Secure Access for the Future

The 451 Take

Information security teams have been handed a big, scary reset button for their access and connectivity environments, and most aren't able to decide whether they can push it without causing disaster. While the upheaval of the current year has clearly shown the limits of traditional approaches, the journey to better options can feel like it's filled with unknown risks. The reality is that there are ways to approach the shift to new models like zero trust that can get organizations on their way with their eyes open and still let them sleep well.
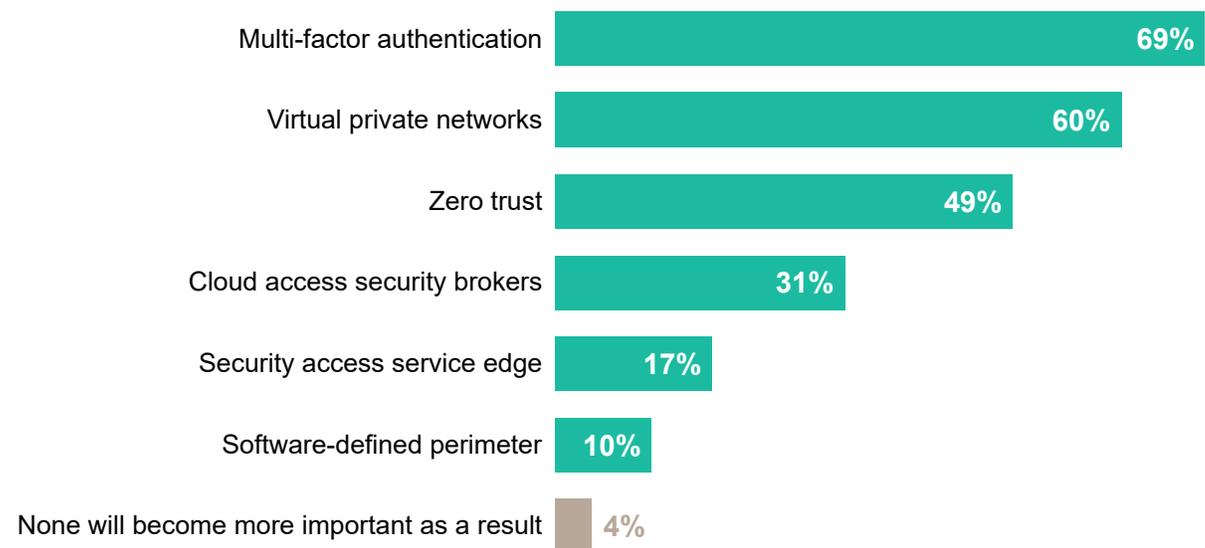
In a recent 451 Research Voice of the Enterprise study, respondents indicated which access technologies they believe will become more important in light of this year's upheavals. With a focus on technologies they already know, the responses show that many organizations are missing an opportunity to leverage technologies that can help them to make their employees more productive and their environments more secure. While an expansion of multi-factor authentication is a good step, a strong preference for VPNs over better access options is startling. It speaks to the level of concern about the risk of changing such a key part of their infrastructure.

Importance of Security Access Technologies Based on Work-from-Home Policies

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2020

Q: Which of the following security access technologies do you think will become more important as a result of the coronavirus (COVID-19) outbreak with more employees working from home? Select all that apply.

Base: All respondents (abbreviated fielding; n=78)

Technology	Percentage
Multi-factor authentication	69%
Virtual private networks	60%
Zero trust	49%
Cloud access security brokers	31%
Security access service edge	17%
Software-defined perimeter	10%
None will become more important as a result	4%

What businesses need for better secure access is a set of capabilities that can give them better identity integration, more granular controls, visibility that encompasses users as well as their resources, and the operational simplicity that will allow them to manage it all effectively. While strict definitions of zero trust may be hard to come by, the principles of least privilege and minimized default access that zero trust embodies have become critically important since remote work has become the norm. Businesses need these capabilities delivered in ways that require a minimum of disruption to deploy.

The 451 Take

Organizations can manage risk in this journey with an intelligent transition strategy. They should select access technologies that will allow them to make a gradual transition and avoid ripping and replacing current VPN systems. A sane migration will allow them to add zero trust protections where they can have immediate effect. This requires a system that has the flexibility to target a single use case initially, and then expand to new ones as the initial use case is successfully embraced. Such a migration will require deployment options that meet existing resources where they are, either on- or off-premises. While exclusively cloud-based systems are grabbing headlines, the reality is that most organizations need both options. The transition strategy will also require the ability to place security controls where users need to get work done.

The rewards that organizations will gain along this course are the ability to reduce the risk associated with remote access while making employees and security teams more productive. They'll accomplish this by integrating better context into their policy controls and giving themselves the tools to improve their security posture.

Business Impact

TRADITIONAL ACCESS APPROACHES CAN'T ADAPT WELL TO TODAY'S REALITY. Organizations need ubiquitous access, better controls and simple scaling.

EFFECTIVE ACCESS APPROACHES CAN IMPROVE SECURITY. Making access capabilities fully functional can increase their use and reduce the risk that users will resort to less secure alternatives.

INTELLIGENT APPROACHES CAN REDUCE RISK IN ZERO TRUST ADOPTION. The transition to zero trust isn't an all-or-nothing proposition. Getting there takes work, but it can be done in ways that minimize disruption.

DIGITAL TRANSFORMATION CAN BE ACCELERATED WITH BETTER ACCESS APPROACHES. Making the necessary resources available when and where they're needed can push forward efforts in enterprise digitization.

Looking Ahead

Organizations need to create a foundation today that will serve them well, no matter what situations present themselves in the future. While their specific paths may vary, all will be well served by access environments that allow them to adapt to a more varied set of work styles, where they'll need the flexibility to make workers productive and secure. Organizations will need to understand that, as with many aspects of successful security implementations, this is not an all-or-nothing proposition. It's a long journey to provide more capable and secure access capabilities, but it's a critical one that needs to start today.

NetMotion®

The transition to zero trust is inevitable, but it doesn't happen overnight. Remote access is evolving fast, and so must your organization. NetMotion is the only security solution that allows you to get the best of both ZTNA and VPN in a single platform, helping you embrace zero trust in a gradual, seamless and strategic way.

For an introduction to ZTNA/SDP, with practical examples and original research on the topic, you can download the extensive report for free by visiting netmo.io/451research.