



## The CyberAngel® Encryption & Tracking Software

*Cutting Edge Security Solutions for Business & Consumer Markets*












### Stolen Computer Recovery Process

**CyberAngel® Security Software** – *"The only computer security product and service offering data protection, intrusion detection, exportable strong encryption, plus a unique tracking system for stolen computers.... 'Ingenious' - The New York Times*

© 2007 CyberAngel Security Solutions, Inc. This document contains confidential and proprietary information of CyberAngel Security Solutions, Inc., intended specifically for Law Enforcement, and all or part of which may be protected under various patent, trade secret, trademark or other intellectual property rights. CyberAngel and Wi-Trac are trademarks of CyberAngel Security Solutions, Inc. All rights reserved.

## Quick Facts

---

-  10% of laptops are stolen within the first 12 months of purchase
-  49% of companies have had laptops stolen within the last 12 months
-  25% of all “reported breaches” involved missing laptops
-  60% of all corporate data assets reside on unprotected PC’s
-  All 19 Federal Government Departments & Agencies reported at least one loss of personally identifiable information since January 2003
-  The vast majority of data loss arose from physical thefts of portable computers, drives, and disks, or unauthorized use of data by employees
-  Since January 2005, there have been 109 reported computer related security breaches at educational institutions.
-  Of the 113 data breaches reported in 2005, 55 took place at universities, and university related medical centers
-  Total cost to recover from a data breach averaged \$140.00 per lost record
-  19% of the victims of a data breach terminate their relationship with the Company
-  Organizations are increasingly integrating physical and information security as they become more aware of the impact of privacy breaches



## The CyberAngel Executive Summary

CyberAngel Security Solutions, Inc. has made it standard practice to provide innovative custom security solutions for corporate and consumer markets for the past 10 years. While many IT security products focus on protecting the network or servers, The CyberAngel concentrates on the workstation; whether it is a desktop, laptop, or tablet computer. We understand that, like physical security, IT security products need to be able to work within different environments, and have different regulations to adhere to when designing a security system. The CyberAngel is an adaptive product, a hybrid of several technologies to provide a comprehensive solution set. The CyberAngel blends Authentication, Data Encryption, Remote Access Restriction, as well as Tracking and Recovery in the event of theft to provide a strong tool to use in the protection of your computer data and assets.

Our Executive Staff has varied backgrounds in Law Enforcement, IT Security and Physical Security, and understands the needs and challenges facing the marketplace today. Our focus on providing strong pre-sales support to best understand the client's environment and needs has proven time and again critical in the successful design, implementation and operation of The CyberAngel within an organization. Our goal is to make sure your critical corporate / client / patient information is encrypted and secure, keeping you in compliance with the many Security and Privacy Acts, as well as providing recovery of the stolen or lost assets. Clients such as **Brown University, Aflac Insurance, Transplant Resource Center of MD, Douglas County Hospital, The University of Toledo, Citizens Bank, WorkForce Solutions, and The State of Arkansas Dept. of HHS**, can testify that The CyberAngel has helped them stay in compliance and provided a secure computing environment.

### Laws

Aside from the existing Federal Privacy Acts, 34 states have already passed a version of the Security Breach Notification Law, which require notification to anyone that may have had unencrypted personal information compromised or stolen. A federal law is before Congress now, which would impose greater fines and even prison for non-compliance. While a stolen computer and / or data breach is extremely expensive and embarrassing, utilizing encryption for data protection can exempt you from these requirements and costs.

### Thefts

The media reports computer / data thefts occurring most every day and according to one survey, the average cost is 14 million dollars per incident, or \$140.00 per lost customer record. One university spent over 2 million in notification cost alone, after one professor's laptop was stolen. Using The CyberAngel and our encryption solution would exempt you from notification and legal costs, while recovering your lost or stolen computers. Although data protection can prevent losing millions, most of our clients see an ROI from the recovered hardware alone.

### Solution

The CyberAngel Security Software is a unique "hybrid" solution combining Data Encryption, User Authentication, and Tracking / Recovery in a single and easily implemented solution. With strong industry approved (and exportable) encryption, The CyberAngel addresses Privacy Acts and recent Security Breach Notification Laws, which have enormous notification costs, liability costs, and the loss of customers / clients / patients. Custom configured for each client, The CyberAngel can be triggered by a two-factor authentication or integrate with existing Windows or Novell passwords and other authentication devices. If the authentication is violated, sensitive data and applications (such as a VPN client, financial application or client database) are encrypted and hidden from the unauthorized user, communication ports are blocked, and a covert signal is sent to The CyberAngel Security Monitoring Center. After capturing the location of the computer, we will immediately send a real-time notification to the registered user or organization informing them of the unauthorized attempt to access that computer. Our Recovery Team will work with local Law Enforcement and the ISP's to facilitate recovery of your stolen computer, and act a liaison between you and law enforcement until a successful resolution.

## The CyberAngel<sup>®</sup> Security Software

### Provides “Real-Time Security” --- Strong User Authentication

The CyberAngel<sup>®</sup> Authentication offers Fully Integrated and Two-Factor Authentication modes, depending on the level of security required. Violation of The CyberAngel Authentication **instantly** protects the information, data, applications and utilities that you feel are sensitive or critical on that computer. **“Real-Time Security” for your computer and the information contained within.** The CyberAngel will **immediately** search for some type of connectivity to alert of that violation.



### Provides “Real-Time Security” --- Data and Information Protection

The CyberAngel<sup>®</sup> Secure Drive protects your confidential data, preventing unauthorized access to your files, company financials, patient / client information, or corporate business plans. If your computer is stolen, and / or The CyberAngel authentication is violated—your sensitive data and information is encrypted and protected as well as rendered invisible to that unauthorized user. This **“Real-Time Security”** is a solid compliance tool for medical or financial information privacy. Proprietary applications can also be placed within the Secure Drive, prohibiting their use by an unauthorized user or thief. The CyberAngel<sup>®</sup> Security Software’s **“on-the-fly”** encryption is transparent and lightning fast, and with all of our security features synced to The CyberAngel<sup>®</sup> Authentication, this patented comprehensive IT security tool truly provides.....**“One Computer Program -- One Password – 100% Security!”**



- **Available encryption algorithms:** Rijndael-AES 128 or 256 bit, Two-Fish 128 or 256 bit, Blowfish 128 or 448 bit, DES or Triple DES
- Prevents unauthorized users from seeing the Secure Drive and files within
- Provides Compliance with HIPAA, GLB, SOX, FISMA, and GISRA
- Compatible with all current Windows<sup>®</sup> platforms.

### Tracks, Locates and Recovers Lost or Stolen Computers

When The CyberAngel<sup>®</sup> Authentication is breached at login or boot-up, The CyberAngel<sup>®</sup> Security Software’s patented technology silently transmits an alert to our Security Monitoring Center, where we identify the location from which that computer is calling. The “unauthorized user” is unaware that an alert is being transmitted. Our Recovery Team helps coordinate notice to all necessary law enforcement officials and works closely with them to provide a rapid recovery of your stolen computer. The CyberAngel is the only company to offer Wi-Trac technology, the first indoor / outdoor laptop positioning system that utilizes Wi-Fi to accurately pinpoint location. With the market today in excess of 80 million portable computing devices, The CyberAngel with <sup>Wi-Trac</sup> is the best possible way to locate stolen assets.

### Additional “Real-Time Security” Features

#### Provides Strong User Authentication

Single & Two-Factor Authentication provides flexibility within an organization for secure access to any computer.

#### Prohibits Unauthorized Remote Access

Prevents VPN technologies from operating—prohibiting access to your remote network.

#### Prevents Unauthorized Application Use

Prohibits applications placed in the Secure Drive from operating---protecting such financial programs as Quicken, Peachtree, or databases such as ACT or Goldmine

#### Notification of Unauthorized Access

Provides immediate notification (via e-mail and / or fax) of any unauthorized access attempts---allows for rapid response to track and locate breaches in security

---

## Stolen Computer Recovery

The CyberAngel<sup>®</sup> Security Software provides the ability for Stolen Computer Recovery for all computers actively protected by The CyberAngel<sup>®</sup>. When Authentication is violated, we are able to identify the location of that computer when it sends a covert alert to our Security Monitoring Center. We then provide that location information to the local authorities, working closely with them to ensure acquisition of a search warrant and follow through to recovery and the return of that computer to its rightful owner.

### Notification of Unauthorized Use

---

When The CyberAngel<sup>®</sup> Authentication is violated, the speaker to the modem (if installed) is silenced, and if dial tone is detected, the program communicates with our alarm servers. If no dial tone is detected, The CyberAngel<sup>®</sup> will attempt a TCP/IP network connection from a Cable Modem, DSL, Wi-Fi, LAN or WAN. Once a telephone and / or network connection is found, the program covertly communicates with our alarm monitoring servers. The unique User Identification Number (UIN) is transmitted as well as the phone number or IP address from which the computer has communicated. The notification servers then contact the client via the notification method designated by the user during registration; either e-mail or fax, of that unauthorized usage. In a Corporate Licensee application, the unauthorized usage notification could be sent to a Systems Administrator or other designated individual instead of or in addition to the individual registered user. **In the event of a stolen computer, it is the responsibility of the client / user to report the computer to our Security Monitoring Center as stolen as soon as possible.**

### Reporting a Stolen Computer

---

When a client notices that their computer is missing, it is their responsibility to report the theft to the local authorities and then to The CyberAngel<sup>®</sup> Security Monitoring Center. Once a client / registered user reports a protected computer stolen, The CyberAngel<sup>®</sup> Team will tag the registered user account as stolen. The CyberAngel<sup>®</sup> Recovery Team will then gather more detailed information about the theft, date, time, and computer type, as well as the police report number and law enforcement contacts. Emergency notification and contact information is also gathered so as to promptly notify the client upon unauthorized use. The CyberAngel<sup>®</sup> Recovery Team will contact the law enforcement officials, making them aware of The CyberAngel<sup>®</sup> presence on that computer and preparing them to act once we have received contact



When an alarm event is generated from that protected computer, the alarm server will automatically generate an unauthorized usage report to the emergency notification preference determined when the registered user reported the computer stolen. An alert to the Support Operations Center is also automatically generated that notifies Support Center staff that a tagged stolen computer has communicated its location.

### Stolen Computer Incident Reports

---

The CyberAngel<sup>®</sup> Incident Report has been developed utilizing several local and federal enforcement agency requirements to assist in the investigative process of a theft. The Incident Report details the registered user, the date and time of the unauthorized access, the phone number or IP address from which the stolen computer has communicated with the alarm server. The telephony services that are utilized provide the ability to obtain an Automatic Number Identification (ANI) that is a verifiable and accurate resource for identifying the phone number from which the stolen computer has called. Utilizing several search utilities, the location address and a map are provided to assist in the location of the stolen computer. The CyberAngel<sup>®</sup> Incident Report has proven to be 100% successful in obtaining a search warrant or subpoena from the local court system to begin the hardware recovery process.

## Local Law Enforcement Coordination

---

When a computer is reported stolen to The CyberAngel® Security Monitoring Center, the Recovery Team then contacts the local law enforcement agency, referencing the police report number for that case, and provides them with information about The CyberAngel® Security Software and how our recovery process works. Nearly 80% of all alarm events from stolen computers happen after normal business hours, so education and coordination of local law enforcement in advance helps the recovery process go smoothly and increases the opportunity for recovery.

When an alert from that stolen computer is reported, we provide the local law enforcement agency with The CyberAngel® Incident Report, an Affidavit of Certified Use, detailing the parameters of the product technology, and the specific information as it relates to that client. The CyberAngel® Recovery Team works with the local authorities and designated representatives of the client to provide any additional information required to help effect recovery of that stolen computer.



## Location Identification

---

The process used to identify the location from which a stolen computer has called utilizes several different databases, both public and proprietary. These include databases found on the Internet as well as subscribed services. All lookups utilize at least six databases to provide the most accurate information possible. However, the addresses listed for the verified phone numbers are provided by third party resources and are in no way affiliated with CyberAngel® Security Solutions, Inc. (CSS, Inc.). While these databases are updated frequently, the accuracy cannot be guaranteed by CSS, Inc. Therefore, local authorities should be consulted to utilize the telephone number provided to ensure that the location and address are current and accurate. Local authorities have access to proprietary databases licensed to government and municipal agencies to provide accurate identification information.

The CyberAngel® Security Monitoring Center is equipped with ANI (Automatic Number Identification) technology, similar to that of e-911 centers. This allows us to receive the identification of the phone number that the stolen computer is calling from, regardless of Caller ID Block, or any other feature utilized by consumers to hide that number.

In the instance that the unauthorized access was transmitted via a TCP/IP connection to the Internet, resources are utilized to identify the domain name and registering company or individual of that domain name. The IP address transmitted to the alarm server is the provider of connectivity to the Internet for that stolen computer. That company, ISP or individual can provide records of connectivity to further identify the location of the alarm event transmission of the stolen computer. A subpoena is often required to secure the release of that user information from an ISP such as Comcast, AOL, Road Runner, etc. Our Recovery Team has established contacts with ISP's across the nation, and often helps facilitate the subpoena process with law enforcement and these ISP's.

## Local Authorities and Jurisdiction

---

The covert communication event from that stolen or missing computer is deemed "probable cause" in the eyes of the court system. In some jurisdictions, the time limit for applying for a search warrant or subpoena from time of "probable cause" is a little as 48 hours from time of incident, and can vary up to several weeks. The CyberAngel® Recovery Team works closely with the law enforcement officials to ensure action within the specified time limitations within that jurisdiction. We provide all of the needed information to designate probable cause, and allow the courts to subpoena the phone company records, if necessary. The stolen computer, when recovered, may be considered evidence until such time as the authorities deem necessary, and will only be returned upon their discretion. In the event the stolen computer is reporting from an address outside the jurisdiction of the local authorities that the stolen computer was reported to, every effort is made to coordinate information and activities between the agencies.

**The information and address provided is intended to be used, along with all other information available concerning the referenced stolen computer, as a basis for investigating details of alarms generated by The CyberAngel® software. It should be utilized only through due process of law and in coordination with the proper authorities. Provision of this information does not imply that the individual or company named in the lookup is necessarily guilty of any misconduct or criminal intent in connection with the referenced computer.**



## The CyberAngel® Security Software **SAMPLE** Stolen Computer Incident Report

Report Generated: November 27, 2006

### CyberAngel® Client Data

CyberAngel® I.D.	Last Name	First Name	MI	City	State/Prov	Zip Code	Country
1000287543	Williams	James		Newark	NU	07931	USA
Home Phone	Work Phone	Cell Phone	Fax / E-Mail Address		Company		
908-345-8831	201-885-2865	908-777-1961	<a href="mailto:J_williams@acme.com">J_williams@acme.com</a>		ACME		
Authentication Code Verified By: _____		Kyle Brown		Stolen Computer Type: _____		Fujitsu :Lifebook S-6231	
Date Computer Reported Stolen: _____		09/27/2006		Stolen Computer Serial Number: _____		R165476YT	
Estimated Theft Date: _____		09/27/2006		Stolen Computer Theft Details: <u>Laptop stolen from vehicle in driveway</u>			

### **\*\* IMPORTANT \*\***

The information and address provided below is intended to be used, along with all other information available concerning the above referenced computer, as a basis for investigating details of alarms generated by The CyberAngel® software. It should be utilized only through due process of law and in coordination with the proper authorities. Provision of this information does not imply that the individual or company named in the lookup is necessarily guilty of any misconduct or criminal intent in connection with the referenced computer, but that a communication as detailed below originated from that number or location at that time from the above referenced computer. Law enforcement officials are obligated to verify the terminating address associated with the provided telephone number or IP address.

### Alarm Event Log from Estimated Theft Date

Event #	Alarm Date	Alarm Time	Type	IP Address	Latitude	Longitude	Telephone	Map
1	11/22/2006	07:45:33 PM CST	Modem				908-219-4280	1
2	11/24/2006	08:06:18 PM CST	Internet	71.250.230.106				
3	11/24/2006	08:07:42 PM CST	W-Fi		40.708816	-74.384308		1

### Telephone Location Lookup

Event #	Telephone	Name	Address	City	State	Country	ZIP Code
1	908-219-4280	Jeffrey Beck	45 Division Avenue	New Providence	NJ	USA	07974

### Wireless Location Lookup

Event #	Telephone	Name	Address	City	State	Country	ZIP Code
3	908-219-4280	Jeffrey Beck	45 Division Avenue	New Providence	NJ	USA	07974

### IP Location Lookup

Event #	IP Address	Internet Domain Name Search	Internet Service Provider (ISP)
2	71.250.230.106	<a href="http://71-250-230-106.nwrknj.east.verizon.net">71-250-230-106.nwrknj.east.verizon.net</a>	Verizon Internet Services

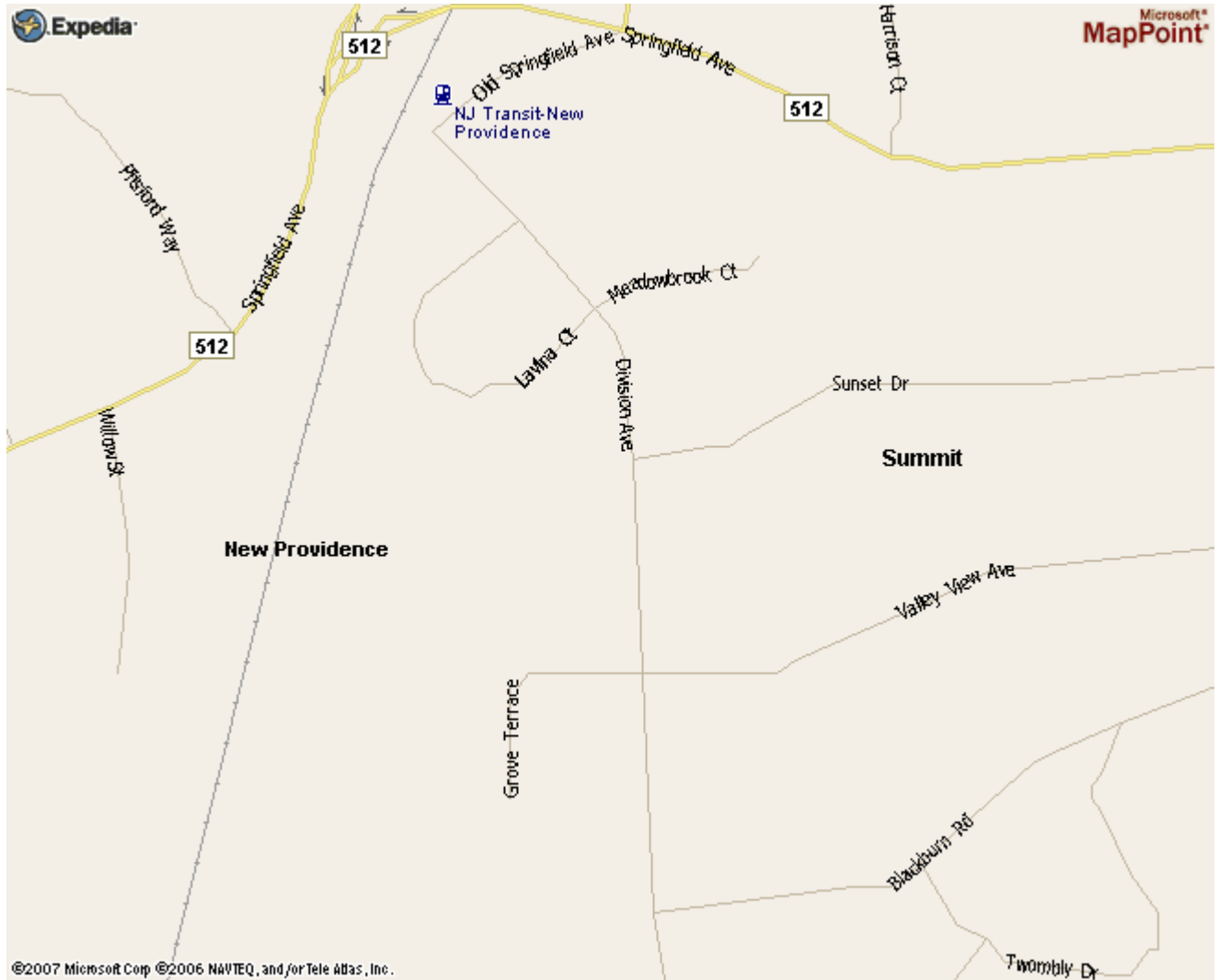
Event #	ISP Address	City	State/Province	Country	ZIP Code
2	1880 Campus Commons Dr	Reston	VA	USA	

Event #	ISP Subpoena Contact	Phone Number	Fax	E-Mail Address
2	Christine Gardener	972-615-4392	800-997-9981	

Event #	ISP Technical Contact	Phone Number	Fax	E-Mail Address
2	IP-Tech ARIN	800-243-6994		

MAP # 1

45 Division Avenue, NJ 07974



---

## Police & Recovery Tips

---

The following are some helpful tips about the recovery process, the reports generated, and common scenarios. If you have any further questions about The CyberAngel Software or the recovery process and information provided, please do not hesitate to call one of our Support Engineers at **800-501-4344**. We typically provide Law Enforcement with 3 documents, an Incident Report, User Account Information, and an Affidavit of Product Authenticity and Use. These provided documents have been 100% successful in obtaining search warrants all over the USA for the past 10 years, culminating with an 83% recovery rate for that time period.

### The CyberAngel Incident Report

The CyberAngel Incident Report details the date, time, and from where that alarm event has called from. In the event of a phone alarm, we can resolve the transmission to a physical location, name, street address, and map. It is recommended that the terminating address be verified by the local phone company as databases used for these lookups are only updated every 60-90 days.

In the event of a network alarm, we can resolve the transmission to the Internet Service Provider (ISP) or company. We provide contact information for that ISP as well as subpoena contact information within that ISP that can provide you with the location information and registered name for that specific IP address used at the date and time.

### The CyberAngel User Account Information

The CyberAngel User Account Information details the User Account, and includes screen shots of the user's record in our Database Management System. This will show the user account, information about the theft, and screen shots of the actual alarm coming in to our database.

### The CyberAngel Product Affidavit & Wi-Trac White Paper

The CyberAngel Product Affidavit provides basic details on the operation of The CyberAngel Software, and details on the reporting of the theft and alarm event history for that user. The Wi-Trac White Paper details the accuracy of WiFi Tracking location information.

### Subpoena Information for ISP's

On The CyberAngel Incident Report, in the event of a network alarm transmission, you will find the contact information for that Internet Service Provider (ISP) that the alarm transmitted through, such as AT&T, Comcast, Road Runner, Earthlink, BellSouth, etc. In most cases, we will have a dedicated contact in the legal department that handles subpoena requests and that will ensure a quick turnaround of location information.

### Mobile Computer Theft

By design, laptops are a mobile device, and we often see stolen laptops communicate from different locations. ISP's today are familiar with this issue and can accept multiple IP addresses in a subpoena request. Also, due to the nature of the laptop being mobile, expediency in requesting and filing for the subpoena and search warrants produces a higher chance of recovery.

### Phone Alarms coming from a Hotel

Should an alarm come from a phone line within a hotel, you will need to check the outgoing phone records at the hotel for the date and time listed in the Incident Report. The CyberAngel Software will call our 800 number (**800-501-4412**) and the hotel records should show what room made that outgoing call at the date and time specified on The CyberAngel Incident Report.