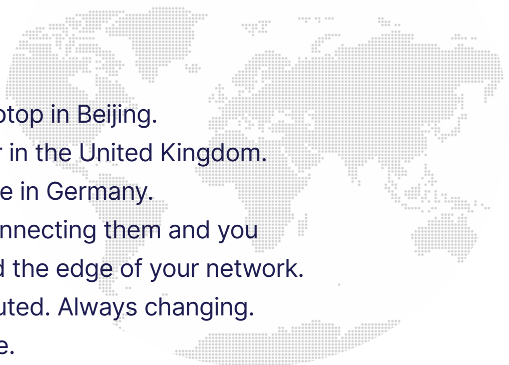
opentext™

DATA IS ON THE MOVE

CAN YOUR BUSINESS KEEP UP?



A company laptop in Beijing.
A cloud server in the United Kingdom.
A remote office in Germany.
Draw a line connecting them and you have identified the edge of your network.
Widely distributed. Always changing.
And vulnerable.

SECURING DATA AT THE NETWORK EDGE

1 THE RISKS

ENDPOINTS

45%
Of business data is on devices that organizations can't control

60%
Of ransomware attacks target endpoints

68%
Of organizations experienced a successful endpoint attack

CLOUD

35%
Of businesses don't know the SLAs of their SaaS providers

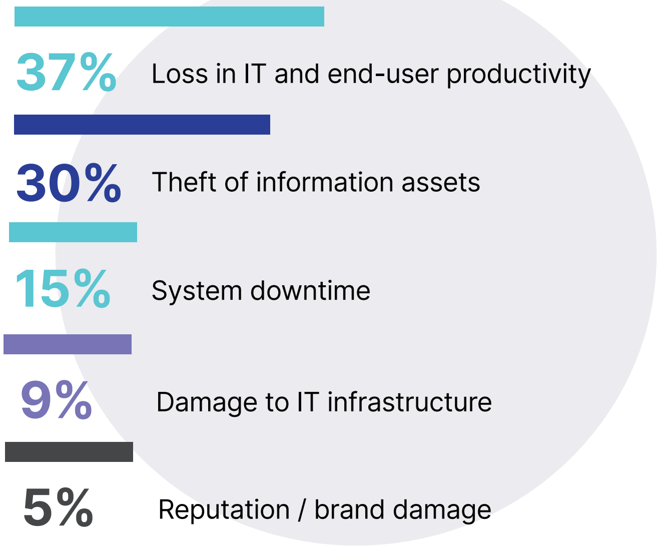
27%
Of organizations lack recovery capabilities for Microsoft Office 365

54%
Of organizations rely on their cloud services' native recovery tools

2 THE COSTS

It's hard to calculate the dollar value of lost data. But businesses that experience it know the impact.

Cost of endpoint attacks by percentage from every lost dollar



SaaS DATA LOSS

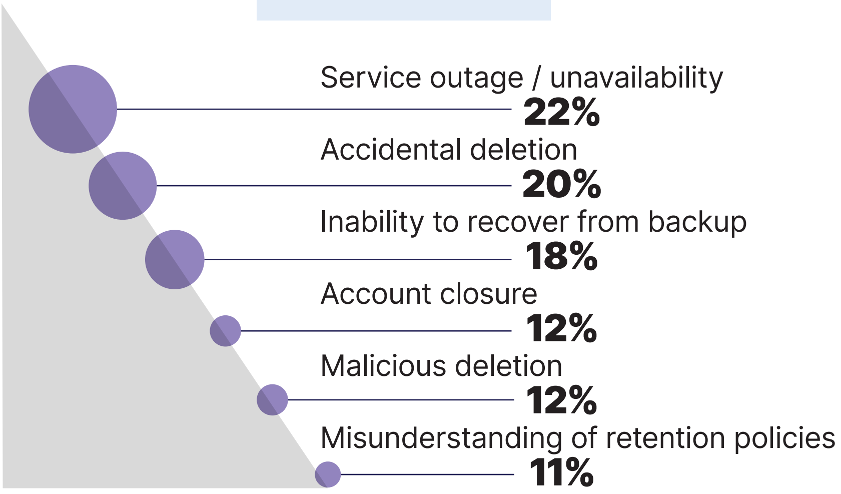
Businesses that use SaaS applications and cloud services gain speed and flexibility. But they also risk losing data in the cloud.

32%

of businesses have lost SaaS data

-Aberdeen

Causes of SaaS data loss:



SECURITY AT THE EDGE

The only thing worse than businesses losing data in the cloud is not being able to recover it.

22%

of businesses recovered 100% of SaaS data

40%

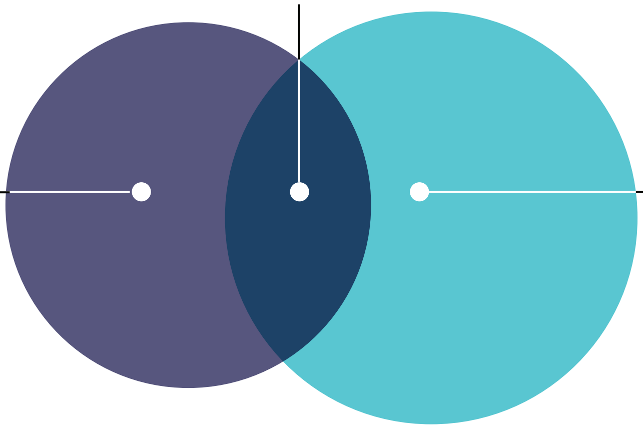
of businesses recovered less than 75% of SaaS data

9%

of businesses don’t know how much SaaS data they recovered

HYBRIDIZATION

Businesses rarely stick to a single cloud platform because of the abundance of these available.



72%

of decision makers plan to use a hybrid cloud strategy

- Forrester

87%

of organizations have already deployed a multi-cloud strategy

- TechRepublic

EDGE COMPLEXITY

BACKUP REQUIREMENTS

Workforces are highly mobile and data lives everywhere – on hardware and in the cloud. Enterprise organizations still need uniform backup policies and common feature sets.

CLOUD

Local caching

Backup centralization

Global deduplication

Device tracking

Remote data wipe

Device migration

Transport layer security

ENDPOINT

Application-specific backup and recovery

Permissions-only restore

Selective or site-level rollback

Data retention for departed users

Bring your own key (BYOK)

Cloud-based/no on-prem hardware

COMBINED

Central policy management and deployment

Granular and full system backup and recovery

Backup scheduling

File versioning and point-in-time restore

Administrative restore

User self-restore

End-to-end security

Flexible repository targets

GDPR compliance

RECOVERY OBJECTIVES

Regardless of where data lives, businesses need access to it and have low tolerances for downtime.

RECOVERY TIME TOLERANCE

10%	No downtime
22%	Up to 15 minutes
23%	Up to 30 minutes
30%	Up to 1 hour
10%	Between 1-2 hours
5%	Between 3-4 hours
1%	More than 4 hours

CLOUD CONFUSION

33% of businesses think SaaS applications don't need to be backed up

28% of businesses have misunderstood SaaS SLAs

COMMON MISCONCEPTIONS ABOUT SAAS DATA PROTECTION:

x - Backup is built-in

x - Immunity to ransomware

x - Scheduled back up

x - Automatic back up of version history

x - You can always recover from the recycle bin

x - You can roll back to a prior point in time

x - You can retain the data of deactivated users

x - Malicious deletion of files prevention

The edge is ever expanding and changing. But the need for backup remains the same. Carbonite® Endpoint and Carbonite® Backup for Microsoft 365 use advanced administrative features and highly efficient, secure processes to help businesses protect data locally, in the cloud and wherever the network's edge extends For questions or to talk to a representative, visit Carbonite.com.

opentext™