WHITE PAPER

CARBONITE® + WEBROOT®
opentext™ Business Solutions

Preparation, Recovery, and Remediation

A Holistic Approach to Ransomware Protection

Introduction

When your organization gets hit by ransomware, it needs to be prepared with an exercised Business Continuity and Disaster Recovery (BC/DR) plan to help it resume operations as quickly as possible. Key steps and solutions must be followed to prepare and respond to cyberattacks against your organization.

These may be as simple as the deployment of antivirus and backup and recovery applications for your end-users or a more complex approach with security operations center (SOC) tools or managed response solutions coupled with network security tools such as DNS and Web filtering, network and endpoint firewalls, VPNs, backup and recovery and others.

The bottom line is if prevention tools fail and your organization is compromised, you need to have a protection plan that gets your company assets and resources back to work quickly and securely.

What preparation is needed

When contemplating an in-depth plan, specific questions come to mind—the whats, hows, whys, and most importantly, the whos, must be defined. When asking these questions, organizations should be prepared to identify the resources, people and applications involved. How to react to the situation and how to execute the steps and processes required to reduce damage as quickly as possible should be worked out in advance.

Below are some questions to get us started. Then we will examine how Carbonite® Endpoint coupled with Webroot® Business Endpoint Security can provide a cyber resilient solution that, when included in your BC/DR plan, can reduce risk to your organization.

Key questions:

1. Who will be involved in recovery and communication when your DR plan is in action?
2. How much downtime can your organization withstand?
3. What service level agreement (SLA) do I need to provide to the business and users?
4. What users should be recovered first?
5. What tools do we have to reduce risk and downtime within the environment?
6. How are user networks separated from operational or business networks?
7. How quickly can data protection tools get us up and running again?
8. Can users get their data back if an endpoint device is compromised?
9. Can we determine when the ransomware first hit the network or endpoint devices?
10. Are we able to stop the proliferation of ransomware or malware throughout the network?
11. Can we recover quickly to a specific point in time?
12. Can our users access their data from the cloud before it's been restored?

Application needs

The solutions below, coupled with an exercised BC/DR plan, will help reduce your organizational risk exposure and allow for quick remediation.

Endpoint security

First, we need a solution for endpoint security to determine what events took place and when. In our example, Carbonite + Webroot using BrightCloud® Threat Intelligence make up the backend of our automated detection and response (ADR) solution.

These tools offer:

- Centralized management
- Notifications when something unknown is seen on an end device
- AI and machine learning to classify threats that become active
- Automate security tasks like threat investigation, validation, and remediation
- Speed up security alert response times, reduce downtime
- Improve detection accuracy with fewer false positives
- Stop present threats and also predict future threat sources for proactive protection
- Boost operational efficiency and efficacy

They can be paired with an endpoint detection and response solutions (EDR) that:

- Ties into security operations center (SOC) tools such as a security information & event management (SIEM) solution
- Automate security tasks like threat investigation, validation and remediation
- Speed up security alert response times, reduce downtime
- Improve detection accuracy with fewer false positives
- Stop present threats and also predict future threat sources for proactive protection
- Boost operational efficiency and efficacy

When Webroot® DNS Protection is added for network security you can:

- Stop 88% of threats at the network's edge
- Enforce web access policies
- Content-Based Filtering

Data backup and recovery

Next, we need a solution for endpoint data protection and recovery should a threat get past the outer permitter

Carbonite® Endpoint for endpoint data recovery:

- Provides a solution for recovering user state data to a new or reimaged device
- Allows users the ability to access via a web portal all of their files
- It gives an easy way to recover from a point in time before the malware/ransomware hit the device/s

Lines of Communication

Equally important as the technology is the people who manage and maintain the systems that support the different business units within an organization. For example, security teams and your endpoint support teams need to be in regular discussions about how the teams will communicate when under attack. Organizations need to determine who is responsible, what systems and when they should be brought into the process when under attack.

System Response Ratings

A system response rating system can assist in determining which systems or employees require a higher degree or speed of response. To do this, you must specify the value of the system or resource and where that resource sits regarding protection or remediation priority. This is often determined by the value of the resource in monetary terms. For example, if the loss of a specific system would incur a massive loss of incoming revenue, it might be necessary to place a higher priority in terms of protection and remediation for it over say a standard file server.

The same can be said for specific individuals. Often C-level resources and mid-tier executives need to be out in front of a situation. Making sure their resources (laptops and portable devices) are protected and uncompromised is critical. They're often as important as specific servers. It is necessary to classify systems, users and customers regarding their criticality to the business and place priorities based on the rating of those resources.

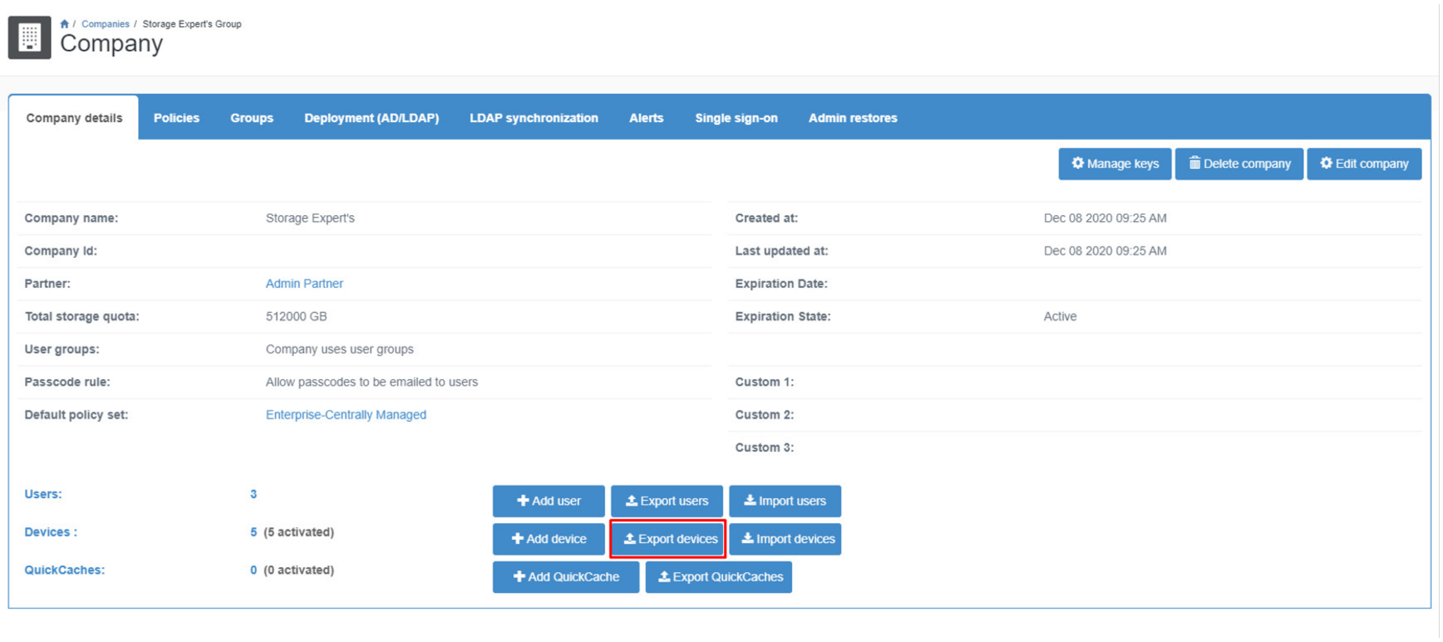
Now that we know a bit of the who, what, and how let's look at how to recover from a single system to an entire enterprise.

Recovery and Remediation

Recovery is an integral part of any BC/DR plan. It gives organizations a playbook of what to do and when. But it's not enough to recover your data. You also need to understand the remediation process for preventing further infection of systems or the proliferation of malware within an organization. The steps outlined here are specific to the Carbonite® Endpoint solution. We will also refer to Webroot ADR for businesses as a tool to determine when an infection hit a system or endpoint.

Scenario

Ransomware hits your users' laptops, encrypting all its the data. The laptops have Webroot® Business Endpoint Protection software but no DNS protection. All other standard network security is in place including firewalls, VPNs and some network segmentation. There is a security team as well as an end-user support team. The ransomware that hit is polymorphic, meaning that it changes to prevent detection even if the first iteration of the ransomware is isolated.



Company name:	Storage Expert's	Created at:	Dec 08 2020 09:25 AM
Company Id:		Last updated at:	Dec 08 2020 09:25 AM
Partner:	Admin Partner	Expiration Date:	
Total storage quota:	512000 GB	Expiration State:	Active
User groups:	Company uses user groups		
Passcode rule:	Allow passcodes to be emailed to users	Custom 1:	
Default policy set:	Enterprise-Centrally Managed	Custom 2:	
		Custom 3:	

Users: 3

Devices : 5 (5 activated)

QuickCaches: 0 (0 activated)

Solution

We look at our Webroot console to tell us when and where the malware was first seen. Admins will want to ensure that, if there are backups still running, they are suspended to prevent infected data from being protected and the ransomware from being backed up.

This can be done either from the dashboard or from an automated script to suspend all devices. With Carbonite's extensive APIs, it's possible to automate processes like bulk suspend devices and bulk restore devices. At this time, it may be advisable to block traffic from the infected area where network segmentation is configured to prevent the spread of malware.

Now we can review our protection platform and determine the date file was noticed, its dwell time and when the ransomware's encryption began executing. After answering these questions, we can investigate how the organization was breached.

Understanding the origin of a breach is critical to stopping further infection. Since ransomware was able to infect devices, we need a tested and reliable recovery process. Recovering systems and data will require leveraging the tools at our disposal to perform mass restores of end-user devices. The best place to get more in-depth detail on the options for a script or API calls for automation can be found here.

With Webroot, you can see when an unknown threat hit a system and when it started to execute the attack. Understanding the timeline of events is also critical to the recovery process. It's essential to know the timing for the first step in the restore process to set your time to restore. We do this in our script with Epoch time. You can convert Epoch time here. After the date and time to restore have been determined, it's necessary to add all the devices to restore into our CSV file.

This can be done simply by exporting devices from the Carbonite® Endpoint dashboard or leveraging a previous emailed device details report. See an example at the bottom of page 3 to locate where admins can export the devices from in the dashboard.

Once the device list is in a spreadsheet, identify where the restores will go using a source device ID number to a target device ID number in the spreadsheet. The source will be the suspended devices for which backups were stopped to keep bad data from being stored. The target will either be the same device or a new device. If these are new devices, it's important to make sure they have been installed and activated.

After gathering the data, source, target device IDs, date and time to restore from, combined with our bulk restore script, we can initiate a bulk restore to the same laptops or new laptops. In the interim, while restores are happening, your end users can login to their Carbonite® Endpoint web access page and return to work immediately.

Summary

Placing the necessary tools and establishing communication channels across a business are essential steps in protecting an organization. Classifying systems in terms of importance is also an essential part of this process. Finally, we want to lock down the attack location and determine the time it hit systems to best remediate and recover.

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.