




The Future of IT Network Security

Digital transformation and work-from-home policies are forcing organizations to choose between user experience and security.

| REPORT



IT Professionals Are Being Forced to Make an Experience Versus Security Decision



Digital transformation has been accelerated by the COVID-19 global pandemic. Users are increasingly logging in to on-premises applications, cloud apps, and Software as a Service (SaaS) platforms from outside the data center in home offices, kids' rooms, and the dining room table. During the past year, IT departments have scrambled to empower newly remote employees, seeking ways to enable ubiquitous application access and improve network performance.

But the acceleration of the “Future of Work” has come at a cost. Business continuity concerns have caused organizations to focus on improving the user experience for remote employees at the expense of security. Malicious actors have noticed, taking advantage of these gaps in cybersecurity policies to target users who now find themselves outside the organization’s security reach. Performance issues caused by latency are making IT professionals reluctant to impose the same security policies that existed inside the office to users who now work primarily from home.

Menlo Security conducted research to capture the concerns of IT professionals at U.S.-based organizations as they grapple with accelerated digital transformation. Here are the results:

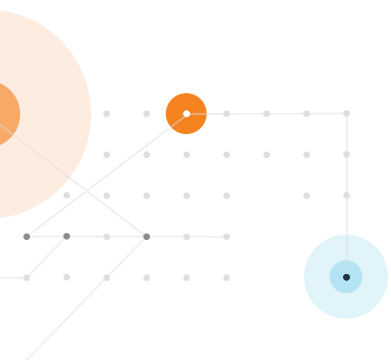
Key Findings

- Digital transformation has led to the increasing popularity of SaaS, enabling more employees to access the network from any location.
- IT decision makers agree that new technologies should integrate seamlessly rather than impede existing network and security infrastructure.
- Eight out of ten IT decision makers have experienced a security breach of some kind, while 40 percent feel these threats are increasing in numbers.
- Despite the expectation of increased compliance and regulatory requirements over the next two years, IT decision makers recognize the need to support a hybrid IT model to accommodate a home office/work balance.
- IT decision makers are concerned that digital transformation is increasing the security risk, but they are more worried about how new security policies may impact employee productivity.



Insight #1: IT Departments Need to Protect an Expanding Threat Surface

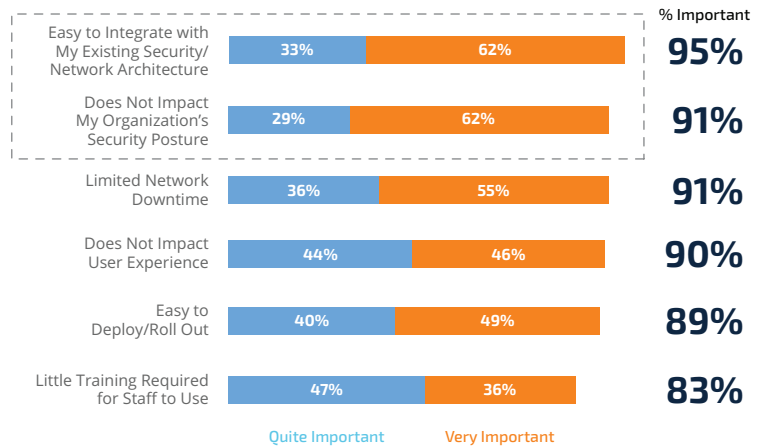
Whether through SaaS platforms, new cloud apps, or traditional on-premises solutions, each access point is a vulnerability that needs to be protected from malicious actors. This expanding threat surface will only expand as new technologies such as the Internet of Things (IoT) and artificial intelligence (AI) continue to mature. And it will become increasingly difficult to integrate these new technologies with existing network and security infrastructure. It's possible that a new way to nondisruptively deliver security services to users will be needed.



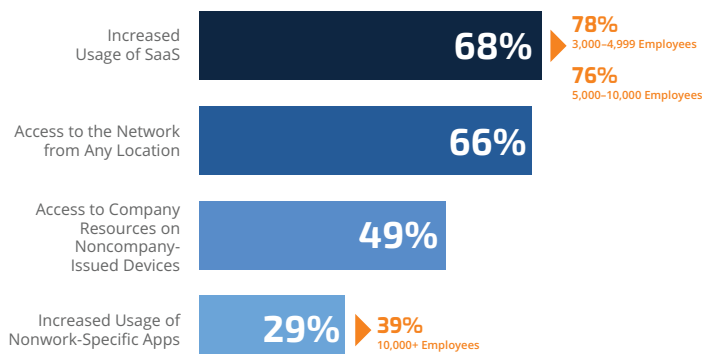
The majority of IT decision makers agree: It's very important that new technology doesn't impact their security posture, and that it's easy to integrate with their existing architecture (62%).



How important is each of the following when it comes to implementing new technology for your organization?



How has digital transformation impacted how your employees access the Internet?

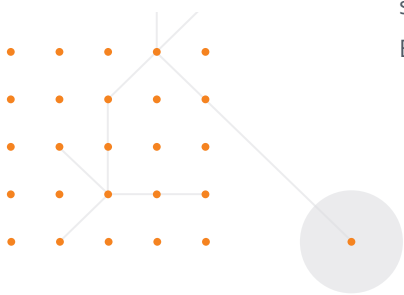


Digital transformation has seen an increased use of SaaS (68%) and enabled more employees to access the network from any location (66%).




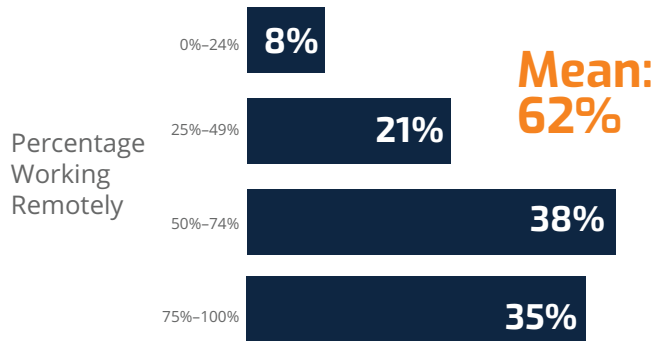
Insight #2: Things Will Get Worse If Changes Aren't Made Now

It's clear that things will never go back to the way they were. The shift to remote work was already happening. It's likely that a large percentage of the workforce will continue to work away from corporate headquarters, and the pressure to deliver office-like experiences at the expense of security will be enormous. This situation will greatly expand threat surfaces, create security gaps, and put tremendous strain on enterprise security teams. Breaches will continue to happen at an accelerated pace.



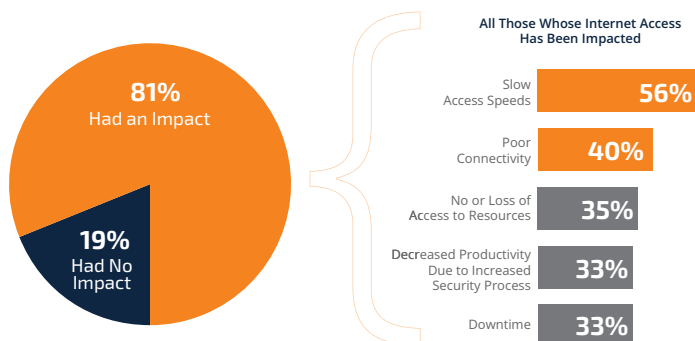
For the majority (73%),
at least 50% of their workforce
is now working from home.

 Roughly what % of the workforce is working remotely as a result of COVID-19?



Base: All respondents (200)

 What impact has COVID-19 had on employees' access to the Internet?



81% of employees have had their Internet access impacted by COVID-19, over half (56%) have experienced slow access speeds, and two fifths (40%) have had poor connectivity.

Base: All respondents (200)/All those whose Internet access has been impacted by COVID-19 (162)

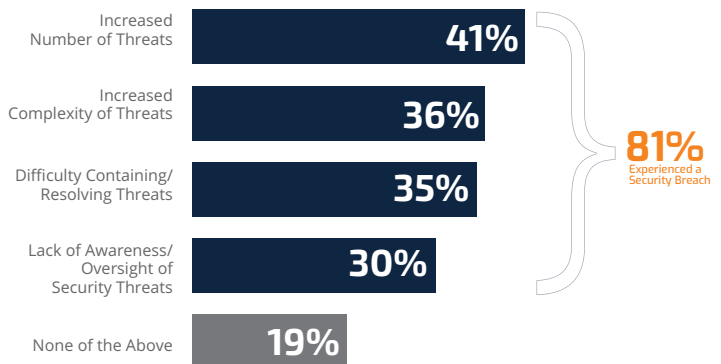


Insight #2: Things Will Get Worse If Changes Aren't Made Now (Continued)

81% of respondents have experienced a security breach of some kind, 41% of which feel that the number of threats is increasing.



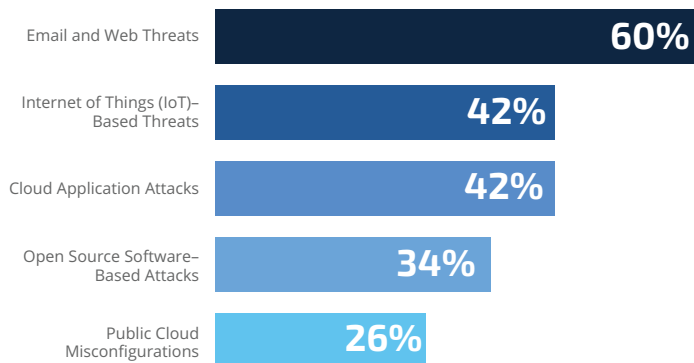
Have you or your organization experienced any of the following when it comes to the security around accessing the Internet since COVID-19?



Base: All respondents (200)/All who have experienced some kind of threat (163)



Which of the following threats have you experienced?



N.B.B. Other = 1%

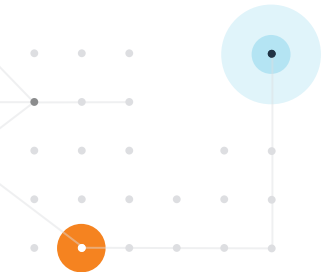
Base: All respondents (200)/All who have experienced some kind of threat (163)

Email and web threats are still causing the most damage (60%).



Insight #3: User Experience Is the Priority

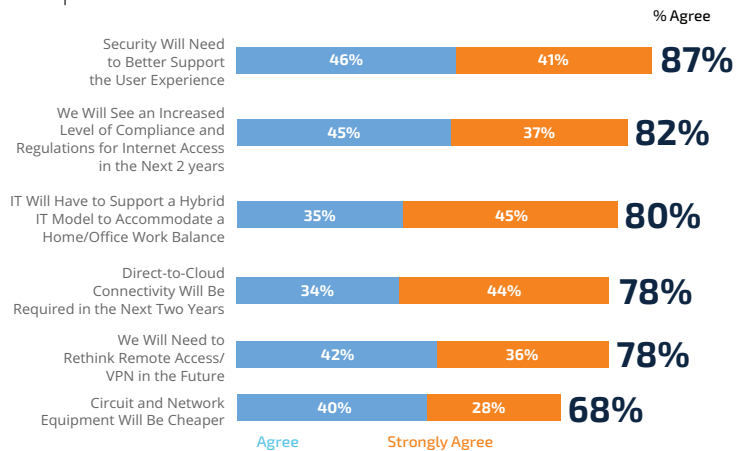
Nearly everyone agrees that compliance and regulatory requirements are likely to get tougher in the next two years. Coupled with the pressures resulting from accelerated digital transformation and work-from-home policies, security teams are well aware that they're going to have to up their security game. However, the user experience will continue to be the priority. Striking the balance between accessibility and security will depend on the adoption of new cloud-based security solutions.



In addition to anticipating an increase in compliance and regulation over the next two years, IT decision makers recognize the need to support a hybrid IT model to accommodate a home/office work balance (80%).



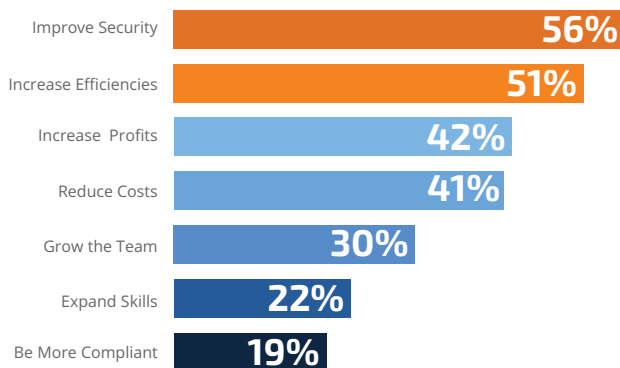
To what extent do you agree with the following statements?



Base: All respondents (200)



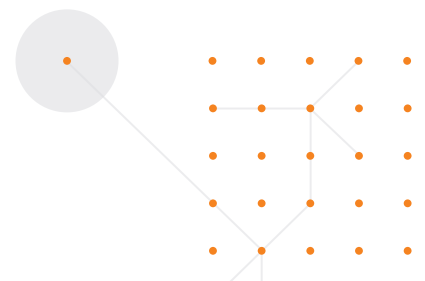
Which of the following are your top priorities for the next five years?



N.B.B. Other = 1%

Base: All respondents (200)

Improving security (56%) and increasing efficiencies (51%) are the top two priorities for business in the next five years.

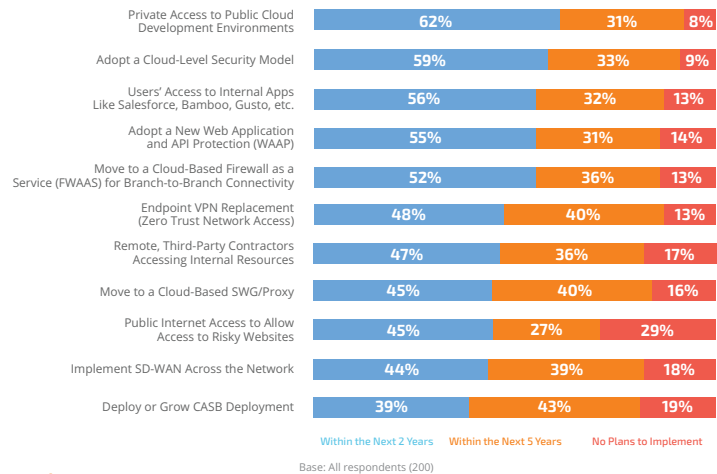




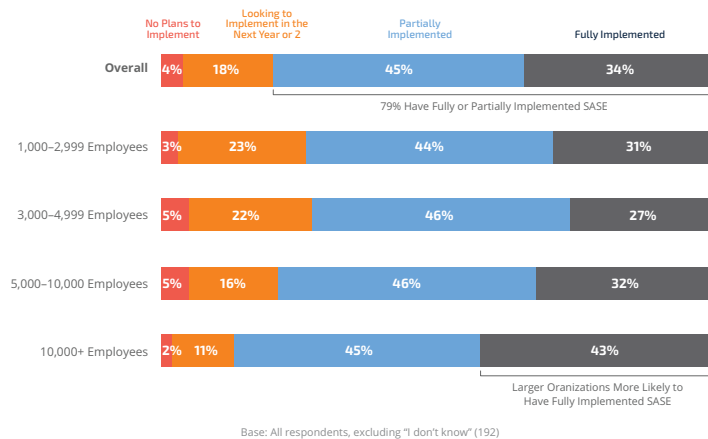
Insight #3: User Experience Is the Priority (Continued)

Private access to the public cloud and a cloud-level security model will be priorities in the short term, while growth or deployment of CASB is a longer-term priority.

Which of the following use cases does your organization plan to address in the next two to five years?



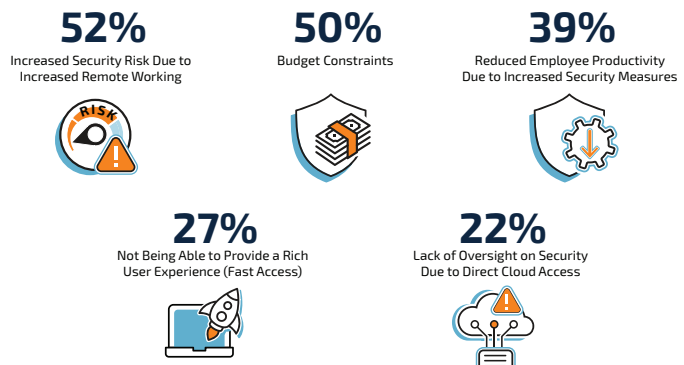
Where are you on your SASE (Secure Access Service Edge)-based architecture?



Over three quarters (79%) have already implemented SASE either partially (45%) or fully (34%).

While the biggest concern with digital transformation is the increased security risk due to increased remote working (52%), IT decision makers also worry about the impact this might have on employee productivity (39%).

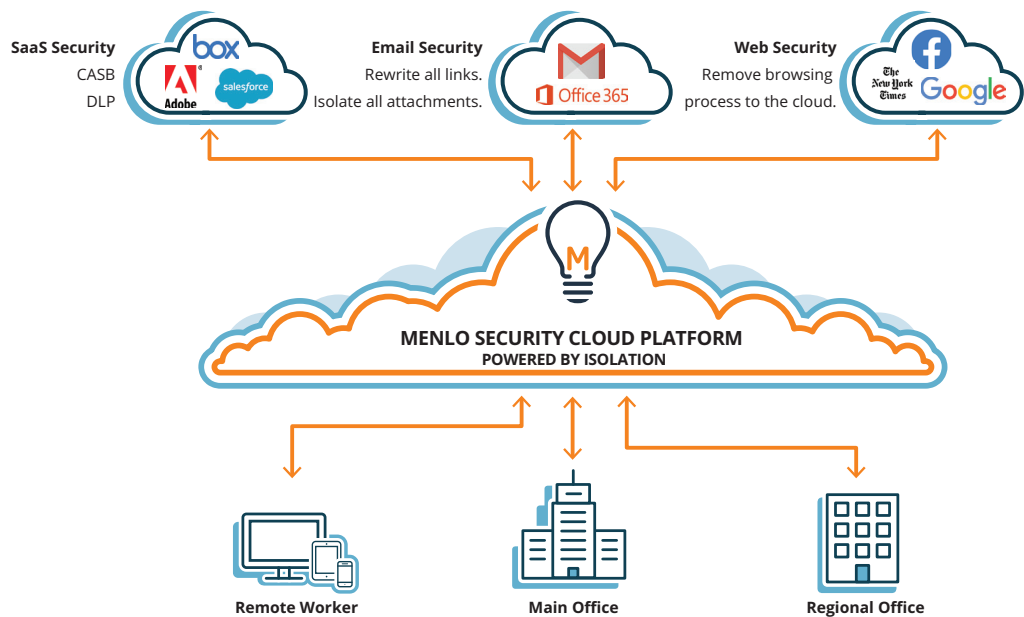
Which of the following do you see as challenges in your digital transformation journey?





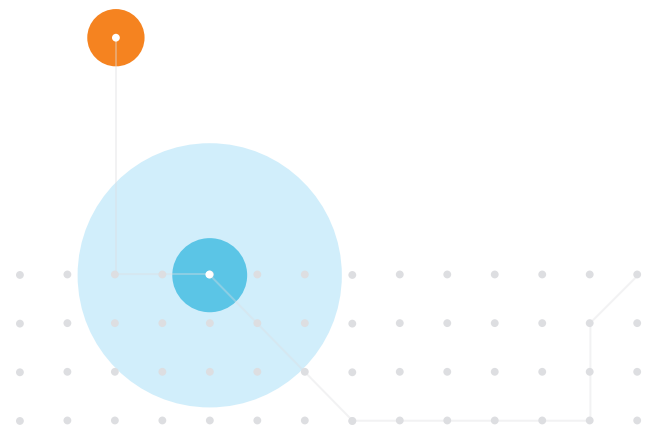
Rethink IT Network Security

Enterprises are facing a major dilemma: Expand accessibility to remote users or clamp down on growing cybersecurity threats. What if you could do both? It's possible, but it's going to take a radically new approach to delivering security services to distributed users, applications, and devices.



Many organizations are moving security to the cloud as part of the network itself, making it infinitely scalable and adaptable to wherever users log in. Policies can be applied through the cloud in a seamless, frictionless way—essentially extending data center visibility and control to home offices.

Learn more at www.menlosecurity.com

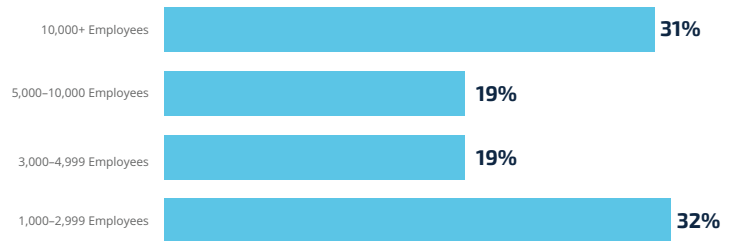




Methodology

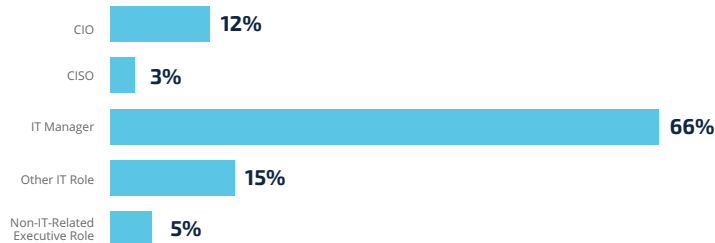
Menlo Security surveyed 200 IT decision makers in the U.S. who work for companies with more than 1,000 employees. The firm sent invitations via email in October 2020 and followed up with a link to the survey for targets who responded. Results are accurate to ± 6.9 percent at 95 percent confidence limits, assuming a result of 50 percent.

Business Size



Base: All respondents (200)

Job Role



Base: All respondents (200)

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The company's Cloud Security Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

© 2020 Menlo Security, All Rights Reserved.

Contact us

menlosecurity.com
(650) 695-0695
ask@menlosecurity.com

