Introduction
Due to the sophistication of today’s threat landscape, ransomware can be difficult to catch right at the door. Once this malicious malware crosses the threshold, a business user is hit by a daunting message, informing the user that their computer and files have been seized, and payment is required. What's equally perturbing is that ransomware doesn't discriminate—it can happen to the mom and pop shops to large enterprises. It’s not a matter of if a business will get hit, but when.

Protecting Your Organization from Ransomware
Attackers have created many different variations of ransomware over the past few years, such as CryptoLocker, CryptoWall, TorrentLocker, TeslaCrypt, Locky, Petya, WannaCry, Bad Rabbit, and Samas. Each of these variations use new methods of infecting their victims’ computers, thereby compromising the data and network of many organizations worldwide.

So how can an organization protect itself from ransomware attacks? Luckily, there are numerous precautions that can be implemented to prevent and recover from a ransomware attack. However, a proper ransomware prevention strategy can be summed up into three categories: education, security, and backup.

Education
Education is the first line of defense against ransomware. In order for malware to successfully infect a system, it needs some form of user interaction. In a research survey conducted by Osterman Research, and sponsored by Malwarebytes, emails with malicious links or malicious attachments account for 90 percent of ransomware infections. Educating your users about the different types of email and web-based threats can drastically reduce the risk of being infected.

Security
Having multiple layers of defense against web- and email-based threats is essential in preventing malware from entering your organization’s network. Since most ransomware attackers target end users, preventive measures on workstations, such as antivirus programs and keeping the operating systems up-to-date, are crucial. While having good antivirus software and patched operating systems are a good start, more advanced layers of security are going to be necessary to prevent most of the threats from even reaching their intended targets. These security measures include securing your network perimeter with a capable firewall, securing your email solution with an email security gateway or service, and having a web application firewall to prevent access to malicious web content.
**Data Protection**

Having a sound backup and recovery plan is usually one of the most overlooked measures in the fight against ransomware, but it is the most crucial. Even with all of the preventive measures listed above, there is still a chance that an end user will become infected with ransomware and put your organization’s critical data at risk. Successful backups with an effective retention policy enables organizations to recover from ransomware attacks without having to pay any ransom to the attackers, or losing the data altogether. Regularly performing and testing backups will help limit the impact of data or system loss and expedite the recovery process.

**Barracuda Cloud Control**

![Diagram of Barracuda Cloud Control]

**Not Just Any Backup and Recovery Solution**

In an [Osterman Research](#) survey, 49.4 percent of companies surveyed indicated that they had been hit with one or more ransomware attacks in the last 12 months. As mentioned earlier, it is not a matter of if, but when your organization will be attacked. Recovering your data and recovering it fast is critical. So how can Barracuda help?

**Fast Backups, Fast Recovery**

Barracuda Backup delivers fast backups, fast offsite and cloud replication, and fast data restores. With Cloud LiveBoot, you can even spin up virtual machines in the cloud, so you can be up and running again in minutes, rather than hours or days. In the event of a ransomware attack or other disaster—from an earthquake to a spilled soda—Barracuda Backup gives you the ultimate protection against compromised, corrupted, lost, deleted, or encrypted data.

Multi-streaming technology built into the Barracuda Backup Agent for Windows and Linux increases initial backup and recovery speeds significantly. Shorter backup windows allow you to run backups more often, shortening

---

"With Barracuda Backup, we were able to quickly restore our stolen data, allowing us to address this attack with minimal business impact."

A.J. Murray,  
IT Manager  
Hayward Tyler
your recovery point objective (RPO). In addition to faster backups, recovery performance is also increased by the presence of multiple streams of data being written to the target location at once. This helps lower your recovery time objective (RTO) and gets your business back up and running quickly.

**Enhanced Offsite Replication**
Fast backups alone aren’t enough. You also need fast offsite replication to close the window of vulnerability to a disaster that might take out your onsite backup. Barracuda Backup uses an enhanced, high-performance replication queuing system. Combined with Barracuda’s inline replication, which begins sending data offsite as soon as data reaches the backup appliance, the queuing system helps to further protect you from losing data.

**Efficient Data Storage and Retention**
With its efficient inline deduplication engine, Barracuda Backup is capable of storing more data for longer periods of time. Having an effective retention policy is key to recovering from a malware attack. Barracuda Backup provides flexible and easy-to-configure retention. Policies can be created on a per-server basis with more maximum granularity and control, or on a global basis for simplicity.

**Protection Against Advanced Threats**
New ransomware variants are appearing rapidly, using new evasive techniques and targeting a variety of your network resources. They may target specific file or data types for encryption—HR, customer data, social security or credit card numbers, emails—whether on mapped network drives or open, unmapped shared drives requiring user credentials.

Barracuda Backup protects you against all the newest ransomware attacks. Additionally, unlike other backup solutions that may store backup files to a network share—where they are vulnerable to certain ransomware attacks—Barracuda Backup does not present itself as a network share. The data stored on Barracuda Backup is inaccessible to any other devices on your network, and the data itself is stored in a proprietary format that is only readable by Barracuda Backup.

**Conclusion**
While there are solutions that help stop ransomware in its tracks, there are cases where new and complex threats still make it onto the end user’s computer. Having a robust backup solution in place helps organizations skip the ransom, and immediately and successfully recover their data. Barracuda Backup does this with ease with fast backup and recovery speeds, an enhanced offsite replication engine, and efficient long-term storage and retention.