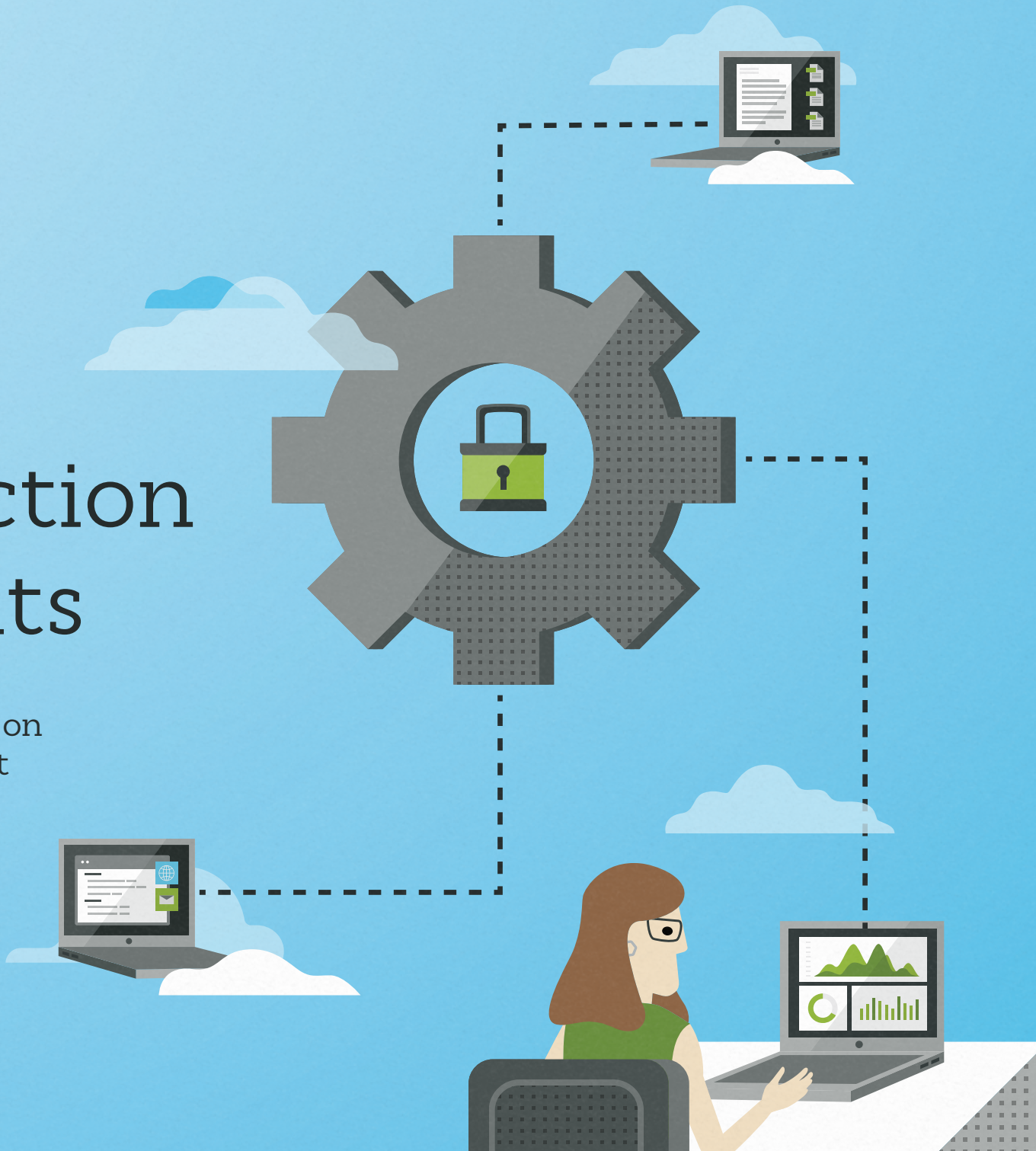
CARBONITE

Data protection for endpoints

Why it's harder to protect data on the move and how to solve for it



Data protection for endpoints

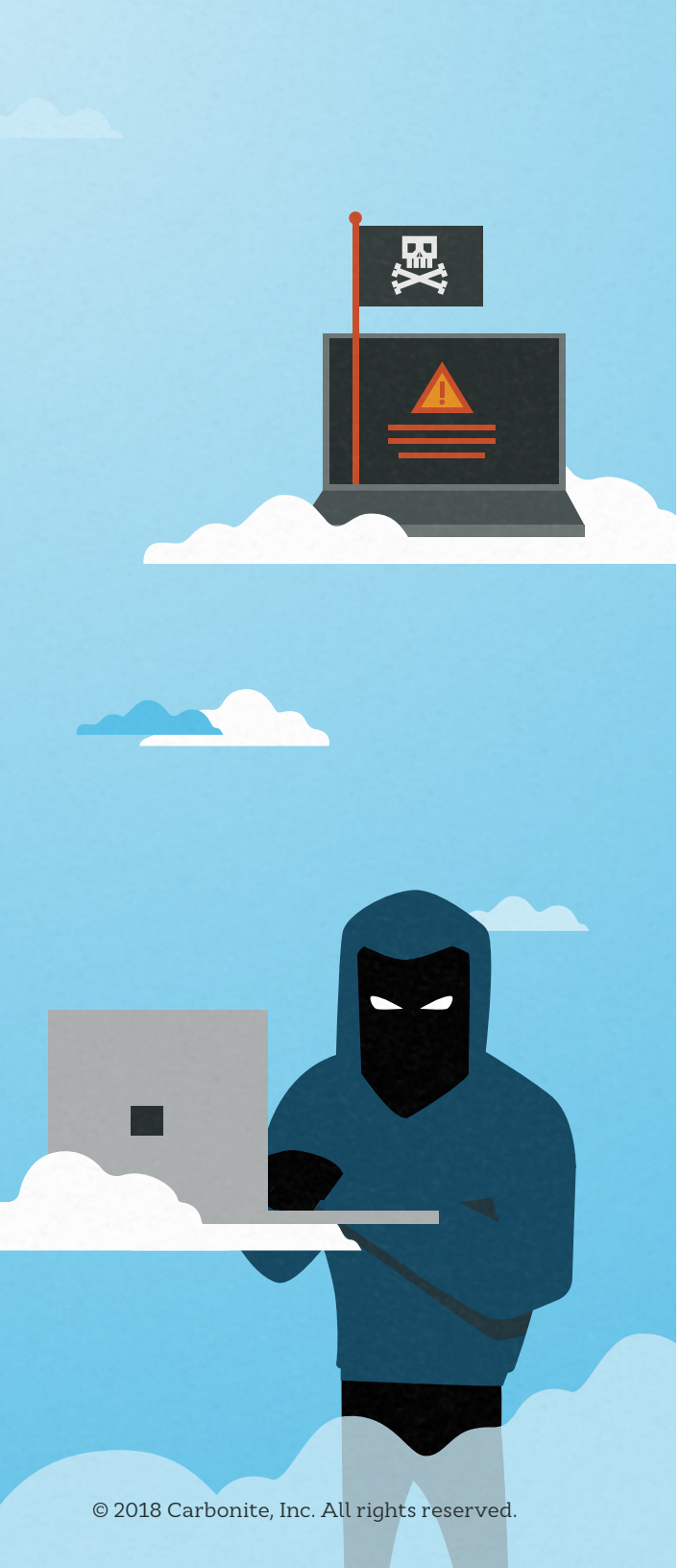
With more and more employees spread around the globe, IT teams face a conundrum: how to secure an increasing amount of data traveling outside the network while preserving workforce productivity in an increasingly interconnected and global market. It's up to IT decision-makers to protect and secure company data in a way that promotes user access without imposing overly restrictive or cumbersome device policies. When it comes to protecting data on laptops and mobile devices, several key factors are essential for today's businesses:

Centralized deployment and management

Efficient technology that doesn't interfere with network or end-user productivity

End-to-end security, including data encryption on the source, in transit and in the cloud

Until now, decision makers have had a hard time finding solutions that satisfy all their business requirements.



Threat assessment

The risks to corporate data are well known. Accidental or malicious deletion and overwriting of files are among the most common reasons why businesses lose data. In addition, device theft and cybercrime have spurred businesses to take action. Ransomware criminals are targeting organizations more frequently and demanding high ransoms due to the high value and sensitive nature of data.

The growing number of threats has led to a much deeper understanding of the true value of a comprehensive data protection strategy.

Beyond the basics

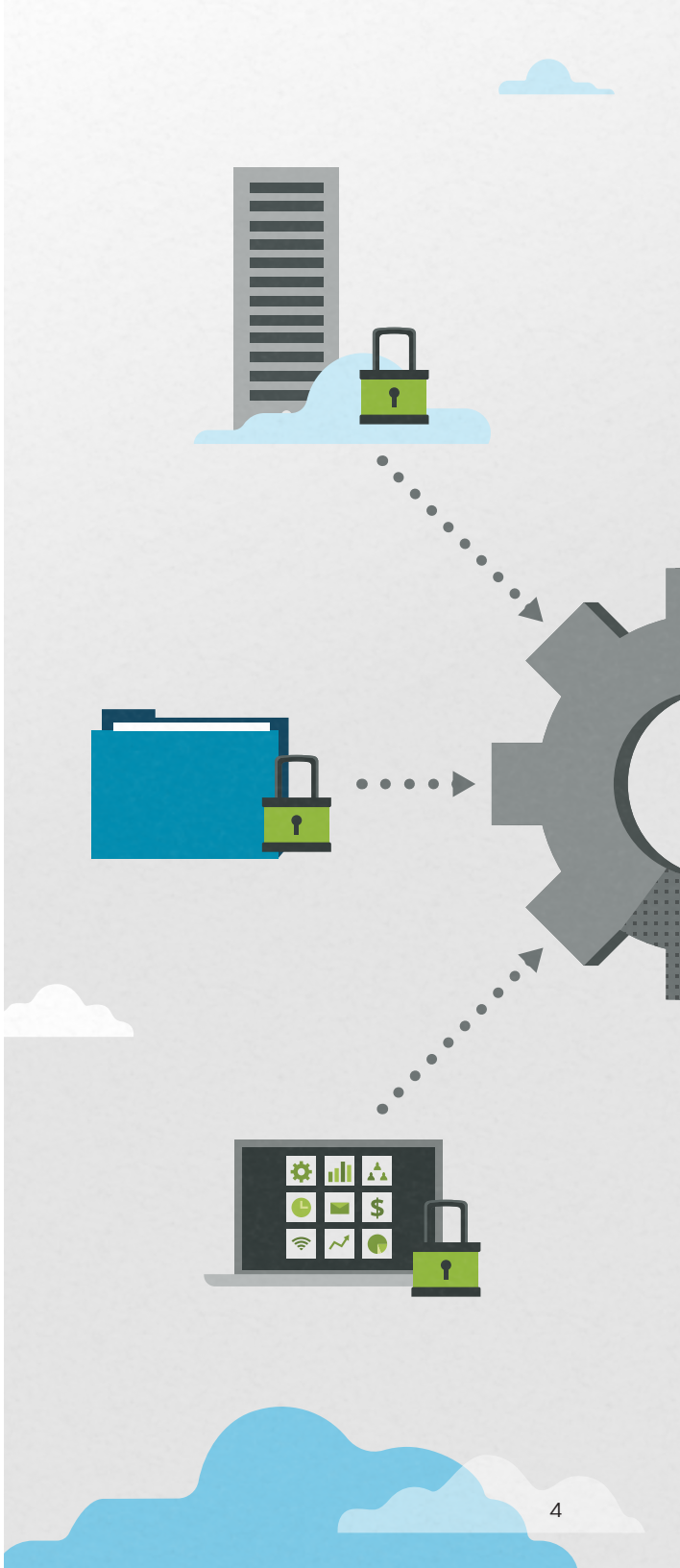
Today's threat landscape, combined with the fluidity and mobility of today's computing environments, require solutions that can overcome technological hurdles and deliver simplicity at scale. IT decision makers need certain critical capabilities when considering endpoint protection for today's mobile workforce.

1. Automatic backup to a centralized repository

Businesses don't want employees improvising their own backup with online file-sharing apps. The lack of automation and central management takes control out of the hands of IT and prevents a business from being able to apply policies consistently across the organization. Additionally, these solutions typically use insufficient encryption, if they use any at all. To protect critical business data from common forms of data loss, a backup solution should have the following features:

- Automated protection for files and folders
- Cloud or other offsite protection
- Encryption for data at rest locally, in transit and in storage

True, purpose-built cloud backup for endpoints protects company data dispersed across the entire workforce, providing a central repository for critical business files so they can be accessed and restored whenever and wherever they're needed.



Beyond the basics

2. Low network impact

The cumulative impact of numerous devices backing up to a central repository has the potential for consuming significant network bandwidth without some form of built-in prioritization of backup workloads. In a comprehensive data protection strategy, extremely time-sensitive data is treated differently than less urgent data for several reasons:

- It optimizes network efficiency for all types of data.
- It accelerates time-to-protection and recovery speed.
- It helps shrink the window where data can be lost.

Establishing a local cache for the most recent data ensures that users always have access to the most critical, time-sensitive data they have on their devices. With scheduled cloud backups taking place at off-peak hours, IT can ensure that backup workloads don't interfere with other critical workloads traveling across the network during times of high usage. In turn, the optimization of backup workloads allows you to take more frequent backups of the endpoint, reducing the potential for data loss to virtually nothing.

3. Flexible deployment and management

Centralized administrative capabilities give IT complete control while self-service recovery options reduce user dependency and increase productivity. Users can get their files back without calling IT. Key features can both save IT time and support consistent application of policies, including:

- Remote policy management via a centralized admin console
- Remote data management, including options for admin restore
- Silent deployment and Active Directory/LDAP integration
- End-user dashboard with custom access policies
- Self-service recovery for files and folders
- Remote wipe and global location tracking

Beyond the basics

4. Enterprise key management

Encryption key management is especially important as businesses seek to leverage the efficiencies and cost savings of public cloud infrastructures like Microsoft Azure. The security model employed by the backup solution will affect where encryption keys are stored and who has access to them. This is important because whoever holds the key ultimately determines who's allowed to access the data. With uncertain provenance of key management, the ability to restrict access for interested third parties may not entirely rest with the business.

5. Advanced deduplication

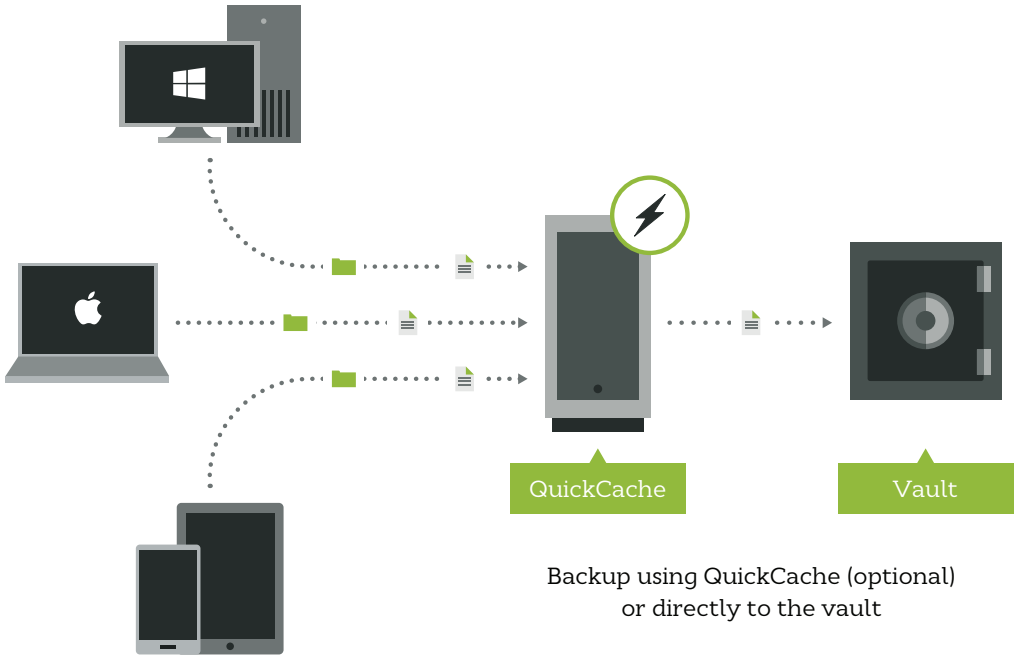
Large quantities of duplicate data can pose challenges. Yes, deduplicating the data is simple enough. But most often, the data has to be unencrypted first, leaving it vulnerable. This is unacceptable for businesses concerned with confidentiality, and a non-starter for businesses in regulated industries. In an ideal solution, deduplication is applied to encrypted data to achieve efficiency without sacrificing security.

Carbonite Endpoint Protection

Carbonite Endpoint Protection is engineered with central management and control features that simplify deployment while minimizing disruptions due to bandwidth restrictions or geographic dispersion of endpoints. It allows IT to mitigate data loss and data breach globally while maximizing network and end user performance.

Carbonite Endpoint Protection applies patented global deduplication technology to encrypted data. Carbonite Endpoint Protection does not require decryption at any point. Carbonite's unique enterprise key controller provides an extra layer of security and control for companies using the public cloud or hosting a vault in their own data center.

Carbonite doesn't just protect data, it protects the endpoint itself. With device tracking and remote data wipe, businesses can track lost or stolen devices, and prevent unwanted access to data with on-demand erasure of the hard drive or a poison pill that is activated based on time-based policy triggers.



Backup using QuickCache (optional)
or directly to the vault

Global protection

Today's interconnected markets compel businesses and employees to be more mobile. But mobility doesn't have to come at the expense of security. Technology exists for simplifying data protection, centralizing administration, ensuring continued access, and maintaining network and storage efficiency—all while using secure processes at every step.

For more information on the Carbonite Data Protection Platform, please contact us or visit our website.

carbonite.com
Phone: 877-542-8637
Email: DataProtectionSales@carbonite.com

CARBONITE