Check Point®
SOFTWARE TECHNOLOGIES LTD.

THE 2022

# WORKFORCE SECURITY REPORT

# INTRODUCTION

Nearly two years into pandemic life, it seems that things are (very) slowly going back to normal. However, some aspects are here to stay, one of them being the way we work. Whether it is a hybrid work model or a completely remote one, WFH is clearly not a passing trend for organizations. This new normal begs the questions **– how are organizations protecting their ever-growing attack surface? How are they keeping their remote workforce secure?**

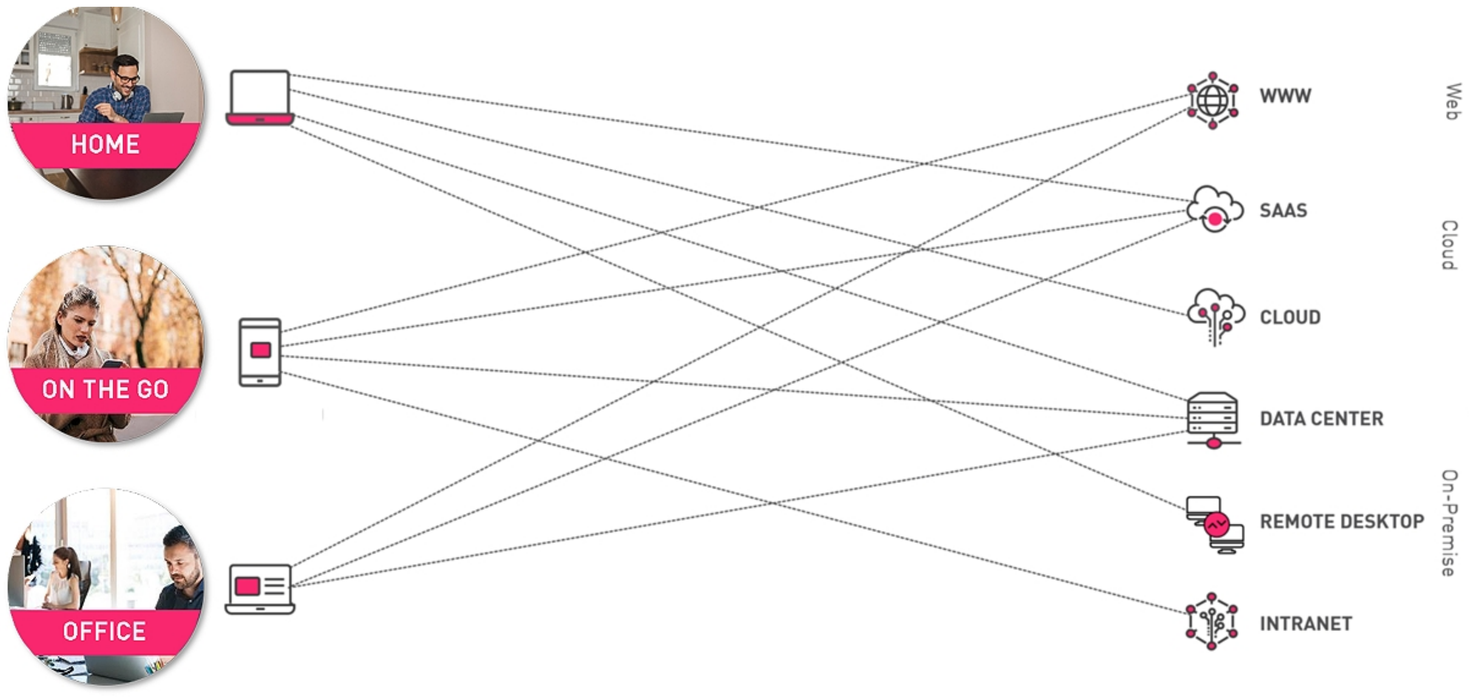
In the past months we have collected (anonymous) answers from 1200 security professionals about the way they work and how they secure their remote employees, through our 5-Minute Remote Workforce Security Assessment. In this report we will share the key insights into how organizations secure remote access to corporate apps and assets, file sharing, data leakage and mobile devices, as well as the state of cloud email & collaboration apps adoption and vendor consolidation. We hope that this report will help to paint the picture of the state of remote workforce security, and how to improve it.

REMOTE WORK IS HERE TO STAY

# 57% REPORT THAT MORE THAN HALF OF THEIR WORKFORCE WORKS REMOTELY AT LEAST 2 DAYS A WEEK

Remote work has introduced many benefits, from saving time on commute to higher productivity and enabling better work-life balance. However, it also introduced more challenges to an already challenging cyber threat landscape.

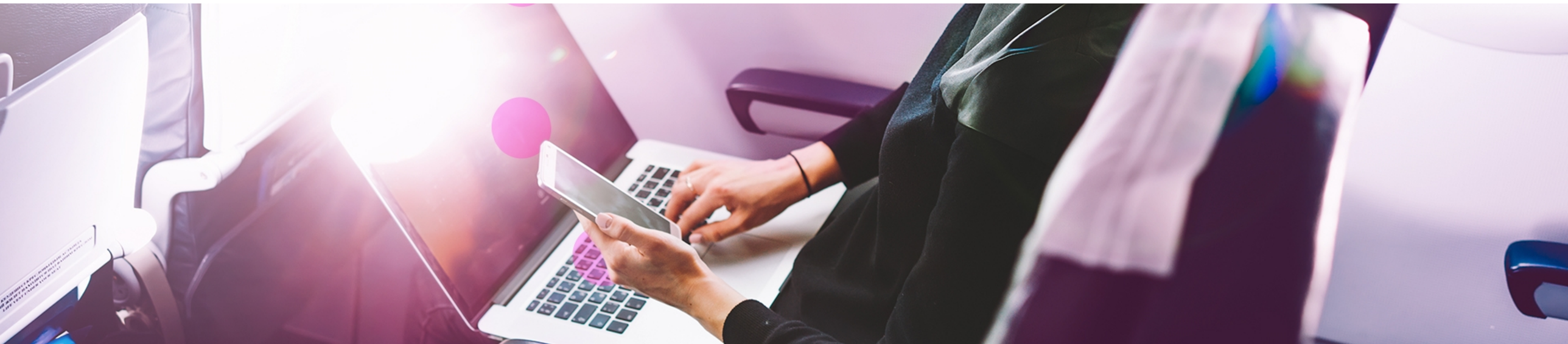
In today's world being productive requires us to always be connected, everywhere, no matter where we are, or what device we are using, and no matter which application we need to access. The result is that sensitive business data is continually flowing from both corporate and BYOD devices to cloud, IaaS, and datacenters, expanding the attack surface wider than ever.



REMOTE CORPORATE ACCESS

# 70% REPORT THAT THEY ALLOW ACCESS TO CORPORATE ASSETS FROM PERSONAL LAPTOPS AND MOBILES

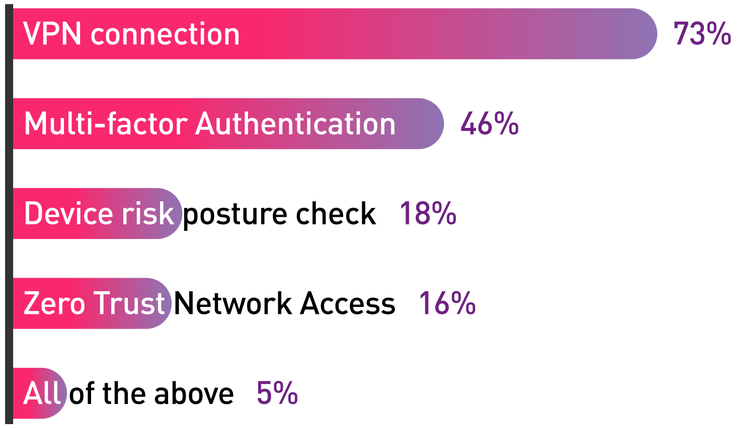
Organizations must allow employees to remotely access corporate apps and data in order to perform their job. 94% of organizations allow remote access to corporate apps and assets from unmanaged and managed devices, while 17% reported they allow remote access only from company-managed laptops.

From those who reported they allow access to corporate apps remotely, 11% mentioned they don't utilize any of the methods listed to secure remote access to corporate applications.

32% mentioned they use VPN alone, while 24% use both VPN and Multi-factor authentication. Only 5% reported they use all of the above mentioned methods, while 10% reported they use three, 28% use two, and 46% use only one method, the majority of which is VPN.

**How do you secure remote access to corporate applications?**

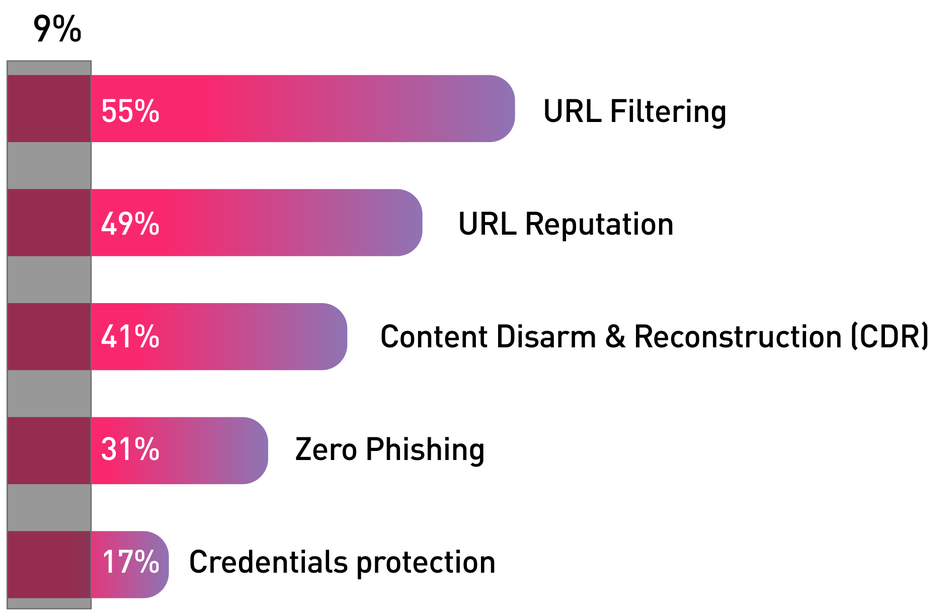



INTERNET ACCESS SECURITY

# ONLY 9% OF ORGANIZATIONS USE ALL THE 5 MUST-HAVE PROTECTIONS AGAINST INTERNET-BASED ATTACKS

The internet has never been more dangerous. In 2021, over 10,000 new malicious files and 100,000 new malicious websites were discovered by Check Point Research every single day. With that in mind, it is surprising that a whopping 20% of respondents reported that they don't use any of the methods mentioned to protect remote users while browsing the internet, and only 9% use all the methods mentioned to protect against internet-based attacks.

**How do you protect remote users while they are browsing the internet?**

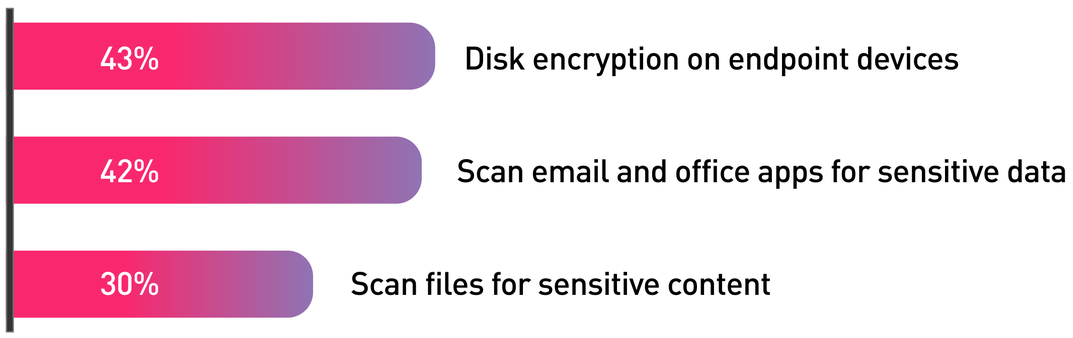


DATA PROTECTION

# 31% DON'T USE ANY OF THE MENTIONED METHODS TO PREVENT SENSITIVE BUSINESS DATA FROM LEAKING OUTSIDE THE ORGANIZATION

Data leakage presents a huge risk to organizations. Employees can unintentionally or sometimes intentionally leak sensitive data to outside the organization. This can result in fines for non-compliance with regulations, losing a competitive advantage due to intellectual property being breached, and even damage to brand equity. This is where automated data protection comes into play.

**How do you prevent sensitive business data from leaking outside the corporate network?**



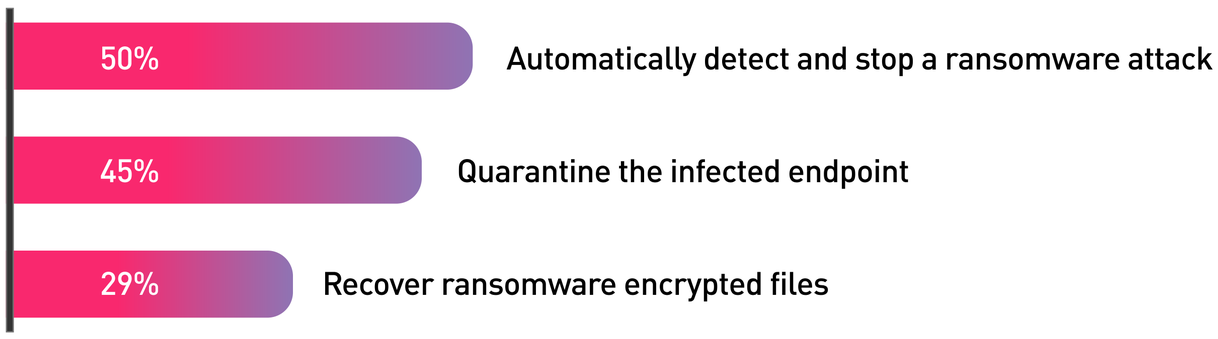

When respondents were asked how they prevent sensitive business data from leaking, **31% reported that they don't use any of the mentioned methods.**

ENDPOINT PROTECTION AGAINST RANSOMWARE

# 26% DON'T HAVE AN ENDPOINT SOLUTION THAT CAN AUTOMATICALLY DETECT AND STOP RANSOMWARE ATTACKS, QUARANTINE THE INFECTED ENDPOINT, AND RECOVER RANSOMWARE-ENCRYPTED FILES

Protecting the endpoint has never been more challenging. The complexity and unpredictability of attacks and threats are continually on the rise. One of the most prominent of which is ransomware. In fact, in 2021 ransomware attacks increased by 93% year over year. With that, it's important that organization's endpoint security solution has strong anti-ransomware capabilities. In our survey, when asked the 1200 security professionals what their endpoint security can do in case of a ransomware attack, only 16% reported it can do all of the mentioned capabilities, and 26% reported their endpoint security solution can't do any of the mentioned capabilities.

**In the case of a ransomware attack, my organization's endpoint protection can:**



EMAIL & COLLABORATION APPS

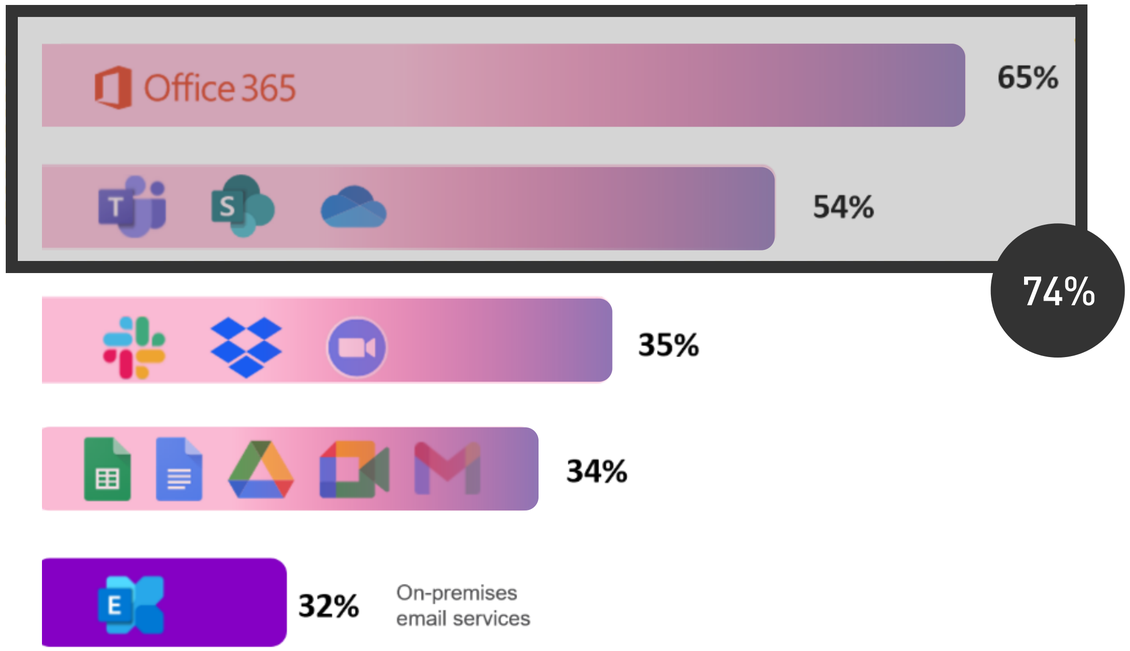
# 74% USE OFFICE 365 EMAIL AND COLLABORATION APPS LIKE TEAMS, SHAREPOINT, AND ONEDRIVE

In the past years, email technologies have evolved and transitioned from on-premises solutions to cloud-based solutions.

Adding to that, our survey results show that the COVID-19 pandemic and the shift to remote work have dramatically accelerated the adoption of cloud email and other collaboration apps beyond email.

In fact, 74% use Office365 email and collaboration apps like Teams, SharePoint, and OneDrive. On the flip side, only 32% report using on-premises email services like Microsoft Exchange.

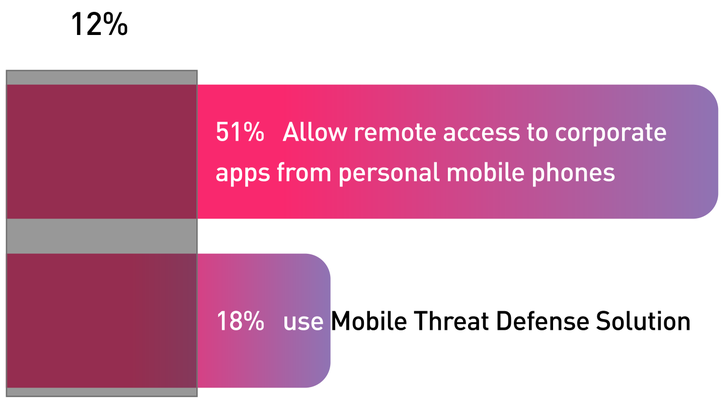
**What applications your company's employees use for corporate email and collaboration?**



MOBILE SECURITY

# ONLY 12% OF ORGANIZATIONS THAT ALLOW CORPORATE ACCESS FROM MOBILE DEVICES USE A MOBILE THREAT DEFENSE SOLUTION

These days, remote employees are accessing corporate data from mobile devices more than ever. Employees often access corporate apps, send emails and share corporate files over public Wi-Fi networks that are easy to compromise. Over the past year, researchers at Check Point have been observing a rise in the number of mobile-related attacks. In 2020 alone, 97% of organizations faced mobile threats, and 46% of organizations had at least one employee download a malicious mobile application. With that, it is worrying that only 12% of respondents that allow corporate access from mobile devices use a Mobile Threat Defense solution to protect their corporate assets and users.



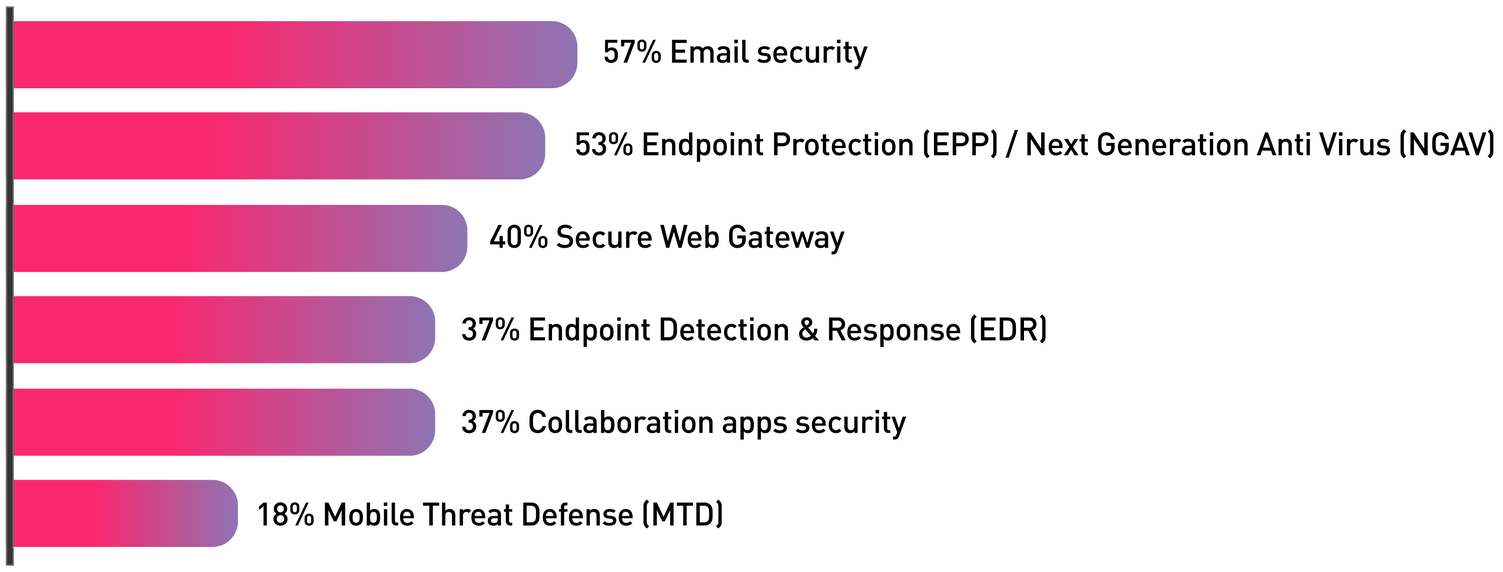



REMOTE WORKFORCE SECURITY & CONSOLIDATION

# NEARLY HALF OF RESPONDENTS REPORT USING 4 OR MORE VENDORS TO SECURE THEIR REMOTE WORKFORCE

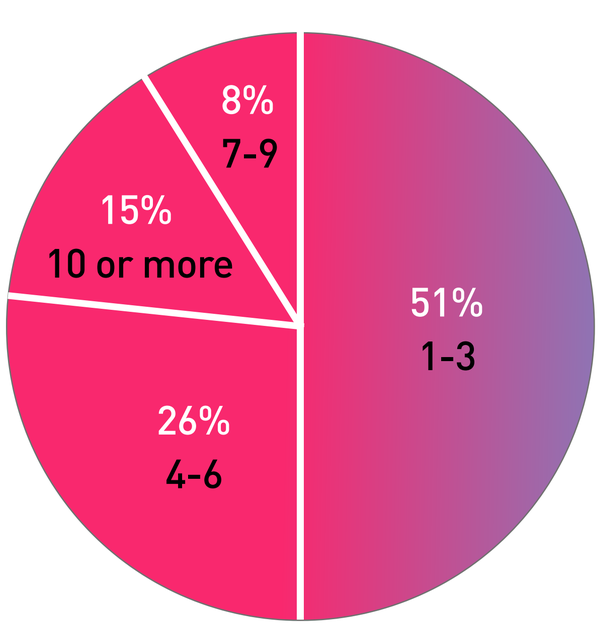
In this new WFH world, staying productive means staying connected. You must be able to work anywhere, with your mobile phone or laptop, and access any application. This expands organization's attack surface to increasingly sophisticated cyber-attacks. When it comes to organization's security strategy, 91% of respondents report they use one or more of the security solutions mentioned.

**Which of the following security solutions are being used in your company?**



When referring to consolidation of security solutions, nearly half of respondents report they use 4 or more vendors to secure their remote workforce.

**How many security vendors do you use to secure remote internet access, corporate access, email, endpoint and mobile devices?**






# IN SUMMARY

By now, organizations have fully adopted remote work as a way of life. However, it seems that when it comes to securing remote users and access, there is still a gap that needs to be bridged in order to balance between remote users' productivity and ensuring the security of their devices, access and corporate assets. Check Point Harmony is the industry's first unified security solution for users, devices, and access. The solution provides organizations with the most comprehensive and robust workforce security, by consolidating 5 security products to provide complete protection for remote users - all in a single solution that is easy to use, manage and buy.

Harmony offers an alternative that reduces the overhead and complexity of using multiple solutions from multiple vendors. The solution is easy to manage, providing a unified and intuitive cloud-based management, and enabling user-centric security policies to be applied across the organizations' environments. Lastly, Harmony is easy to buy with a simple and all-inclusive per-user subscription pricing model. Learn more about Harmony here.