IDC ANALYZE THE FUTURE

Rethinking Security to Enable Distributed Work Environments

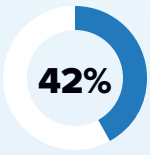
The shift to remote work requires us to adapt to the decentralized security needs of today's evolving workforce.

MANY ORGANIZATIONS BELIEVE THEY'RE **PREPARED TO PROTECT SENSITIVE DATA:**

Are able to protect access to sensitive corporate data and its usage/storage on PCs and mobile devices outside their corporate perimeter.

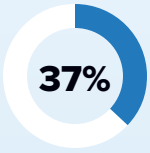
Source: IDC 2020 U.S. Enterprise Mobility and Workspace Management Software Survey n = 360

BUT, FEWER THAN 50% **TAKE A MODERN, CLOUD-CENTRIC APPROACH TO SECURITY:**



Use modern security principles and architectures when it comes to overall security for end users and data access.

Source: IDC 2020 U.S. Enterprise Mobility and Workspace Management Software Survey n = 360

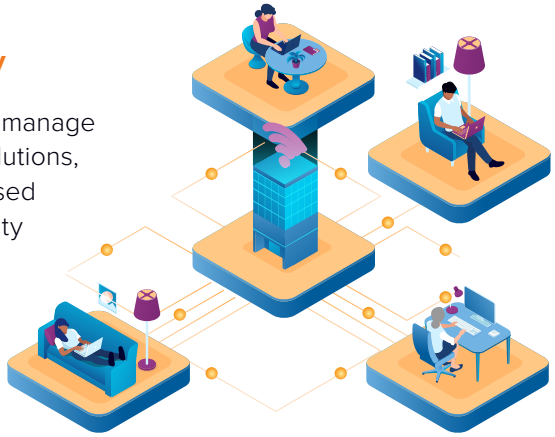


Will make changes to IT security strategy or systems.

Source: IDC COVID-19 Impact on IT Spending Survey, Wave 4, May 2020 n = 160

Remote Worker Security: Perception Versus Reality

The pandemic exposed weaknesses in enterprises' ability to secure and manage remote workers at scale. Many organizations rely on perimeter-based solutions, or extensions of the corporate perimeter (via VPNs), to secure devices used by remote workers. Monitoring, analytics, patch management, and security remediation capabilities all rely on the end user's device being tied into the corporate security infrastructure to receive these services. Cloud and SaaS apps have changed "where" employees access important business tools and apps. But, the "how" in terms of security has not shifted to the cloud as dramatically.



Supporting a remote workspace requires a mix of tools focusing on both traditional security and architectures, as well as modern solutions that protect devices, apps, and data beyond the perimeter. VPNs are not going away, and supporting access to legacy, behind-the-firewall apps and IT resources will be an ongoing requirement for IT. Organizations are gradually adopting modern security technologies such as two-factor authentication (42% have this in place). Meanwhile, more than half of U.S. enterprises anticipate that 25% of their workforce or more will remain remote in 2021. Furthermore, according to *IDC's COVID-19 Impact on IT Spending Survey, Wave 5, May 2020,* many organizations have plans to increase their VPN and remote access infrastructure. Lastly, more than 40% plan to redesign their network and security architectures to support remote work next year (*IDC's COVID-19 Impact on IT Spending Survey, Wave 12, September 2020*).

Over 60% of enterprises say they have mobile VPN solutions to support remote work, with another 22% saying they plan to deploy them in the next 12 months.

What Modern Security Architectures Look Like

Another key trend is the redesign of remote access and networks for remote teams. What this means is a shift to new "zero-trust" models of modern remote access and user authentication. Technologies such as two-factor authentication, conditional access, and authentication will become more prominent. Control points will shift from physical and virtual networks to apps and data themselves. Overall, security approaches must shift from device and network-based controls to modern security principles that wrap security around the data and apps used and accessed by workers. Modern identity acts as a main control point for securing access to data, ensuring end-user activity is secure and compliant.

Technologies that define the corporate perimeter via software, as opposed to physical presence in a building or extended virtual presence via VPNs, are a key component for securing the new remote/dispersed workforce. More than 45% of U.S. enterprises expect to see increased demand from end-users for modern security solutions, such as data security, secure application delivery, and virtual workspaces, to meet the needs of a distributed, beyond-the-perimeter workforce. This approach of modern remote workspace management—as opposed to a focus on securing specific devices or requiring workers to be attached to specific networks—will help organizations maintain security and compliance controls as remote worker populations surge. It will also help organizations adjust to new hybrid office/remote workspace plans as they begin back-to-office scenarios in a phased manner.