September 2021

MARKET REPORT

The state of network security in 2021

Network breaches, ransomware attacks, and remote-work challenges highlight need for cloud-native Secure Access Service Edge (SASE) deployments. »

Barracuda
Your journey, secured.

Contents

Introduction

Digital transformation, pandemic, and cybersecurity

The COVID-19 pandemic was a catalyst, thrusting global businesses into a world of remote work. With the drive for digital transformation also came the need to evaluate current security architectures.

Public cloud has and will continue to support digital transformation. The bad news is twofold: Businesses are getting breached, and ransomware makes up a sizeable portion of the attacks. The good news is that businesses are aware of and are investing in Secure Access Service Edge (SASE) solutions to defeat attacks and protect their networks while supporting a hybrid work model.

This report takes an in-depth look at cloud adoption, working from home, security concerns, and a variety of issues and challenges related to cybersecurity risks.

Methodology

Barracuda commissioned independent market researcher Vanson Bourne to conduct a global survey of **IT decision makers responsible for their organization's networking, public cloud, and security.** There were **750 survey participants** from a broad range of industries, including **construction, energy, financial services, media, manufacturing, retail, technology, and others**. Survey participants from the **U.S., Europe, and APAC** represented organizations with 500 employees or more. In Europe, respondents were from the United Kingdom, France, and Germany. In APAC, respondents were from India, Australia, Singapore, and Hong Kong. The survey was fielded in July and August 2021.

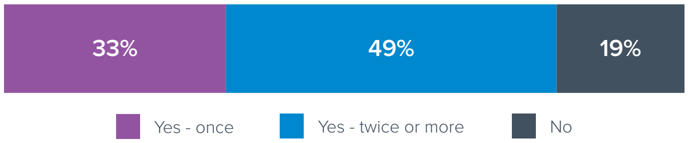
Security breaches

FINDING #1

Organizations are experiencing breaches, and ransomware makes up a significant portion of the attacks.

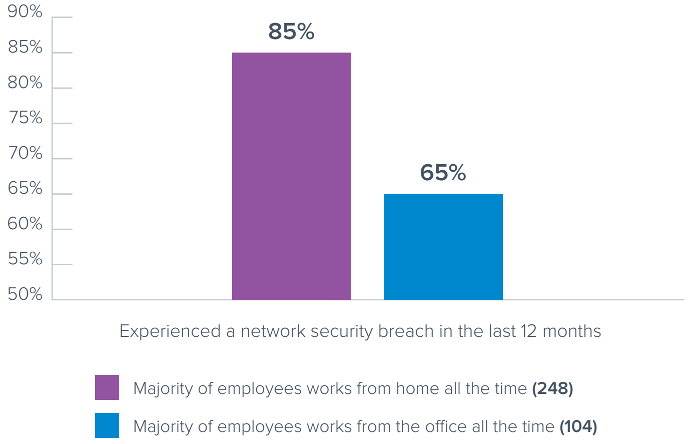
In the last 12 months has your organization suffered a successful security breach as a direct result of a network attack?

(n=750)



One-third of those surveyed (33%) said their organization has been the victim of a security breach once in the last year, and almost half (49%) said they've been breached twice or more.

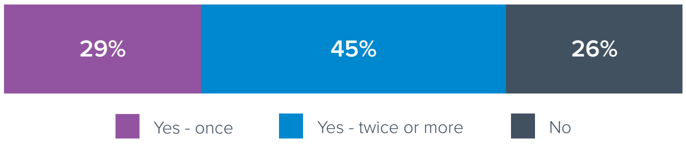
Network security breaches in relation to remote work



Companies with staff working predominantly from home had a significantly higher network security breach rate of 85%, compared to companies with staff working predominantly in the office, which experienced a 65% breach rate. Interestingly, issuing company-owned devices didn't yield any improvement. On the contrary, businesses that provided company-owned devices to employees experienced slightly more security breaches (82%) than businesses that that did not (81%).

Has your organization suffered a ransomware attack in the last 12 months?

(n=750)

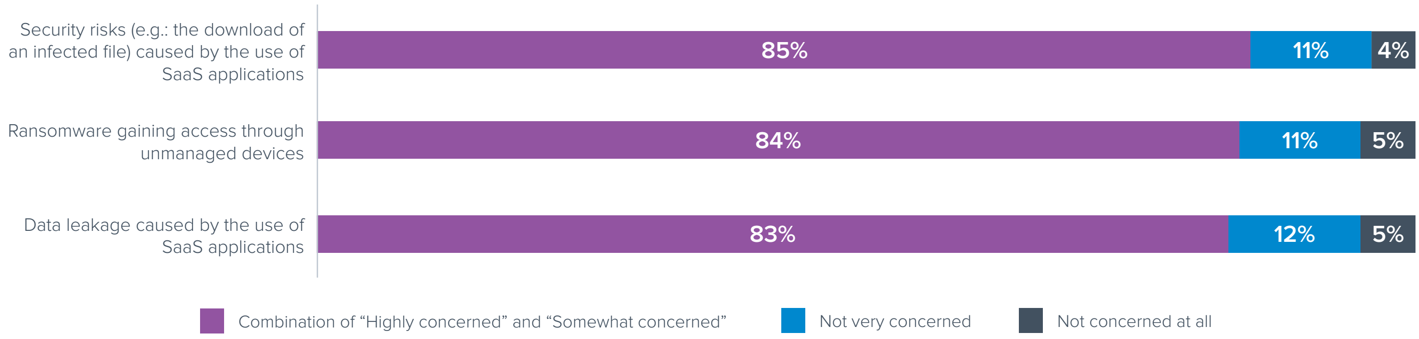


A full 74% of those surveyed said their organization has been the victim of at least one ransomware attack in the last year. Close to half (45%) said they've experienced two or more attacks in the same timeframe. Comparing the ransomware rates to the network breach rates discussed above, we can see that most network-layer breaches involve ransomware.

Remote work may be contributing to an increased risk of successful security breaches and ransomware attacks, due to a combination of lack of control over at-home IT systems and employees facing a higher likelihood of receiving COVID-19 themed phishing emails.

How concerned are you about the following: security risks, data leakage, and ransomware gaining access through unmanaged devices?

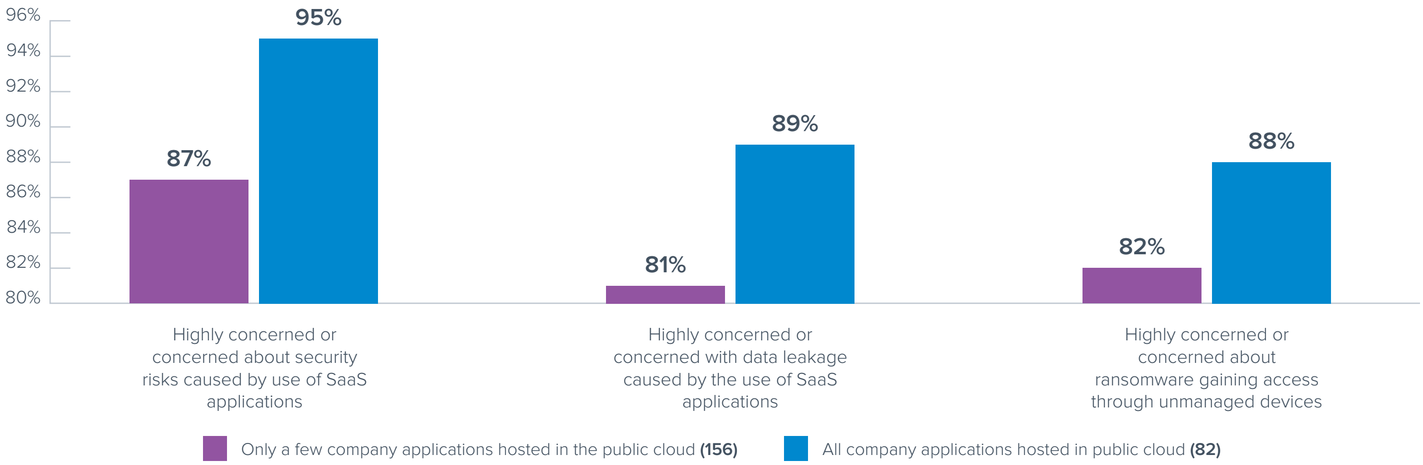
(n=750)



There are concerns about the cybersecurity risks and attacks associated with the use of Software-as-a-Service (SaaS) applications. Nearly half of all respondents are highly concerned about security, data leakage, and ransomware. When you add respondents who are somewhat concerned, those numbers spike to above 80%.

When companies host more of their applications in the public cloud, they are more concerned about SaaS application security. This makes sense, and it also indicates that organizations are concerned about the security of their SaaS apps.

SaaS security concerns in relation to public cloud adoption



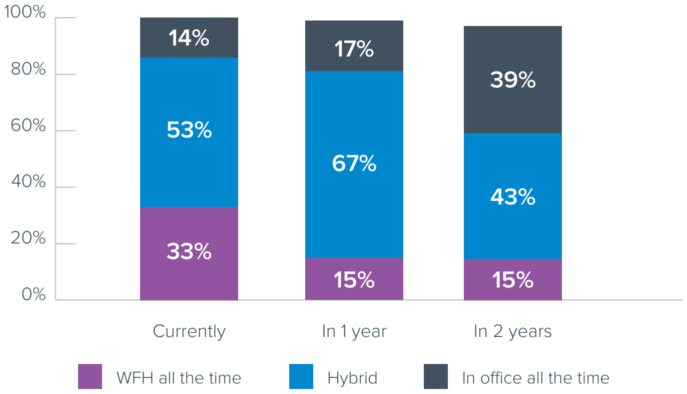
Remote work

FINDING #2

Despite fast connectivity, employees working from home are still experiencing operational and quality-of-service challenges.

Approximately what proportion of your organization's workforce currently works/will work remotely in the following timeframes?

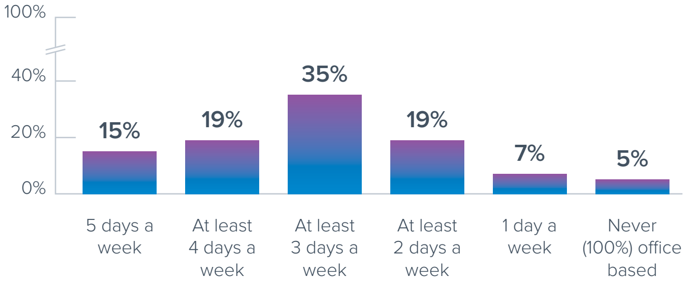
(n=750)



On average, only 14% of employees at the businesses surveyed currently work in the office all the time. In one year that percentage is expected to be up slightly to 17%. Even two years from now, only 39% of employees are expected to work in the office all the time. The majority will be working partly from home (43%) or from home all the time (15%). Clearly, the future of work is hybrid, and IT teams should expect to be supporting a hybrid workforce going forward.

How often do you work from home?

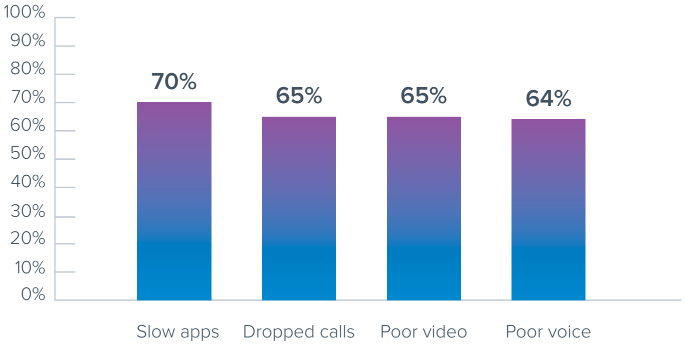
(n=750)



95% of those surveyed work from home at least one of five workdays. Nearly one-fifth (19%) work at home at least four days a week. Just over a third (35%) work at home at least three days a week.

When working from home, how often do you experience any of the following IT pains that interfere with your work?

(n=712)

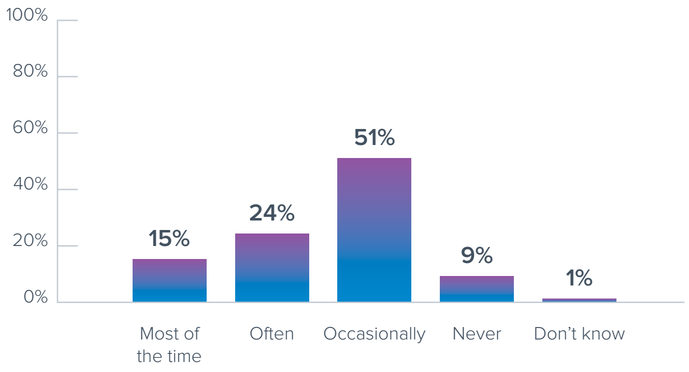


More than 75% of respondents who work from home have high-speed internet, but they still encounter difficulties, including slow apps, dropped calls, poor video, and poor voice.

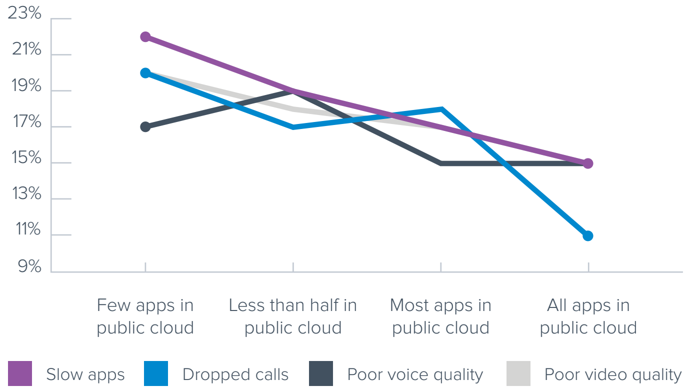
A full 94% of respondents with company-issued devices share their home internet connection with other members of their household. Only 6% have a dedicated line, so the risk of breach remains.

When working from home, how often do your users experience IT pains that interfere with their work?

(n=646)



Work-from-home IT issues often reported vs. public cloud adoption



More than half of respondents (51%) said users occasionally experience disruptions. 39% said they do so often or most of the time. Only 9% said users never have interference.

Even the IT team struggles with these types of difficulties. 70% experience slow applications, dropped calls (65%), poor voice quality (64%), and poor video quality (65%). About 30% said they never experience any of those problems when working from home.

One thing that seems to help is when more apps are hosted in the cloud. SaaS apps and more cloud deployments help improve user experience.

Companies that have their security issues under control also report significantly fewer issues when it comes to work-from-home IT problems. Organizations that suffered a network breach had 44% of their employees report IT pains. On the other hand, those that did not experience a network breach had only 16% of their employees report IT pains. This is good news as it indicates that making security improvements also improves user experience.

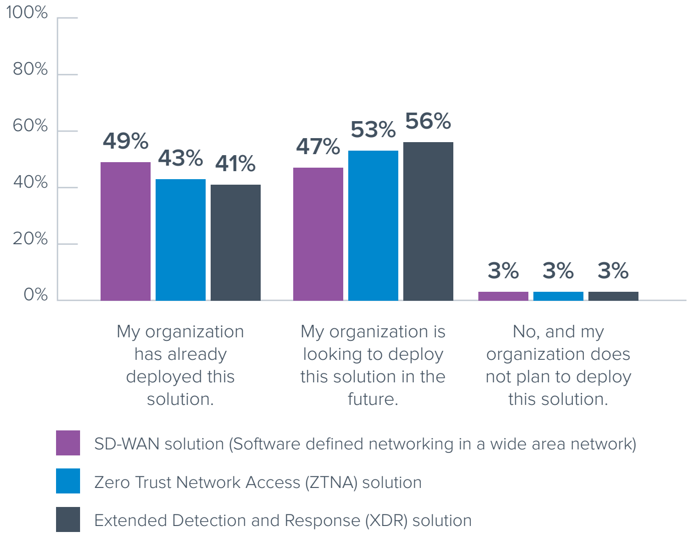
SASE: Software-Defined Wide Area Network (SD-WAN)

FINDING #3

Secure Access Service Edge (SASE) technologies are looked at as solutions to defeat security breaches and overcome work-from-home challenges.

Has your organization already, or does your organization plan to deploy any of the following solutions in the next two years or beyond?

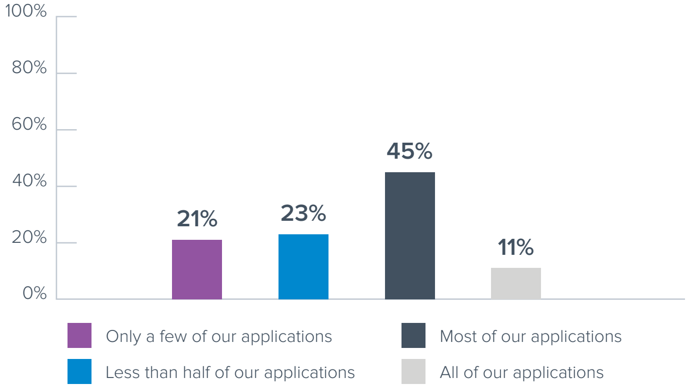
(n=750)



96% of respondents said they have already deployed (49%) or plan to deploy (47%) SD-WAN in the future.

Approximately what portion of your organization's applications are currently hosted in the public cloud?

(n=750)



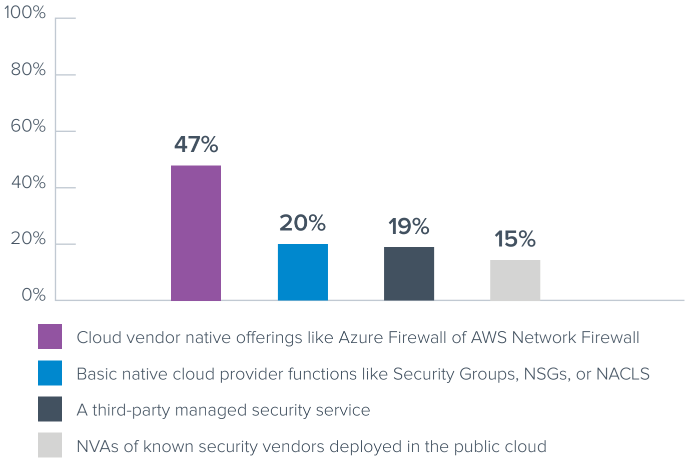
11% of respondents said they have all apps hosted in the public cloud, and another 45% said they have most apps hosted in the public cloud. Clearly, app deployment in the public cloud is significant.

Public cloud deployments drive the adoption of SD-WAN and Zero Trust Network Access (ZTNA), which makes sense because both technologies are designed to support cloud environments.

Almost three-quarters of companies with all apps in the public cloud have already deployed SD-WAN (73%), twice as many as companies with only a few apps in the public cloud (37%). Similarly, 68% of companies with all apps in the public cloud have deployed ZTNA, while just 38% of companies with only a few apps in the public cloud have deployed it. Organizations that are more dependent on the public cloud are more likely to have deployed an SD-WAN solution.

Which of the following does your organization predominantly use to handle security inside its public cloud environment?

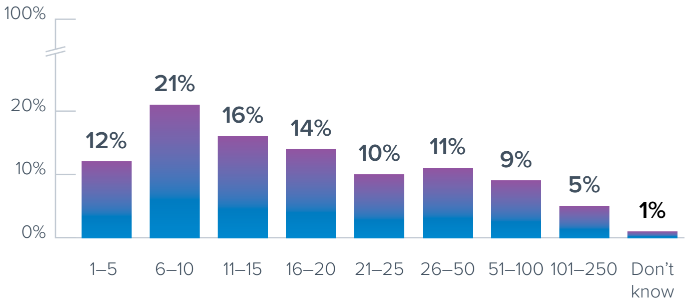
(n=750)



Nearly half of respondents (47%) use cloud-vendor native offerings, such as Azure Firewall or AWS Network Firewall. In addition, 20% use basic cloud offerings.

How many SaaS applications are officially used in your organization?

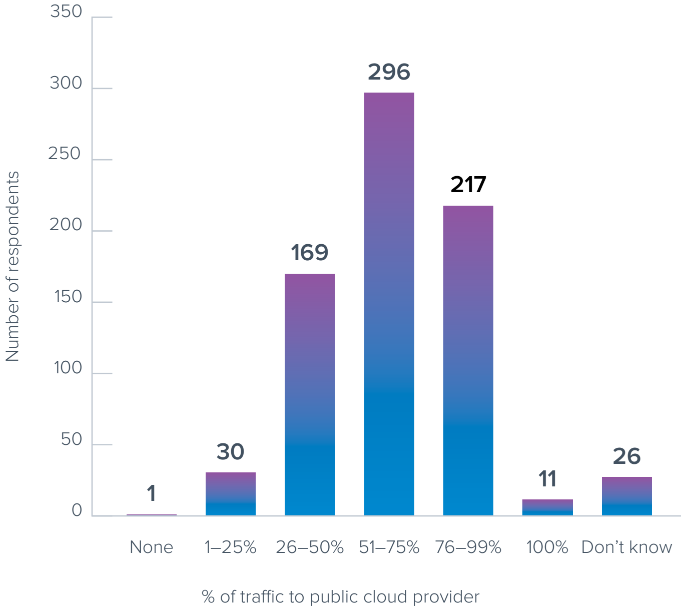
(n=750)



On average, organizations have 31 SaaS apps deployed. 12% have between one and five applications. 21%, the majority, have between six and 10 applications. 5% have more than 100 applications.

Besides officially used SaaS applications, what percentage of business-related traffic from your offices or remote endpoints do you estimate is directed to your public cloud providers (e.g., Azure, AWS) versus other offices or data centers?

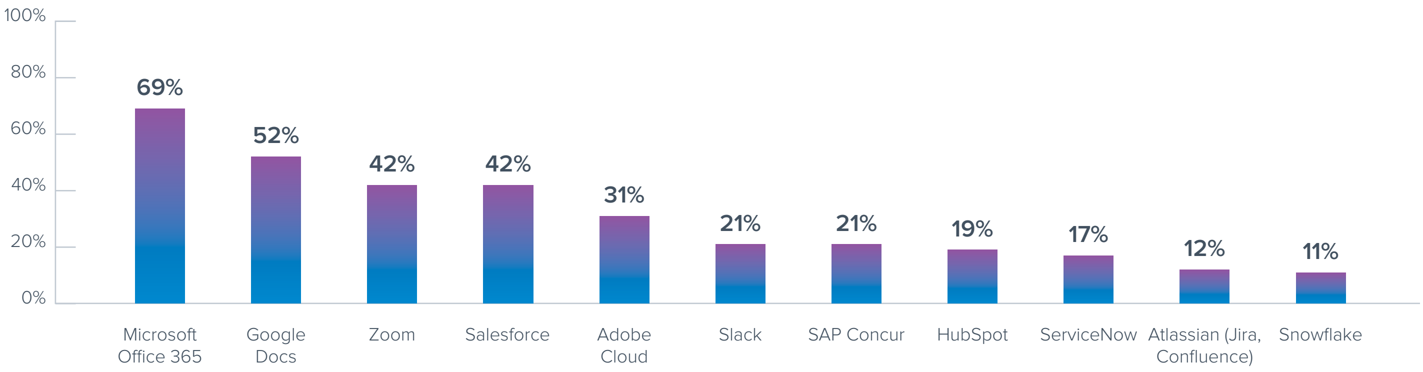
(n=750)



On average, respondents said 64% of their traffic is directed to public cloud providers. 39% said between half and three-quarters of business-related traffic is directed to their public cloud providers.

Which SaaS applications are used the most in your organization?

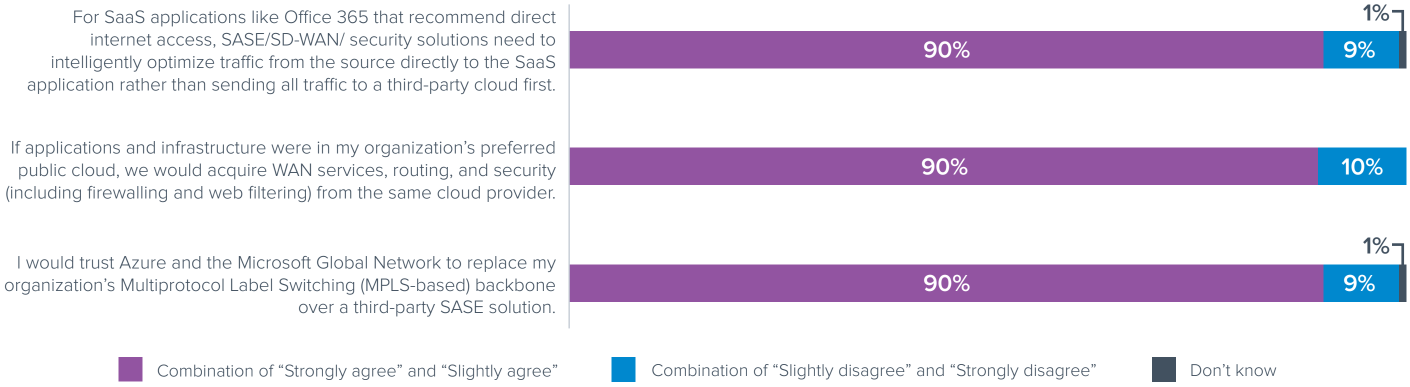
(n=749)



Office 365, Google Docs, Zoom, and Salesforce are the most used applications.

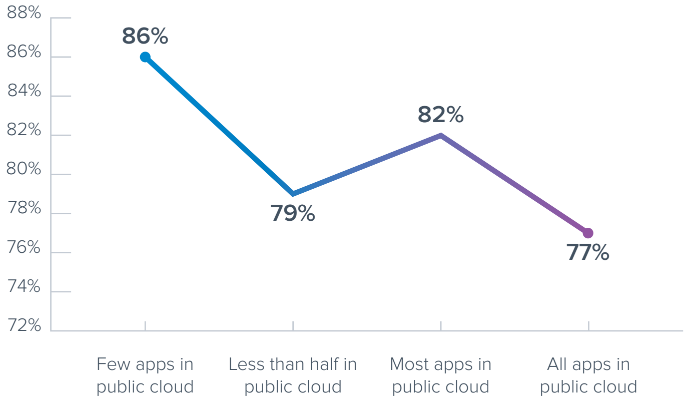
Do you agree or disagree with these statements?

(n=750)

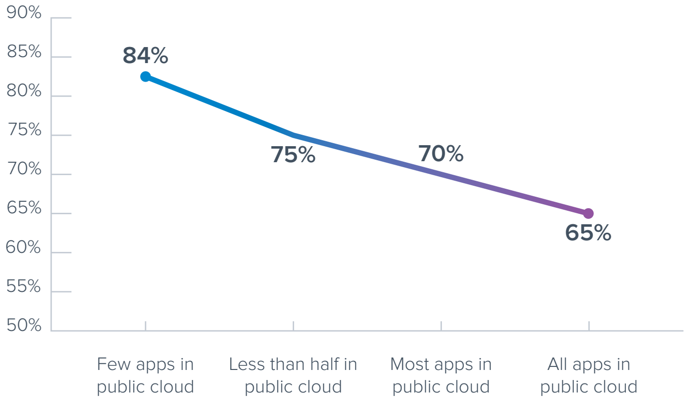


Respondents prefer to avoid third-party providers and solutions. A vast majority (90%) expect to directly access SaaS applications. The same number (90%) said if applications and infrastructure were in their organization's preferred public cloud, they would buy WAN services, routing, and security (including firewalls and web filtering) from the same cloud provider.

90% said they would trust Azure and the Microsoft Global Network to replace their organization's Multiprotocol Label Switching (MPLS) backbone over a third-party SASE solution. Organizations see the benefits of cloud-native and SaaS solutions and tend to trust public cloud providers with their network infrastructures.


Experienced a network breach once or more in the last 12 months

Cloud adoption also plays a role in breaches. The more organizations adopt the public cloud to host their applications, the less often they get breached.


Experienced a ransomware attack once or more in the last 12 months

Organizations with all applications hosted in the public cloud are less likely to have suffered from security breaches and ransomware attacks in the last 12 months.

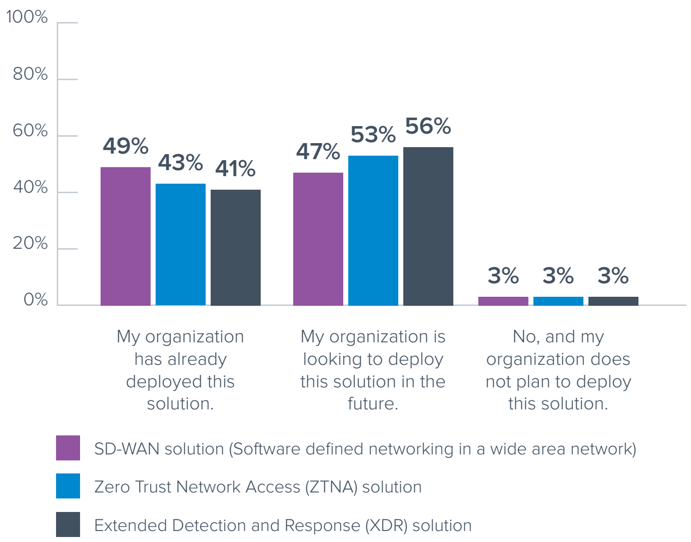
SASE: Zero Trust Network Access (ZTNA)

FINDING #4

Organizations are investing in Secure Access Service Edge (SASE) technologies.

Has your organization already, or does your organization plan to deploy any of the following solutions in the next two years or beyond?

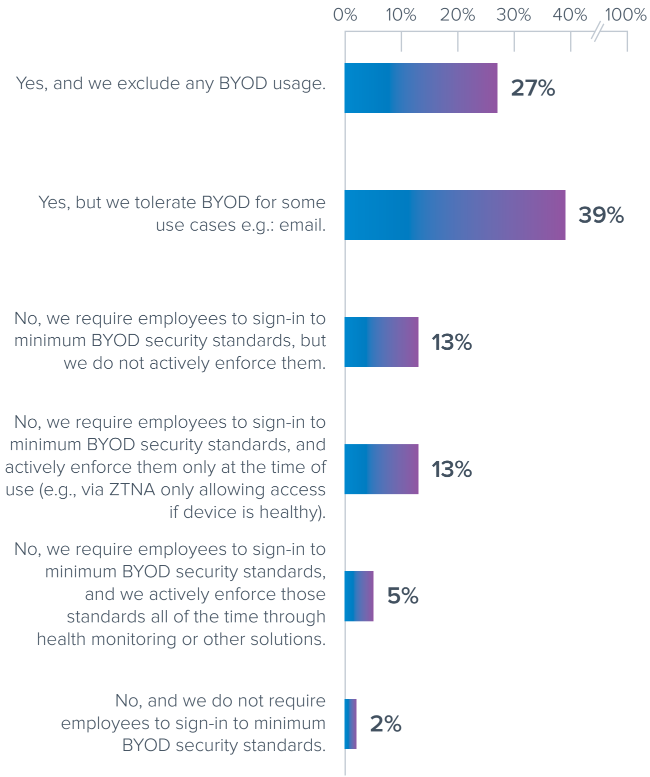
(n=750)



96% of respondent said they have already deployed (43%) or plan to deploy (53%) ZTNA in the future.

Does your organization require its employees to work from company-issued devices (rather than personal/BYOD devices)?

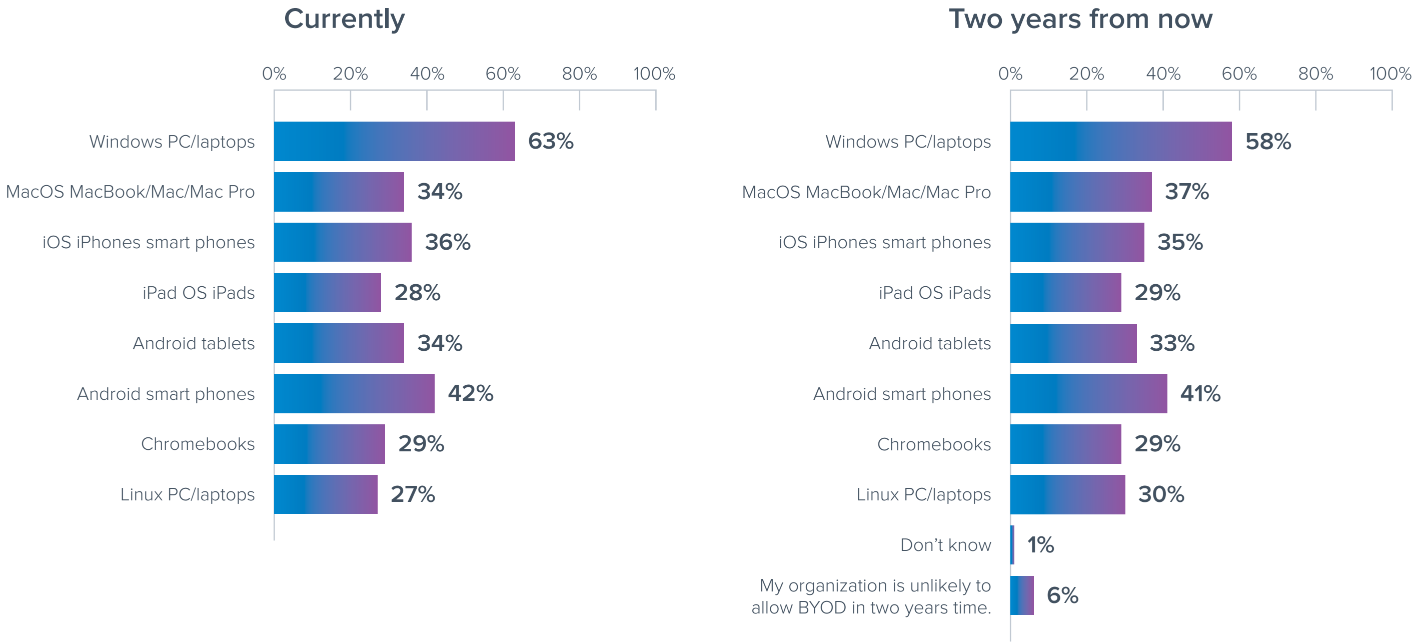
(n=750)



Nearly seven in 10 respondents (67%) said they must use company-issued devices, although 39% of those said Bring Your Own Device (BYOD) is allowed in some cases.

In your organization, for which of the following endpoint devices is BYOD currently allowed/will be allowed two years from now?

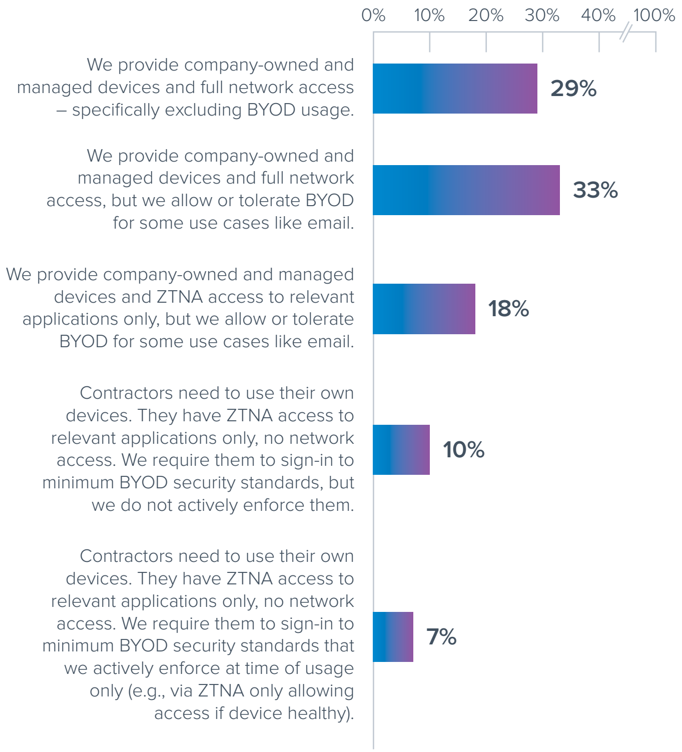
(n=543)



A wide range of devices are used by organizations for BYOD, including devices running Windows, MacOS, iOS, Android, Chromebook, and Linux. No significant changes are expected over the next 24 months. To support BYOD, ZTNA must be available for all device types and operating systems.

Which of the following statements best describes how your organization provides network/application access to full-time contractors?

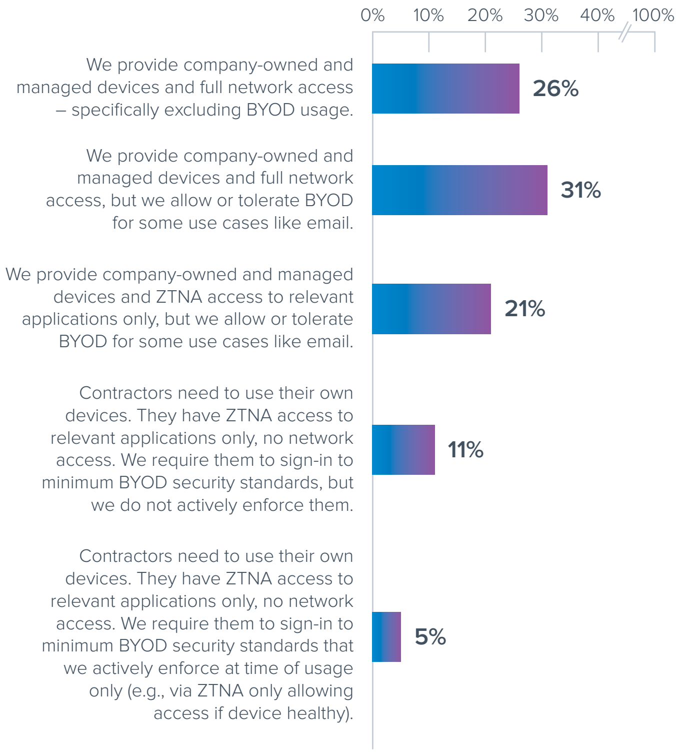
(n=750)



Just under two-thirds (60%) of respondents that have reported a successful ransomware attack issue company-owned devices to contractor's with full network access. In comparison, 20% of respondents who report a successful ransomware attack issue company-owned devices to contractors with ZTNA access.

How does your organization provide network/application access to temporary contractors?

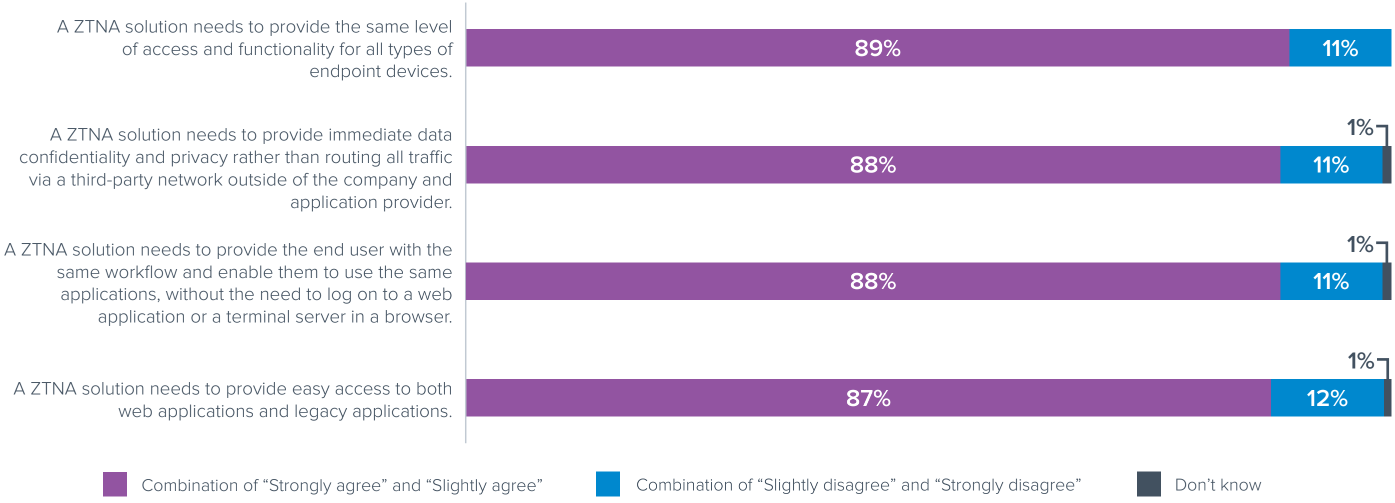
(n=750)



The majority of respondents (78%) surveyed give out company-owned devices for temporary contactors who require full network access. Varying numbers of organizations require ZTNA with BYOD for direct application access. 21% issue company-owned devices and require ZTNA access only.

Do you agree or disagree with these statements?

(n=750)



Nearly 90% of respondents expect a ZTNA solution to provide:

- easy access to web and legacy apps (87%)
- the same level of functionality for all endpoint devices (88%)
- support for existing workflows (88%)
- full data confidentiality (88%)

Respondents with Zero Trust Network Access (ZTNA) technology were significantly less affected by network security breaches compared to companies that haven't adopted ZTNA. For organizations that experienced a network security breach in the last year, 43% had ZTNA deployed and 57% did not.

Conclusion

Organizations are currently experiencing a high level of network breaches, and ever-increasing ransomware attacks are contributing to the security risks. This challenging situation is not surprising, given the pandemic-induced remote work environment and rapid technology transformation.

Work-from-home is here to stay, and IT departments will need to support a hybrid environment that enables work from home and from the office. Despite broadband connections and company-issued devices, remote workers continue to experience IT pains, such as slow applications, dropped calls, and poor video. User-experience issues and security challenges are related: Companies that work to resolve security issues tend to also improve their user experience.

Organizations are realizing that moving SaaS applications to the public cloud improves the user experience, and new technologies are available to support cloud presence and improve security. These Secure Access Service Edge (SASE) technologies include networking and security components. Along those lines, companies are investing in and plan to continue to aggressively invest in SD-WAN and Zero Trust Network Access. To take full advantage of SASE deployments, organizations are choosing cloud-native SASE solutions. There is growing evidence that these investments are going to help organizations better adapt to the new work environment.

> Despite broadband connections and company-issued devices, remote workers continue to experience IT pains, such as slow applications, dropped calls, and poor video. User-experience issues and security challenges are related: Companies that work to resolve security issues tend to also improve their user experience.

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-enabled, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organizations worldwide trust Barracuda to protect them—in ways they may not even know they are at risk—so they can focus on taking their business to the next level.

Get more information at barracuda.com.

Barracuda®

Your journey, secured.

THE STATE OF NETWORK SECURITY IN 2021 • US 1.0 • Copyright 2021 Barracuda Networks, Inc. • barracuda.com