Point of View +

The Right Security Enables Successful Hybrid Work

How to Unlock the Potential of Your Workforce—Anywhere, Anytime

Rapid Transformation Results in Turbulence

Digital transformation has firmly taken hold in the majority of organizations around the world. A recent survey of CIOs shows that 60% of companies will continue to make significant investments in digitalization this year to enhance competitive capabilities, enable greater business agility, and aid in decision-making.[1]

One aspect of this evolution is that enterprise applications and data are increasingly moving out of corporate networks and data centers and into the cloud. According to Gartner®, 70% of all enterprise workloads, up from 40% in 2020, will be deployed in cloud infrastructure and platform services by 2023[2]. What's more, over 80% of all enterprise traffic is destined for the internet and 53% of all web traffic is cloud related.[3]

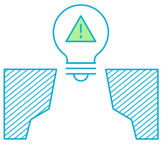
Another critical factor is the rapidly expanding volume of data being generated. Between 2020 and 2025, the amount of data in the world will increase from 57 zettabytes (ZB) to an astounding 175 ZB[4]. More data is being collected and shared across more points of access than ever before, and this information is widely distributed across both networks and clouds, as well as a number of managed and unmanaged devices. Without purpose-built protection, these vast quantities of distributed data are quite vulnerable—more than one-third (40%) of organizations experienced a cloud-based data breach last year.[5]

A third related factor is that a significant proportion of the user population will continue to work outside of a traditional corporate office location with the expectation of being able to access information from any device and location, all without having to make trade-offs between security and network performance. As businesses settle into the new normal of post-COVID-19 protocols, at least 50% of the U.S. workforce is expected to continue to work from home long-term.[6]

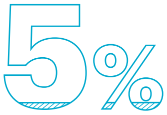
Facts

Digital technologies have so far not fully delivered their expected dividend in higher productivity growth.[7]

Risk management has not kept pace with the proliferation of digital and analytics transformations—a gap is opening that can only be closed by risk innovation at scale.[8]



Today, the success rate of digital transformation may be as low as 5% due to the challenges and complexities faced by IT professionals.[9]



[1] "CIOs, CTOs and technology leaders: Latest findings from PwC's Pulse Survey," PwC, January 27, 2022.
[2] "Gartner, Hype Cycle™ for Cloud Security, 2021," By Tom Croll, Jay Heiser, July 27, 2021.
[3] "Cloudy With a Chance of Malice," Netskope, February 23, 2021.
[4] "Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025," Statista, March 18, 2022.
[5] "40% of organizations have suffered a cloud-based data breach," Security Magazine, October 29, 2021.
[6] "A Stanford Economist Who Studies Remote Work Says Half of All Workers Will Make This Big Change in 2022," Inc., January 8, 2022.
[7] "How digital transformation is driving economic change," Brookings, January 18, 2022.
[8] "Derisking digital and analytics transformations," McKinsey & Company, January 5, 2021.
[9] "How to reduce IT complexity during digital transformation," Lucidchart, May 27, 2021.

While these changes are having an immediate impact right now, none of them are new. For some time now, organizations have faced the stark reality of having to adapt their IT infrastructure to business digitalization or find themselves less competitive. Even before the pandemic, 92% of companies believed their business models would have to change given rates of digitalization at the time.[10] COVID-19 only accelerated that process—moving three to four years forward in digital adoption in a matter of months, by some estimates.[11]

Early steps toward transformation at many enterprises were done within the confines of existing budgets—and while maintaining IT environments that were largely architected to accommodate an office-bound user population with standard corporate managed devices accessing traditional applications and data across local networks. But as a result of the sudden shift to the cloud, an explosion of data, and the new work-from-anywhere (WFA) reality, organizations are struggling with several key problems:

- **User productivity** is being slowed by an unreliable, high-latency user experience.[12]
- **Security gaps** arise from a lack of cloud awareness and security circumvention.[13]
- **High cost and complexity** of siloed, legacy network and security infrastructures.[14]

To enable the future of work and gain the full benefits of digital investments, organizations need to take a look at their existing security infrastructure with clear eyes—and an even clearer understanding of where their users, applications, and data are going.

Maximizing Enterprise Agility

To accelerate network performance and achieve the business agility that digital transformation promises, organizations need a fully converged, cloud-native security platform—one that eliminates the architectural inefficiencies hindering traditional solutions and those that are "retrofitted" for the cloud or may be marketed as such, but aren't purpose-built for the cloud.

Leaders Should Look for

□ A ubiquitous cloud-native security architecture with points of presence (POPs) around the world, eliminating the need to send traffic back to a central network for security inspection

□ A security platform that ensures low latency and exceptional reliability so that distributed users maintain exceptional web and cloud performance at all times

□ Convergence of key security capabilities—such as secure web gateway (SWG), cloud access security broker (CASB), zero trust network access (ZTNA), and data loss prevention (DLP)—into a "single-pass" architecture that performs all inspection in one place for greater efficiency and lower latency

□ Granular end-to-end visibility of user activity, making it easier to troubleshoot and optimize the user experience

[10] "5 Questions Boards Should Be Asking About Digital Transformation," Harvard Business Review, June 21, 2021.

[11] "How COVID-19 has pushed companies over the technology tipping point—and transformed business forever," McKinsey & Company, October 5, 2020.

[12] "The Economics of Network and Security Transformation," SDxCentral, December 21, 2021.

[13] "Misconfigurations: Still the Biggest Threat to Cloud Security," Network Computing, August 25, 2021.

[14] "WAN report: Complexity continue to grow as more organizations close legacy data centers," TechRepublic, January 20, 2022.

Mitigating Security Risks

You can't secure what you can't see, and in order to de-risk digital transformation, organizations need to extend visibility and control to web, cloud, and private applications. Security teams need to mitigate risk exposures even as enterprise applications, data, and users move beyond the network perimeter. This requires cloud-based protection that allows them to secure all assets without creating performance bottlenecks that drive networking teams to bypass controls.

Leaders Should Look for

□ Comprehensive embedded data protection that extends to wherever data resides

□ State-of-the-art threat protection, including sandboxing and remote browser isolation to detect and prevent even the most advanced attacks

□ Risk management that automatically assesses and improves organizations' cloud security postures

□ Advanced behavioral analytics that use artificial intelligence (AI) and machine learning (ML) to spot and correlate anomalies and provide visibility of threats that slip past conventional security tools

□ Reverse proxy capabilities that enable unmanaged devices to access corporate resources without compromising corporate security

□ Highly granular access to applications and resources, reducing the lateral movement risk entailed by granting network-wide access to VPN users

Reducing Cost and Complexity

Today, much of security is expensive, inefficient, and difficult for teams to control and manage. Security teams have too many siloed tools, which require incremental and personnel-related costs. Maintaining an advanced security posture is becoming an increasingly complex and costly task for security teams. The average organization manages 76 disparate security tools—and every time a new threat or IT change emerges, organizations must consider adding a new one-off solution to close the gap[15]. As a result, it becomes especially difficult to scale these kinds of traditional security architectures. To gain the full benefits of digital transformation projects and save money, organizations must consolidate their security technologies and embrace a more efficient WAN architecture.

Leaders Should Look for

□ Support simplified installation and optimized solution management via a common agent and management console

□ Enable unified policy management that simplifies administrative processes while ensuring consistent enforcement across web, cloud, and private applications

□ Offer SD-WAN integration that helps organizations switch from slow, inefficient, and expensive MPLS branch office connections in favor of fast, affordable broadband links

□ Eliminate the need for heavy VPN clients while reducing bandwidth and VPN infrastructure costs at the HQ network

[15] "Organizations Now Have 76 Security Tools to Manage," Infosecurity Magazine, December 1, 2021.

The Drive to Empower a Digital Workforce—Anywhere, Anytime

The current challenges of digital transformation are diminishing the intended benefits—and the problems will only become more pronounced as cloud, data, and mobility transformations continue to scale. Organizations need to realign their IT network and security environments to realize hybrid work by enabling WFA and achieving branch office transformation. If it's to succeed, the future workplace must help enterprises make their businesses more agile, mitigate security risks, simplify operations, and realize a better TCO.

Gartner and Hype Cycle are registered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

netskope

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply Zero Trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything, visit netskope.com.