State of Enterprise

MAC SECURITY

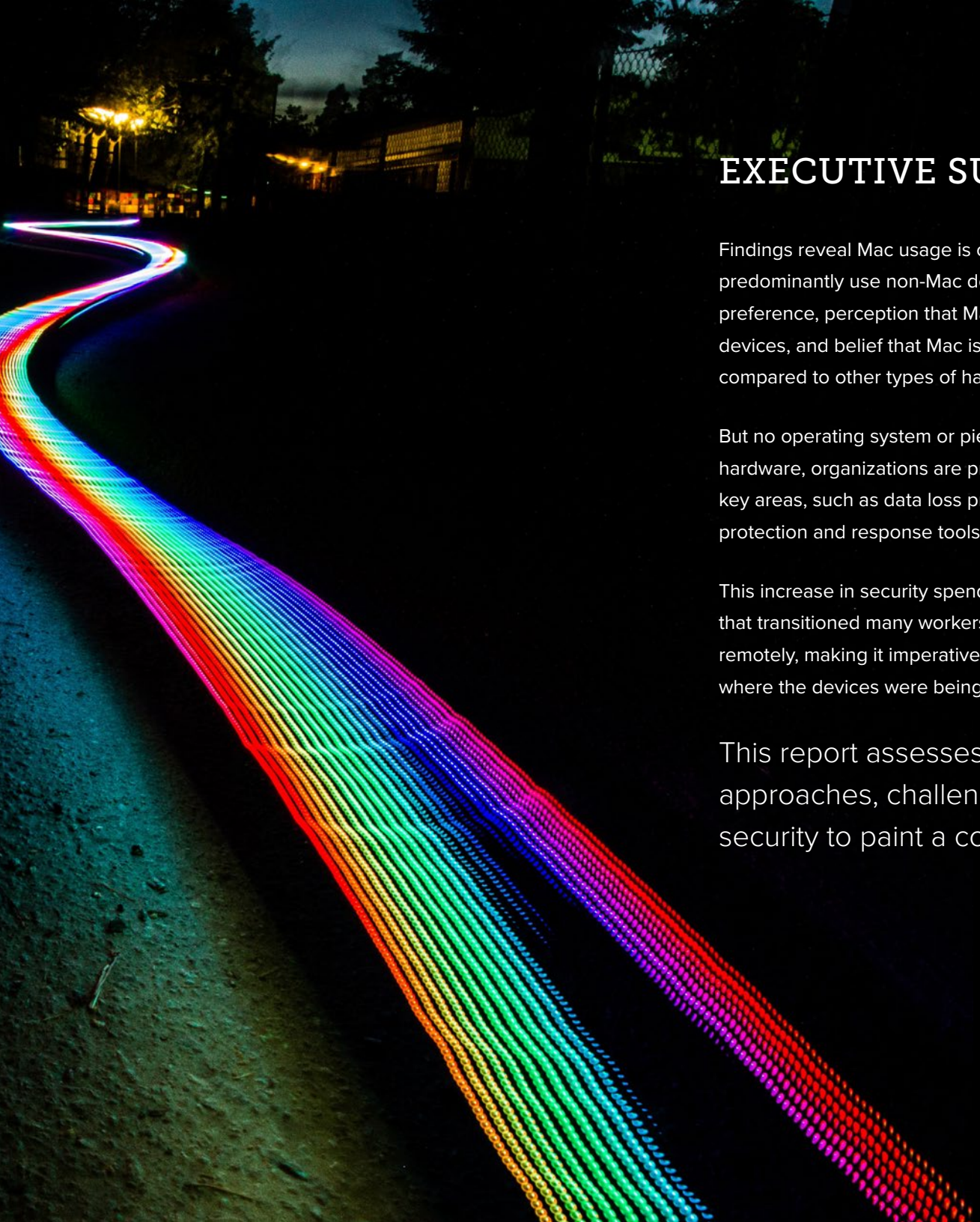
jamf

INTRODUCTION

Offering employees top-of-the-line technology is the foundation for building a thriving enterprise — and it's truer today than ever before. Since the onset of COVID-19, we have seen shifts worldwide from on-site offices, devices and networks to remote work and workforces. This shift has propelled security to the forefront as modern ways of protecting work-anywhere employees are paramount to organizational success.

But how do organizations assess their current security state to know where they stand on the spectrum? And what factors go into selecting hardware and software to not only maintain security compliance, but also protect the end-user experience?

To evaluate Mac security within the enterprise to answer these questions and more, Jamf commissioned Vanson Bourne, a third-party market research firm, to survey 1,500 IT and InfoSec (Information Security) professionals across North America and Europe.



EXECUTIVE SUMMARY

Findings reveal Mac usage is on the rise, even among organizations who predominantly use non-Mac devices. Leading factors include IT and InfoSec preference, perception that Mac is more secure out of the box than non-Mac devices, and belief that Mac is easier to maintain complete security over compared to other types of hardware.

But no operating system or piece of hardware is perfect. Regardless of hardware, organizations are prioritizing future security spending in several key areas, such as data loss prevention, anti-virus software, and endpoint protection and response tools.

This increase in security spending is a reflection of the COVID-19 pandemic that transitioned many workers from on-site office locations to working remotely, making it imperative that endpoints remained secure no matter where the devices were being used or resources accessed.

This report assesses current device usage and approaches, challenges and future state of endpoint security to paint a complete enterprise picture.

DEMOGRAPHICS

To gain a global perspective, we surveyed IT and InfoSec individuals from companies across North America and Europe, ranging from small to large enterprises. Of the 1500 respondents, there was an even split of primarily Mac and non-Mac environments.

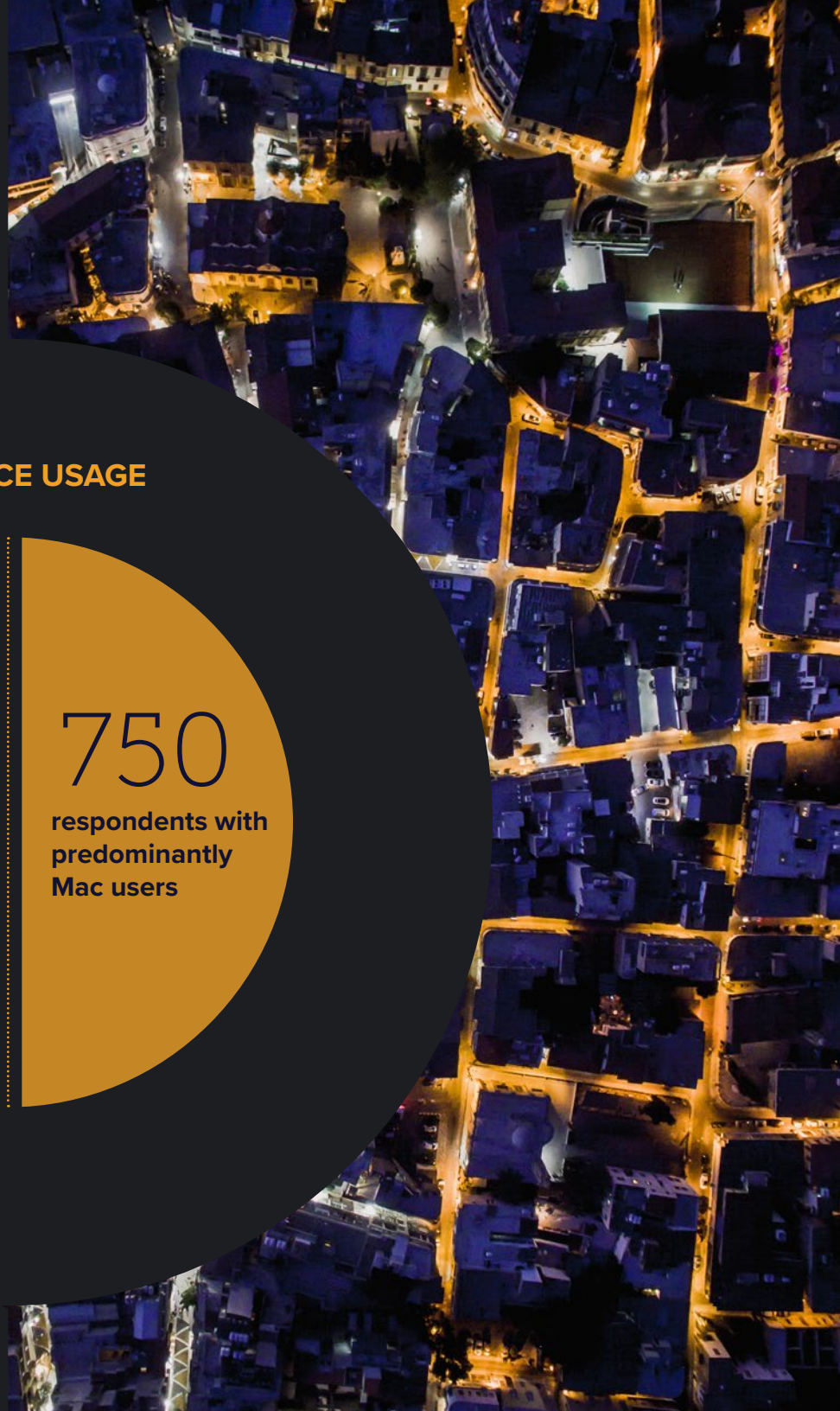
BY ORGANIZATION SIZE

Number of Employees	Respondents
100-199	150
200-499	252
500-999	327
1,000-2,999	358
3,000-4,999	261
5,000 or more	152

BY DEVICE USAGE

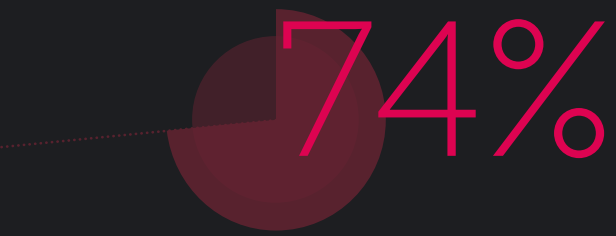
750 respondents with predominantly non-Mac users

750 respondents with predominantly Mac users

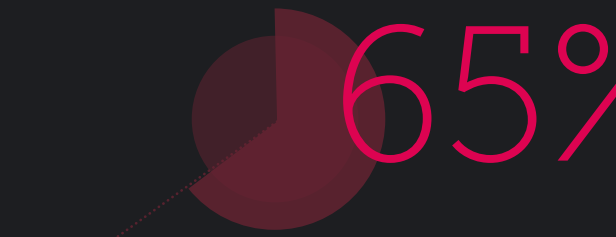


MAC USAGE IS ON THE RISE

There are clear indications that all IT and InfoSec respondents, regardless of which devices their organizations are predominantly using, expect to see an increase in the number of Mac used over the next 12 months.

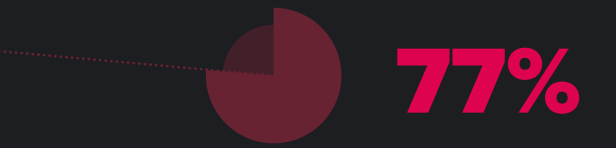


74% of respondents with primarily Mac environments say they will increase device count at their organization

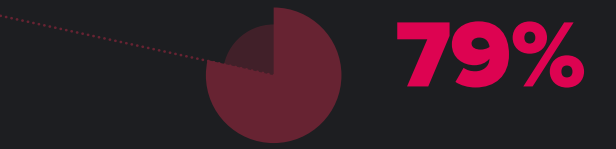


65% of respondents with primarily non-Mac environments say their organizations will consider increasing their Mac count

Why do IT and InfoSec professionals prefer Mac?

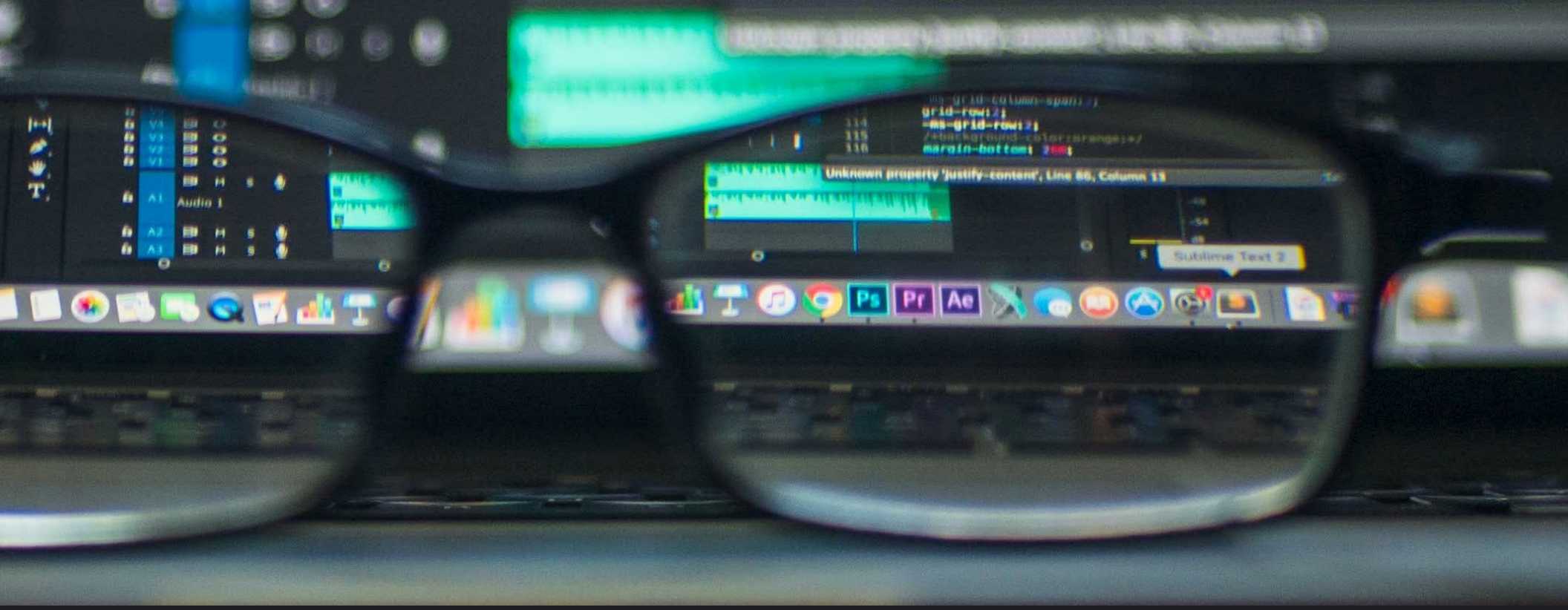


77% of Mac and non-Mac organizations view Mac as more secure out of the box than non-Mac devices



79% of respondents with primarily Mac environments say its perceived security reputation encourages their purchasing decision of Mac devices

57% of respondents with primarily non-Mac environments say its perceived security reputation encourages their purchasing decision of Mac devices



MAC USAGE IS ON THE RISE

Among IT and InfoSec professionals, there was a consensus that oversight and endpoint visibility are easier on Mac, but also that Mac security maintenance is easier. Plus, with all security tools active, **71% of survey respondents** whose organizations use both Mac and non-Mac have better end-user satisfaction with Mac.

Perceived reputation and end-user satisfaction leads **84% of respondents** whose organizations use both Mac and non-Mac devices to say they would choose Mac if all their organization's end users had to use the same device type.

71%

say Mac delivers better end-user satisfaction

84%

would choose Mac for their entire workforce

OS UPDATE CHALLENGES

Despite the positive security perception for Mac, organizations still have challenges and concerns around operating system (OS) and device security across their fleet.

Mac users report less time, on average, than their non-Mac counterparts to roll out OS security patches. But despite the speed difference of Mac upgrades, there is still an average of four days from patch release to deployment.

Mac users roll out OS security patches

30% **FASTER** than non-Mac, on average

Four-Day **AVERAGE** for Mac users to roll out OS security patches

For major OS releases, the discrepancy for Mac versus non-Mac is even greater.

Mac users roll out major OS releases nearly

2.5 times **FASTER** than non-Mac, on average

Five-Day **AVERAGE** for Mac users to roll out major OS releases

OS UPDATE CHALLENGES

The time taken to roll out the latest major operating system leaves devices open to vulnerabilities. Large organizations are especially struggling with this. **Why?**

TOP 5 REASONS

Compatibility Testing
Security Tool Compatibility
Internal Application Compatibility
Compliance Requirements
Third-Party Application Compatibility

Delays in upgrading to the latest major operating system exacerbate security concerns for organizations by leaving known vulnerabilities accessible to attackers. Across the globe, enterprises are facing a wide range of threats on end-user devices and constant pressure to stay protected from potentially detrimental cybersecurity attacks. Especially in a remote-working environment, organizations have to protect themselves from common attacks on their devices, users and data.

TOP 5 CYBERSECURITY CONCERNS

Malware
Data Loss
Phishing/Spear Phishing
Unauthorized Software
Ransomware

SECURITY CHALLENGES

When it comes to containing a potential security incident, many concerns —**37% on average across North America and Europe** — turn out be false positives. This leads to costly time and resources spent investigating threats that don't exist. And when time is spent inspecting false positives, the time to identify an actual threat is increased.

NEARLY HALF of IT and InfoSec teams cite unknown threats as their largest challenge to containing (47%) and remediating (45%) a potential security incident, with other key challenges to remediation including:

LACK OF

- Time
- Staff
- Tools
- Money

Although Mac is seen as the best out-of-box secured device, as adoption rises in the enterprise, so too will the attention towards cyberattacks and threats. To combat, precision and the right allocation of tools and resources are essential.

FUTURE OF SECURITY

With this in mind, investing in the right devices and additional security tools today positions organizations for a more secure future. And this is exactly what organizations plan to do; organizations are investing in security.

96% of organizations plan to spend more on endpoint security, specifically:

1. Data Loss Prevention (DLP)
2. Anti-Virus/Next Generation Anti-Virus (AV/NGAV)
3. Endpoint Detection and Response (EDR)
4. Security Information and Event Management (SIEM)
5. Cloud Access Security Brokers (CASB)

With this greater investment in security, IT and security teams are aiming to harden their fleet and strengthen security incident prevention, detection, response and remediation. And it's imperative they do so, as a dispersed workforce only puts more stress on IT and InfoSec teams, especially considering there was a 38% spike in remote workers as a result of COVID-19.

CONCLUSION

COVID-19 has spurred the greatest movement of the workforce into their homes in history. The technology experience is now a major factor of the employee experience. Organizations need to focus on providing workers with the best end-user experience, while keeping them secure.

It's more important than ever to ensure the security of endpoints and devices as enterprises adapt to work-anywhere workforces. And to allocate resources accordingly to best stop threats.

JAMF APPLE ENTERPRISE MANAGEMENT

Jamf is the only Apple Enterprise Management solution of scale that automates the entire lifecycle of Apple in the enterprise, including device deployment, management and security, without negatively impacting the end-user experience or requiring IT to touch the device. And within Jamf's portfolio, Jamf Protect — endpoint protection built exclusively for Mac — is ready to expand on the secure out-of-box Mac state and empower you to detect, prevent, respond to threats and remediate security incidents. With same-day support of Apple operating system releases, Jamf solutions will never be the reason you delay updates and leave devices open to attack.

That's why security-minded organizations, such as 10 of the largest 10 U.S. banks (according to bankrate.com) and 24 of the world's 25 most valuable brands (according to Forbes), trust Jamf to manage their Apple environment.

See the power of what Jamf has to offer with a free trial.

REQUEST TRIAL

Or contact your preferred authorized Apple reseller for a test-drive.