologies took the CyberAngel® into our labs to see if version 3.0 qualified for our acceptability rating.

Installation and Use

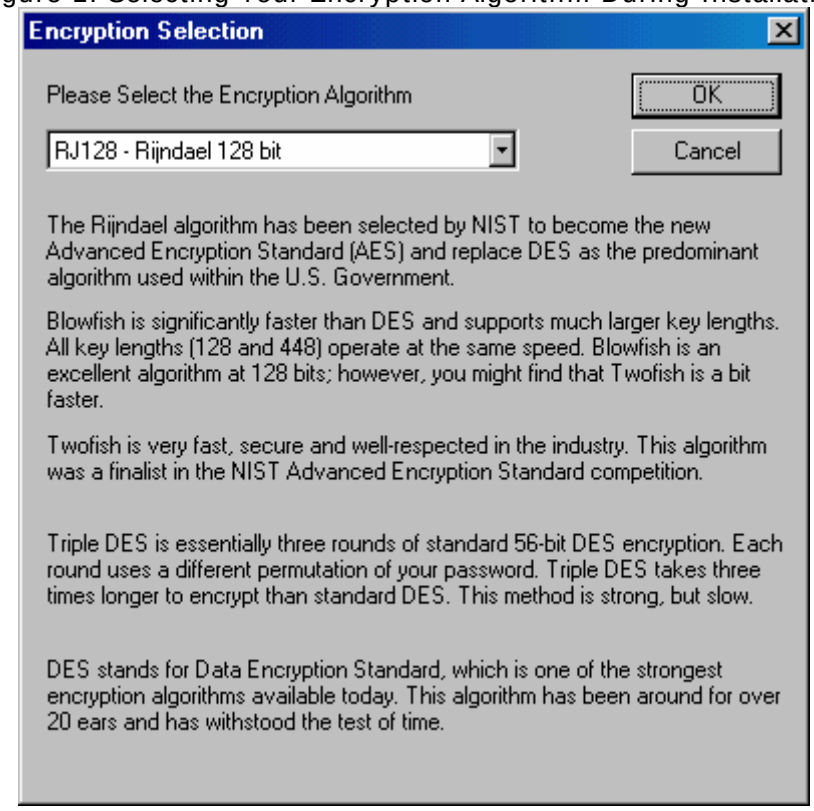
The CyberAngel was easy to install, and the entire installation took less than 10 minutes, including the time it took to reboot the test system. With version 3.0, the CyberAngel includes a new stealthy, secure drive that is protected by strong encryption. The secure drive is a logical drive protected by strong encryption where you can put all your confidential and classified information. During the installation process, you are prompted to select an encryption algorithm to use to protect your secure drive. The choices available are:

- Rijndael 128 bit
- Rijndael 256 bit
- Blowfish 128 bit
- Blowfish 448 bit
- Twofish 128 bit
- Twofish 256 bit
- DES 128
- DES 56

The nice thing about the installation program is that it provides you with background information on each of the encryption algorithms to better assist you in making your

decision on which one to select. Government agencies will like the fact that the NIST AES standard is supported.

Figure 1. Selecting Your Encryption Algorithm During Installation



After the CyberAngel finished installing, we testing the secure protected drive by inserting some would be confidential information (a spreadsheet called PatientRecords.xls), to see if an unauthorized user could access it. To pose as an unauthorized user, we rebooted the system, and failed to provide the correct logon password after reboot. The secure drive was not visible in any way, and when we poked around on the laptop to try to find it, we couldn't find any signs of it, or the spreadsheet dubbed PatientRecords.xls. We then rebooted the system and inserted the correct password, and voila, our secure drive and spreadsheet was back. Between when we inserted the wrong password, rebooted, and inserted the right password, an alert had already been emailed to us notifying us that someone had attempted to use the test laptop without proper authorization. We were sent the 24 x 7, 800 number to call at the CyberAngel Security Monitoring Center if we suspected that the laptop had been stolen.

When the alert email was mailed to us, it included a "Created" timestamp, but not a "Sent" timestamp. We're not sure why the CyberAngel monitoring server did not register a "Sent" timestamp with the messaging server, however, in the body of the email, it did include a correct timestamp of the unauthorized access. This seems to be a problem that is trivial at best, though we'd like to see it fixed in the next version.

When using the secure drive, you need to actually "move" your files into the drive to make them secure. Leaving a copy of the file on your insecure drive will defeat the purpose of using the secure drive. For documents that you'd like to keep secret, you'll have to be sure that temporary and recovery files are also kept in the secure

drive. For Microsoft Word or Excel, this is easy enough to do by going into the Tools → Options menu and modifying the default path for the AutoRecover and Documents directories.

Table 1. Corporate Information

Vendor	CyberAngel Security Solutions, Inc.
Headquarters	475 Metroplex Drive, Suite 104, Nashville, TN 37211
Product	The CyberAngel®
Customer Scope	Financial, Government Agencies, Medical Establishments
Industry Focus	Security for laptops and confidential information
Key Features	Laptop recovery software, secure encrypted drive, 24 x 7 unauthorized access alert service, configuration manager
Web site	http://www.thecyberangel.com
Contact Information	800-501-4344

The user documentation also provides instructions on how to modify your Outlook preferences so that you can move all of your email to the secure drive. Even if you don't anticipate your laptop getting stolen, it's sure nice to know that your email is secure, encrypted, and not accessible unless you know the password unlock the secure drive. Securing email encrypted was a pleasant surprise since it was not a feature we were expecting to see.

You can secure applications, such as a VPN client, by moving them into the secure drive. By moving applications into the secure drive, if an unauthorized user fails to authenticate properly, they do not even see that the application exists on that computer. Applications can also be installed directly on the secure drive.

Figure 2. The CyberAngel Configuration Manager

Though it's not possible for you to configure the alerts to be sent to a second email address yourself, we were advised by CSS, Inc. that this can be setup by calling the CyberAngel Security Monitoring Center. Users may want to setup the alerts to be sent to a cell phone as well as a traditional email account, additional notification paths can be added or changed by calling the CyberAngel Security Monitoring Center. If the laptop contains classified information, the alert could be sent to a U.S. Federal Agency's Computer Security Incident Response Center (CSIRC).
We tested the port locking feature by inserting a wrong password into the password authentication box and then proceeded to try to HotSync some data to a Palm Pilot. The password violation blocked all the COM ports preventing the HotSync from taking place. The port locking feature also prevented us from initiating outgoing communications lines. However, in stealth mode, the Cyberangel initiated a call back to the recovery server to alert it of the laptop's geographic location verifying that COM ports are locked to unauthorized users, but not to the Cyberangel recovery software.

Recommendations

The CyberAngel has evolved into much more than laptop recovery software and works as advertised. You can secure documents, applications, and even your email. You can prevent unauthorized remote access to servers or accounts, and restrict information transfer to PDA's or handhelds. Medical establishments that need to protect patient information as required by the Health Information Portability and Accountability Act (HIPAA) will find the CyberAngel to be an easy HIPAA compliance solution to deploy on laptops. U.S. Federal Agencies can prevent embarrassing losses of laptops by deploying the CyberAngel, and can also develop new security policies around this product by articulating that confidential data be stored on the secure drive. Agencies working on complying with the Federal Information Security Management Act (FISMA) will also find the CyberAngel potentially useful. Financial institutions also have the capability to comply with the privacy regulations related to the Gramm-Leach-Bliley Act (GLBA) using the CyberAngel.

It would be great if in the next version, the CyberAngel came with documentation targeted specifically for HIPAA, FISMA, and GLBA end-users with specific examples on what information to put on the secure drive. It seems that there is a lot of potential to use the CyberAngel to comply with these information security laws, however without focused documentation on HIPAA, FISMA, and GLBA, some end-users may not see the potential at first glance.

One license will cost you $59.95, and volume discounts apply for packages of multiple licenses. CyberAngel Security Solutions, Inc. will also apply a 10% discount for U.S. Government Agencies and 20% discount for Educational institutions and Non-Profit organizations.

Relevant Technologies
Quality Acceptance Rating