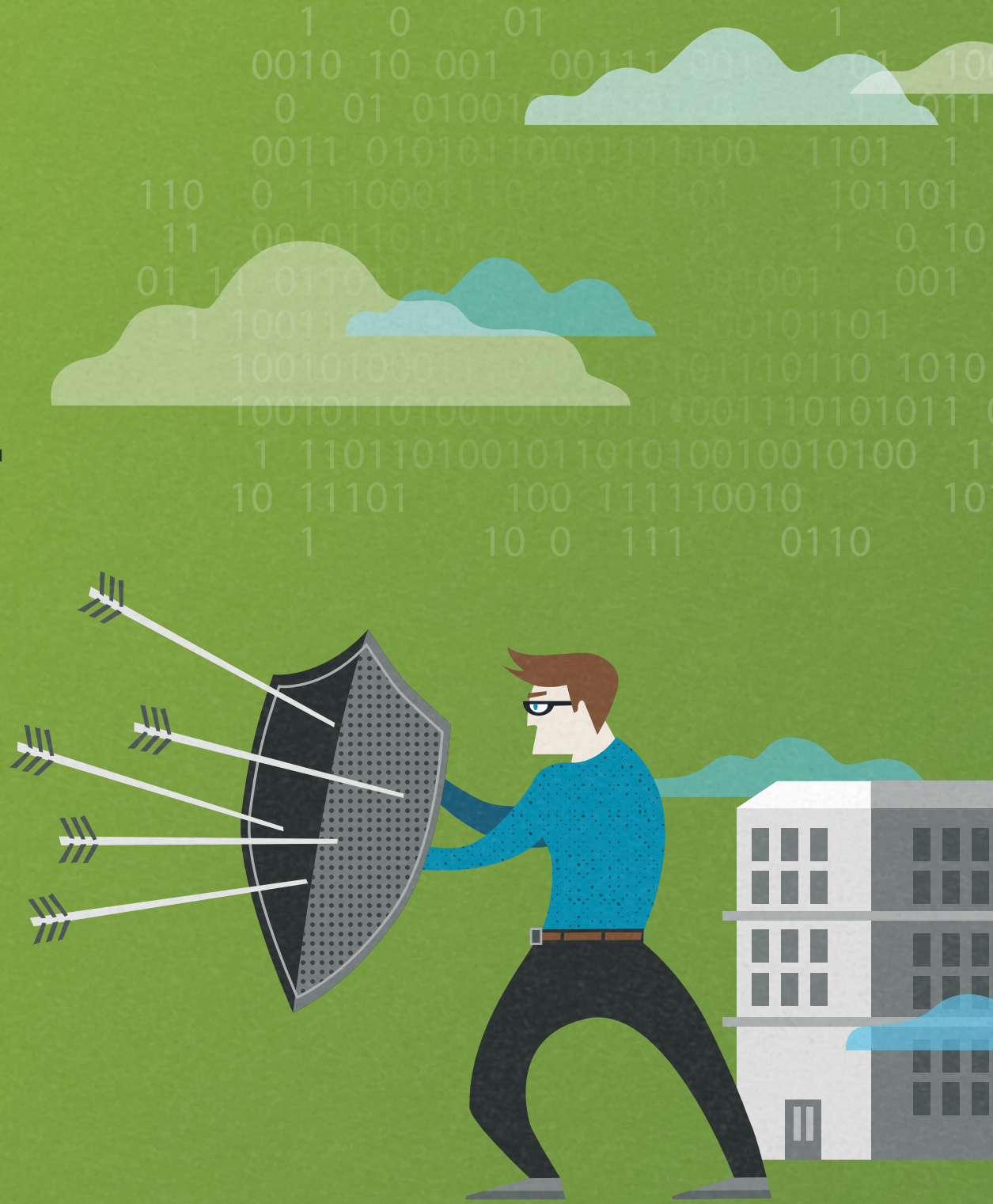
CARBONITE

Sharpen your ransomware defenses

Hidden truths and simple steps to help you win the battle

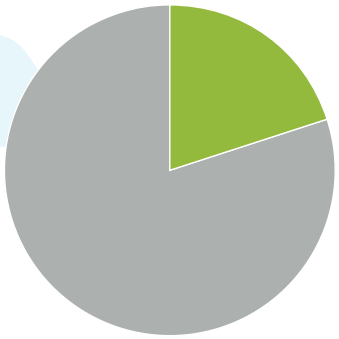


If you're not looking for an edge against ransomware, you need to be.

Businesses are getting attacked far more frequently than anyone is talking about. Half of businesses hit with ransomware never report it. In addition to underreported attacks, there's also the problem of undetected attacks.[1]

The IT pros who are winning the battle against ransomware are doing so by using a backup solution and thinking about ransomware before it strikes. Backup is the number one reason why businesses are able to avoid paying a ransom to retrieve their data. A smart backup strategy ensures businesses have a second, clean copy of data in the event of an attack. But backup can also help you identify suspicious activity that can go undetected.

In fact, a sound backup strategy combined with a proactive—as opposed to reactive—approach to fighting ransomware can give you exactly the edge you need.



20%

of businesses worldwide reported an incident involving ransomware in 2016.

—Kaspersky Labs, IT Security Risks Report 2016

Sharpen your ransomware defenses

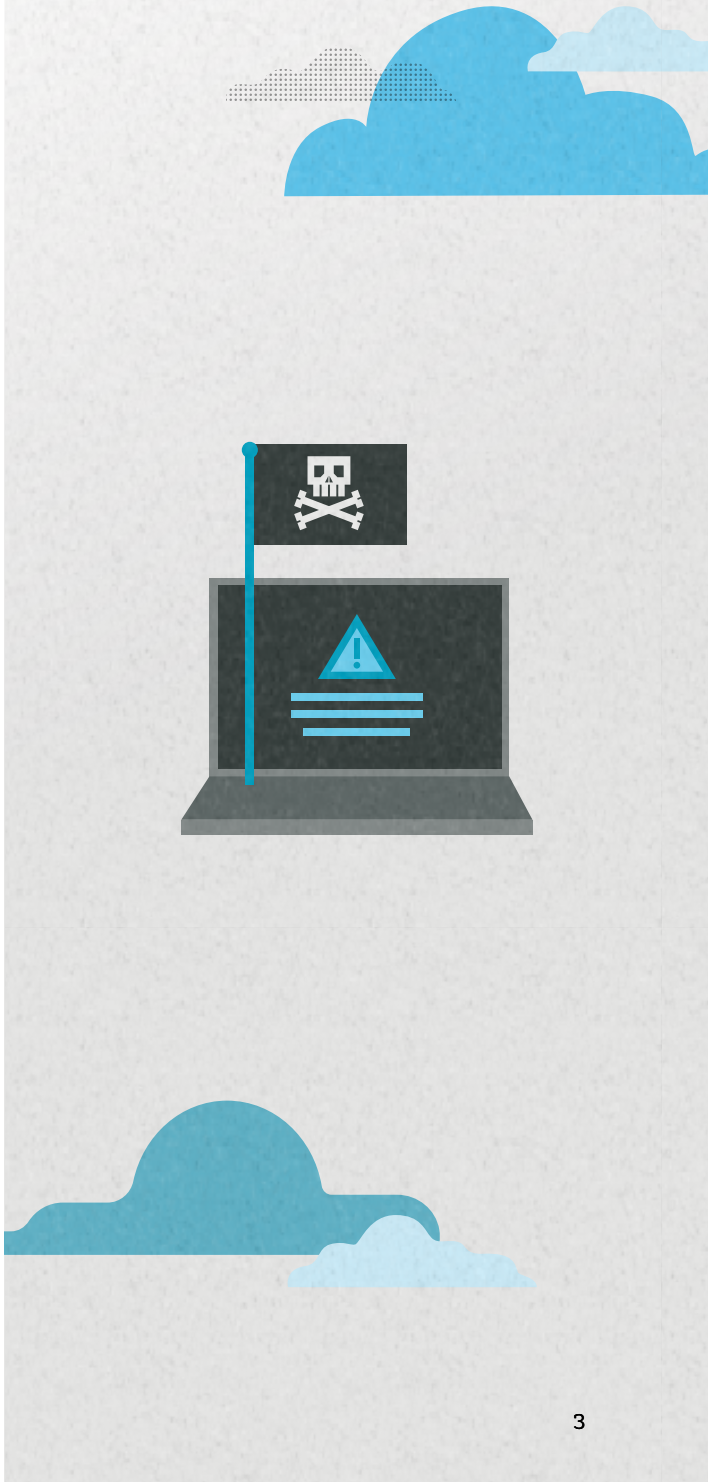
The value of early-stage detection

When it comes to ransomware, a lot can happen between the initial attack and the moment when the virus reveals itself. Detecting an attack early can mean the difference between a simple recovery effort and a catastrophic event that can take days or weeks to remediate. Anyone who manages a network of significant size knows how important it is to have backup with point-in-time recovery. But backup is useful for more than just recovery. You can also use your backup solution to discover an infection early and simplify any recovery effort you may have to undertake.

Detecting an attack early can mean the difference between a simple recovery effort and a catastrophic event that can take days or weeks to remediate.

Ransomware signals

Ransomware doesn't always reveal itself immediately upon penetrating the network. From the time it enters the system to the time it reveals its presence—by making a ransom demand—ransomware will often propagate deeper into the network, far beyond the infected workstation. Shared drives and anything connected to them are vulnerable. Anyone who runs a program on an infected file server could introduce the virus to his device. And each additional infected device increases the threat, and the cost of remediation, by an order of magnitude. But if you're running daily backups, and you have a retention schedule that preserves them for up to 30 days, then a quick examination of backup sets can reap rewards.



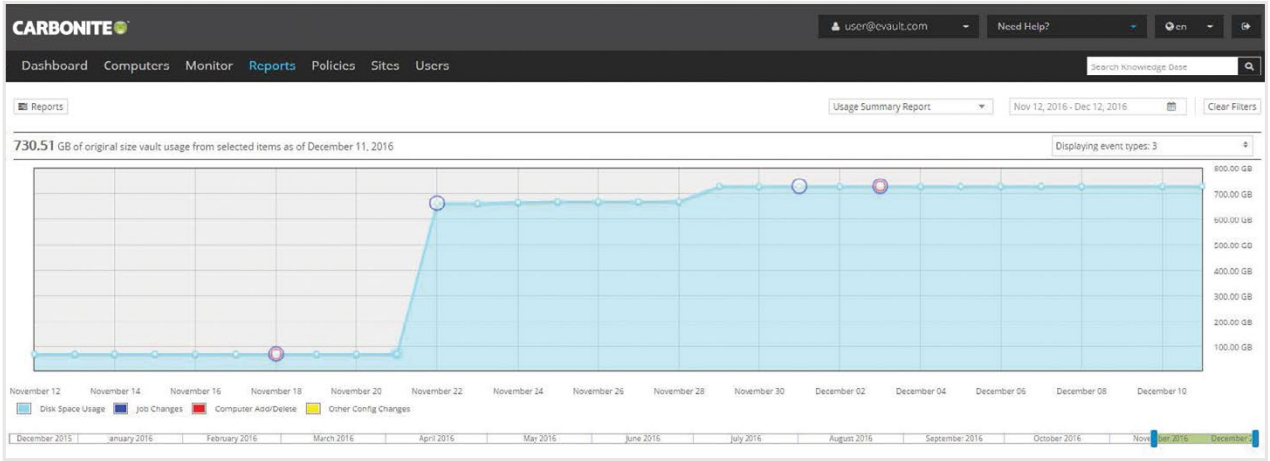
Backup sizes: clues to malware infections

It's normal for backup sizes to change from day to day, especially if they contain files that are constantly being worked on. But the rate of change should fall within a normal range, roughly 2% to 3%, for benign activity. The great thing about backup is that it gives you a direct comparison between what a file looks like from one day to the next.

If your backup size changes dramatically over 24 hours, it could be a sign that a ransomware virus has changed the contents of your files. You might also see files added to the backup that were not put there by you.

There are other forms of abnormal activity to look out for. An excessive number of access attempts by a device on the network could be a sign of suspicious activity. Repeated attempts that return error messages should be investigated immediately. Anomaly detection software can automate the task for environments where manual methods are not practical.

If your backup size changes dramatically over 24 hours, it could be a sign that a ransomware virus has changed the contents of your files.



Sharpen your ransomware defenses

Turning back the clock

By running daily backups and checking backup sizes regularly, you stand a better chance of full recovery after an attack. The way Carbonite delivers on this is simple. Carbonite solutions powered by EVault technology are configured with a default retention schedule of 30 daily and 11 monthly backups for a total of one year of backups. Most organizations that experience ransomware find out within 30 days of the infection. If you discover suspicious activity or an infected file, Carbonite allows you to recover from a clean backup set, most likely the prior day's backup. If there's an infected file that's older than 30 days, you can recover a clean version from a prior monthly backup.

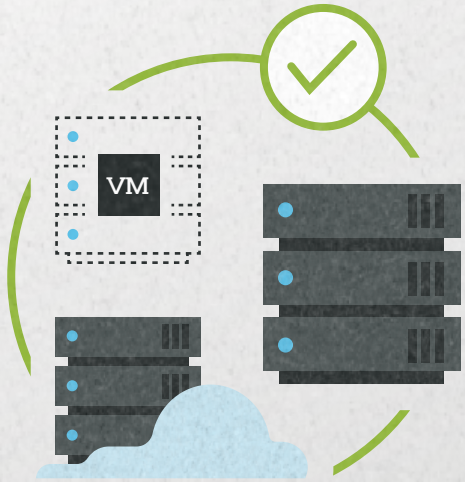
Files backed up are encrypted and cannot become infected by ransomware. But files that are already infected and have not been detected will be added to the backup set. That's why it's critical to catch ransomware and other malware as soon as they penetrate your system and before they demand a ransom payment.

This default retention schedule, combined with proactive monitoring for suspicious activity, will ensure that you never lose more than a day's worth of data. Businesses with more stringent recovery point objectives should consider a high availability solution.

For mission-critical applications and data, a dual approach combining high availability with backup including point-in-time recovery can deliver always-on services while reducing the risk of criminal encryption.

The truth about prevention

Prevention is easier than recovery. End user education combined with firewalls and anti-virus software is always the first line of defense. But anti-virus can only discover known viruses, while new ones are popping up all the time. Backup with daily and monthly retention, and faithful monitoring for suspicious activity, will pay dividends in the fight against ransomware—and protect your growing business from threats to crucial data.



Extra security for critical data

Most organizations cannot tolerate interruptions to critical applications like email and databases. Extra security is necessary to protect these high-value targets. A high availability (HA) solution is designed for this level of protection. With HA technology—like Carbonite Availability *Powered by DoubleTake*—early detection and point-in-time recovery drastically improve recovery speed and minimize data loss. Within seconds of detection, you can fail over instantly to the nearest clean recovery point, immediately prior to the infection.

Four key takeaways

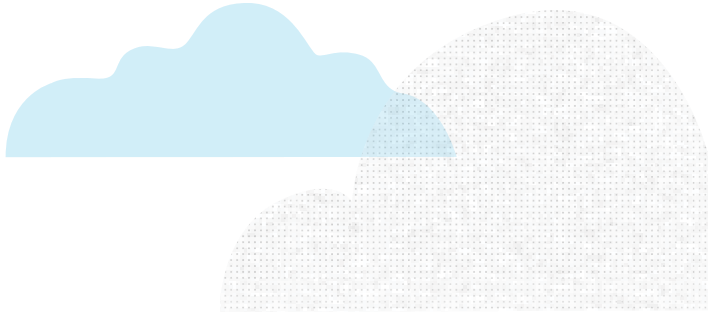
Ransomware doesn't have to cripple your business.

1. Determine your RPO and RTO requirements.

2. Keep at least 30 days of daily backups.

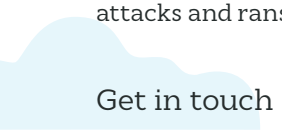
3. Look out for drastic changes in your backup size.

4. Educate your users about ransomware and other email scams.



Join the fight

The ransomware epidemic is growing due to the increasingly strategic role data plays within organizations. If data weren't so valuable, criminals wouldn't devise elaborate means to gain unauthorized access to it. But businesses can deprive cybercriminals of this lucrative revenue stream by taking steps to defend against ransomware. The rate of attacks is increasing. Education is your first line of defense. To find out the latest information on ransomware threats, attacks and ransom demands, visit fightransomware.com.



Get in touch

Phone: 800-683-4667
Email: DataProtectionSales@carbonite.com

[1] "The Rise of Ransomware," by Ponemon Institute, sponsored by Carbonite, November 2016.