DigitalOcean

Small businesses and cybersecurity

How startups and SMBs are viewing security threats in 2023

Table of contents

DigitalOcean

Introduction

Cybersecurity is more of a threat than ever before, with both individuals and businesses relying on a combination of software and hardware to conduct business, store data, and connect with others. Given this, one security breach can quickly multiply and give malicious actors access to a wide range of systems and data.

In the past years, there have been several widespread security breaches and vulnerabilities that have impacted millions of people worldwide, including vulnerabilities such as Log4j, and data breaches of popular email systems, password managers, ridesharing applications, and more. These security incidents can have devastating effects, exposing sensitive user data and leading to potential financial losses and identity theft.

For businesses, a security breach risks not only exposure of customer data and a decrease in customer trust but can also result in loss of revenue if systems are taken offline through an attack, such as a Distributed Denial of Service (DDoS) attack. Because of this, many businesses have increased security measures in recent years, ensuring employees are trained on phishing scams, implementing two-factor authentication for applications, and increasing their security budgets and team size.

However, small businesses and startups often face a dilemma when it comes to cybersecurity — a security breach can be devastating to a new business, but to provide an effective cybersecurity solution, companies must spend their valuable resources on maintaining and updating their systems, hiring and training staff, and implementing dedicated security software.

In this report from DigitalOcean, we examine the current state of cybersecurity among small and medium-sized businesses (SMBs).

> **How concerned are SMBs about cybersecurity going into 2023, and what steps are they taking to protect themselves and their employees from a breach?**

> **How much are small businesses thinking about data privacy, and what privacy requirements do they have for their vendors?**

> **How many businesses have actually experienced a recent breach, and what type was it?**

This report focuses on the results of a survey of over 550 SMB founders and executives, examining their thoughts on cybersecurity, data privacy, and the measures they have taken to protect their businesses from threats. **Read on for the results.**

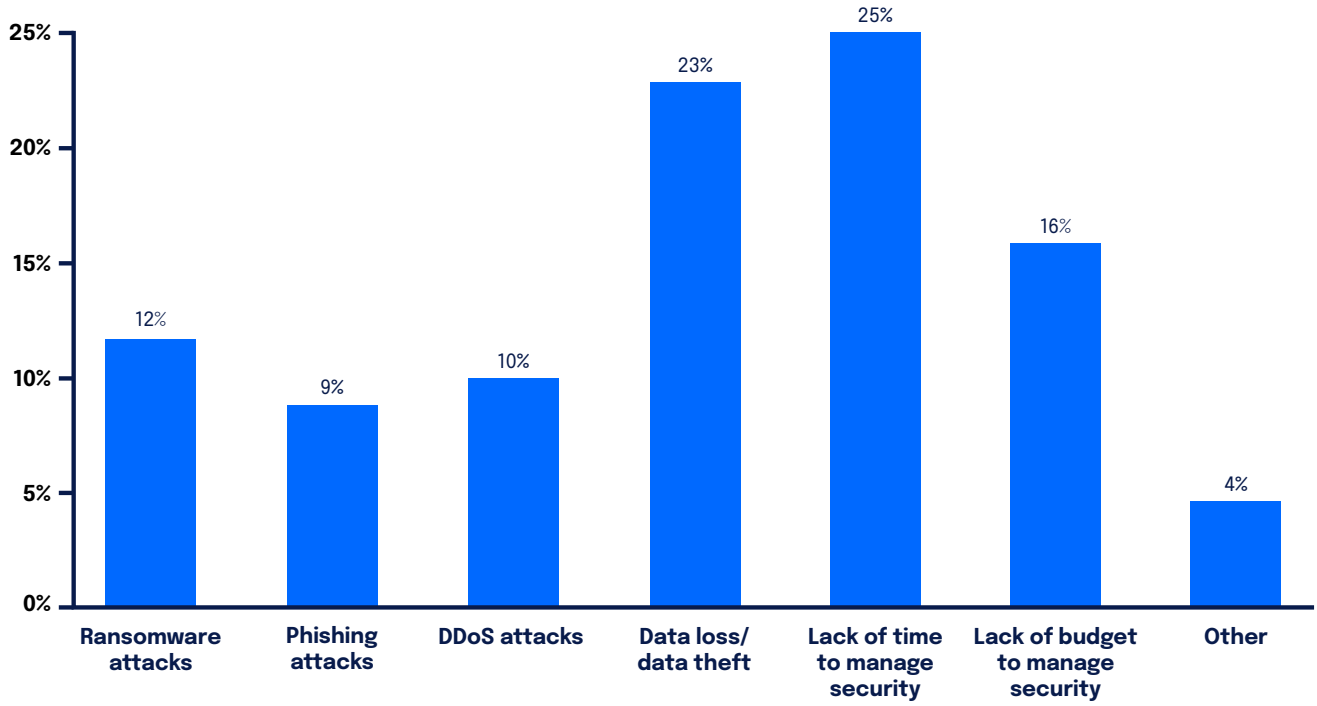
Cybersecurity and small business

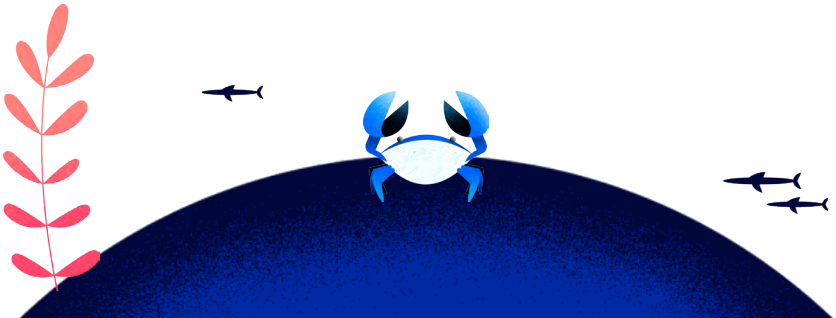
Cybersecurity is of growing concern for small businesses, with 54% stating that they are more concerned about cybersecurity now than one year ago, and just 15% disagreeing with the same statement.

54% of respondents say they are more concerned about cybersecurity now than one year ago.

Looking specifically at the concerns SMBs have about security in 2023, we found that lack of time to manage security was the biggest security concern facing businesses (25%), followed by data loss or data theft (23%), ransomware attacks (12%), and DDoS attacks (10%). This demonstrates that many small businesses find it challenging to dedicate staff and time to maintaining their security systems, which can put them at greater risk of various forms of security attack.

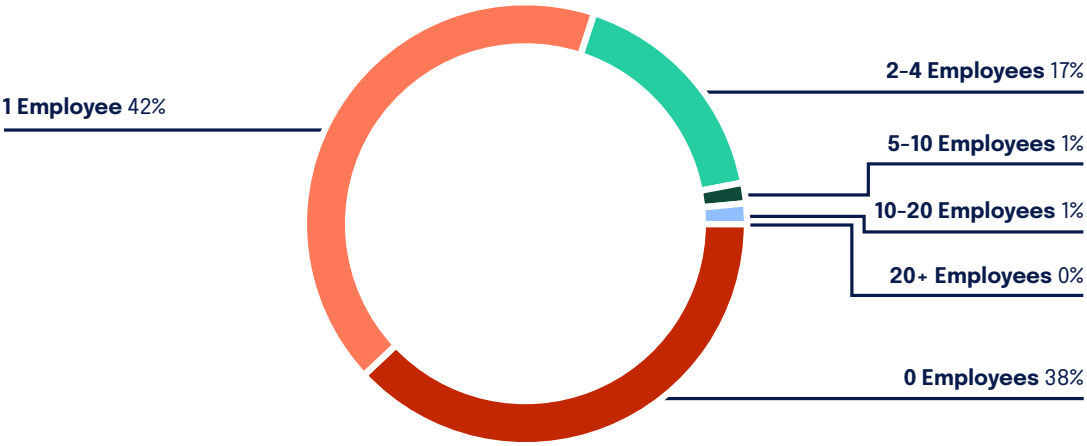
Looking to 2023, what is your biggest concern related to security?





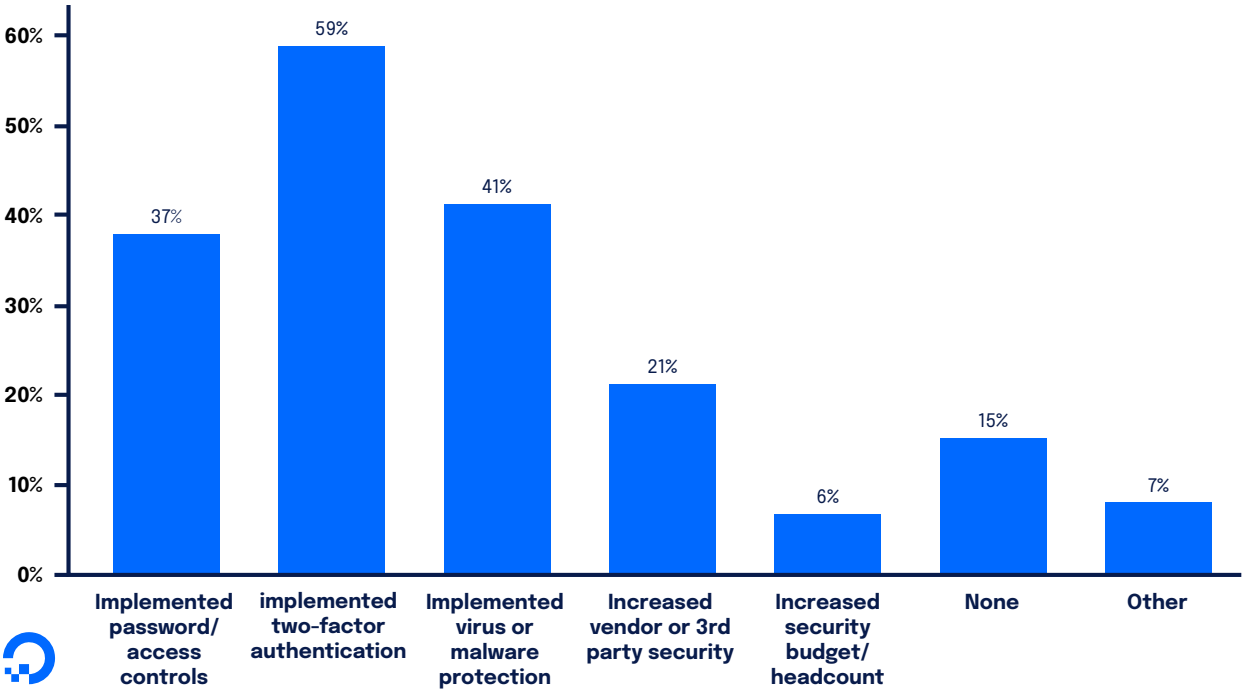
Although security is a concern, SMBs often don't have any employees fully dedicated to security — 38% of surveyed businesses said they had zero employees dedicated to security as all or part of their role, and 42% had just one employee working on security.

How many employees dedicated to security as part or all of their role do you currently have?



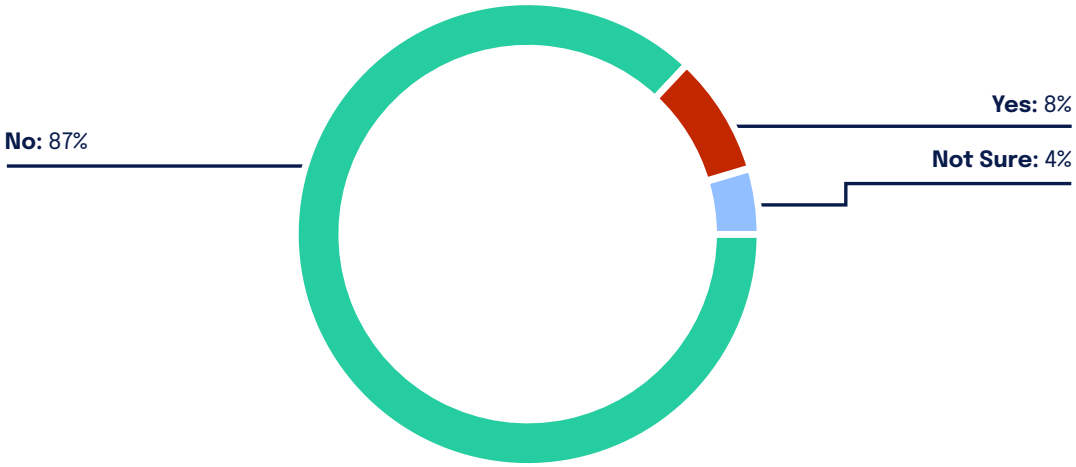
Even if businesses don't have many resources dedicated to security, it's clear they are taking the measures they can to protect their business from attack. Just 15% said they have not taken any measure to increase their security in the past year, while 59% have implemented two-factor authentication, 41% have implemented firewalls or security applications, and 37% have implemented password or access controls. Consistent with the finding that businesses often struggle with time and budget to manage security, only 6% have increased their security budget or headcount in the past year, showing that the lack of resources to focus on security will likely continue for many SMBs.

What measures have you taken to increase your security in the past year?

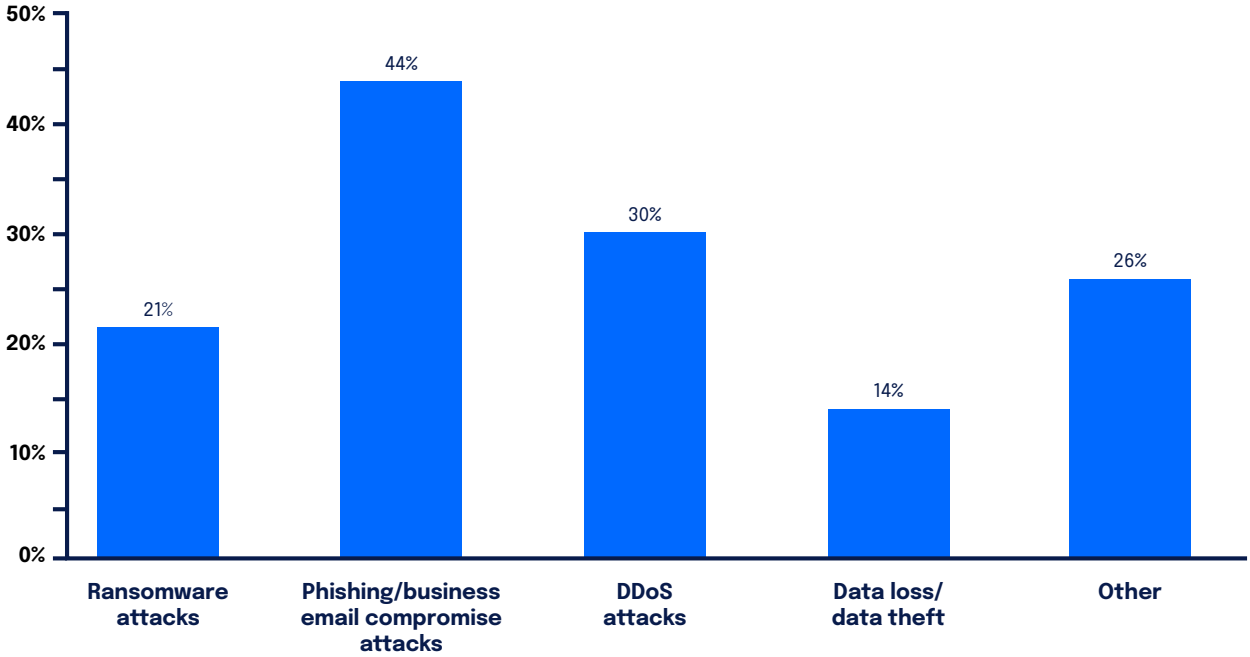


To assess how widespread actual security attacks were in the past year, we also asked respondents if they had experienced a security breach in the past year, finding that 8% had experienced a breach, while 87% had not and 4% weren't sure. Of those who experienced a breach, the most common type was phishing or business email compromise attacks (44%), followed by DDoS attacks (30%), and ransomware attacks (21%).

Has your company experienced a security breach in the past year?

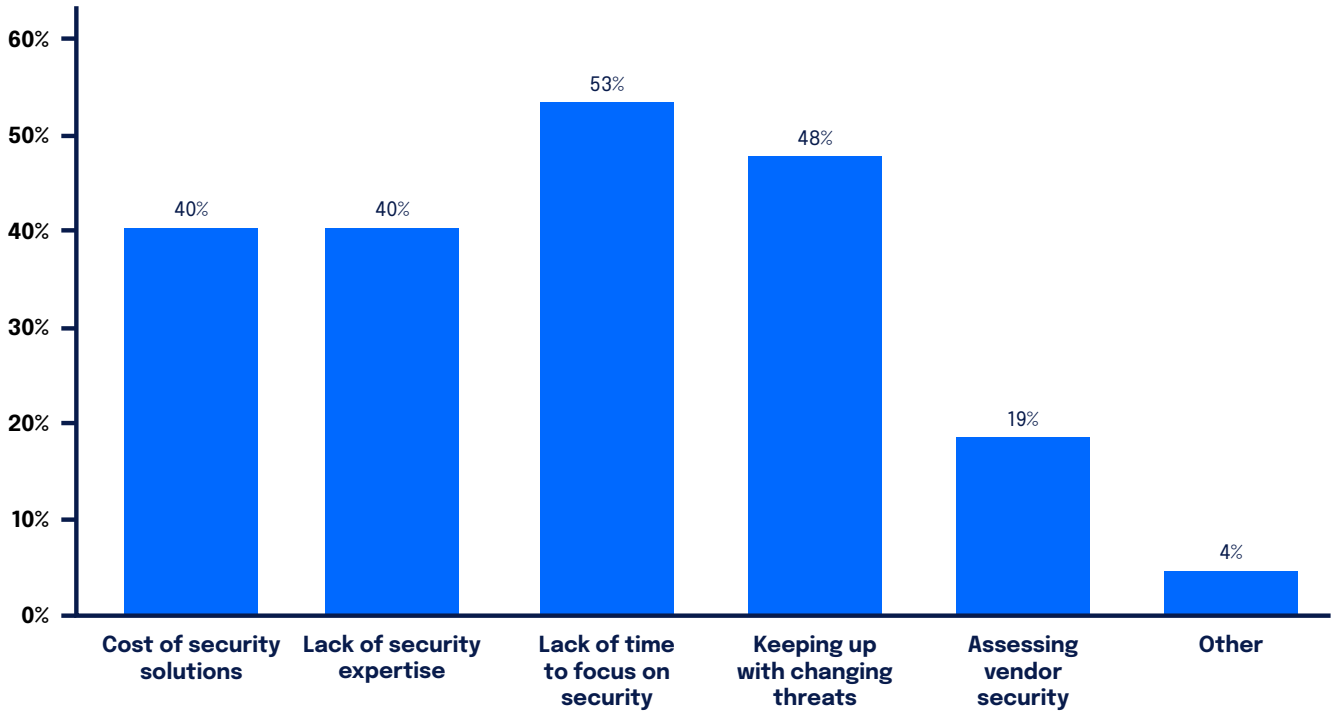


What kind of security breach did you experience?



Finally, we looked at the biggest challenges SMBs and startups face in securing their business and found that lack of time to focus on security was the most cited challenge (53%), followed by keeping up with changing threats (48%), cost of security solutions (40%), and lack of security expertise (40%). Nineteen percent said that assessing vendor security was a challenge.

What are the biggest challenges in securing your business?



Data privacy and small businesses

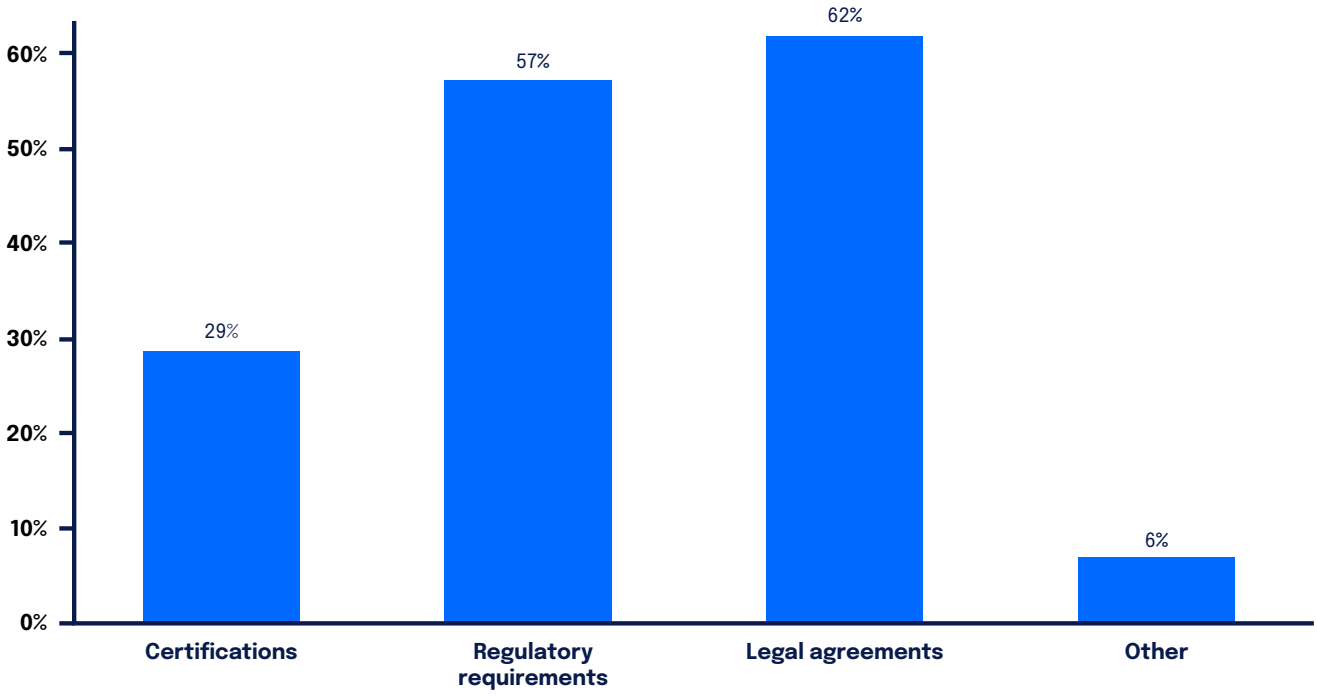
Data privacy is a subset of cybersecurity that handles the protection of data, especially personal information such as name, location, email address, and IP address. There are now several laws in place, including the General Data Protection Regulation (GDPR) for the EU, that regulate how companies collect and store personal data, which has brought data privacy to the forefront of cybersecurity in recent years. However, data privacy is a relatively new field, which means that small businesses may not be focusing on taking recommended data protection measures in addition to protecting their properties from other attacks.

74% state that data privacy is a top concern, but **over half (57%)** of small businesses have **zero employees** dedicated to data privacy.

We found that 74% of businesses say that data privacy is a top concern for their business, but the majority (57%) have zero employees dedicated to data privacy, with 42% stating they have one to five people focused solely on data privacy.

One area of focus for companies that want to ensure their data is protected and secure is reviewing the security and data protection policies of third-party vendors, which can include cloud providers and other technology vendors. We asked respondents what privacy requirements they have for their cloud and technology vendors and found that 62% request legal agreements, such as data protection agreements and privacy policies; 57% request regulatory requirements, such as GDPR, HIPAA, or FedRAMP; and 29% request certifications, such as SOC and ISO. Requesting that vendors comply with these requirements can help companies looking to protect their customer and business data.

What privacy requirements do your customers request from your cloud provider or other technology vendors?



Conclusion and methodology

The results from this study demonstrate that while cybersecurity is a concern for many small businesses, they often don't have the time or resources, including budget and employees, to dedicate to securing their business. Data privacy is also a concern, but similarly, a majority of small businesses do not have employees dedicated to data protection. As threat landscapes are often changing, maintaining a high level of security will continue to be a challenge for SMBs, and those that don't dedicate resources to this can risk customer attrition, reputation damage, and revenue loss. Without dedicated cybersecurity employees, SMBs rely on their vendors, including cloud providers and other security products, to maintain a secure environment.

This report was based on survey responses from 554 founders, CEOs, and C-suite and VP-level executives at startups and small businesses. The survey was conducted through an online survey link from October 18 to November 7, 2022. The link was distributed to various sample sources, including DigitalOcean email lists, Cloudways email lists, and tech founder groups. Seventy percent of the respondents were CEOs/founders/owners, 23% were CTOs, and the remainder were C-level or VP-level executives.

Respondents represent 76 countries, with 27% in the United States, 8% in the UK, 5% in India, 5% in Germany, and 5% in Canada. The questionnaire was developed by DigitalOcean and was distributed via link through email and social media channels to both DigitalOcean customers and non-customers. Respondents come from a range of digital industries, with 37% being in software/Software as a Service, 19% technology consulting, 6% marketing/advertising, 4% ecommerce, and 6% other technology industries.

The gender breakdown was 90% male, 4% female, 1% nonbinary, 1% who self-describe, and 4% who preferred not to say their gender. Respondents represent a range of ages: 3% are aged 18–24; 24% are aged 25–34; 36% are 35–44; 22% aged 45–54; 10% aged 55–64; and 4% are 65 and older.

DigitalOcean

About DigitalOcean

DigitalOcean simplifies cloud computing so developers and businesses can spend more time building software that changes the world. With its mission-critical infrastructure and fully managed offering, DigitalOcean helps developers, startups, and small- and medium-sized businesses (SMBs) rapidly build, deploy, and scale applications to accelerate innovation and increase productivity and agility. DigitalOcean combines the power of simplicity, community, open source, and customer support so customers can spend less time managing their infrastructure and more time building innovative applications that drive business growth.

> **To get started, sign up for an account at DigitalOcean.com.**
> **For more information or help migrating your infrastructure to DigitalOcean, speak to a sales representative.**