odaseva

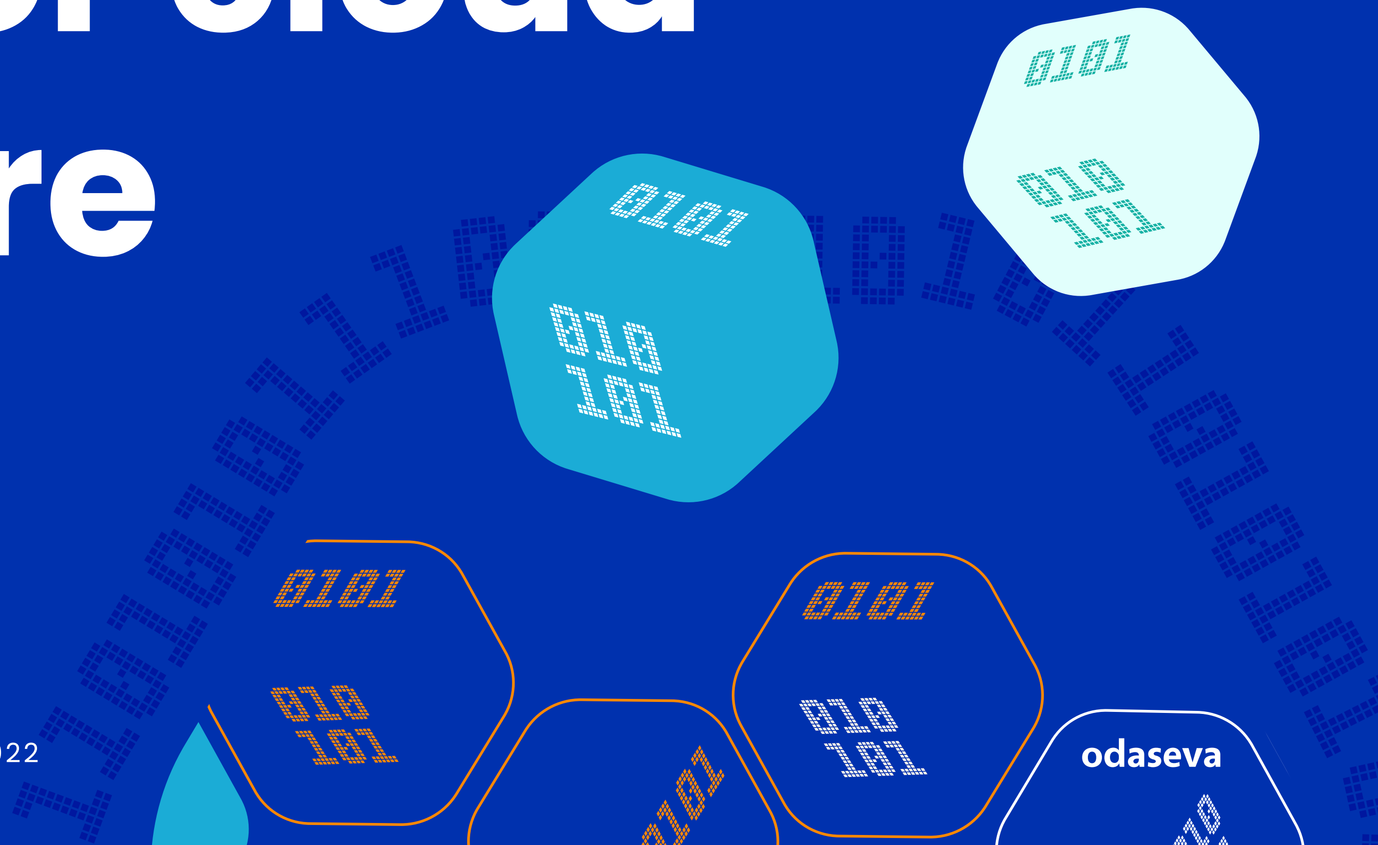
The State of SaaS Ransomware Attack Preparedness

A survey of cloud data decision-makers in large enterprises

AUGUST 2022

TABLE OF CONTENTS

Large enterprises are **not fully prepared** for cloud ransomware attacks



EXECUTIVE SUMMARY

Executives and managers at companies with more than 10,000 employees responded to a global survey in August 2022, and the results reveal that **very large enterprises are not fully prepared for a ransomware attack on SaaS data.**

This report details the survey findings that relate to the three main aspects of a ransomware attack against SaaS data:

THE THREAT

Companies are increasingly hit with ransomware attacks on data stored in all environments including on-premises data, data in public infrastructure clouds, and SaaS data. But **attacks on SaaS data are more likely to succeed** than attacks on data in other environments.

THE RECOVERY

Surprisingly, the survey results show that leaders aren't particularly concerned about ransomware attacks on SaaS data, even though **this type of data is the least likely to be recovered after a ransomware attack**. And when the data could be fully recovered, 79% of respondents said **recovery took days, weeks, or months**.

THE PREVENTION

Given the often mission-critical nature of SaaS data, large enterprises must understand the risk of ransomware attacks, and **protect their data** against this increasingly common and damaging threat.

EXECUTIVE SUMMARY

SaaS data - not SaaS platforms - are the target

While the SaaS platform itself is a highly unlikely potential victim of a ransomware attack because bypassing the platform's strict technical controls is simply too difficult, SaaS data can be targeted through phishing, malware, API key leaks, or other malicious methods.

Attackers can then use the SaaS platform's API to export the data and overwrite it with an encrypted version. To obtain the decryption key, victims must pay a ransom.

Survey methodology

Odaseva partnered with Dimensional Research®, an independent research firm specializing in enterprise technology, to conduct this survey. A total of 157 qualified individuals completed the survey. All were executives or managers who had decision making responsibility for data solutions for both IaaS and SaaS cloud environments.

All worked for a company with more than 10,000 employees and more than 10% of their corporate data in cloud (IaaS or SaaS) environments. Responses were captured between August 2 and August 9, 2022.

KEY FINDINGS

Ransomware attacks targeting SaaS data are a real threat, and recovery is often difficult, incomplete, and time-consuming

- Almost half (48%) of organizations have experienced a ransomware attack over the past 12 months, and SaaS data was the target of more than half of them (51%).
- Ransomware attacks on SaaS data were the most likely to be successful, with 52% of them penetrating enterprise defenses to encrypt the data.
- Attacks targeting data in public infrastructure clouds, on the other hand, were only successful 42% of the time.
- Data lost in successful SaaS ransomware attacks was least likely to be fully recovered, with data loss 50% of the time.
- 79% report that recovering from a ransomware attack took days or longer.
- SaaS is the least likely type of data to be ranked a "Top 2" concern for ransomware.

Read on for the detailed findings.

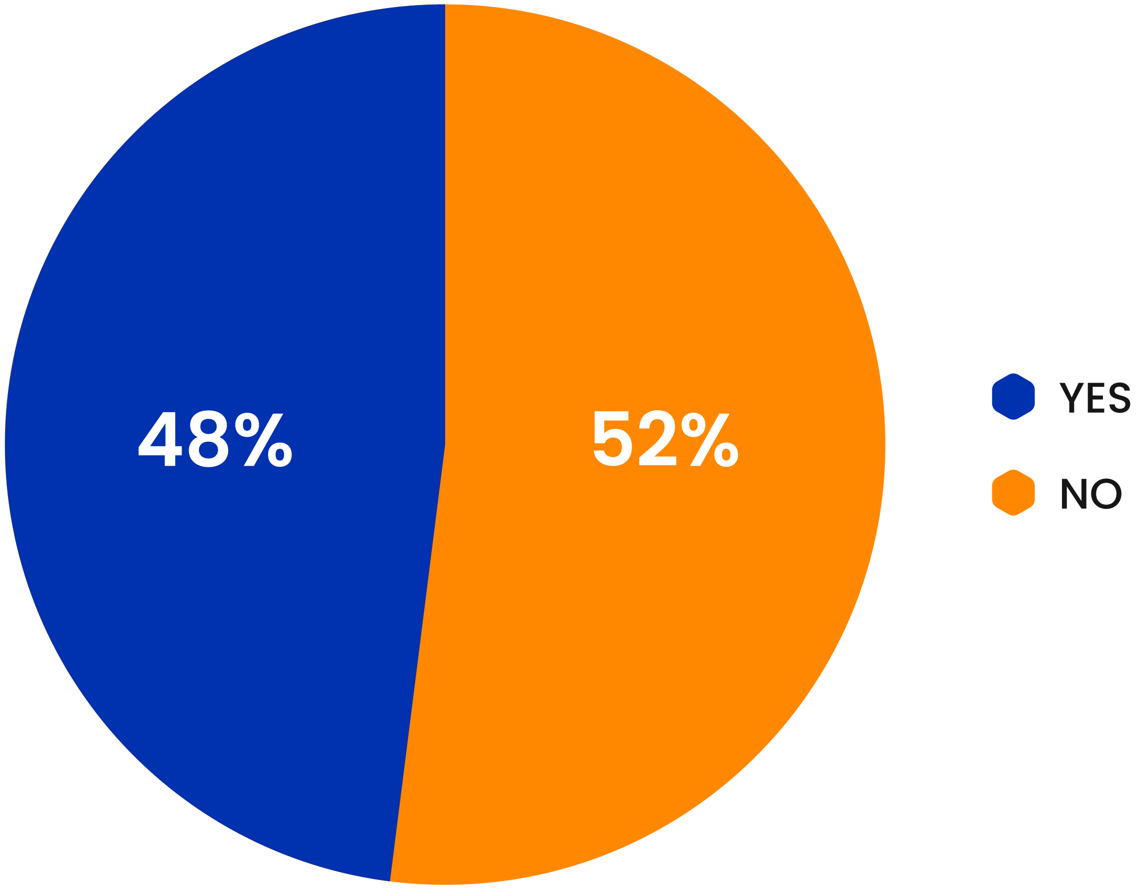
THE THREAT

Cloud ransomware attacks are increasing – and succeeding

THE THREAT

Almost half (48%) report they have been the target of a ransomware attack in the past 12 months

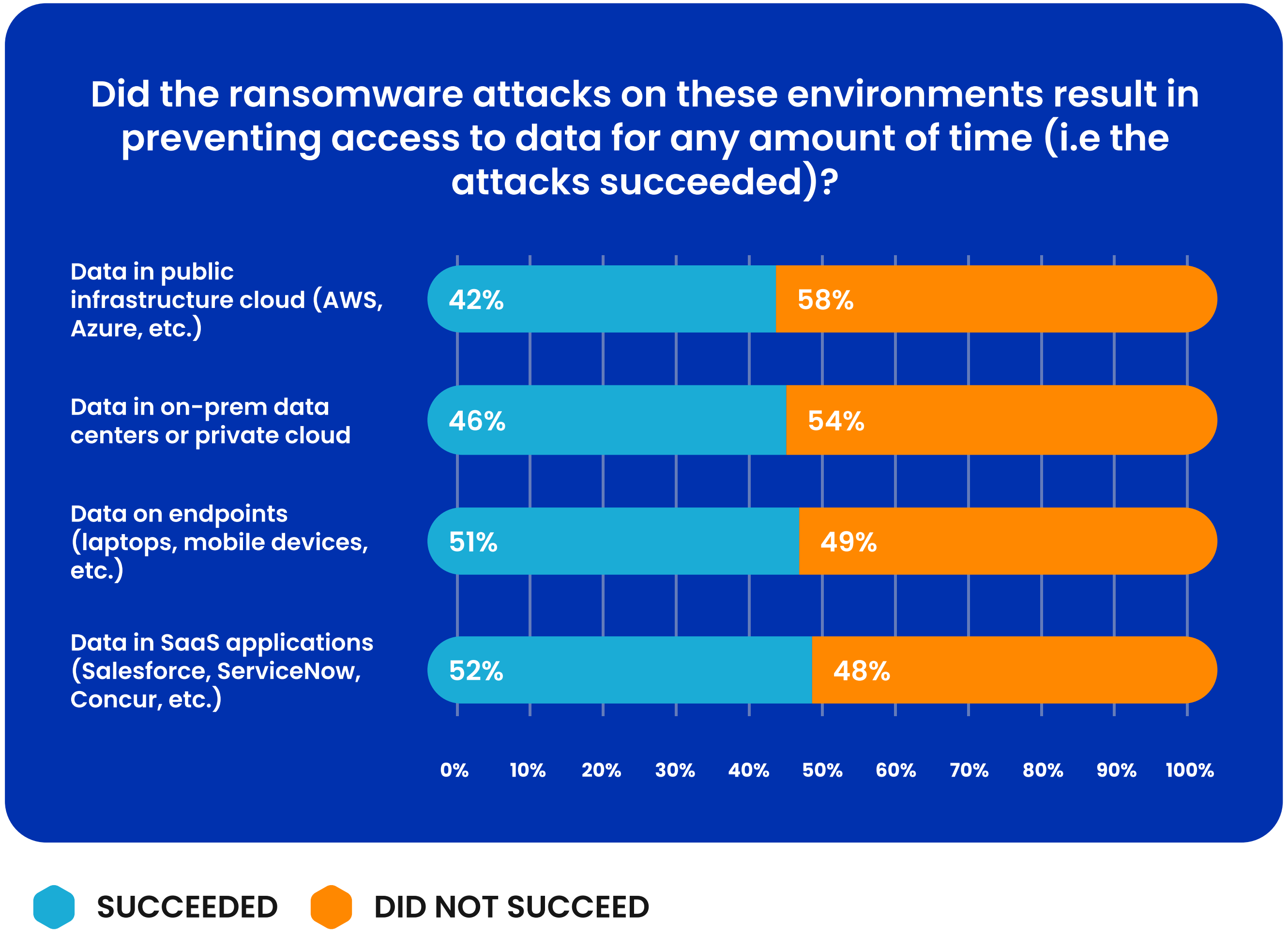
The threat of ransomware attacks on business data is very real.



THE THREAT

Attacks on SaaS environments were more likely to succeed than those in other environments

52% of ransomware attacks on SaaS data succeeded - more than any other environment.



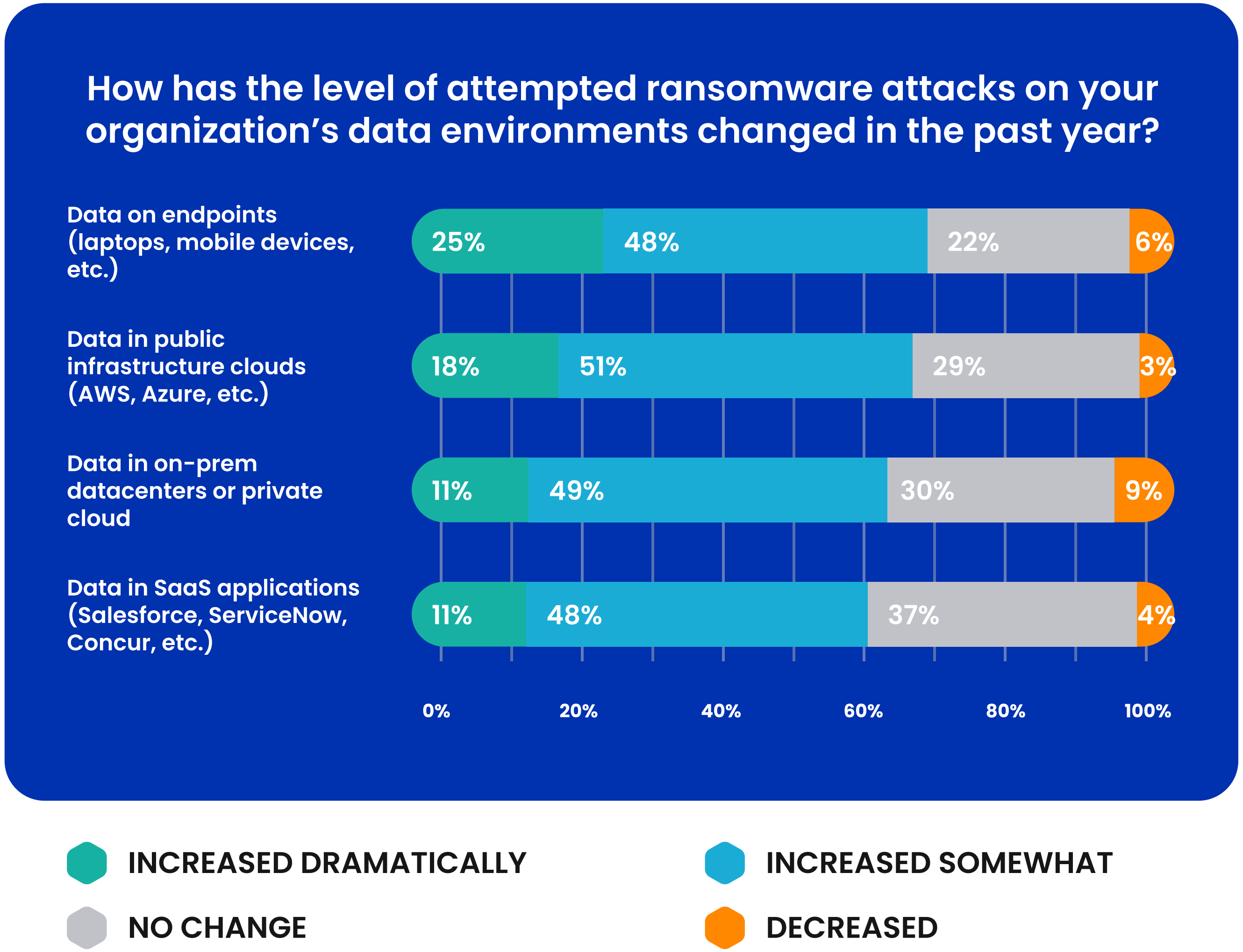
Did the ransomware attacks on these environments result in preventing access to data for any amount of time (i.e the attacks succeeded)?

n = have been targeted by ransomware in the specified environment

THE THREAT

For all types of environments, more than half report an increase in ransomware attacks

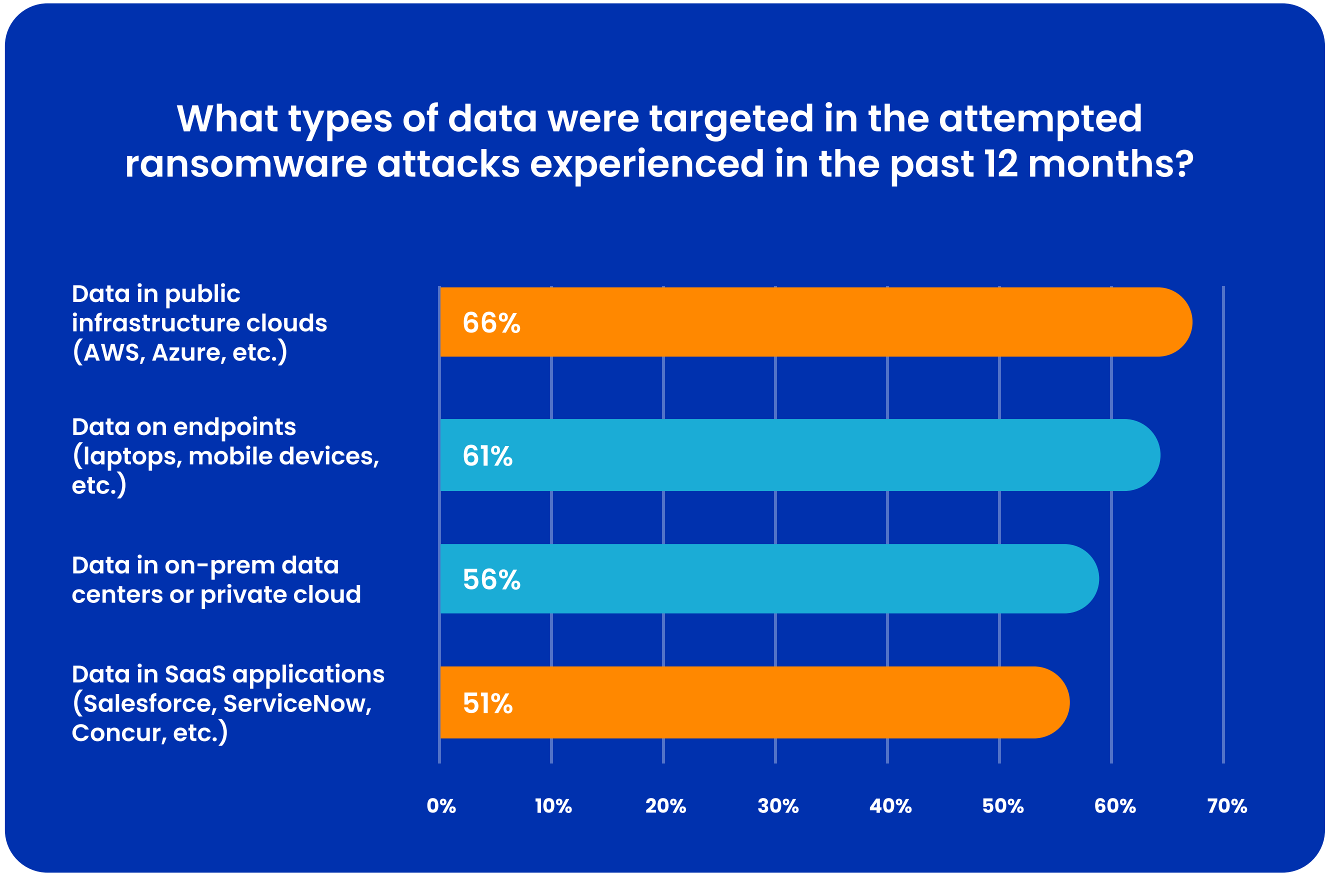
Ransomware attacks are occurring more often against all types of data, wherever it is located.



THE THREAT

Ransomware attacks targeted both IaaS and SaaS environments

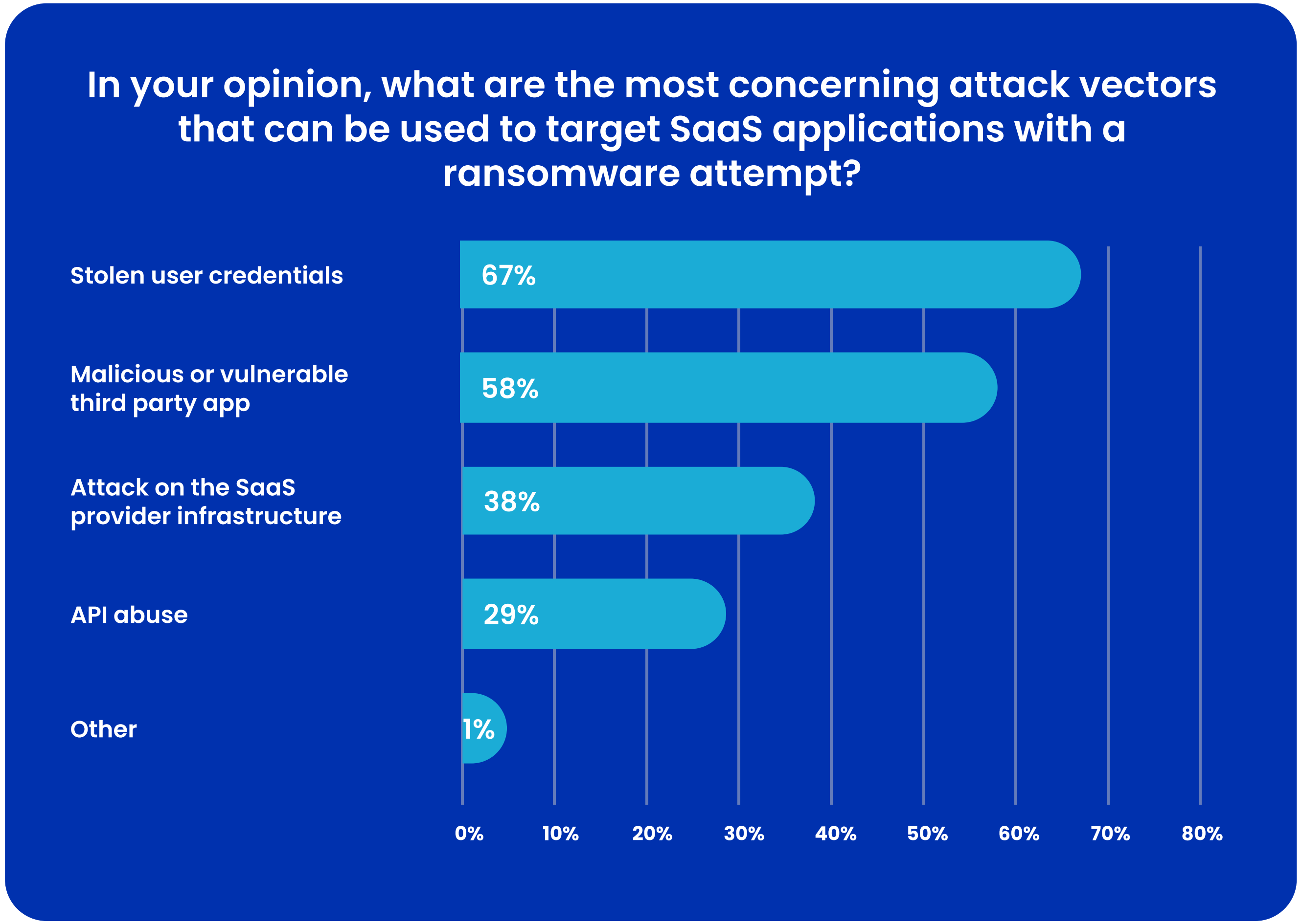
All data is a target, no matter where it is stored.



THE THREAT

A wide range of attack vectors are viewed as creating an opportunity for a SaaS ransomware attack

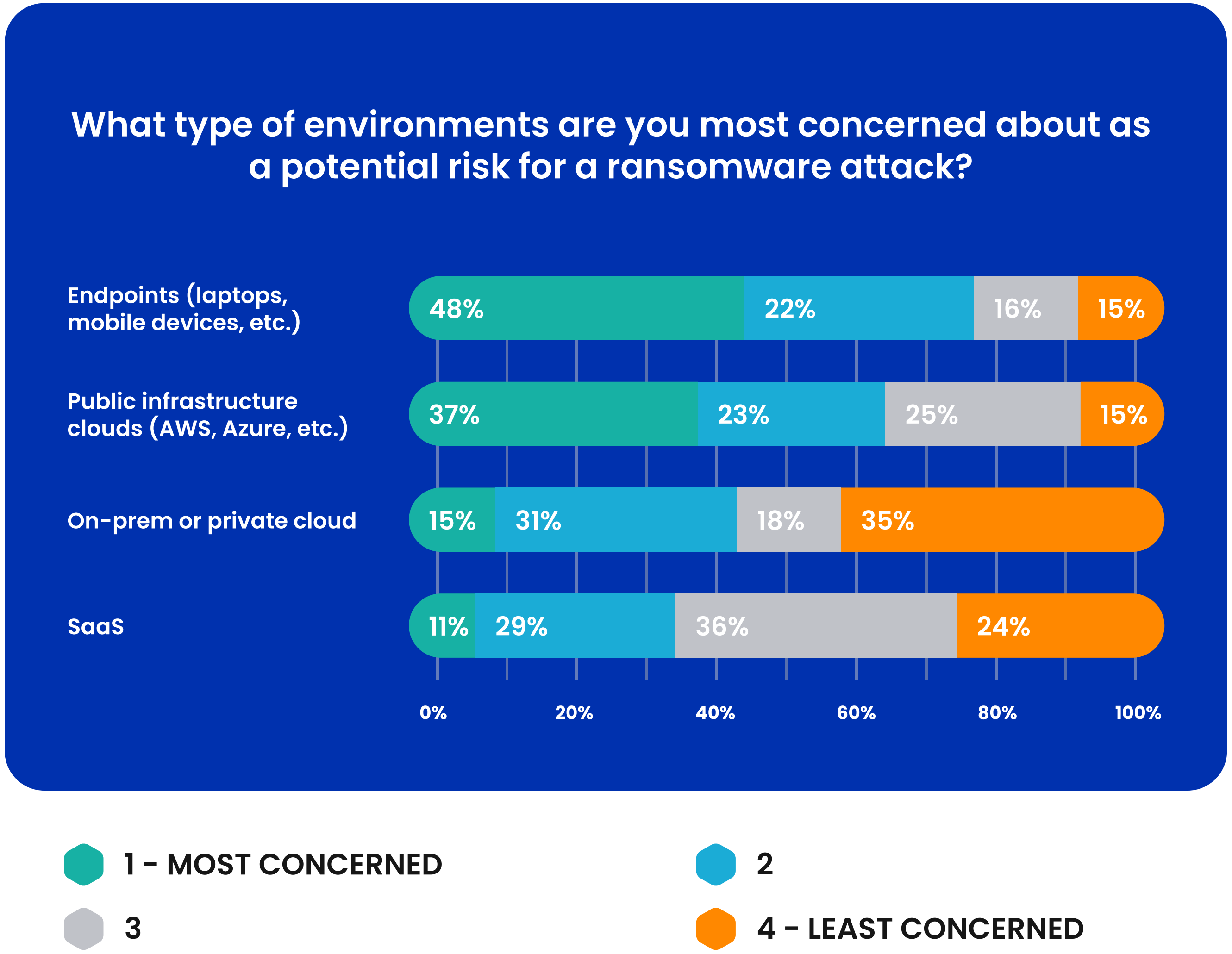
While the SaaS platform itself is highly unlikely to be successfully attacked, attackers can target a customer's SaaS data through a variety of ways.



THE THREAT

SaaS is the least likely to be ranked a “Top 2” concern for ransomware

SaaS data is of lower concern than other types of data - but the data reveals that the threat of a ransomware attack is real - and potentially highly damaging.



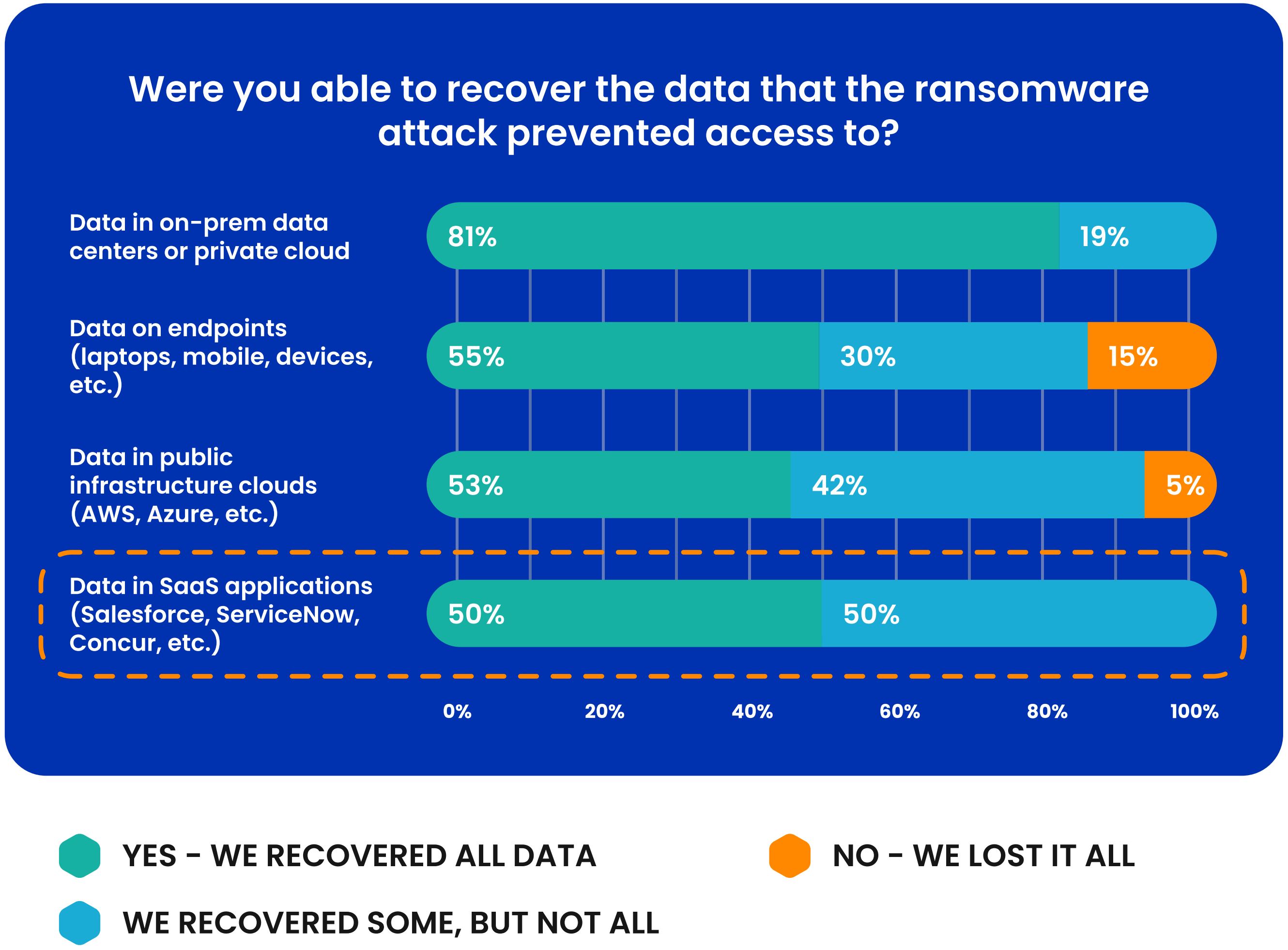
THE RECOVERY

Days, weeks, months to get back to business

THE RECOVERY

Data lost in successful SaaS ransomware attacks was least likely to be fully recovered

SaaS data is tricky to restore - especially if it's not backed up properly. If enterprises are not using a backup and restore solution specifically designed for their data volume and complexity, they're at risk of failing to recover data.

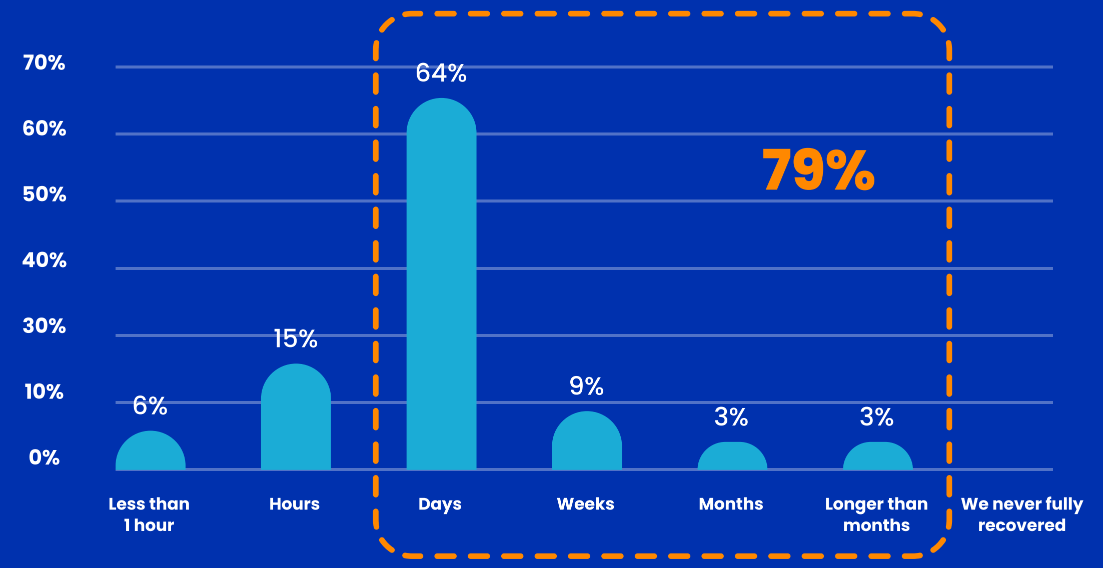


THE RECOVERY

79% report that recovering from a ransomware attack took days or longer

The fallout from an attack, which can grind business to a halt, lasted days or longer for most respondents.

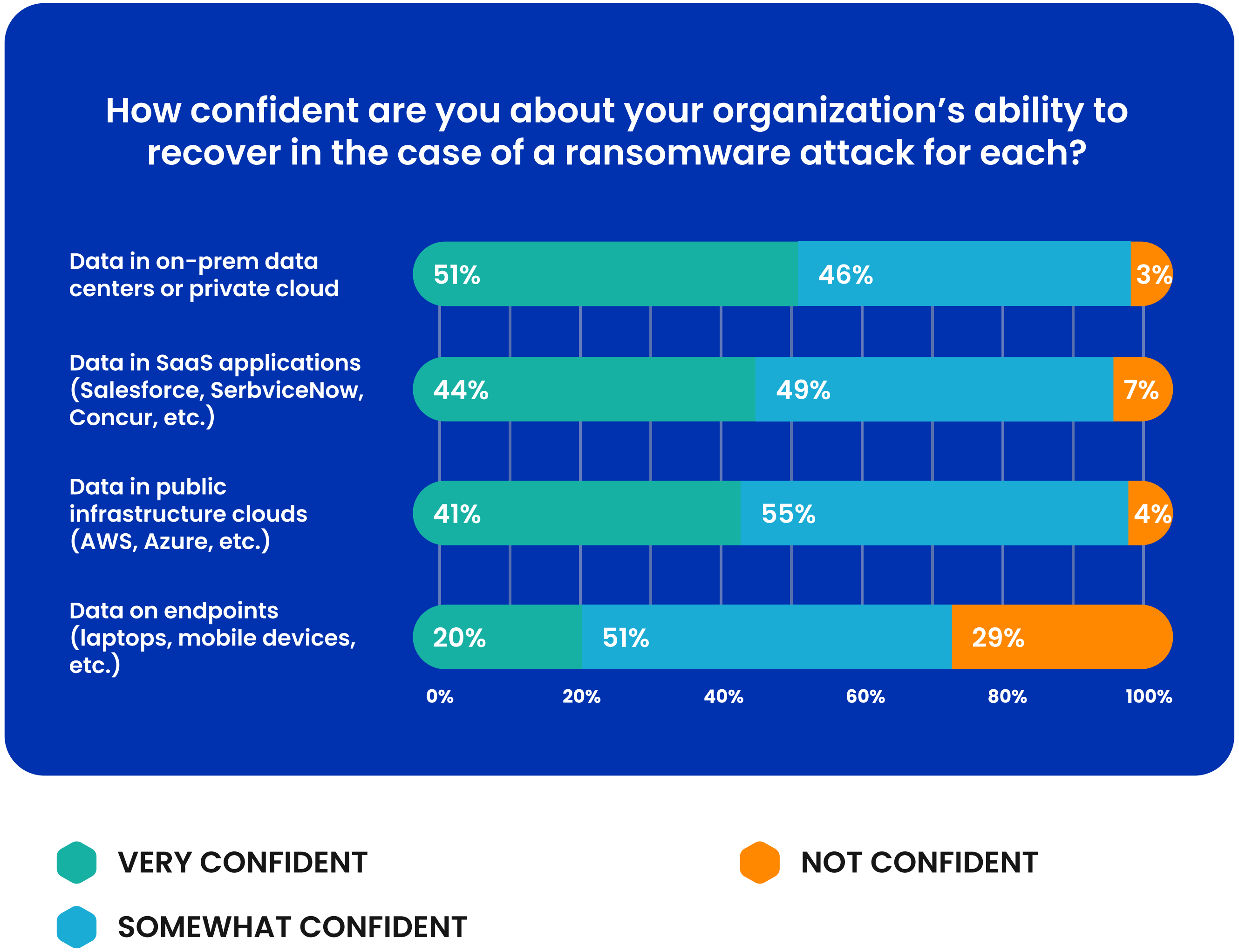
How long did it typically take to recover after a ransomware attack?



THE RECOVERY

Confidence in recovery of data after a ransomware attack is lowest for endpoints

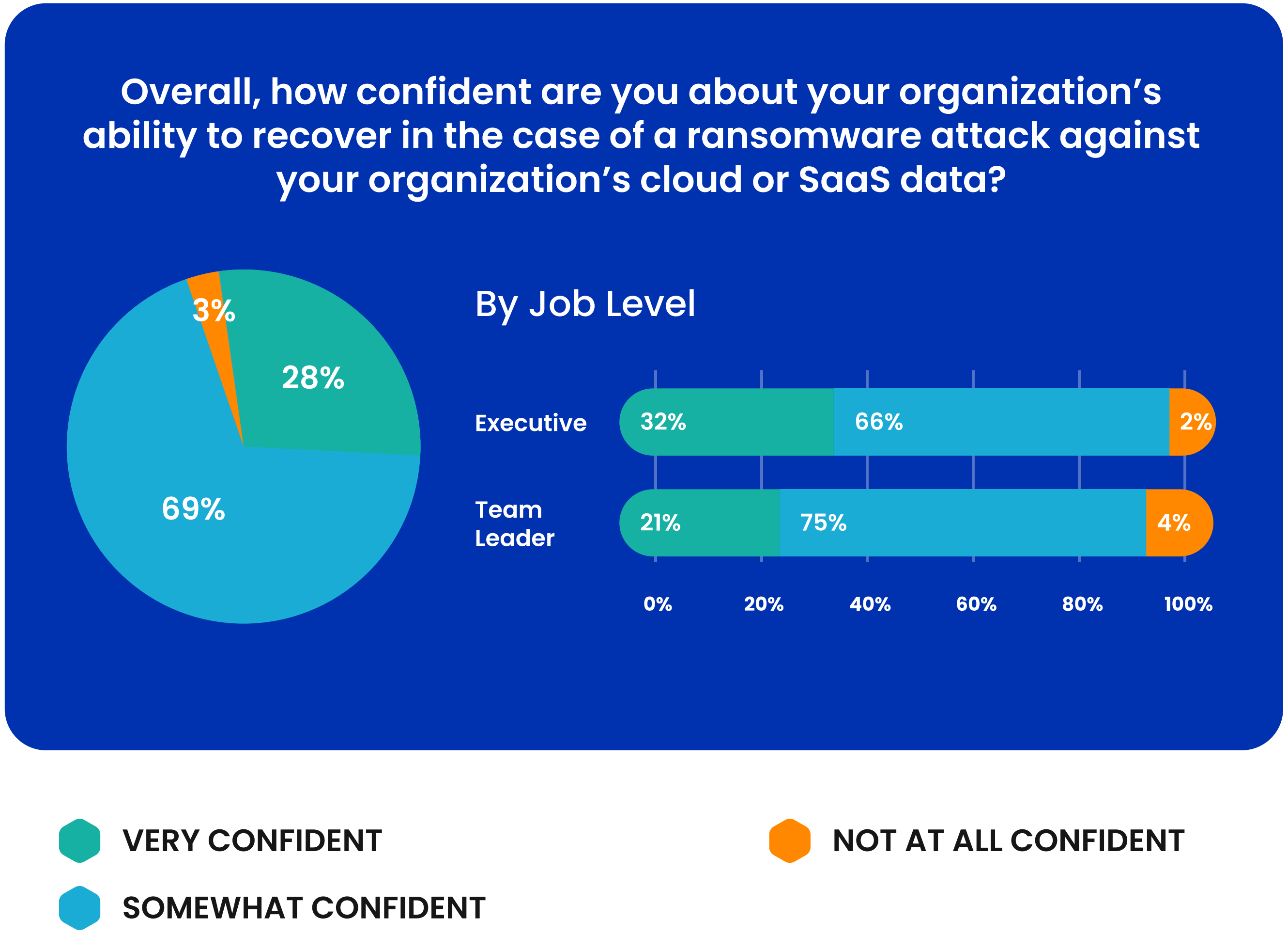
Only 20% of of respondents are very confident they can recover SaaS data.



THE RECOVERY

Only 28% are "very" confident about their ability to recover after a cloud or SaaS ransomware attack

Team Managers are less confident than Executives that SaaS data is recoverable.



THE PREVENTION

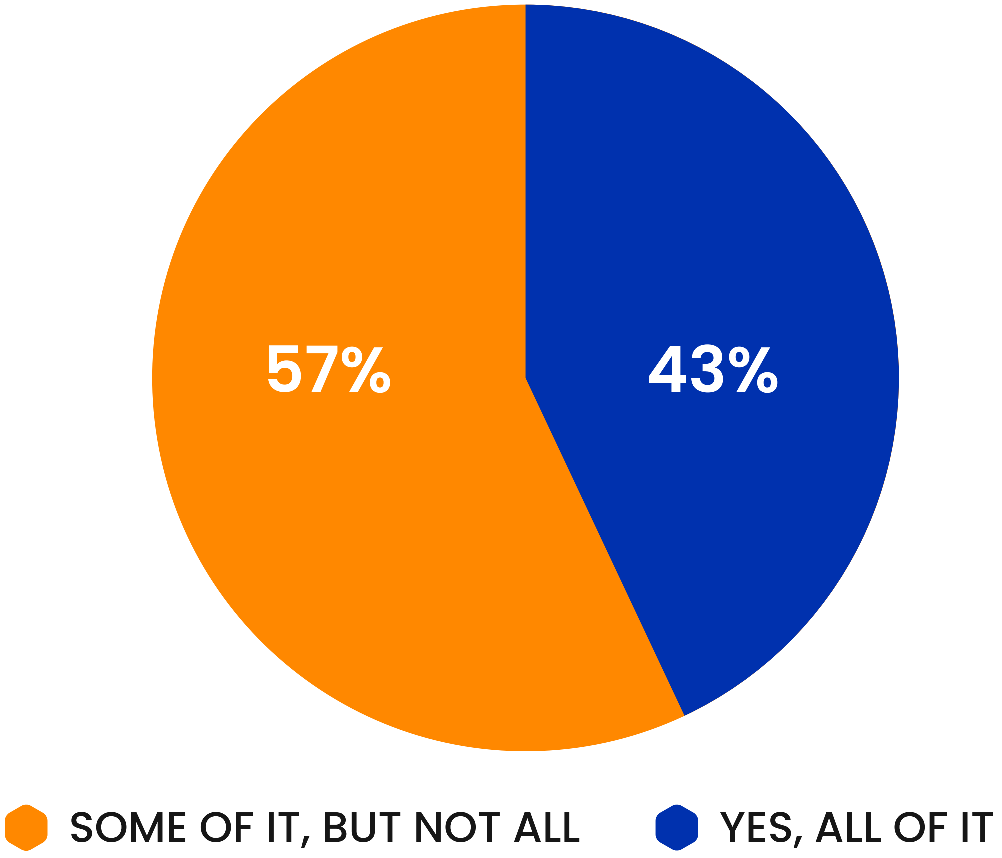
Data Protection begins with Backups

THE PREVENTION

All backup SaaS data, but less than half back up all of it

Data cannot be restored if it isn't backed up.

Is your company's SaaS data backed up?

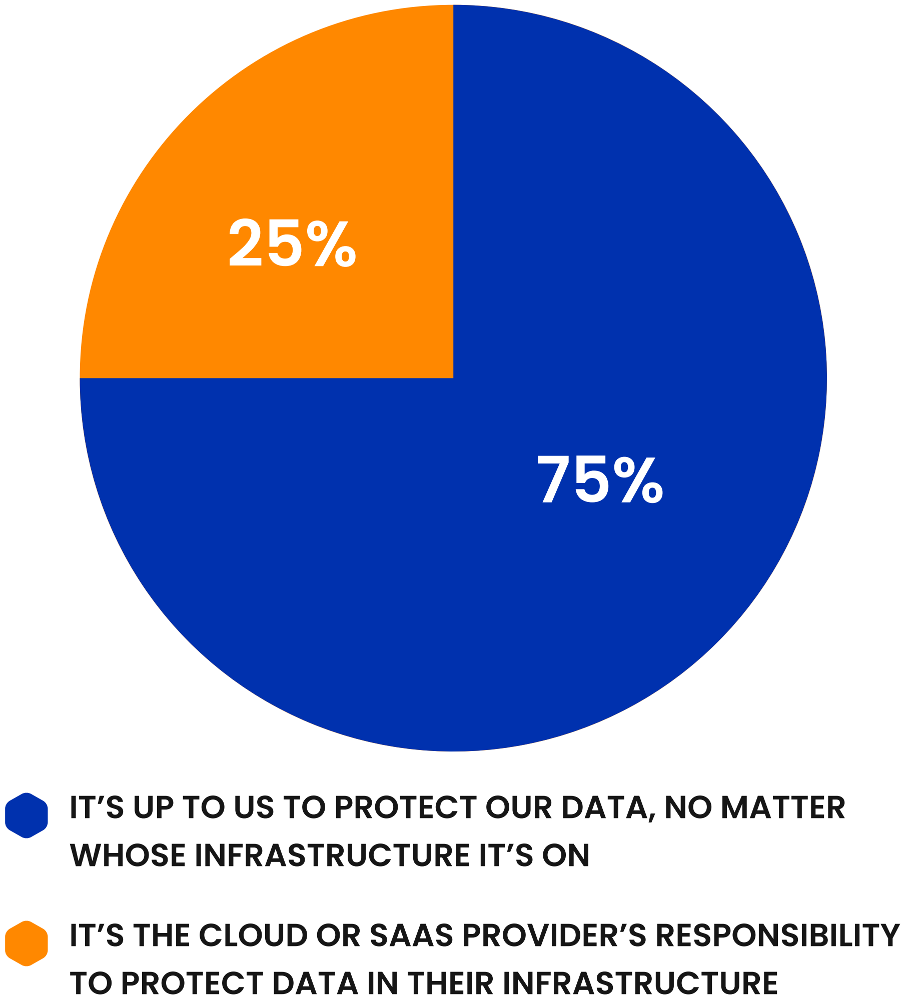


THE PREVENTION

25% believe it isn’t their responsibility to protect their SaaS data

A quarter of respondents mistakenly believe that the SaaS provider is responsible for protecting their company’s data. But SaaS platforms embrace a ‘shared responsibility’ model for data. That means the SaaS provider ensures the security and integrity of the platform, but the customer is responsible for securing and managing the data generated.

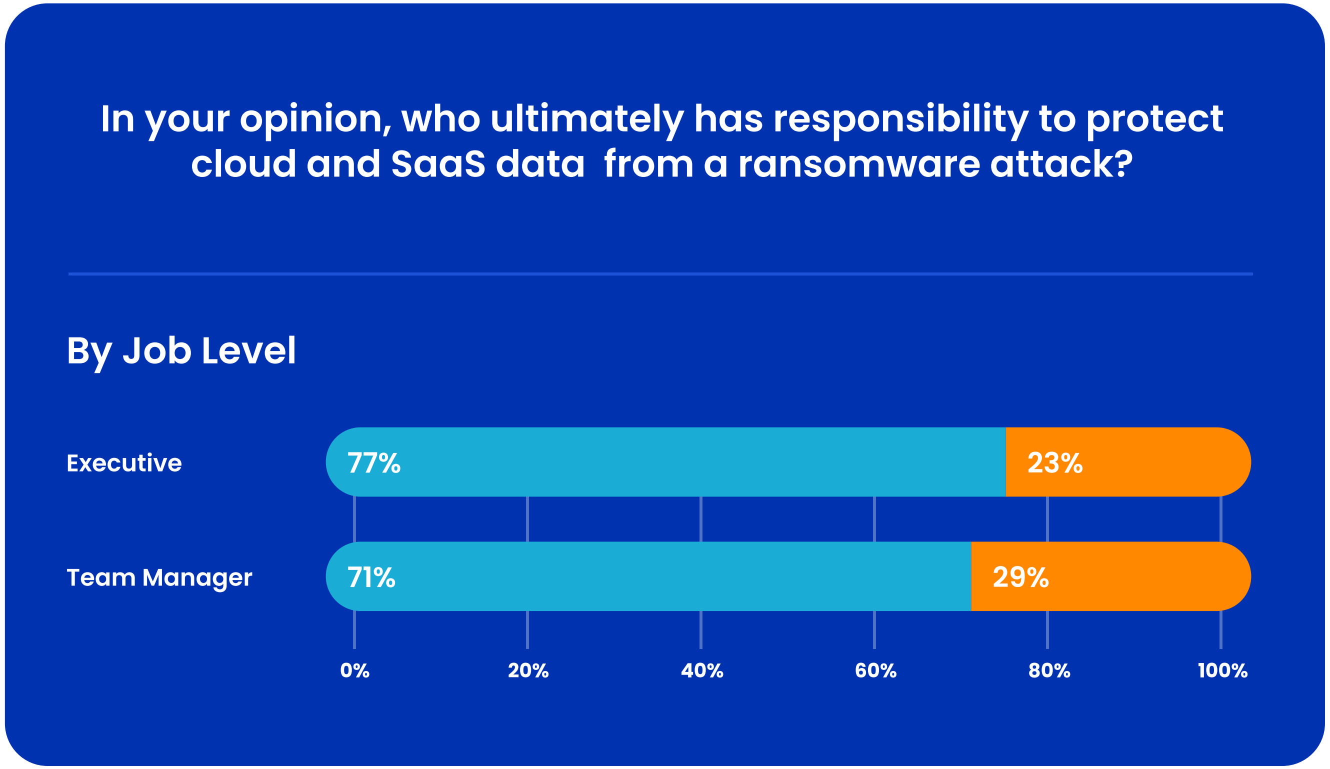
In your opinion, who ultimately has responsibility to protect cloud and SaaS data from a ransomware attack?



THE PREVENTION

Executives more likely to feel ownership for cloud data protection

Team Managers are more likely to mistakenly believe that the SaaS provider is responsible for protecting their company's data.



In your opinion, who ultimately has responsibility to protect cloud and SaaS data from a ransomware attack?

By Job Level

⬢ IT'S UP TO US TO PROTECT OUR DATA, NO MATTER WHOSE INFRASTRUCTURE IT'S ON

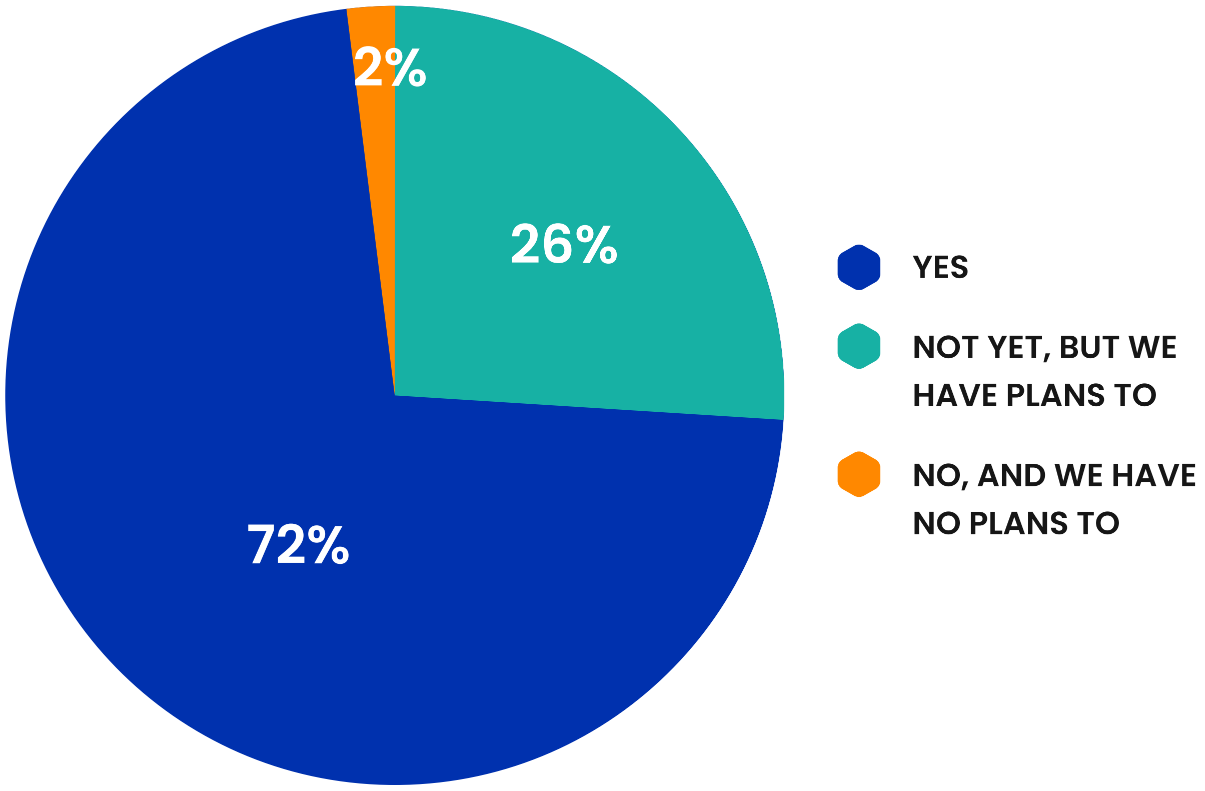
⬢ IT'S THE CLOUD OR SAAS PROVIDER'S RESPONSIBILITY TO PROTECT DATA IN THEIR INFRASTRUCTURE

THE PREVENTION

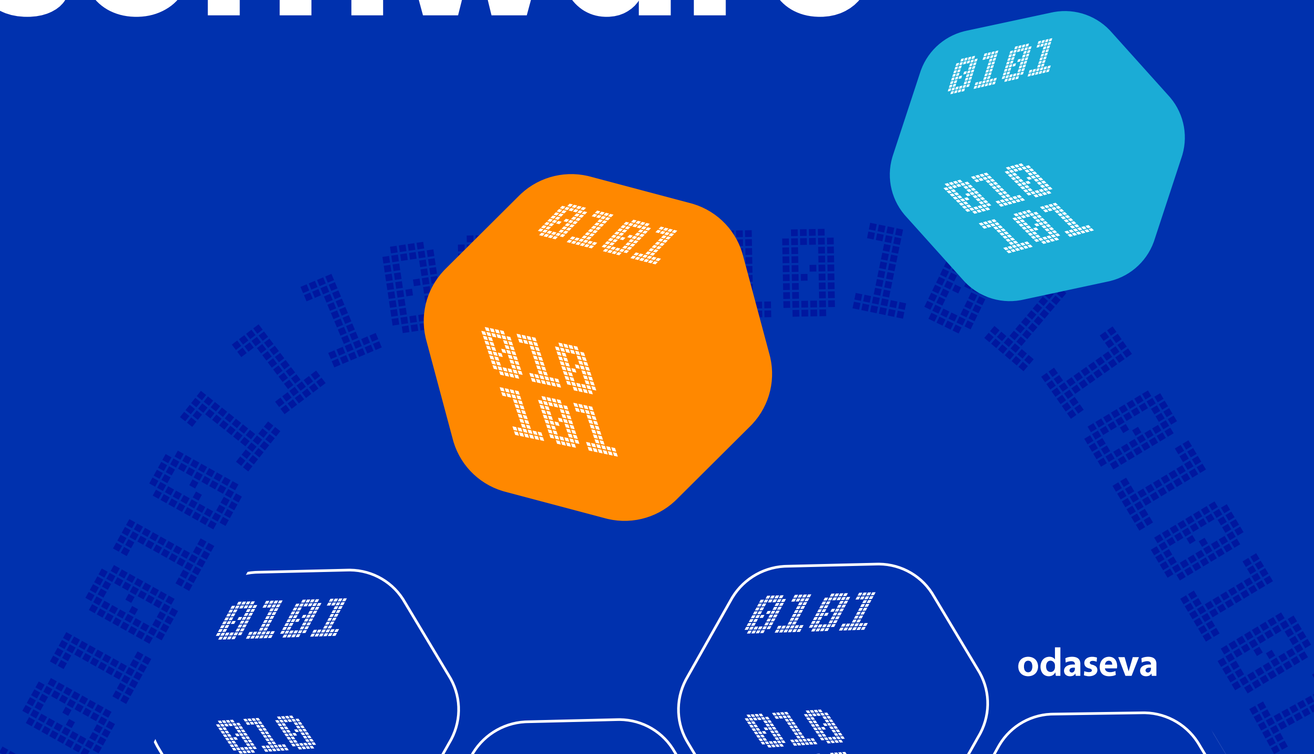
98% have invested in or have plans to invest in data protection for cloud and SaaS ransomware

Data protection is top-of-mind, but finding an **enterprise-grade solution** for backup and recovery is critical to a successful Disaster Recovery Plan.

Has your organization implemented security or data protection measures specifically to protect cloud and SaaS from ransomware attacks?



Enterprises can protect SaaS data against ransomware attacks



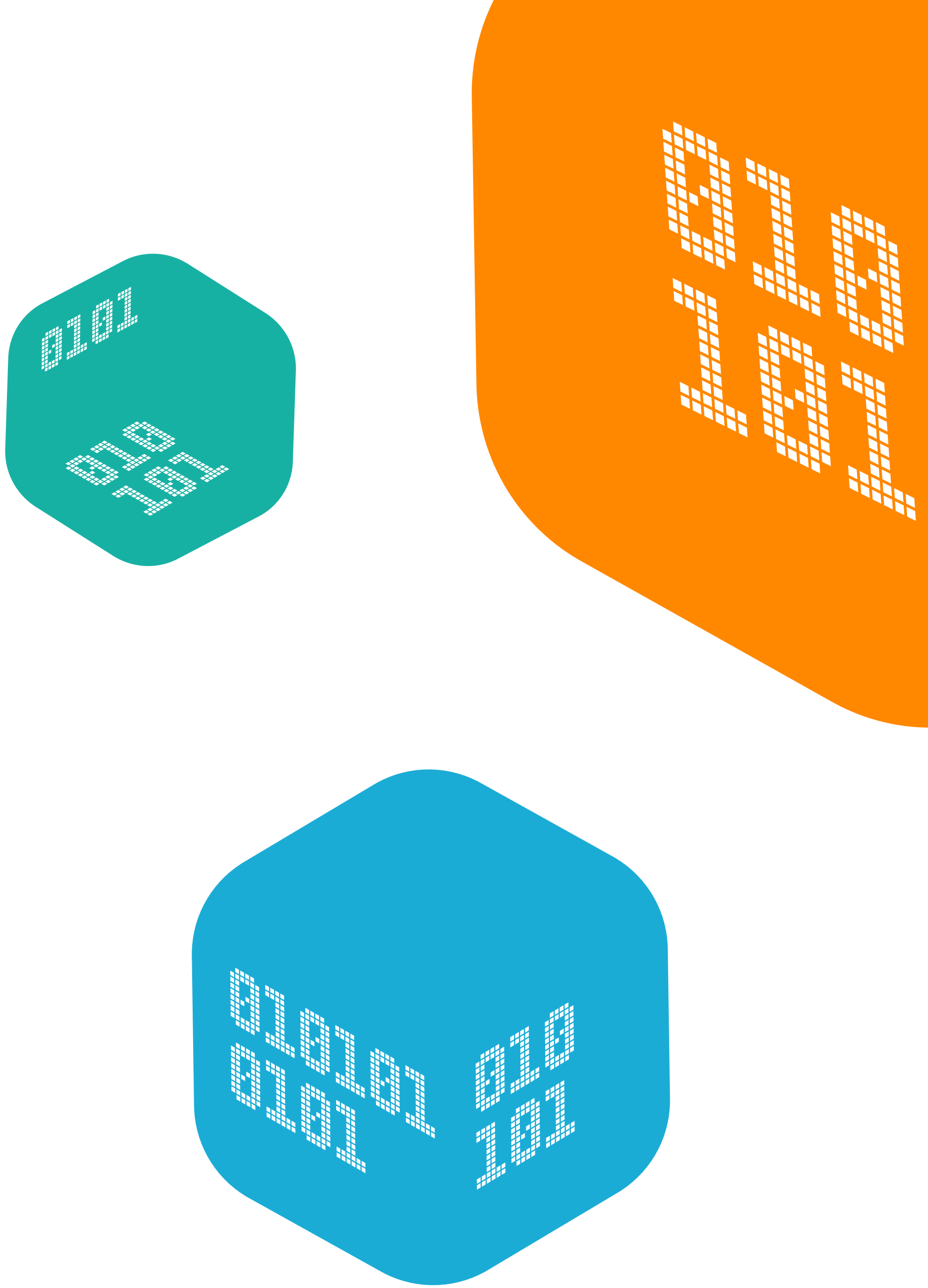
CLOSING THOUGHTS

Enterprises can protect SaaS data against ransomware attacks with the right backup and restore solution

Very large enterprises require data protection tools that are designed and built specifically for their needs.

That's because at enterprise scale, SaaS data is different. Data volumes are large. Data models are more sophisticated. Integrations, regulations, and business processes are much more intricate.

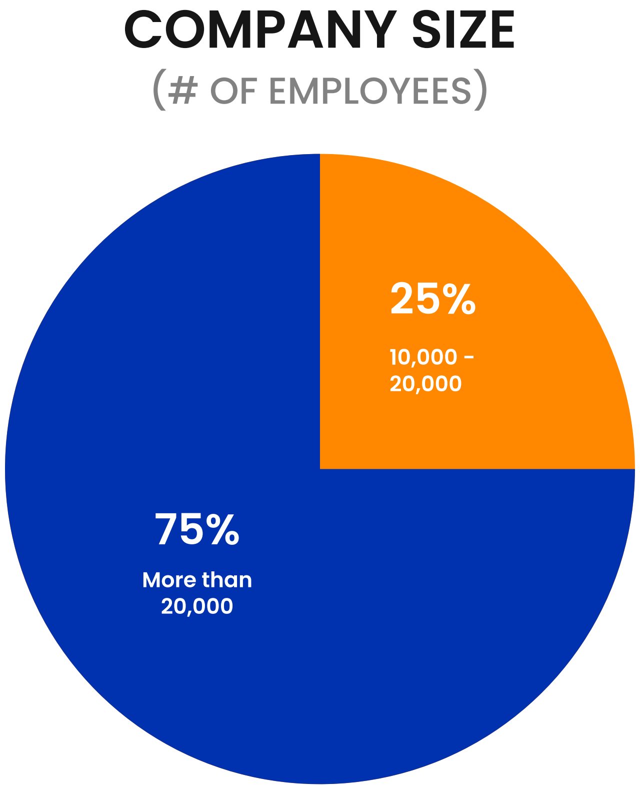
To protect this data against ransomware attacks, it must be securely protected - and that begins with a powerful backup and restore solution. By ensuring that SaaS data, metadata, and files are properly backed up, enterprises can restore this data if a ransomware attack or other data disaster strikes.

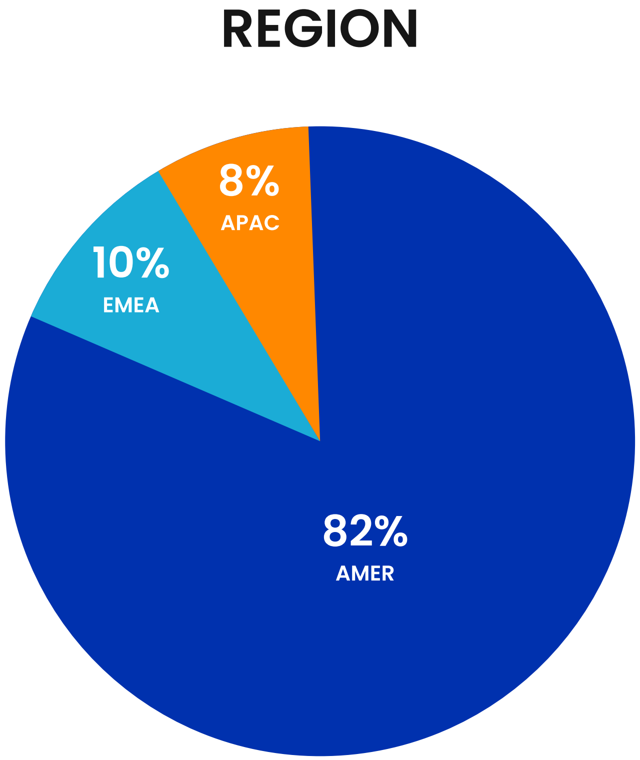


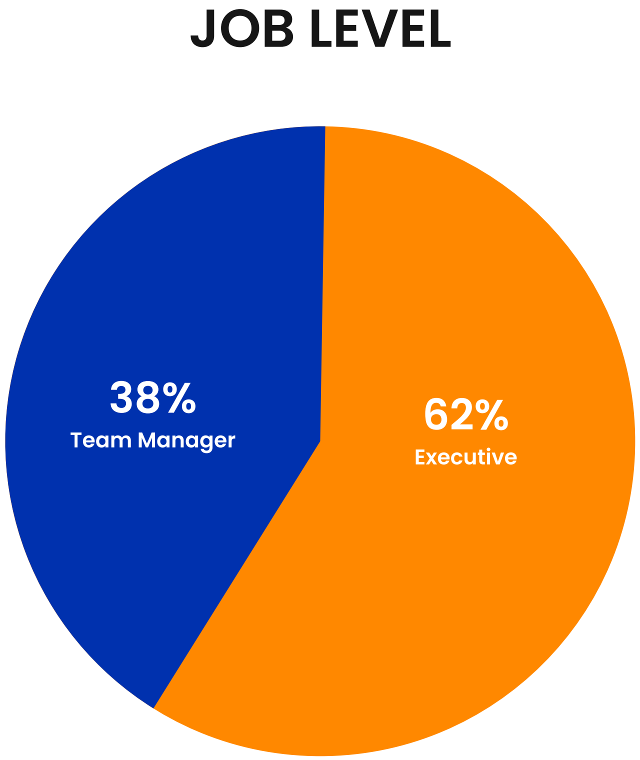
What you can do now to protect SaaS data against ransomware attacks.

- ✓ Backup SaaS data as frequently as necessary, depending on the criticality of the objects
- ✓ Run restore tests regularly to identify any potential roadblocks to a speedy and effective data restoration
- ✓ Visit odaseva.com to learn how we protect Salesforce data with the strongest security, power, control and governance available to the enterprise

WHO WAS SURVEYED?

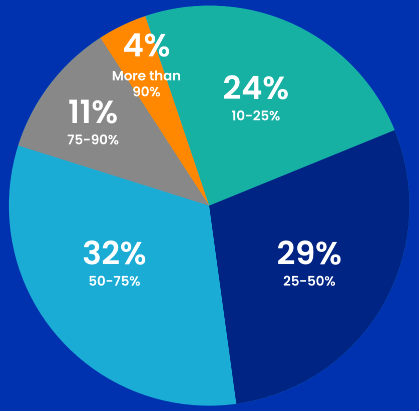




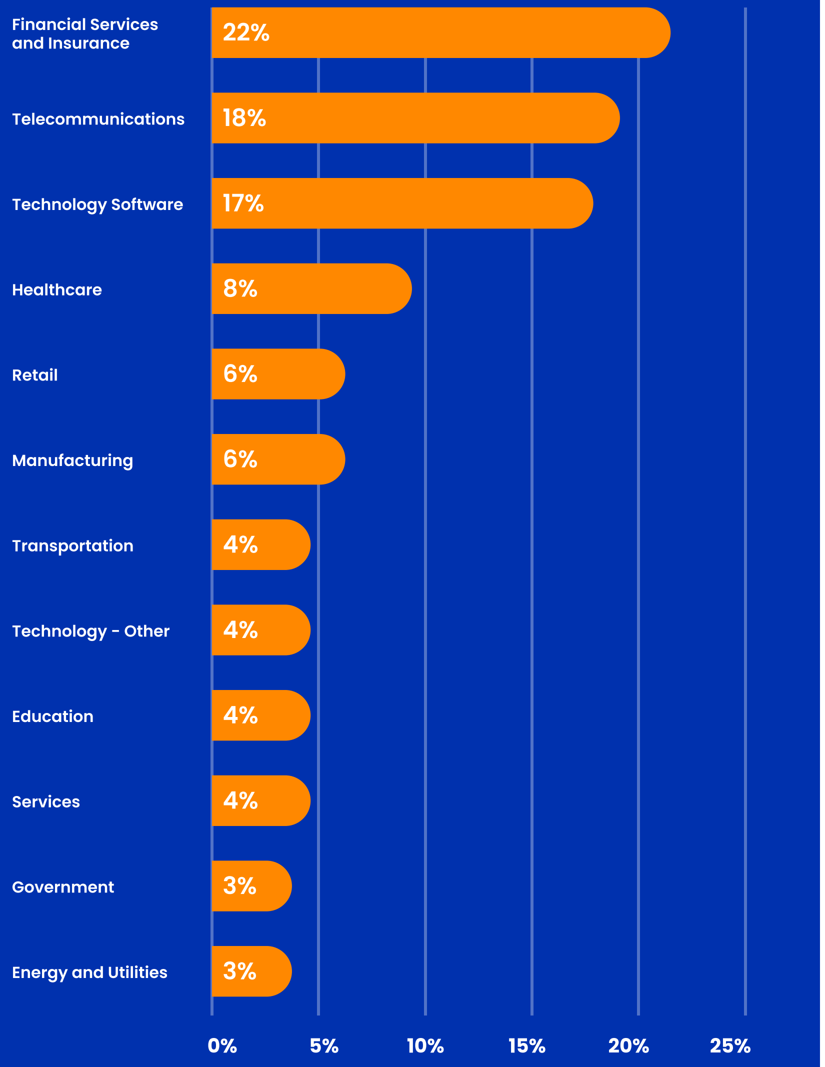


WHO WAS SURVEYED?

% of Corporate Data in the Cloud (IaaS or SaaS)



Industry



THANK YOU

Visit odaseva.com today for more information and to get a personalized demo