



NXdrive



**- A Holistic Solution for Data Storage
and Protection**



InfoBeyond Technology LLC
www.InfoBeyondtech.com

CYBERCRIME TO COST THE WORLD \$6 TRILLION ANNUALLY BY 2021



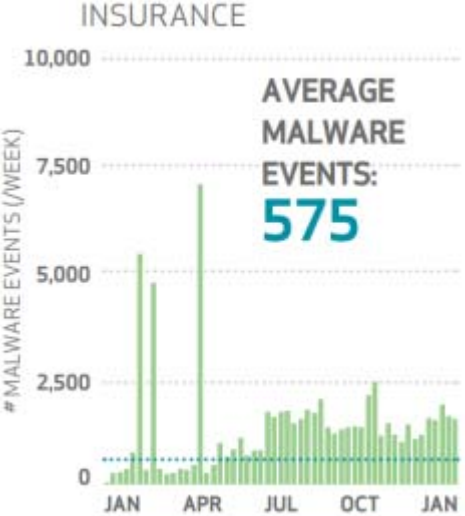
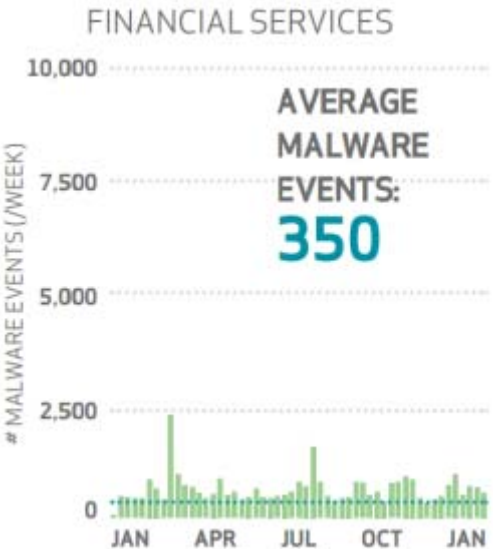
InfoBeyond Technology LLC – Property and Confidential

Cybersecurity Ventures predicts global annual cybercrime costs will grow from \$3 trillion in 2015 to \$6 trillion annually by 2021, which includes **damage and destruction of data**, stolen money, lost productivity, **theft of intellectual property**, **theft of personal and financial data**, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, **restoration and deletion of hacked data and systems**, and reputational harm.

2

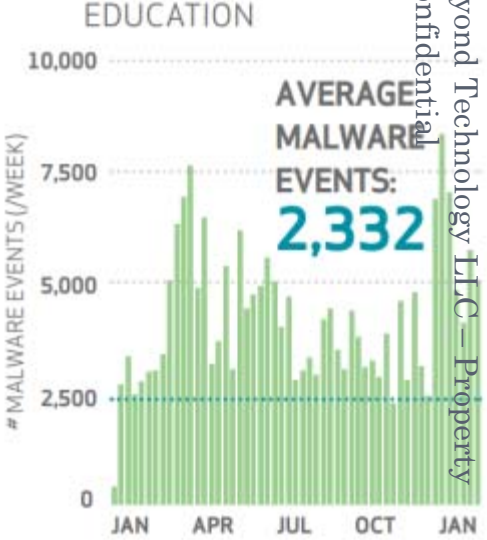
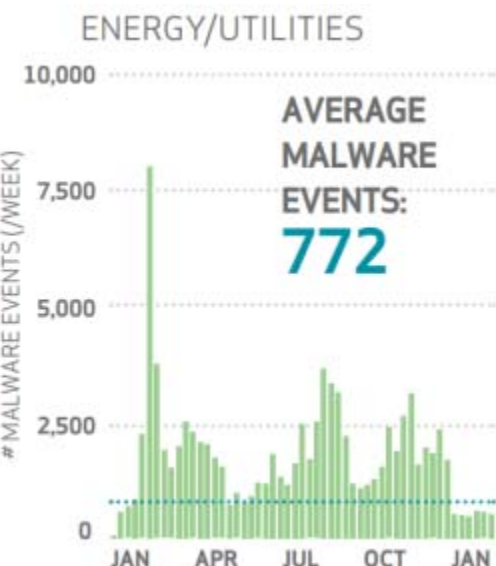
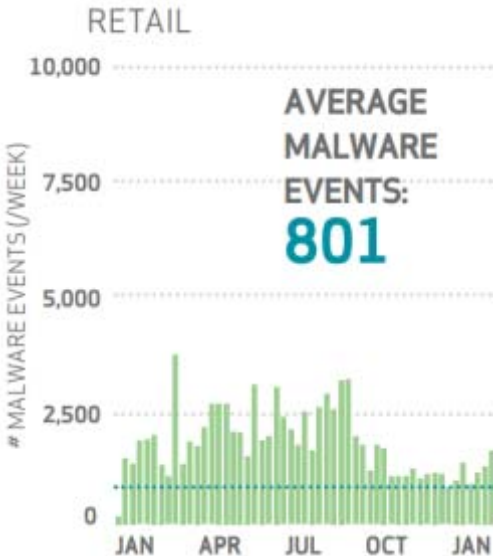
NXdrive data protection gives the solution to the highlighted sections.

DATA BREACHES ARE MOSTLY CONDUCTED VIA MALWARE



Weekly average number of malware events for five industries: Financial Services, Insurance, Retail, Utilities, and Education.

InfoBeyond Technology LLC - Property and Confidential



Five malware events occur every second. 70-90% of Malware samples are unique to organization.

NXdrive data protection prevent Malware data breaches

DATA SABOTAGE: THE LATEST THREAT TO THE FINANCIAL/BANKING INDUSTRY



Forget data thieves, data sabotage will be your next IT nightmare

RSA 2016 For years, the security industry has been primarily focused on stopping information theft. Now more and more people in the trade are worried that the next wave of attacks won't steal data – they'll alter it instead.

Data tampering is the second of the [top three IT nightmares](#). We're used to data being stolen, he said, or even deleted as in the case of Sony. But if data has been subtly altered rather than stolen, then the results could be severe.

HOLISTIC DATA PROTECTION: CONFIDENTIALITY, ANTI-DESTRUCTION, RESTORATION, SUSTAINABILITY, MAINTAINABILITY, CONTROLLABILITY



The top three industries affected are Public, Information, and Financial Services.

- ❑ **Data Encryption is designed for protecting the data confidentiality/privacy, but not for**
 - ❑ Data integrity from cyber attackers (Anti-integrity)
 - ❑ Data restoration/availability/loss from cyber attackers
 - ❑ Data stolen from cyber attackers
- ❑ **Network Security for data protection, but have many problems:**
 - ❑ Gateway/Firmware
 - ❑ Anti-Malware
 - ❑ Real-time intrusion detection, and Network Monitoring, etc.

Highly regulated industries such as health care and financial services have the most costly data breaches because of fines and the higher-than-average rate of lost business and customers.

NXDRIVE DATA PROTECTION

❑ Fragmentation builds extra features over encryption to provide holistic data protection capabilities

- ❑ The fragmentation is a security process that set up a set of security fences
- ❑ Fragments are distributed over different places
- ❑ Encryption key is destroyed after data encryption
- ❑ No centralized key storage
- ❑ More data, more secure

❑ Fragmentation builds/enables mechanisms in addition to encryption:

- ❑ Data anti-tamper
- ❑ Data restoration/redundancy/reliability
- ❑ Data integrity protection

- ❑ **Deployment Flexibility:** Meet different industrial operation models. Fragments can be deployed over different ways for different industrial security requirements.

NXDRIVE FEATURES

❑ External and Internal Data Theft Protection (Attacker reads the data)

- ❑ The fragmentation is a security process that sets up a set of security layers
- ❑ Fragments don't contain data in its original form
- ❑ Encryption key is destroyed after data encryption
- ❑ Crash (Decrypt) a fragment give no data information

❑ Data Loss Protection (Attacker deletes the data)

- ❑ Data redundancy/reliability using replication of distributed fragments (protected separately)
- ❑ Requires less storage than standard replication

❑ Data Attack Identification (Attacker is attacking the NXDrive)

- ❑ Data integrity validation of fragments on a continuous basis

NXDIRVE FEATURES

❑ Data Tamper Protection: (Attacker has modified the data)

- ❑ Capable to rebuild the original data from fragments even if some fragments are modified
- ❑ Coping a whole fragment on the data service has no fact on the data protection
 - ❑ Fragment self-regeneration

❑ Data Access Control Protection: (Limiting the attacker's access to original NXDrive data)

- ❑ Only a valid user can access the original data content
- ❑ All external data files (excepted authorized requests) are fragmented and a Malware will lost is functions.

Malware's three possible data manipulation on the data storage

Hacker intentions	Malware's Operations for Data Breaches	NXdrive Data Protection
Data thieves (most case in the current attacks)	Hacker manipulates Malware to read/steal data	Fragment is meaningless for hacker.
Data sabotage (recent trends)	Hacker manipulates Malware to modify the data information	NXdrive can detect the modification of the fragment and respond with self-generation to create a new fragment and save it to another place.
Data destroy (Very bad cases but happened in some cases)	Hacker manipulates Malware to delete the data information	NXdrive can detect the loss of fragments and respond with self-generation to create a new fragment and save it to another place.

CASE I: 2012 DROPBOX DATA BREACH - SIMPLE ENCRYPTED DATA ARE NOT SECURE ENOUGH

How it happened at Dropbox	Step 1: Access to the Network	The hacker remotely access to the Dropbox network by penetrating the network protection
	Step 2: Steal the database from a central place	Malware retrieves the user database that includes the user name and password, where the password is encrypted.
	Step 3: Crash the encrypted password	Using a crash tool (similar to brute-force decryption, e.g., dictionary) to recover the encrypted password.
	Note: Attackers can purchase a password cracker for less than \$20,000. This tool would enable attackers to test a trillion passwords every second, which means every eight-letter password could be tested in just 2 seconds and every nine-letter password in under a minute. The average time will be much less this delay in a smart way.	
NXdrive Protection	The hacker will be first stopped at Step 2. The password (user name as well) is fragmented as a number of secrets (e.g., fragments) and protected in different authorities.	
	In Step 3, suppose the attackers compromised the fragments and they no tool (no new tools) to crack the password as they are no verification is available to verified if the tested results are corrected or not. A fragment has multiple layers of protection.	

Target confirms encrypted PIN data stolen

Dropbox has finally confirmed that the email addresses and hashed passwords of 68,680,741 accounts were exposed in a hack that took place in 2012.

CASE II: SONY PICTURES ENTERTAINMENT – DATA DESTRUCTION

FBI observed that the hacker stole large quantities of personal and commercial data, and then **destroyed** systems.

NXdrive enables not only data confidentiality, but also anti-destruction and restoration. A destroyed fragment has the self-regeneration capability from other fragments

SONY Data Breach

Vol NCH, No. 311 Wednesday, April 27, 2016 \$1.25

'Guardians of Peace or GOP'

SONY HACKED?!

November 26th, 2014, Sony announced that there was a breach into its network. A group of hackers took credit for the breach and they called themselves "Guardians of Peace" or "GOP". Two days later, from hackers began leaking sensitive company data, email, finances, employee information and even four unreleased films which they put out into the internet places and they claimed to have collected about 800TB of data from Sony Service and only a tiny fraction of it has been made public. What was in this was pretty devastating to people, 47000 Social Security numbers, credit card information, passport details. Sony stated that it is a people that had had left off by not informing them that their sensitive information had been leaked and by not giving them credit restoring services which was given to current employees.

Paid by North Korea?!

SONY hacked? The Guardians?!

Sony Pictures Entertainment and Hollywood studios have been hit by a massive data breach. The breach is believed to be the work of a group of hackers known as the Guardians of Peace (GOP). The breach is believed to be the work of a group of hackers known as the Guardians of Peace (GOP). The breach is believed to be the work of a group of hackers known as the Guardians of Peace (GOP).

FBI blames North Korea for SONY hack!

Washington Post

A "technical analysis" of the data stolen from Sony's servers in the breach, said the FBI, "strongly suggests" that the breach was the work of a group of hackers known as the Guardians of Peace (GOP). The breach is believed to be the work of a group of hackers known as the Guardians of Peace (GOP).

SONY accused for racial discrimination by GOP

SONY accused for racial discrimination by GOP

Sony and Sony Pictures have made major news headlines and have been accused of racial discrimination. The breach is believed to be the work of a group of hackers known as the Guardians of Peace (GOP). The breach is believed to be the work of a group of hackers known as the Guardians of Peace (GOP).

Issue with SONY?!

Issue with SONY?!

Sony and Sony Pictures have made major news headlines and have been accused of racial discrimination. The breach is believed to be the work of a group of hackers known as the Guardians of Peace (GOP). The breach is believed to be the work of a group of hackers known as the Guardians of Peace (GOP).

InfoBeyond Technology LLC - Property

CASE III: TALKTALK WAS HACKED. BUT IT'S SILLY TO ASK IF THE DATA WAS ENCRYPTED!

Encryption is 'Get Out of Jail Free' Card but Compromising the encrypted data is not acceptable for any sensitive data protection:

- ✓ Encrypted data on a laptop/computer can be accessed with credentials (preconfigured)
- ✓ Decryption of the encrypted data is expensive but feasible by high performance computers.

NXdrive: Compromising fragments leaves no vulnerabilities on data protection.



- ✓ Accessing, Copying, and Distributing the encrypted data.

Source Code, Encrypted Data Stolen as 2.9 Million Affected in Adobe Breach

NXdrive provides the significant and practical data protection capabilities that are not offered in current solutions.