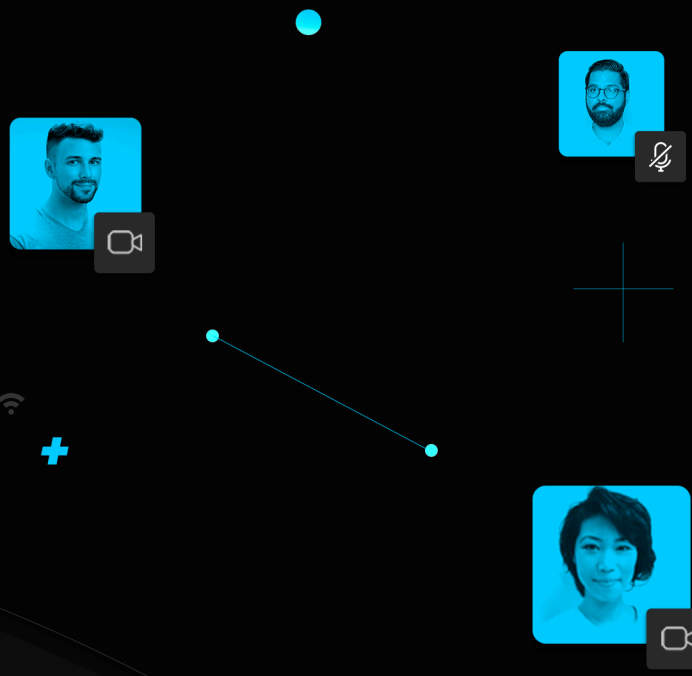


Electric

THE STATE OF REMOTE WORK REPORT

A Whitepaper by Electric

Executive Summary

More people than ever are now working from home to comply with stay-at-home orders and social distance due to the COVID-19 pandemic. This massive shift has forced many organizations to determine that it's still possible to enable workers to remain productive while not in a physical office. However, special considerations should be made to secure both your company and customer's sensitive information.

This new way of work with a greater emphasis on remote has surfaced the notion that the actual endpoints, meaning the mobile devices and computers that remote workers use to access company information are critical to maintaining such security. However, we found that a majority of IT decision makers have yet to implement key security measures for their remote workforce like virtual private networks (VPN), multi-factor authentication (MFA), and mobile device management (MDM).

Endpoints being used in less-controlled networking environments like employee homes has introduced its own set of concerns. To keep business running smoothly, organizations must be prepared to enable their workforce to conduct work from these less-controlled network environments in a productive and secure manner.

We wanted to conduct this study to help organizations benchmark how they are adapting to this unprecedented shift compared to others. This whitepaper will present our findings from surveying a group of IT decision makers in the United States at small and medium-sized businesses with 1-500 employees on their respective organization's shift to remote work.

Findings at a Glance:

People: The shift to how many individuals at respondent organizations are working remotely.

250%
increase in respondents saying more than three-quarters of their organization's full-time employees are now working remotely than prior to March 2020.

Tools: How companies are communicating, specifically what chat and video tools are enabling collaboration.

Chat Applications:

18.62%
of respondents use Slack

50.34%
of respondents use Microsoft Teams

42.07%
of respondents use Skype for Business

Video Conferencing Applications:

57.24%
of respondents use Zoom

29.66%
of respondents use Google Hangouts

41.28%
of respondents use Skype

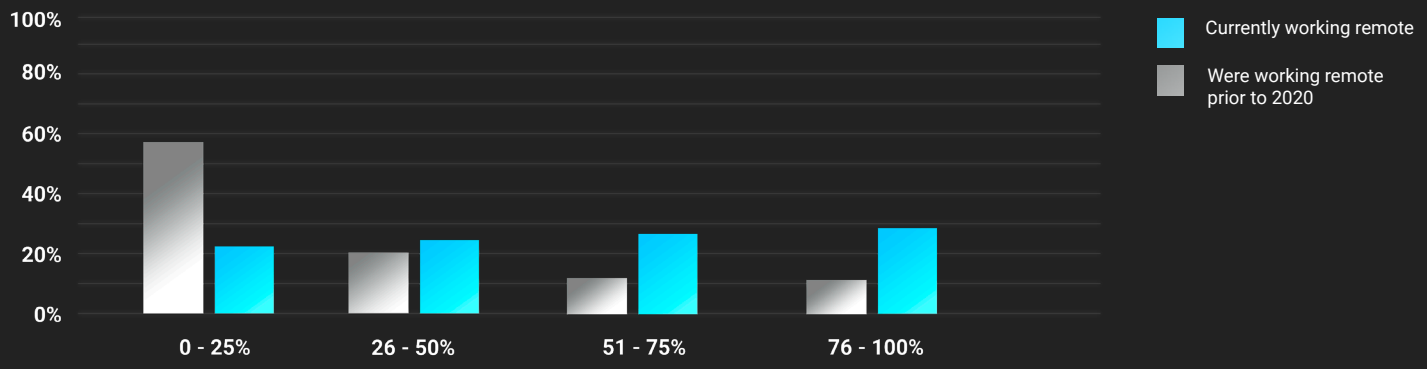
**Please note, respondents were able to choose more than one option for the above questions.*

Remote security measures: What organizations are currently doing to secure endpoints and protect their sensitive data.

- Only **48.28%** of respondents indicated that MFA (Multi-Factor Authentication) was enabled company-wide on email and other mission critical applications.
- Only **19.31%** of Respondents indicated that nearly all (75-100%) of the individuals at their organization access the network through a Virtual Private Network (VPN).
- Only **13.79%** of respondents indicated that nearly all (75-100%) of their company issued devices had a Mobile Device Management solution installed.

An Accelerated Shift to Remote Work

Percent of Respondent Organization's Full-Time Employees Working Remotely Prior to March 2020 vs. Now



- A **250%** increase in respondents saying more than three-quarters of their organization's full-time employees are now working remotely.
- A **223%** increase in respondents saying between half to three-quarters of their organization's full-time employees are now working remotely.
- A **116%** increase in respondents saying a quarter to half of their organization's full-time employees are now working remotely.
- A **39%** decrease in respondents saying zero to a quarter of their organization's full-time employees are now working remotely.

The results above compare two questions, one asking how many full-time employees are working remotely now and comparing it to how many worked remotely prior to March 2020 before the virus arrived in the U.S.

Results indicate that many more individuals at respondent organizations are working remotely now than prior to stay-at-home orders being issued. While it may have been expected that respondents would indicate an even bigger shift to their organization's full-time employees being remote, it's important to note that respondents could be IT decision-makers in industries that either were forced to have employees not work at all like retail and entertainment, or they work in industries that continued to have employees attend the respective place of work like healthcare.

Regardless of industry, it's clear that the COVID-19 pandemic has accelerated a shift to remote work and introduced a new normal for many. The new normal will involve employees working more frequently from these less-controlled networking environments like homes, and as parts of the country reopen, potentially third spaces like cafes and libraries once again.

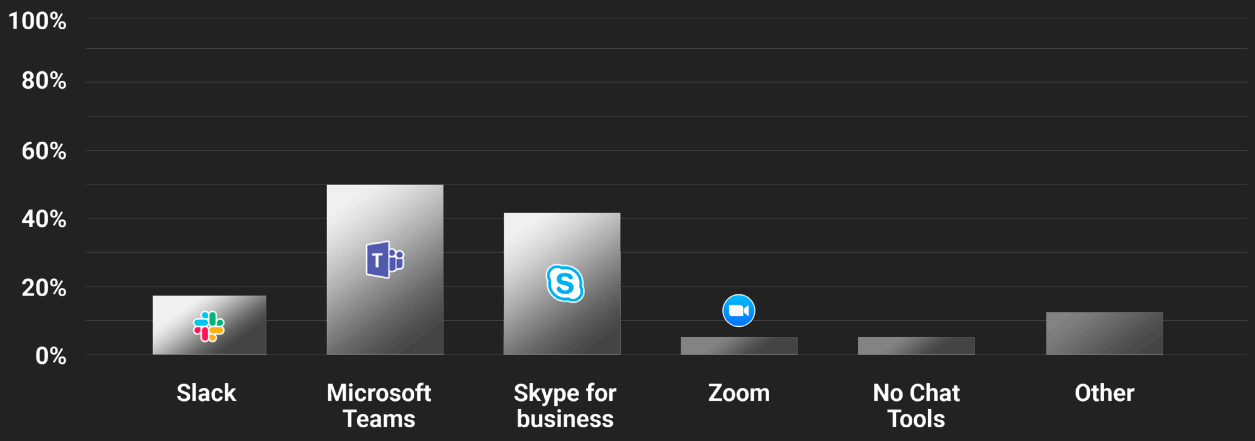
Instead of huddling into conference rooms for meetings we now virtually log into teleconferencing applications and instead of popping over to a colleagues desk to ask a question we now interface via chat tools like Slack and Microsoft Teams.

How Companies Are Collaborating Remotely

Benchmarketing Chat & Video Tools

Chat Tools

What Chat Tools Does Your Organization Use to Collaborate Remotely?



We found that respondent organizations use the following chat tools:

18.62% use Slack

6.90% use Zoom

50.34% use Microsoft Teams

6.90% use no chat tools

42.07% use Skype for Business

12.41% use another platform

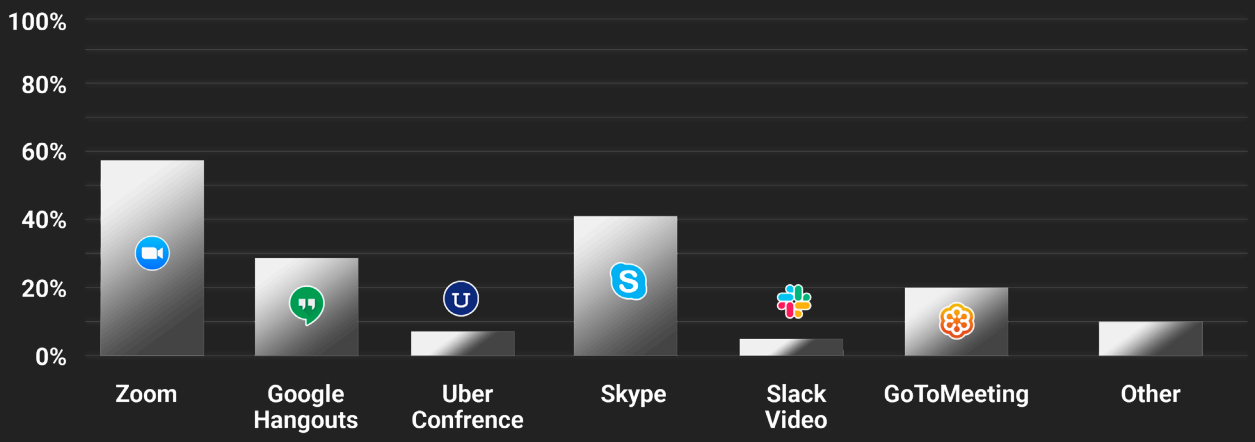
**Please note, respondents were able to choose more than one option for the above questions.*

Making up for the loss of in-person contact means that there's a big emphasis on using chat platforms like the ones mentioned above to keep teams connected. Most organizations will have probably already been using one, but it's important to ensure that your organization sets expectations on response time and etiquette between colleagues.

Team chat applications can help remote employees feel more connected to their teammates, combining the best aspects of online forums and instant messaging into one service. Used properly they can improve communication, streamline workflow, and keep employees better engaged.

Video Conferencing Tools

What Video Conferencing Tools Does Your Organization Use?



We found that respondent organizations use the following video conferencing tools:

57.24% use Zoom

41.28% use Skpe

29.66% use Google Hangouts

6.21% use Slack

8.28% use UberConfrence

20% use GoToMeeting

**Please note, respondents were able to choose more than one option for the above questions.*

Effective communication is essential for the success of any organization and online video conferencing platforms are helping people communicate as many are forced to work remotely.

Our survey indicates Zoom as the most common among respondents. Some credit the rise in the popularity of Zoom above other video conferencing platforms as due to the platform's ease of access and careful work to keep latency below 150 milliseconds (the maximum before conversations start to feel unnatural).

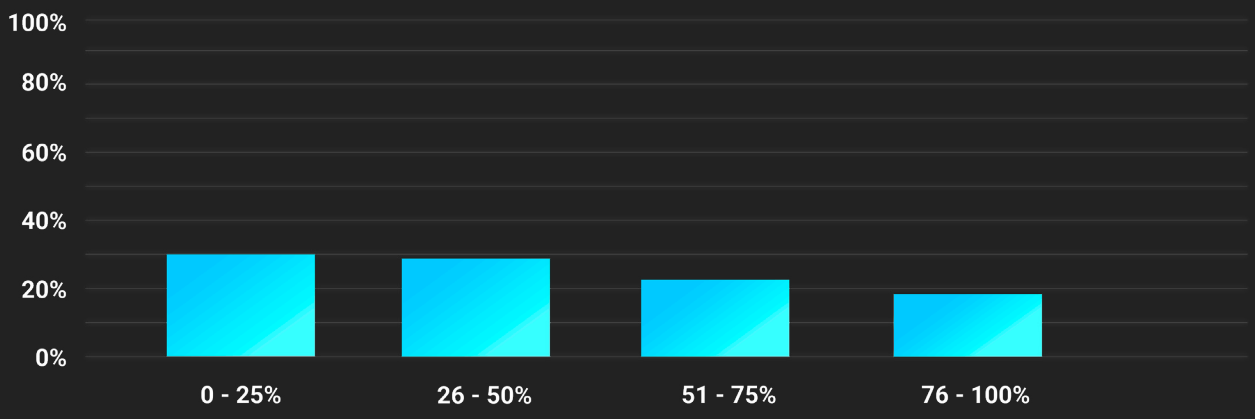
The numbers don't lie—individuals are using this online video calling resource more than any other. According to **Reuters**, Zoom's average user numbers in March were nearly three times that of its nearest rival. Further, **Zoom said** daily users spiked to 200 million in March, up from 10 million in December of last year.

Regardless of which platform your company uses, it is important that your organization sets remote meeting guidelines as using the remote meeting format can be frustrating to employees who are accustomed to talking in person, over email, or over the phone when previously needing to address business concerns.

How Organizations Are Securing Endpoints & Protecting Sensitive Data

Virtual Private Networks

How Many Individuals at Your Organization Access Your Network Through VPN?



- Only **19.31%** of respondents indicated that nearly all (75-100%) of the individuals at their organization access the network through a Virtual Private Network (VPN).
- 29.66% of respondents indicated that up to a quarter (0-25%) of the individuals at their organization access the network through a VPN.
- 28.97% of respondents indicated a quarter to half (26-50%) of the individuals at their organization access the network through a VPN.
- 22.07% of respondents indicated half to three-quarters (51-75%) of the individuals at their organization access the network through a VPN.

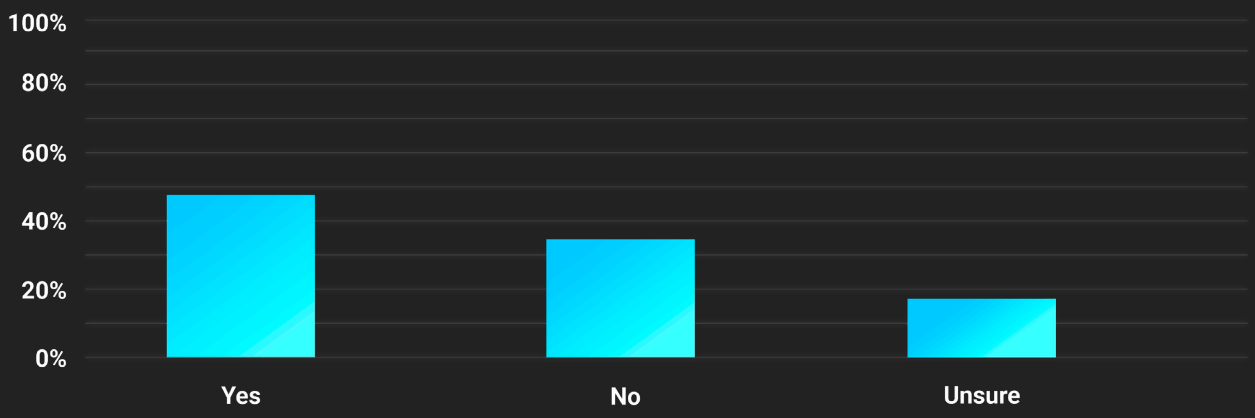
Virtual private networks (VPNs) ensure a secure connection between a device and the company network. Depending on the type of information an employee has access to, it's important to consider the use of a VPN for all remote employees. Due to discrepancies in security between home networks and those found in an office setting, VPNs are one way to ensure sensitive data remains secure.

The most important thing is to avoid public wifi. As parts of the country start to reopen, if your employees must use public or hotel wifi, the use of a VPN is strongly recommended to protect and encrypt the connection. For extra measures, you should also warn your employees never to partake in sensitive personal activities such as banking over public wifi, in order to avoid their own identity theft.

How Organizations Are Securing Endpoints & Protecting Sensitive Data

**** Multi-Factor Authentication

Is MFA (Multi-Factor Authentication)/2FA (2-Factor Authentication) Enabled Company-Wide on Email and Other Mission Critical Apps?



- Only **48.28%** of respondents indicated that MFA (Multi-Factor Authentication) was enabled company-wide on email and other mission critical applications.
- 35.17% of respondents indicated that MFA was not enabled on company-wide email and other mission critical applications.
- 16.55% of respondents indicated that they were unsure that MFA was enabled on company-wide email and other mission critical applications.

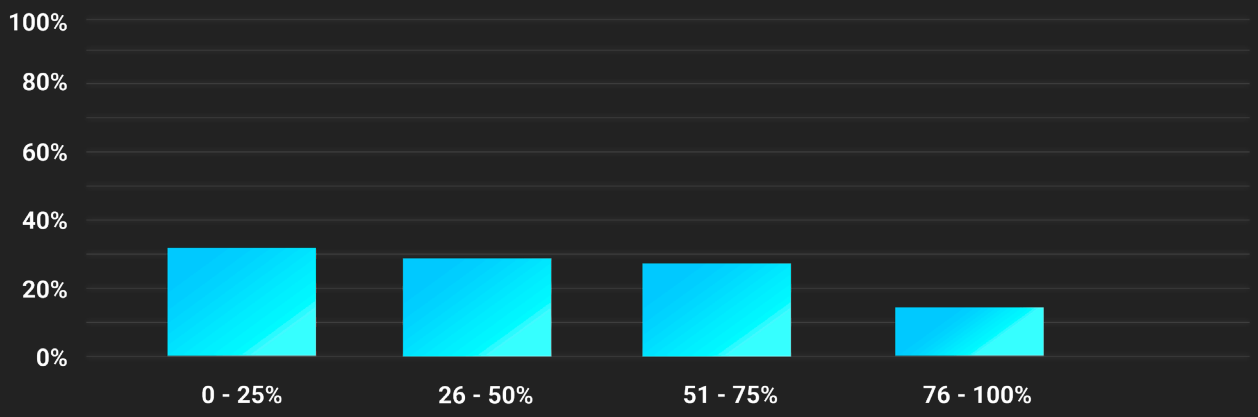
As a policy, multi-factor authentication should always be used so it is harder for somebody to access the company network from a stolen device. This is having a secondary form of authentication, usually a multi-digit code sent to a separate mobile device—for when employees sign in into applications with critical information.

By utilizing additional layers of authentication, even if your employee has their company device stolen, someone won't be able to log into any important online accounts that store your sensitive company data.

How Organizations Are Securing Endpoints & Protecting Sensitive Data

Mobile Device Management

On How Many of Your Company-Issued Devices Do You Have a Mobile Device Management (MDM) Solution Installed?



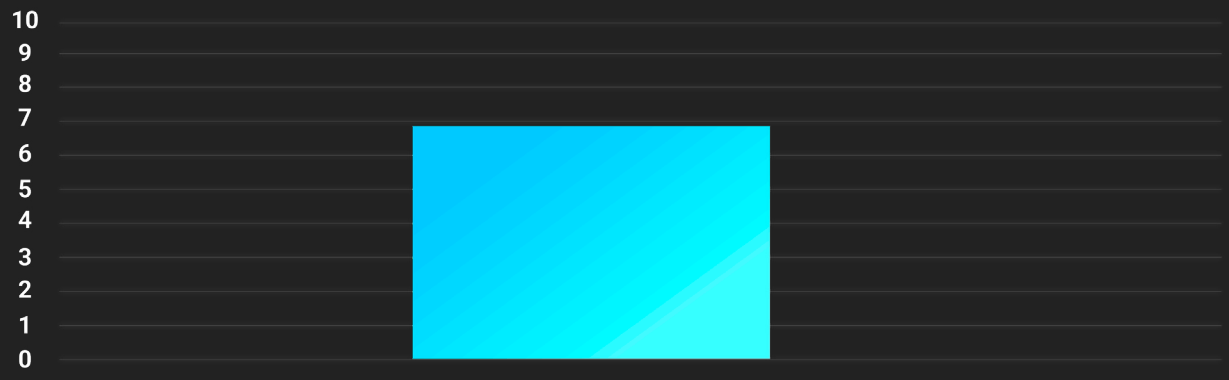
- Only **13.79%** of respondents indicated that nearly all (75-100%) of their company issued devices had a Mobile Device Management solution installed.
- 31.03% of respondents indicated that up to a quarter (0-25%) of their company-issued devices had an MDM solution installed.
- 28.28% of respondents indicated a quarter to half (26-50%) of their company-issued devices had an MDM solution installed.
- 26.90% of respondents indicated half to three-quarters (51-75%) of their company-issued devices had an MDM solution installed.

MDM allows for IT teams to push updates and patches to devices remotely at scale with ease and should be a staple in this new normal of accelerated remote work. Enabling an MDM solution on all company and approved devices will allow your organization to have better insight into your endpoint security. This is essential for tracking inventory and rolling out security policies in bulk if need be. Look at it this way— for most organizations the cost of lost data is far greater than the cost of a lost device. It's for this reason incorporating an MDM solution to manage, monitor, and secure mobile devices for official use is vital.

So what happens if a device is lost or stolen? Make sure employees know that their devices can actually be remotely wiped if stolen so they can make sure to back up their data if not using cloud storage.

Accessing Confidence in Current Security Measures

How Confident Are You In The Cybersecurity Measures Your Organization Has in Place as it Relates to Working Remotely (1 being the least confident, 10 being the most confident)?



Respondents indicated an average confidence of **7 out 10** in the security of their organization despite not an overwhelming majority having implemented the three measures mentioned above—Virtual Private Networks, Multi-Factor Authentication, and Mobile Device Management.

The measures above are not a foolproof solution by any means but are the basics your organization must consider in light of the new nature of work impacting many organizations. Now more than ever, it's important for IT decision makers to ensure workers have access to an environment that fosters near-seamless production of work free from technical disruption while still reducing business risk.

Conclusion

The COVID-19-accelerated shift to remote work has forced organizations to think about preparing their employees to work in a different way at a scale that was unheard of prior to the pandemic. With companies like **Twitter** already announcing that employees will have the option to work from home forever, it's clear that remote work is going to continue to be a larger and larger fixture of modern business.

The notion of the home office being an extension of your company needs to sink in now, not just for IT decision makers, but also for business leaders at all levels.

The office of the future has arrived early. Excellence in the "new" office now starts with leveraging IT as an enabling-function for the entire organization. It starts with rethinking IT and the definition of "office" from the ground up in support of a more remote workforce.