



## Using Cloud Services to Protect Files from Malware Including Ransomware

This white paper discusses the challenges facing IT from increasingly vicious threats and how Eyonic Systems' online backup service addresses these issues to provide data confidentiality, integrity and availability.



## Table of Contents

Introduction .....	3
Vicious Trends Increase the Risks Facing IT .....	3
Ad Based Threats .....	4
Ransomware .....	4
Using Business Devices for Personal Use .....	5
Loss of Data Integrity.....	6
Need for More Flexible Backup Jobs .....	6
Challenges with Existing Backup Solutions .....	6
Traditional Onsite Backups .....	6
Cloud Based File Storage .....	7
Eyonic Systems' Online Backup Service .....	8
Service Comparison.....	10
Conclusion.....	11
References .....	11
About Eyonic Systems .....	12

## Introduction

Finding the calmness confidence brings at a time when user and business information is under increasingly advanced attacks is difficult. The increase of external attacks and internal misuse create opportunities for data loss, while file corruption and exposure become prevalent. As a result, working in IT is both more exciting and more challenging than ever depending upon the moment.

Threats against data exist because private information is valuable. Keeping customer information private is important to both the company and the individual, but intact company files are integral to daily operations. For outsiders, accessing these files provides a way to control and sell the data. At times companies can be forced into paying a ransom to regain access to their own files. Other times individuals' personally identifying information is sold and the company never has a chance to recover their files. Sometimes devices are compromised for unknown reasons or seemingly without intentions.

Whether running a small business or managing a data center for a fortune 500 company, data confidentiality, integrity and availability are critical for business continuity. Cloud services provide an offsite disaster recovery copy of data while also protecting files from external attacks and internal misuse. Maintaining a copy of business data is merely one step in a series of critical steps for a business to provide data protection. Other important steps to ensure data usability are:

- Testing the integrity of backup files regularly
- Keeping at least one copy of the data in a secure offsite location
- Limiting the amount of time required to recover files after a disaster

## Vicious Trends Increase the Risks Facing IT

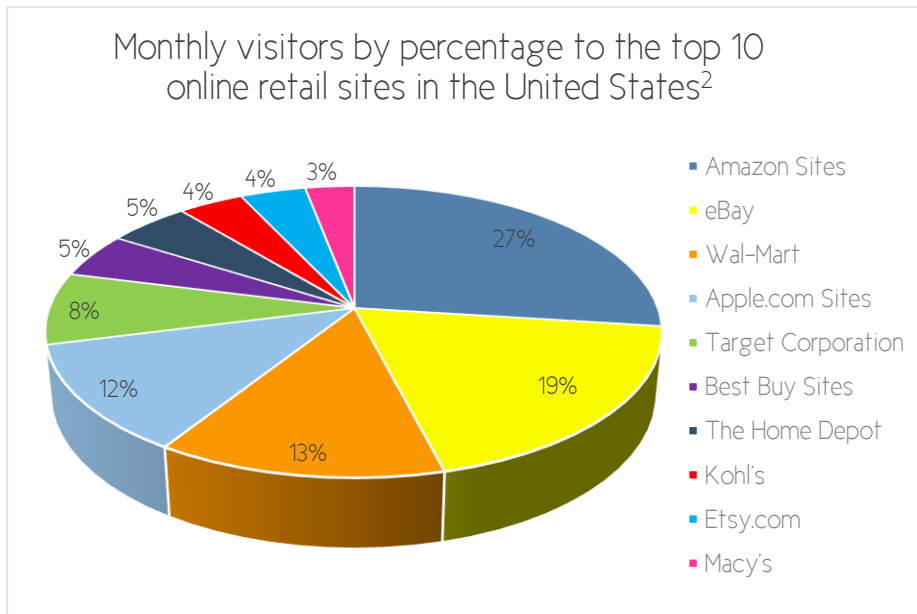
Once a business has information worth protecting, there will be other people who feel the information is also valuable. Business information is often viewed as worth any effort to gain unauthorized access to the information, and businesses face many issues when protecting their customer base. Over time the creative ways in which people try to gain access to private information changes. People developing external threats are adapting to use newer and cleverer ways to gain access to business data, often faster than businesses can implement controls and procedures to protect their data from compromise.

As attacks change, businesses need to change the way they protect, prevent and respond to threats. Regardless of the way, when information is successfully compromised the effects to the original owners are the same. Data breaches cost time and money to recover from and can at times be catastrophic. Three examples of recent trends are:

- Ad Based Threats
- Ransomware
- Using Business Devices for Personal Use

## Ad Based Threats

Ad based threats are delivered to users via web page ads harboring malicious code. Once a user clicks on an infected ad their machines can become infected with malware, viruses or spyware. Malicious ads can exist within even the most common websites including Yahoo who confirmed some of the ads they displayed delivered viruses and malware to unsuspecting users in 2014.<sup>1</sup>

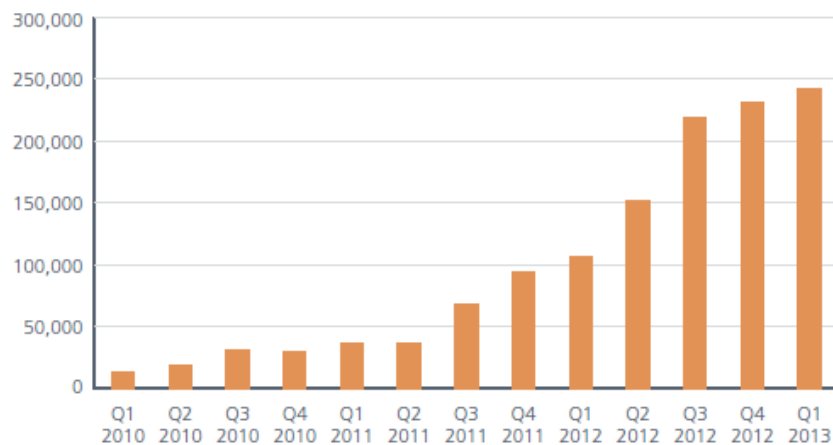


Ad based threats grew more popular as online shopping became widespread and an increasing number of sites incorporated them. In 2014 there were more than 196 million digital shoppers in the US alone.<sup>3</sup> This represents a 14% increase over the number of digital shoppers just four years prior in 2010.<sup>3</sup>

## Ransomware

Ransomware attacks grew at an exponential rate between mid-2011 and the first quarter of 2013 when McAfee reported reaching more than 250,000 unique samples.<sup>4</sup> This figure represents an increase in samples more than double that found during the same quarter one year earlier.<sup>4</sup>

Table 2: Ransomware samples as observed by McAfee over a 3-year period.<sup>1</sup>

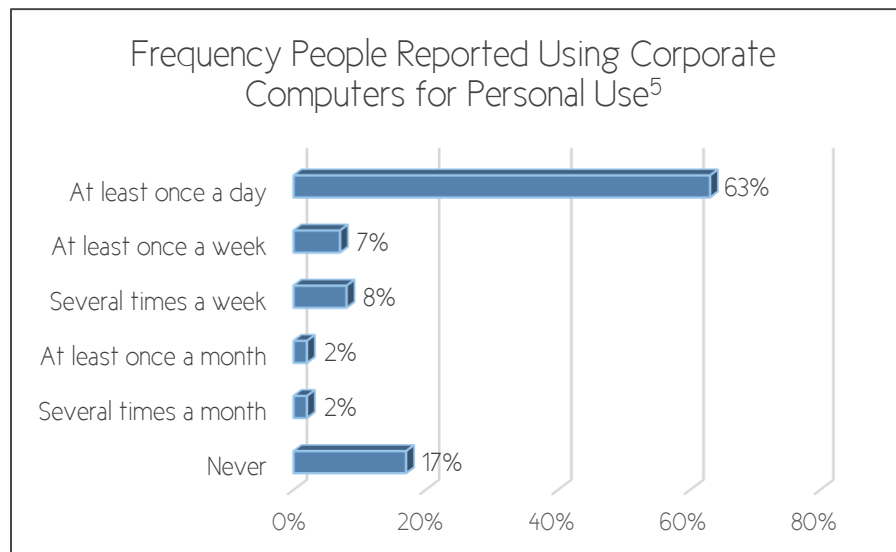




Ransomware versions like Cryptolocker and Locker placed Ransomware attacks in the crosshairs of IT departments, security professionals, and businesses alike over the last year. Ransomware is an effective attack because it encrypts all the files on an infected device, preventing the user from accessing any of the files. In addition to the local files, Ransomware encrypts any files the device has access to including attached devices and network, or mapped drives. Once encrypted, the only way to decrypt the files is to pay the requested ransom. Lastly, ransoms are demanded using anonymous payment systems making them harder to trace.

## Using Business Devices for Personal Use

The average US Internet user spends 32 hours a month online.<sup>5</sup> With so many hours spent online, it would be foolish to think none of these hours occur during work hours or on business owned devices. In a study by InsightExpress commissioned by Cisco, 83% of people admitted to using a business computer for personal



use some of the time, while a staggering 63% admitted to using a business computer for personal use every day.<sup>4</sup> When unauthorized use is spent shopping online the exposure to ad based threats increases.

As society becomes more accustomed to responding instantly and having access to people at any hour, the likelihood corporate computers will be used for personal use increases proportionally. Being 'connected' at all times is more accepted each year and brings with it additional risks to business continuity. Keeping up with trending threats is a constant battle for many IT professionals. Winning the battle requires balancing the need to protect the network while allowing users to effectively do their jobs. Cloud services offer a cost effective way to easily manage both.

Recent ad based threats, Ransomware attacks, and personal use of business devices have led to new challenges facing IT professionals including:

## Loss of Data Integrity

Backup copies of files become critical when existing files get corrupted. Unfortunately, some types of corruption like Ransomware can ruin all existing copies of files. If file backups are stored on local network drives or drives attached to a compromised device, these files may be lost forever.

The need to have more than one version of a file backed up is increasingly important to business continuity. These files should also be easily accessible at any time, from any place and device, to accelerate the recovery process. The right cloud backup service will provide seamless integration using automated jobs, and will support file versioning via retention to prevent any files from being lost when a device is compromised.

## Need for More Flexible Backup Jobs

Traditionally backups are run on network equipment rather than individual user devices. User files are stored on network drives and these drives are located on the devices being backed up. These backups generally occur at night when the likelihood users will be accessing files or network resources are minimal.

One of the greatest challenges facing IT today is finding a solution which will back up larger and larger amounts of data while having a smaller footprint on network resources. As files are increasingly stored on local devices and threats mutate, backing up files on individual devices becomes essential. Just as importantly, these backup jobs need to be quick and efficient so they do not slow down network or local device resources.

## Challenges with Existing Backup Solutions

The two main types of business backups are:

- Traditional Onsite Backups
- Cloud Based Backups

### Traditional Onsite Backups

Traditional backups include data backups created and stored locally. These backups can include tape backups, NAS devices, or other local storage. Storing a rotating version of recent backups at an offsite location is important when using a traditional backup solution. However, even when accompanied with offsite storage, access to the files is not available remotely and onsite backups do not protect data from natural disasters, backup hardware or media failure, or theft.

Some of the benefits of a traditional onsite backup are:

- Equipment and Data are all Local – Complete control over backup equipment and each copy of business data are controlled by the business. This reduces the physical risks to the data including theft, loss or unauthorized access.
- Reduced Recovery Time – Traditional onsite backups are available for immediately starting the recovery process. Depending upon the connection type and network cards in place, communication between an onsite backup device and other equipment can be faster than downloading the data directly from the cloud. When recovering large amounts of data after an equipment disaster this speed can prove extremely helpful in reducing costly down time.

Some of the limitations of a traditional onsite backup are:

- Testing Backup Files – Testing backup files is an integral part of the backup process. If files are never tested, there is no guarantee backup copies will restore business data if an emergency occurs. Restoring from a tape or NAS device is a manual process which includes finding a data set to restore a file from, copying the file, and testing the file to verify it is intact.
- Offsite Location for Backup Copies – Traditional onsite backups are extremely limited in their ability to provide data recovery if at least one copy of the data is not regularly rotated to an offsite location. Often the backups are stored onsite causing them to have almost the same risk as the live files. If an offsite location is used, it needs to be secure and far enough away to avoid the same natural disasters. Offsite locations can add to the total cost of data backups.

## Cloud Based File Storage

Cloud based backups use very different methods to protect files. By default, cloud based backups are available at any time as they are hosted in the cloud. Any device with Internet access can recover files at any time using a web interface.

Some of the benefits of cloud based file storage are:

- Testing Backup Files – Testing backup files from cloud based storage is quick and simple. All files are available for download at any time from any device with Internet access. Simply download any file and verify the file is intact.
- Disaster Recovery – Files are stored at an offsite location meaning they are still accessible and recoverable in the face of equipment failure, theft or loss, vandalism, or natural disasters.

Some of the limitations of cloud based file storage are:

- Network Bandwidth Needed for Backups to Run – Initial file uploads, especially when large amounts of data are being transferred, can take days to run. This means business data could be potentially unprotected during this time until the first copy of the data is uploaded to the

cloud account. As the initial upload runs, network bandwidth can become heavy and affect other programs using the network to communicate between devices and users.

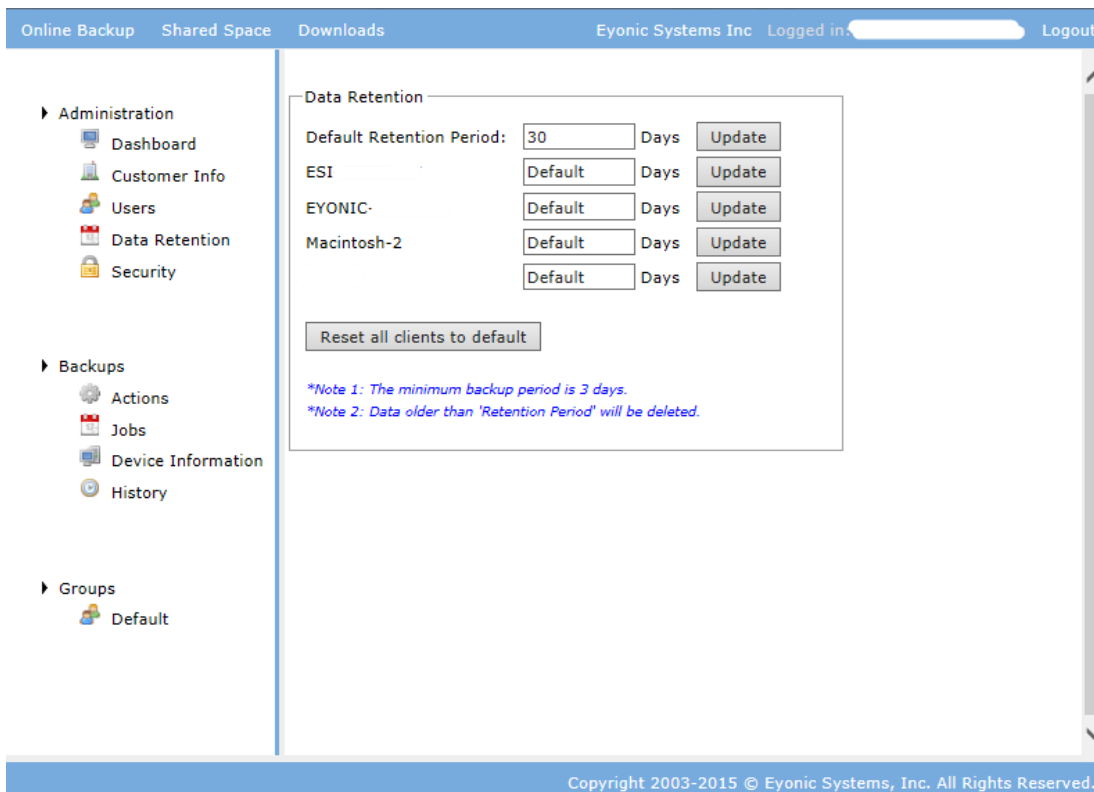
- Slower Recovery from Data Loss – As with the initial file upload, recovering from data loss by downloading all the files from the cloud can take time. Additionally, the network bandwidth is once again heavy which can affect other programs and users accessing network resources and the Internet.

## Eyonic Systems' Online Backup Service

Eyonic Systems' online backup service is a cloud based service. With an offsite copy, business data is safe even in the face of natural disasters, onsite device failures, theft and loss. Our online backup service can save most businesses time and money as plans are scalable on demand. No need to sign up for plans based on future needs the way equipment must be purchased. Eyonic's cloud services allow you to sign up for current requirements and grow as needed.

Some of the other benefits of using Eyonic's online backup service are:

- File Versioning to Protect Files – In addition to protecting from device failure and natural disaster, overwrites can also be detrimental to files and business continuity. File retention protects overwritten files from corruption due to malware, viruses and Ransomware, whether on a business or personal device. Retention also protects files when they are updated with mistakes and previous versions are desired.



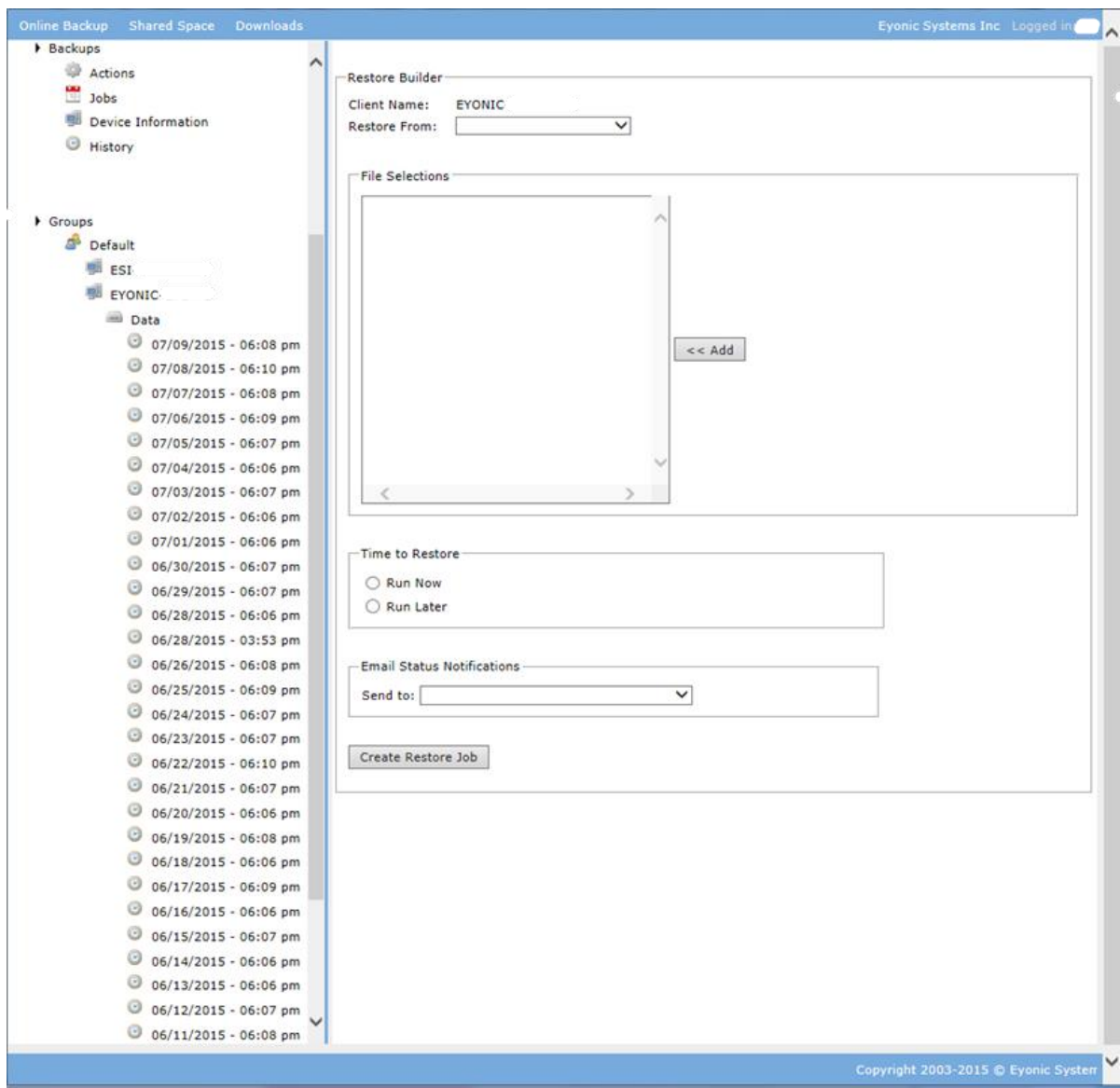
The screenshot shows the 'Data Retention' settings page in the Eyonic Systems online backup service. The page has a blue header with navigation tabs: 'Online Backup', 'Shared Space', and 'Downloads'. The user is logged in as 'Eyonic Systems Inc' and can click 'Logout'. A left sidebar contains a navigation menu with categories: Administration (Dashboard, Customer Info, Users, Data Retention, Security), Backups (Actions, Jobs, Device Information, History), and Groups (Default). The main content area is titled 'Data Retention' and contains a table of settings for different clients:

Client	Retention Period	Unit	Action
Default Retention Period:	30	Days	Update
ESI	Default	Days	Update
EYONIC-	Default	Days	Update
Macintosh-2	Default	Days	Update

Below the table is a 'Reset all clients to default' button. Two notes are displayed: '\*Note 1: The minimum backup period is 3 days.' and '\*Note 2: Data older than 'Retention Period' will be deleted.' The footer of the page reads 'Copyright 2003-2015 © Eyonic Systems, Inc. All Rights Reserved.'
























- Testing Backup Files – Files can be tested at any time in a variety of ways including:
  - Creating a scheduled restore job – perfect for a large number of files or folders
  - Opening a file in the web interface – great for testing random files
  - Downloading a file from the web interface – the best way to check a database or special application file type
- Easy Access to Files after Data Loss – Instant access is always available to any files backed up using the web interface. Additionally, Enterprise customers can request overnight shipment of an encrypted copy of their data. Enterprise customers can have their data shipped overnight for free once a year in the case of data loss or failure.



- Uploading Files & Seed Backup – Initial backups are not throttled by Eyonic Systems and run as fast as customer Internet connections allow. Daily and monthly upload limits do not exist. Enterprise customers can request to copy their data onto a supplied encrypted device for initial seed backup. Jobs can be scheduled for any day and time to prevent them from interfering with other bandwidth intensive applications.
- Quick File Backups – After the initial seed backup only new and modified files are uploaded to the cloud. All folders and files are scanned for changes allowing backups to be quick since only new and changed files are transferred. Additionally, data is deduplicated and compressed before sending, reducing the impact on bandwidth and making the storage more efficient.
- File Availability – Files can be accessed, recovered, or downloaded from any device with Internet access at any time using the web interface. This means files are immediately available to a mobile user even if a device is lost or stolen. Simply log into the web interface from a different device and access the needed files.

## Service Comparison

The following table breaks down the different features and their availability with each type of service including Eyonic’s online backup service.

	Traditional Backup	Cloud Based Storage	Eyonic Online Backup
Offsite Location for Disaster Recovery	 N/A	 Limited Capabilities	 Complete Backup
Quick Data Recovery			
Data Protection via File Versioning			
Easy Access to Multiple File Versions			
Quick File Backups			
On Demand Scalability			
Efficient Bandwidth Usage			

## Conclusion

With the increase in external attacks and internal misuse, threats to business data are very real. Maintaining business continuity requires keeping the confidentiality, availability and integrity of data at all times. This requires a balance between allowing access to those who require it to do their jobs and preventing everyone else from gaining access. Recent trends including attacks focused on users' data require better disaster recovery protections if business data is going to stay safe.

Eyonic Systems' online backup service provides data protection in multiple ways. By providing an offsite backup of business files, they are protected from natural disaster, onsite device failures, theft and loss. Using our data retention features, previous versions of files are maintained allowing them to be accessed at any time which is important after a malware, virus, or Ransomware attack rendering the existing files unusable. Additionally, because files are scanned, deduplicated and compressed before being uploaded, backup jobs are bandwidth and storage efficient. Lastly, plan sizes are scalable on demand, meeting the needs of your business every step of the way.

## References

1. ["Yahoo ads may have infected thousands with malware; what to do if you're one"](#). *Examiner*. January 5, 2014.
2. ["Most Popular retail websites in the United States as of March 2015, ranked by visitors \(in millions\)"](#). *Statista*. March 2015.
3. ["Online Shopping by the Numbers"](#). *Statista*. November 13, 2014.
4. ["Update: McAfee: Cyber Criminals using Android malware and ransomware the most"](#). *InfoWorld*. June 3, 2013.
5. ["How Do People Spend Their Time Online?"](#). *Social Times*. May 7, 2012.



## About Eyonic Systems

Eyonic Systems is dedicated to simplifying technology. We offer a suite of responsive technology services for people and businesses with any level of experience to save them time and money. These services include network integration, online backup, drive destruction, and enterprise file sharing. Our services are built to provide the confidentiality, integrity, and availability people expect from technology services. Our services are a great value because they are flexible and provide on demand scalability.

Businesses of all sizes and types use Eyonic's services to safely manage their offsite data both for disaster recovery and accessibility. Whether protecting data, sharing data, or preventing data from falling into the wrong hands, we have a service to meet your unique needs. We believe protecting the integrity of data starts with the right network design, and does not end until equipment once storing data is professionally destroyed.

Eyonic Systems is a privately held business located within the United States. For more information, visit us at [www.eyonic.com](http://www.eyonic.com). To get started with your free 15-day trial, visit [www.eyonic.com/signup](http://www.eyonic.com/signup).

### Connect with Us



1-855-439-6642  
1-707-317-1167 Fax  
607 Elmira Road Ste 113  
Vacaville CA 95687

© 2015 Eyonic Systems Inc.

Trademark Information: Eyonic Systems logo and tagline are registered trademarks of Eyonic Systems Inc. in the US. All other trade names are trademarks or registered trademarks of their respective holders.