

▶ **LOCKDOWN
LESSONS:
CYBER RESILIENCE
STARTS HERE**



Introduction

They say the best defense is a good offense, but in cybersecurity we often say the best defense is prevention. Yet, as cybercriminals continue to innovate and refine their methods, the truth is complete prevention of attacks may never be fully possible. Despite efforts by organizations to layer up their cyber defenses, attackers are innovating and automating in new and unpredictable ways, forcing business leaders to shift focus from prevention to response and recovery. In order to keep your business and customers safe, it's essential to understand how to build cyber resilience and put practices and policies in place that not only help to prevent attacks, but also enable you to recover quickly when they inevitably happen.

► **Shifting from Cybersecurity to Cyber Resilience**

Businesses trying to achieve cyber resilience are confronted with a rapidly evolving threat landscape. With attacks on MSPs and small and medium-sized businesses (SMBs) on the rise and increased fines for breaches, maintaining a strong cyber resilience posture is a matter of survival. This section explains the difference between cybersecurity and cyber resilience and why it matters for businesses.

Cyber Resilience is Vital in a Remote Work World

The massive shift to remote work leaves work-from-home employees vulnerable to data breaches, ransomware and other internet-enabled attacks. Business leaders must prepare for the unique challenges of supporting virtual employees. This section explores the biggest threats to remote workers and explains how to keep remote workforces secure.

How to Build a Cyber Resilient Business

Effective cyber resilience starts with people and is bolstered by technology. A layered approach of user education and cybersecurity solutions is the strongest way to secure your business and customers. This section describes the framework for achieving cyber resilience and explains how people and technologies work together to protect businesses from end to end.





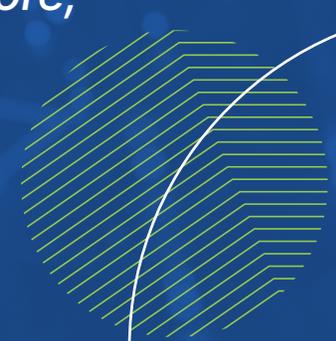
LOCKDOWN
LESSON **ONE**

Shifting from

Cybersecurity to Cyber Resilience

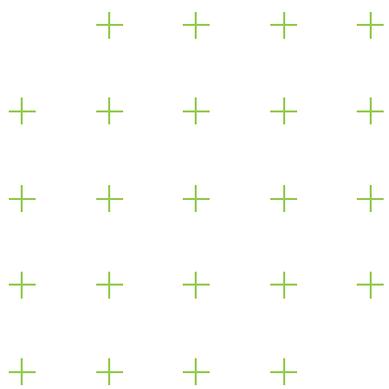
What is cyber resilience?

Think of Cyber Resilience as “digital fitness.” It’s the ability to keep data and devices online no matter what threats come your way. Like an athlete preparing for competition, a cyber resilient business has the necessary training and tools to protect businesses and their customers before, during and after an attack.



▶ Those in cybersecurity circles commonly borrow from military strategies when approaching digital safety. For example, “Defense in Depth” is a well-known method for protection. When one security protocol fails, the next layer in a series of defenses takes over to turn away an attack. It’s a useful framework, for sure, but without an end-to-end strategy and a cyber-aware mindset, this approach alone can fall short.

Often, cybersecurity and cyber resilience are used as synonyms, whereas cybersecurity should be considered an essential component of cyber resilience. Businesses need both security and resilience to achieve complete end-to-end protection against cyber threats. So, what exactly is the difference?



CYBERSECURITY

is the protection of users, connected devices, systems and data from cyberattacks.

CYBER RESILIENCE

refers to a company’s ability to mitigate damage to systems, processes, and reputation, and carry on once systems or data have been compromised.

Cybersecurity is just the first step to cyber resilience. It centers on protecting organizations through firewalls, VPNs, anti-malware software and security awareness training (SAT). On the other hand, cyber resilience accounts for what happens when those cybersecurity measures fail. It includes backup and recovery strategies that support business continuity. The ultimate goal in creating resilience is to put systems and a company culture into place that help to effectively prevent, detect and react to any adverse cyber event.



Cyber resilience is the culture and story around your approach to security. It’s about building a set of practices and products that lay a strong foundation and adopting a mindset where everyone in the business is security aware.”

-Nick Emanuel, Senior Director of Product, Webroot



► WHY DO BUSINESSES STRUGGLE WITH CYBER RESILIENCE?

Businesses trying to achieve cyber resilience are often vexed by the fact that threats are always shifting. What's more, as humans, we're often bad at accurately assessing our own cyber-hygiene. In fact, our latest Webroot U.S. Cyber Risk report¹ found that in 2020, 89% of Americans thought they were good at security, but only 10% received an 'A' grade when questioned about their habits. No U.S. state actually managed better than a 'D' grade. This overconfidence combined with increasingly unpredictable, polymorphic threats is a recipe for disaster.

“*The ever-changing threat landscape makes cyber resilience hard because you're never sure what to look out for. Cyber resilience requires constant education as well as trust in your technology.*”

-Holly Spiers, Senior Product Marketing Manager, Webroot

“*Companies need to maintain their reputation and the trust of their customers. Having a breach doesn't make you a bad company, but how you respond will make a difference in customer perception. Making the best effort to protect your business is cyber resilience.*”

-Holly Spiers, Senior Product Marketing Manager, Webroot

► WHY SHOULD ORGANIZATIONS CARE ABOUT CYBER RESILIENCE?

In a digital-first world, cyberattacks and data loss are inevitable. No single layer of protection offers complete immunity. With attacks on SMBs rising, and hefty fines for breaches now enshrined in laws like GDPR or CCPA, maintaining a strong cyber resilience posture is a matter of survival. The good news is that by leveraging a layered cybersecurity approach and adopting a security-aware culture, businesses can bounce back from attacks. True cyber resilience is an organization's ability to keep business running and returning to normalcy quickly.

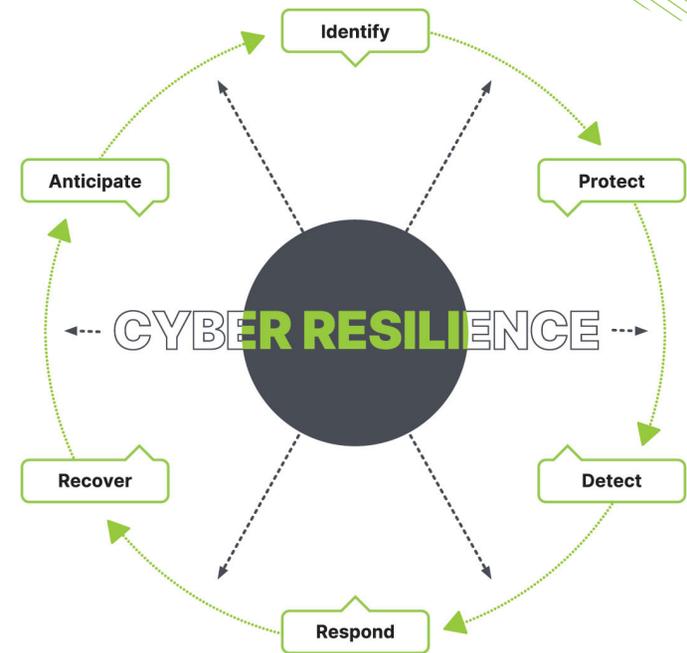


▶ WHAT DOES A CYBER RESILIENT BUSINESS LOOK LIKE?

Achieving cyber resilience should be high priority for all businesses, regardless of size or industry. Ultimately, resilience is the responsibility of every employee, not just the IT department. Building a resilient culture starts from the top down, with leadership encouraging sustained, long-term engagement and strategies that enable employees to internalize cybersecurity best practices. In other words, cyber resilience is not just an annual checkbox, but an ongoing part of business as usual.

The framework for successful cyber resilience includes four key areas:

- 1 Identify and detect:** The objective is to develop an organization-wide understanding of cybersecurity risks to systems, assets, data, people and capabilities, including those across that make up the IT supply chain.
- 2 Manage and protect:** This involves developing and implementing suitable safeguards to protect people, technology, assets and data and includes identity management and access control, protective solutions and SAT.
- 3 Respond and recover:** This entails implementing adequate incident response planning to ensure business continuity even if the business is the victim of a cyberattack (i.e., backup and recovery planning).
- 4 Educate and assure:** The final element involves ensuring the cyber resilience program is part of normal business operations. Ongoing training is vital and should be overseen from the top of organizations so that every employee engages in a culture of cybersecurity.



▶ THE MARKET OPPORTUNITY FOR RESILIENT BUSINESSES

Beyond the basics of protection, cyber resilience also offers the opportunity for MSPs to keep SMB customers and their end users safe. As ubiquitous connectivity and digital transformation continue to stretch IT resources for smaller companies, business leaders will look to cybersecurity experts who can help them protect their data and educate their employees. Together with Webroot and Carbonite's world-class solutions and training, MSPs are perfectly positioned to offer a suite of tools and training that provide end-to-end protection as well as ongoing security awareness training to keep users resilient.

“MSPs are perfectly suited to lead the charge of cyber resilience into the SMB market. They are already trusted advisors and can ensure customers are getting the most out of their cybersecurity tools and strategies.”

-Nick Emanuel, Senior Director of Product, Webroot

THE BENEFITS OF HAVING A CYBER RESILIENT BUSINESS:

- ✔ Security and Protection
- ✔ Enhanced Productivity
- ✔ Advanced Protection
- ✔ Operational Efficiency
- ✔ Ease-of-Use
- ✔ Peace of Mind



LOCKDOWN
LESSON **TWO**

Cyber Resilience is **Vital in a Remote Work World**

A cyber resilient mindset for the “New Normal”

As businesses send their employees home to work safely during the pandemic, their environments are significantly less secure. It's essential for organizations to extend their cyber safe policies and culture to this new playing field.



Nearly half of the entire workforce is now remote

34%

of American employees
have transitioned to
working from home

14.6%

of workers
(approximately)
already at home

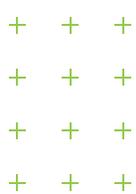
- ▶ One of the most significant challenges to cyber resilience is the shift to remote work. According to a joint study by MIT, Stanford, and the National Bureau of Economic Research (NBER)², more than a third (34%) of American employees have transitioned to working from home. They join approximately 14.6% of workers already at home to bring the total to nearly half the entire workforce.

Cybercriminals know many remote workforces are less likely to be under the watchful eyes of IT teams, with many working from their own personal devices outside the protection of group network policies, mandatory patches and updates, data backup and VPNs. What's more, with today's distributed systems, users don't always follow cyber-hygiene best practices, and may save files in locations that are not backed up onto a corporate network. How do businesses recover those files once they've been hit by ransomware?

Remote workers are prime targets for data breaches, ransomware, and other internet-enabled attacks, and our research reflects the urgency of protecting them. In March 2020, we identified 522 thousand phishing sites, a 350% increase from the month before. While many of these sites were COVID-related, these attacks are nothing new. Malicious actors are still looking to take advantage of rising angst and unpreparedness around the rapid shift to remote work, and business leaders need to be ready.

“We see more companies using BYOD, but that can increase risk. Inside the business you have IT teams that can protect data, but home networks and poorly secured IoT devices are a challenge to cyber resilience.”

-Grayson Milbourne, Director of Security Intelligence, Webroot



► NEW AND OLD THREATS TARGET REMOTE WORKERS

To help remote workers achieve cyber resilience, it's imperative businesses understand the risks and threats targeting them.

New and old remote worker threats include:

- [Phishing and Business Email Compromise \(BEC\)](#)
- [VPN brute-force attacks](#)
- [RDP and unsecured WiFi](#)
- [Microsoft Office 365 vulnerabilities](#)
- [COVID-19 malware threats](#)
- [Bypass of multifactor authentication](#)
- [Insider threats and human error](#)

Cybercriminals have a full arsenal when it comes to circumventing standard cybersecurity measures and launching attacks against remote workers. For instance, if a business offers RDP for remote employees but doesn't have two-factor authentication (2FA) enabled, hackers have a much easier time breaching a system. Without proper SAT, employees may not understand how authentication impacts security, and can be left vulnerable even if the right technology is in place.

The best way to secure home networks is to use a multi-layered cyber resilience strategy with both cybersecurity solutions and SAT to provide defense in depth.



Remote workers are very reliant on vulnerable technologies like VPN and RDP, and when we look at the home network infrastructure it's usually out of date, which makes a bad problem worse."

-Grayson Milbourne, Director of Security Intelligence, Webroot



► WHY SAT IS A “MUST HAVE” TOOL FOR REMOTE WORK

As Webroot’s Jonathan Barnett says, “If I’m a bad actor, I don’t want to crack a firewall when the user is the easiest target.” Firewalls, VPNs, antiviruses and threat intelligence solutions can help protect remote workers from network-based attacks and malware, but humans are still the weakest link in the security chain. That’s why SAT is the first line of defense.

Security awareness training can help remote employees learn to:

- ✔ Combat phishing, spear-phishing, vishing and smishing by identifying red flags that social engineers leave behind
- ✔ Secure their work-from-home space (and the business) from threats
- ✔ Identify proper data classification and how to handle data safely outside of the corporate network
- ✔ Change default credentials and protect IoT devices
- ✔ Report insider threats and suspicious activity

In addition to understanding the dangers, it’s essential that every employee – remote or otherwise – take ownership for the security of the business and understand the necessary steps to protect their own data as well as the company’s data.



Ownership is a big factor in cyber resilience. Who is responsible for security? The answer is everyone. It’s about building a culture where every single employee understands their role in protecting the business.”

- Nick Emanuel, Senior Director of Product, Webroot



▶ WHAT TO KNOW ABOUT PROTECTING A REMOTE WORKFORCE

As remote work continues to rise, businesses should follow these best practices to help protect their employees in off-site locations, as well as the networks and systems of their customers' employees:

- **Endpoint security.** Install robust endpoint security on all devices so employees and data stay safe.
- **Access to a VPN.** Give all employees access to a VPN to help protect corporate data and only enabling VPN access from secure, managed devices whenever possible.
- **DNS Filtering.** By controlling DNS, exposure to threats and potentially harmful content can be greatly reduced.
- **Safe RDP.** Ensure the use of RDP solutions that encrypt the data and use 2FA authentication when remotely accessing other machines.
- **Data Replication and Migration.** Implement high-availability data replication and migration safeguards to back up data saved on local devices while workers are remote.
- **Mobile Device Management.** Use a cybersecurity solution with device monitoring, tracking and remote erase functionality so lost or stolen devices can be located or wiped.
- **Office 365 Protection.** Add protection for Microsoft Office 365 and other collaboration platforms so content stored and shared in the cloud stays safe.
- **Security Awareness Training.** Warn employees about remote worker attacks such as phishing and BEC and encourage employees to be extra vigilant about unexpected invoices or other financial requests.

▶ WHY MSPS SHOULD OFFER REMOTE WORKER PROTECTION AND TRAINING

As the world adapts to remote work, there will be a greater need to help small businesses rapidly secure their remote workforce. According to a recent study³, 57% of SMB owners say they are likely to continue increased remote working options for employees in the near future. MSPs have a unique opportunity to offer significant guidance and support to smaller businesses to help build resilience for the long term. This includes cybersecurity solutions and ongoing SAT that protect the home network and personal devices from recurring and emerging threats.



Cyber resilience is a differentiator for MSPs. You can say to your customers, 'We've got the data, the products, and the knowledge to protect you, and we can build a deeper relationship that benefits everyone.'

-Nick Emanuel, Senior Director of Product, Webroot



LOCKDOWN
LESSON **THREE**

How to Build a Cyber Resilient Business

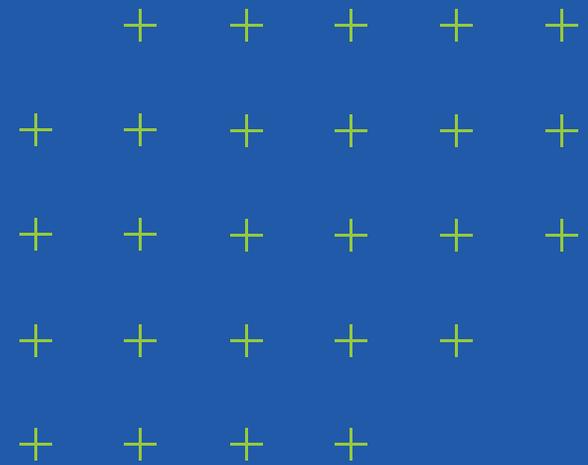
How to build resilience with data backup and security solutions

In order to offer a complete, end-to-end cyber resilience strategy to customers and your business, you must employ solutions that bring all the pieces together in a cohesive package. This is where the marriage between Webroot and Carbonite can help you shine.



▶ Just as people are generally bad at judging their own cyber resilience, it's easy to misjudge the technology and tools needed to protect a business and its customers from end to end. While antivirus and endpoint protection are a great starting point, true cyber resilience includes multiple technologies that ensure businesses can protect against attacks and recover compromised data at a moment's notice. When working toward cyber resilience, it's important to understand how these technologies work together and how each solution makes the experience as seamless as possible.

The basic framework for cyber resilience is: Train, Block, Protect, Backup, and Recover.





Layer 1: **TRAIN**

- ▶ Phishing attacks, social engineering and human error are still major vulnerabilities for businesses of every size. In fact, 90% of all successful cyberattacks start with phishing or user error. SAT should include ongoing education that provides every employee with enough relevant information about new and recurring threats to protect themselves. It should also test their cyber-awareness by covering all aspects of data security and regulatory compliance such as GDPR, PCI DSS and HIPAA.

Solutions such as [Webroot® Security Awareness Training](#) serve up easily consumable courses designed to improve the effectiveness of cybersecurity education. And tools like phishing simulations put businesses in the driver's seat by testing and measuring real-world employee cyber-awareness. For MSPs, these tools make it easy to educate and protect SMB customers and their end users while also bolstering recurring revenue.



The cyber resilience story starts with people. Technology helps but it's a shared responsibility where everyone knows the policies and procedures, and everyone is prepared."

-Philipp Karcher, Product Manager, Webroot

- ▶ Of course, security awareness training is not an end-all, be-all solution. When a user takes the bait from a cybercriminal and clicks on a phishing link, the right technology must be in place to mitigate threats before there is data loss or financial compromise. That's why the next layer after SAT is DNS protection, followed by endpoint security and threat intelligence.

Uncontrolled internet access is a high-risk activity for any business and managing DNS can be a powerful way to protect your users and your networks. Think of DNS as an address book for the internet. By applying intelligence to DNS through [Webroot® DNS Protection](#), a user can effectively cross off the addresses of malware, phishing sites and other undesirable internet locales. In addition to reducing exposure to threats, it also allows visibility into what requests are being made from the office network and by users while working remotely.

If an attack does manage to slip past DNS filters, the next line of defense is endpoint security. For example, [Webroot® Business Endpoint Protection](#) can help defend against the attack by automatically shielding users against multi-vector threats.

Endpoint protection is vital for businesses to stay on top of modern threats such as malicious websites or dangerous polymorphic malware. When combined with timely and accurate intelligence that can quickly identify threats, these solutions work together to bolster security with an advanced, multi-layered approach. What's more, Webroot solutions are powered by [BrightCloud® Threat Intelligence](#), which leverages machine learning to identify, analyze and classify known and zero-day threats by processing more than 500 billion objects per day, helping to stop threats before they wreak havoc.



Once the user has clicked on a malicious link, the question becomes, 'What do we do next?' DNS, endpoint and threat intelligence are the second layer after user education."

-Jonathan Barnett, Senior Product Manager, Webroot



Layer 2: **BLOCK AND PROTECT**





Layer 3:

BACKUP AND RECOVER

- ▶ Cyber resilience is all about bouncing back after an attack has occurred, and backup and recovery solutions are a key part of that process. Business continuity and productivity are paramount to every business, and the first sign of resilience is the ability to quickly restore data and keep operations up and running, even in the middle of a full-scale attack or following a natural disaster.

Backup and recovery solutions like Carbonite® Endpoint and [Carbonite® Server Backup](#) can help protect your data and quickly restore it in the event of data loss. Carbonite Endpoint automatically protects endpoints and their data, while Carbonite Server backs up data from physical and virtual servers.

[Carbonite® Recover](#) provides fast recovery by failing over to a secondary environment, keeping businesses running and data available.

This suite of data protection solutions helps with more than just cyberattacks. Data is commonly lost due to hardware or software failure, data corruption, natural disasters, human-caused events (like an employee spilling coffee on a laptop) or accidental deletion of data.

Being able to quickly recover data is especially important when protecting remote workers who may not always save important files or documents to the businesses' network or cloud. Solutions like Carbonite® Backup for Microsoft 365 not only protect against threats but can also help to prevent data loss when it matters most.

All of these solutions and security layers work together to create an umbrella of protection for the entire business, their customers and the customers' end users. What's more, Webroot and Carbonite businesses get a full suite of tools from a single source, reducing bills from different vendors and streamlining communication. We believe that the simpler we can make cyber resilience, the easier it will be for MSPs and SMBs to protect their data.



Each one of these layers is important because they all work together. Adding one layer helps but it's really the encompassing suite of tools and training that matters from end to end."

-Jonathan Barnett, Senior Product Manager, Webroot

► CREATING AN EFFECTIVE CYBER RESILIENCE STRATEGY

While a layered approach mitigates risk, a proper cyber resilience strategy is also crucial. It's important for businesses to document their strategy in writing, share it with employees and customers, and promote a culture that embraces cybersecurity best practices.

Think of your cyber resilience strategy like a fire drill: you don't want to try it for the first time when the alarm bell rings. You need to know where to go and what to do to keep everyone safe. Likewise, your cyber resilience strategy should standardize the process so users can remain calm and clearheaded when faced with a potential breach or data disaster.

Your strategy should cover:

- ✓ Which cybersecurity solutions are necessary to protect your business, your employees, your customers and their end users.
- ✓ What to do in the event of a failure or breach and who is responsible for doing it.
- ✓ How to communicate the incident to customers and stakeholders.
- ✓ How to assess and report the impact of resilience measures.
- ✓ How to get back to normal operations as quickly as possible.
- ✓ How to recover data if data it's been lost or accidentally erased.
- ✓ A plan for enabling employees and remote staff to follow cybersecurity best practices.
- ✓ A plan for continued security awareness education.



It's important to have a documented plan and to practice walking through it. If you experience data loss as the result of a breach, it's essential nobody panics because every minute matters."

-Johnathan Ferrick, Product Manager, Webroot



► LEVERAGE THE CYBERSECURITY COMMUNITY TO STAY RESILIENT

The last piece of the cyber resilience puzzle is cooperation. There's no single solution or approach that can protect a business, and it really does take a village to protect against today's cyber threats. Relying on expertise and support to fill in the remaining security gaps is needed now more than ever.

For instance, MSPs looking to transition to managed security by offering SAT and endpoint protection for their customers can lean on Webroot's SAT training modules and phishing simulations to provide world-class training and monitoring. We also have outstanding customer support and a community of like-minded Webroot Partners who can offer guidance on going to market with Webroot products, creating cyber resilience strategies, and finding and implementing the right cybersecurity solutions.

Don't go at it alone. Let the Webroot and Carbonite team help you grow and protect your business every step of the way.

CONCLUSION

No two organizations will follow the same path to cyber resilience. Each has unique cybersecurity and data protection demands that require different cybersecurity solutions and strategies to effectively protect the business. That said, every business should have a strategy in place, because cyberattacks and data loss happen every day. But with the right knowledge and support, you can stop threats, protect your customers, grow your business and become truly cyber resilient. Whatever comes your way.



At Webroot and Carbonite, cyber resilience is about community. It's more difficult to protect yourself as an individual, but when you have a strong group of organizations ready to protect you with technology and people, you gain resilience."

-Nick Emanuel, Senior Director of Product, Webroot

Boost your cyber resilience with a free trial of Webroot + Carbonite solutions today.

Start Trial



¹ <https://www.webroot.com/blog/2020/04/03/2020s-most-and-least-cyber-secure-states/>

² https://john-joseph-horton.com/papers/remote_work.pdf?

³ <https://www.intermedia.net/blog/study-finds-half-smb-owners-believe-working-remotely-is-here-to-stay/>

CARBONITE[®]
an **opentext** company

WEBROOT[®]
an **opentext** company

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.

© 2021 Open Text. All rights reserved. OpenText, Carbonite, and Webroot are trademarks of Open Text or its subsidiaries. All other trademarks are the property of their respective owners.