

# KineticD™ Security White Paper

Today more than ever, companies and organizations are choosing online backup as their preferred method of storing and protecting their data. Indeed this makes business sense; online backup far outperforms traditional backup methods in terms of cost efficiency and ease of use. It is therefore critical that security protocols remain top of mind for any business considering the most effective ways of protecting their most important asset.

The purpose of this white paper is to demonstrate how KineticD meets and exceeds its clients' demands and expectations for the security of its online backup SaaS offering.

KineticD achieves the highest level of security for its customers — working in partnership with industry leaders, including:

- ADP Cabinets & Cooling
- Dell
- GeoTrust
- Microsoft Corporation
- McAfee Virus Scan
- Cisco System



# Physical Security

KineticD provides state-of-the-art physical site security, application security, network security, and data security.

KineticD security is built on a foundation that is strong, flexible, multi-faceted and redundant. If, or when, it is targeted by a security threat, multiple safeguards are already in place, and additional safeguards are triggered to protect the system.

## Data Centre Security

HIPAA compliant information systems require a combination of administrative procedures, physical safeguards and technical measures to protect patient information during storage and transmission across communication networks. As a significant part of your overall contingency plan, KineticD provides secure, automated data transmission and storage services for data backup and recovery.

## Secure Access

151 Front St. acts as a primary North American communications hub for telecommunications carriers and data centre firms from around the globe. As an essential connection point for corporate data networks, local and long distance telephony, Internet peering, and critical data storage facilities, the 151 Front St. building has been designed to accommodate the highest standards of security, reliability, and connectivity.

Uniformed security patrol the premises and surrounding area 24/7/365 as part of a customized security system and protocol, while optical turnstiles and door entry card access provide a second level of security. Tenants also deploy their own proprietary security systems. Access to all high-security areas, such as the Meet-Me Room and Riser Systems, require a supervisor to monitor all personnel.

There are multiple CCTs to monitor perimeter and common areas of the building, and 24 hour monitoring of MMR facilities. Elevators have 24 hour card reader access.

## Electrical

In 2001, two new 4000/5000KVA transformers were added to ensure the reliability of 151 Front St.'s power supply. These transformers are fed by dual underground 13.8 Kv feeder lines from the local substation.

## Power

151 Front St. can provide up to 100 watts per sq. ft.

## Back-up Generators

151 Front St. has structurally engineered space for growth (18 generators currently installed) and offers back-up power solutions.

## Cooling

New district cooling provides chilled water to the building according to pre-determined temperature, capacity, and consumption.

## **Rooftop**

Pre-engineered structural steel supports the added weight and vibration (now housing 18 generators) in full operation. To facilitate requirements for secondary cooling, a similar structural steel grid is installed on the uppermost roof to accommodate the array of condensers, fluid coolers, glycol pumps, and chillers.

## **Diesel Fuel Farm**

To support the generator power plant, 151 Front St.'s environmentally compliant diesel fuel storage facilities can house up to 44,000 gallons in tenant-owned tanks providing fuel to the generators. 151 Front St. owns the street at the back of the property, ensuring that refueling trucks and rollup generators enjoy unrestricted access to ensure their facilities 7/24/365 operation during an emergency.

## **Connectivity**

With over 25 fiber optic entrances into 151 Front St., network diversity and business continuity are ensured. 151 Front St. has more than 25 points of entry (POE) penetrating the building, offering an extensively diverse pathway solution for any subscriber or service provider wishing to enter. 151 Front St. St. can be entered from all sides, increasing the number of right-of-ways that can be used to gain access. Further, the proximity to the rail lines, a major right-of-way for national fiber optic loops, enhances access to national networks.

## **Telecom Infrastructure**

151 Front St. manages a highly secure fiber optic Meet-Me-Room located in the heart of the building offering easy access from building points of entry and is adjoined by a diverse riser system. This allows 151 Front St.'s all-encompassing telecommunications tenants an array of dynamic and centralized access to service providers and carriers. Built in 2000, this room now houses access points for networks that literally spans the globe.

The Meet-Me-Room is equipped with an aspirating smoke detection apparatus, which is linked to an FM-200 fire suppression system. Along with this feature, there is a water and leak detection system around the perimeter of the floor and running over the ceiling. Access to the room can only be gained via escort and with security "card in and card out," and even with this protocol in place, there are 4 CCTV cameras covering every inch of the room.

## **The Riser System**

The Riser System consists of two diverse pathways linked directly to the Meet-Me Room and connecting vertical pathway to the penthouse level. The system offers diversity for your networking requirements, ease of installation for speed and cost savings. Access to the room can only be gained via escort and with security "card in and card out," and even with this protocol in place, there are 4 CCTV cameras covering every inch of the room.

## **Servers**

Data is written to RAID 6 disk arrays (including hot spare drives). Each storage server is then replicated in real time to a second storage server for backup.

# Data Security

## Individual Password Protection

Each user maintains an individual account and password and therefore a unique encryption key. The password is encrypted before it is stored in our database. At no point is an administrator able to retrieve your password, nor does an administrator have the ability to set a password to a known value.

When you activate your account, you are required to choose a password and set up a security question. If you forget your password, or repeatedly try to log in with an incorrect password, the system will lock you out after a few attempts. You may then reset your password by correctly answering your security question.

If you incorrectly answer your security question, you are again locked out after a few attempts. In the unlikely event that you forget your password and the answer to your security question, you must contact KineticD directly for manual identity verification.

## End-to-End Verification

The integrity of all data files are verified against a known CRC signature. Files are re-verified each time they are written to disk. If any file fails verification, it is retransmitted from the PC or recovered from the replica server. This ensures that the data stored on our servers is the same data that was stored on your PC.

## Secure Protocol

The KineticD client communicates with our servers over a proprietary protocol that was designed specifically for Internet backup. Other Internet backup products that use popular web protocols like HTTP, FTP, or WebDav can be vulnerable to hacker and virus attacks. The extreme popularity of these protocols makes them a target. It is extremely unlikely that a hacker is going to invest the time and effort to go after a proprietary protocol. Even if they did, the 448 bit Blowfish Encryption has never been broken.

## Firewalls

To maximize compatibility with home and corporate firewalls, the protocol used by our Backup Client was designed to look to a firewall just like the SSL protocol used in web browsers. This means that if you are able to surf to our web site, you will be able to connect with our backup software. Specifically, our backup client runs on port 443 and mimics SSL's handshaking protocol. Almost all firewalls will pass our backup traffic without reconfiguration. We also support the use of proxy servers. Our web browser interface also uses generic HTTP and HTTPS on ports 80 and 443.

## Corporate Remote Access Policy

Many organizations have a policy to control access to their data from outside of the organization. VPNs and Firewalls are generally used to control this, but become ineffective when the data is stored off-site. The same features that empower a laptop user to backup and restore his or her data while on the road may violate corporate information policy. KineticD includes the ability to restrict data access to only specific IP addresses. A Corporate Administrator can define the IP address ranges of their firewalls and access points. Once the definitions are in place, users can only access the data from the allowed locations.

## Encryption

Files are protected using 448 bit Blowfish Encryption. This extremely secure “bank grade” encryption algorithm has never been cracked. KineticD considered many factors when choosing Blowfish as its encryption technology, including peer review, speed and key strength. It is clear that Blowfish will set the standard for years to come, and will continue to be the preferred encryption algorithm for corporations worldwide.

## The Blowfish Algorithm

Of the hundreds of encryption algorithms available today, Blowfish stands out as the industry leader and has been selected by KineticD as its encryption algorithm.

Blowfish is a symmetric encryption algorithm designed in 1993 by Bruce Schneier as an alternative to existing encryption algorithms such as DES. Unlike DES, however, the Blowfish algorithm has a variable key length, which can be extended from 32 bits to 448 bits, making this a more secure alternative. Blowfish is a 64-bit cipher (i.e. a cryptographic key and algorithm are applied to a block of data rather than single bits).

Blowfish is a fast, free alternative to existing algorithms and has been analyzed considerably through years of peer review.

Finding the plain text of an encrypted message without knowing the key is called “cracking” an algorithm. This brute-force attack consists of trying all possible values of keys until the right one is found.

It is easy to demonstrate that in the case of brute-force attack, the security increases together with the length of the key. If the key is 8 bits long, there are 2 (to the power of 8), or 256 possible combinations. With a key of 40 bits this is increased to 2 (to the power of 40), or one thousand billion combinations. The protection then resides on the time needed for a computer to perform its attack. Based on these premises as well as numerous industry trials, it is common opinion today that 40-bit key algorithms are useless as they can be “cracked” within a few hours by an average personal computer. 64-bit algorithms are safe today but will become threatened as technology evolves. 128-bit and over algorithms are almost unbreakable. In other words, it would take millions of years to try every possible combination of bits in a 128-bit key.

Based on calculations it can be said that a 128-bit encryption is not just three times stronger than a 40-bit encryption—it is 309,485,009,821,345,068,724,781,056 times stronger. Likewise, a 448-bit encryption key is  $2.1 \times 10^{96}$  times stronger than a 128-bit key.

## Speed

The speed of the Blowfish algorithm is also impressive. The table below illustrates the effective throughput of the algorithm and shows how even large key lengths result in much faster performance than other encryption algorithms.

Algorithm	Clock Cycles per round	# of rounds	# of clock cycles per byte encrypted	Notes
Blowfish	9	16	18	Free, unpatented
Khufu/Khafre	5	32	20	Patented by Xerox
RC5	12	16	23	Patented by RSA Data Security
DES	18	16	45	56-bit key
IDEA	50	8	50	Patented by Ascom Systec
Triple-DES	18	48	108	Very Popular

## Conclusion

With the rise in popularity of online backup as a solution for businesses comes the rise in demand for data integrity, physical site security, and application security. KineticD can ensure the top-of-industry standard in data protection and recovery.

60,000 business users worldwide rely on KineticD every day to backup their data, boost productivity and save costs. KineticD gives its clients the piece of mind to know that all their mission-critical data remains safe, from unauthorized users, natural disasters, computer viruses or human error.