SPOTLIGHT
Sponsored by: Netskope

As new technologies and business practices introduce previously unimagined threat vectors, digital transformation presents the opportunity to address these threats as well as legacy security challenges, including the "human factor."

The Network as Linchpin of Security Transformation and Successful SSE Adoption: Key Considerations

July 2022

Written by: Christopher Rodriguez, Research Director, Security and Trust

Introduction

The cybersecurity industry has been scrambling to adapt to increasingly clever and elusive attacks since the earliest high-profile advanced persistent threats such as Operation Aurora and Stuxnet. The years that followed have been an ongoing cat-and-mouse game as threat actors have innovated with new tactics and capabilities, including sophisticated evasion tactics and zero-day vulnerabilities.

In 2020, the threat landscape accelerated drastically, leading to several high-profile breaches in government agencies, critical infrastructure, large enterprises, and even security companies. As a result, an urgency to modernize security has emerged, leading to new practices such as the zero trust framework and security service edge (SSE). However, the threat landscape is only worsening. According to IDC's *Future Enterprise Resiliency and Spending Survey, Wave 3* (April 2022, n = 828), business leaders are expecting the Russia-Ukraine War to lead to more cyberattacks, with 38% of respondents increasing their cybersecurity defenses in response.

AT A GLANCE

KEY STATS

- 30% of IT buyers cited "an ongoing struggle between employee flexibility and security requirements" as a top business challenge when implementing work transformation initiatives.
- 27% of businesses cited cloud and mobile device security concerns as top technical challenges; 20% cited "inadequate network bandwidth."

Source: IDC EMEA's *Future of Work Survey*, March 2020, n = 415

The urgency to secure sensitive data and systems is constantly counterbalanced by real-world business considerations. The unique security challenges of the digital transformation era are not solely technical in nature. Security systems must provide protection without hindering business operations. History has shown that disruptive security tools may be set to monitor-only mode, avoided, or switched off entirely, leading to reduced security efficacy. Put simply, security must be accurate, reliable, performant, and frictionless. Security transformation must go beyond mere adaptation to technological change but must account for the "human factor" as well.

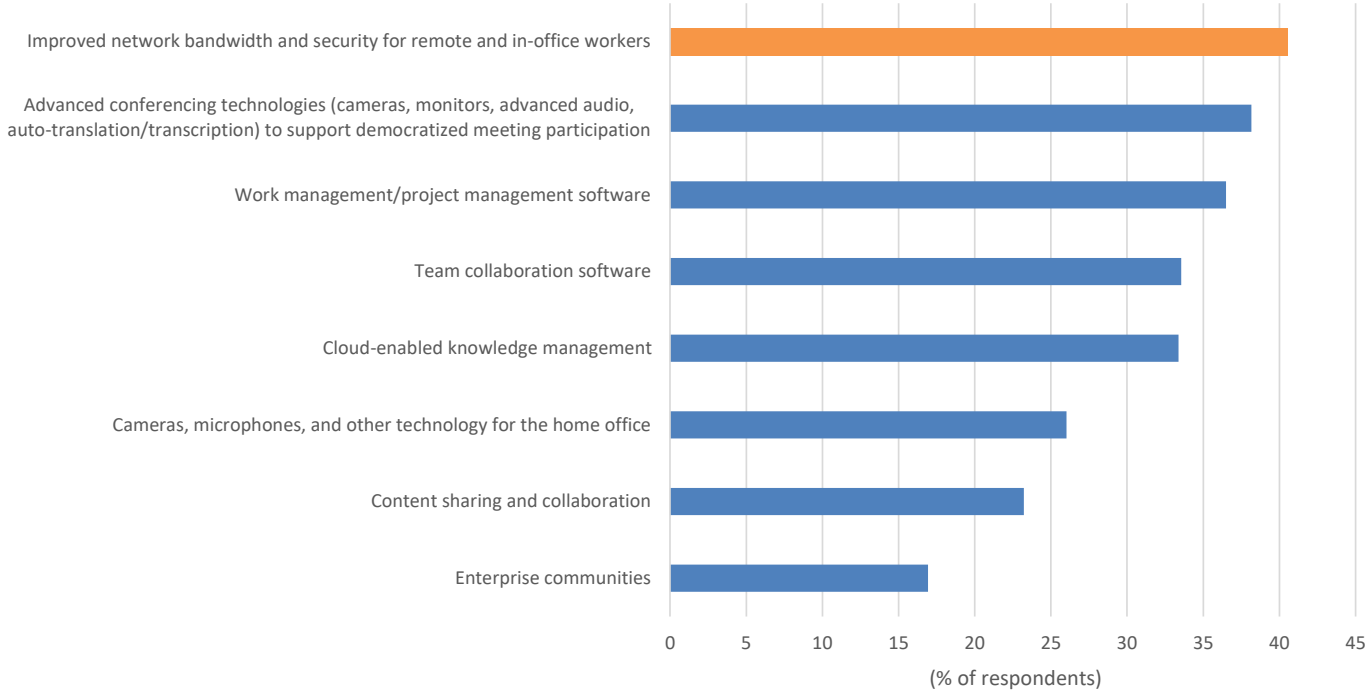
Smart Security Strategy Adjustments Offer Business Benefits

Embracing Digital Transformation to Maximize Business Value

Digital transformation has unlocked innovative new practices, reshaping where, when, and how business happens. IDC research confirms the process has yielded tangible benefits, such as business resiliency, scalability, and employee productivity. For example, despite the challenges of a rushed migration to "work from home" in 2020, respondents also reported increased employee productivity resulting from digital transformation, with most organizations reporting gains of 25–50% (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 3*, April 2022, n = 231). IT buyers noted "improved network bandwidth and security for remote and in-office workers" as the top investment that businesses made or planned in 2021 to enable communication and collaboration among the workforce (see Figure 1).

FIGURE 1: ***Security and Networking as Business Enablers in the Digital Transformation Era***

Q *What are the top 3 technology investments your organization made in 2021 or planned for 2022 to enable communication and collaboration among all members of the workforce?*



n = 828

Note: Multiple responses were allowed.

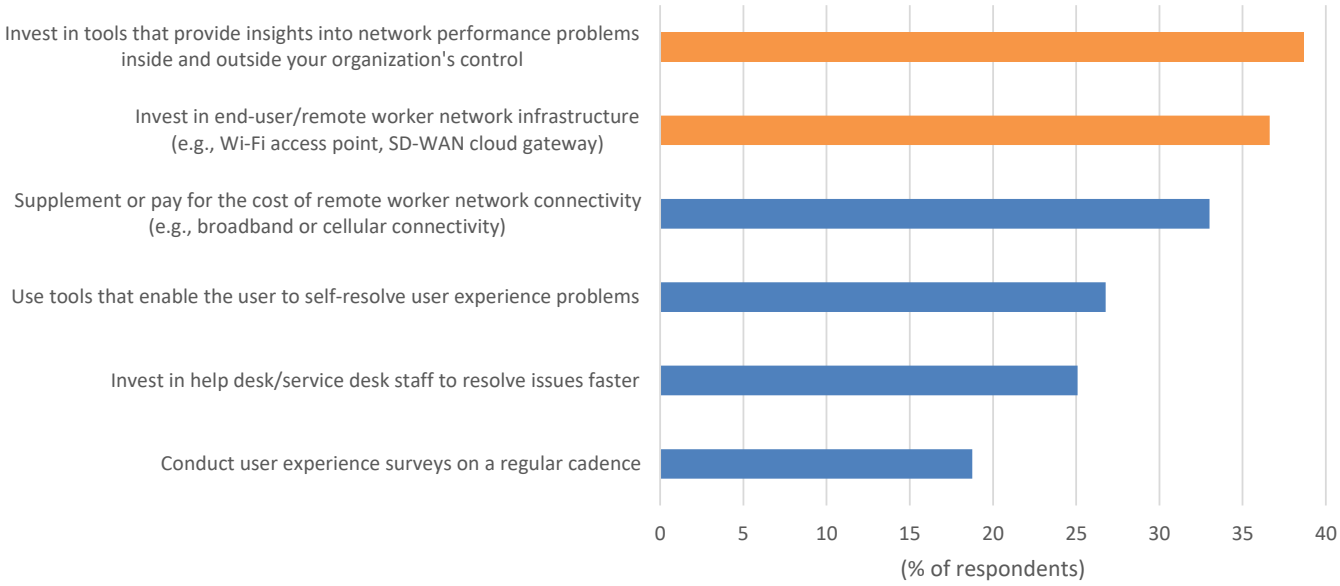
Source: IDC's Future Enterprise Resilience and Spending Survey, Wave 3, April 2022

Many organizations are now embracing hybrid and flexible work models for the future. But when respondents were asked how they would rate their team's ability to monitor and measure work-from-home/remote worker end-user experiences (1 = no ability, 5 = high ability), 23% rated their ability as a 5 while 33% rated their ability as a 3 or lower.

To improve the end-user experience, businesses noted plans to invest in specialized performance monitoring tools as well as end-user/remote worker network infrastructure (see Figure 2).

FIGURE 2: ***Business Leaders Focus on Improving the User Experience***

Q *What investments is your organization planning to make to increase your ability to manage work-from-home/remote worker network and application user experience?*



n = 828

Note: Multiple responses were allowed.

Source: IDC's Future Enterprise Resilience and Spending Survey, Wave 3, April 2022

Security Transformation Adapts to the Human Factor to Reduce Risk

The changing nature of work inherently introduces new vulnerabilities while exacerbating known threat vectors. As the network evolves, security practices must also evolve to unlock the full benefits of digital transformation. Digital transformation without a commensurate security transformation is a recipe for disaster. For example, simple user errors during rushed cloud migrations led to several high-profile data breaches including the exposure of years of sensitive airport employee records in January 2022. Moreover, the process is cyclical: The development of new security control points generates the need to adapt networking requirements.

Positively, the digital transformation era also presents an opportunity for security providers to address a long-standing trade-off in cybersecurity*: performance versus protection*. This pain point is a familiar one, hearkening back to a time when firewall vendors first added inline intrusion prevention capabilities. Then, key considerations were technical in nature, expressed in terms of bandwidth and latency. Now, the technological and operational changes introduced by digital transformation require security practitioners to consider performance in the context of the human factor. Through this lens, performance becomes a security imperative.

Consider the profound and direct impact that poor network performance can have on end users. Performance degradation can lead to disruption, distraction, and distress for end users. An outage will have a direct and quantifiable impact on productivity. Multiple small disruptions also add up. Users may waste time troubleshooting connection problems on their own. Any of these situations can lead to end-user frustration.

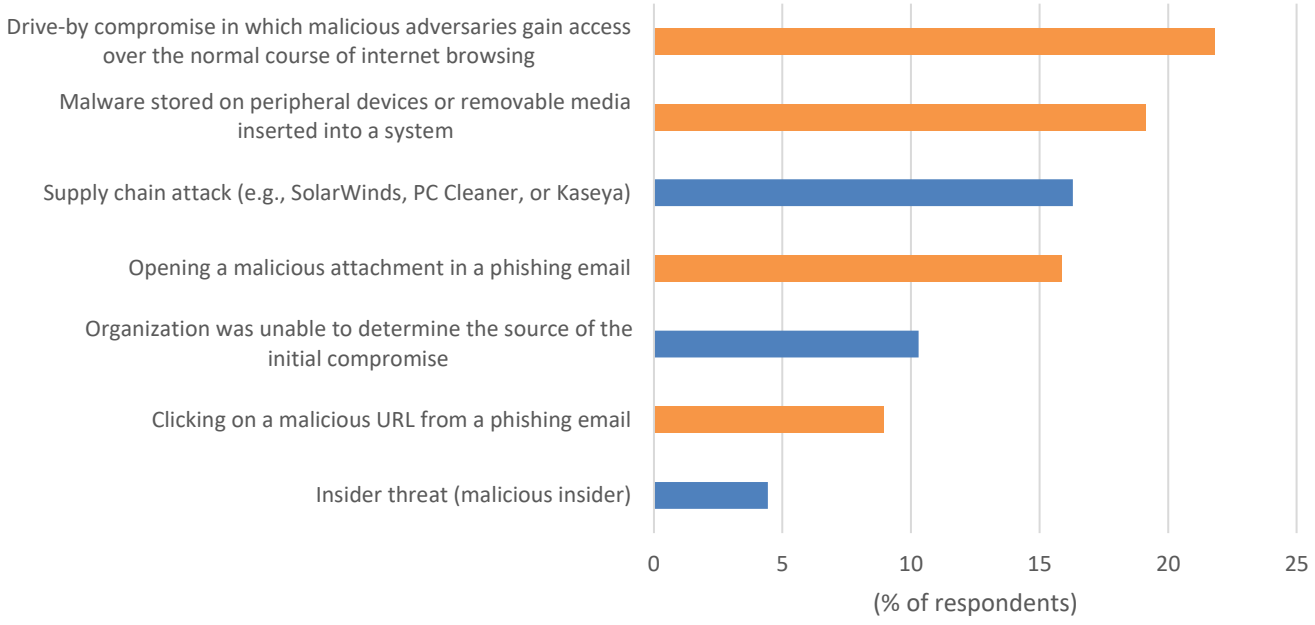
Ultimately, these poor user experiences are clear drains on productivity and business value. However, they also present an imminent risk to the business. Frustrated end users may search for workarounds, and users may attempt to disable or circumvent security controls. The subsequent lack of corporate IT control leaves data unprotected and IT organizations blind to user behavior, telemetry, and other key security signals. Users are vulnerable to malware, phishing, and social engineering attacks, including extortion, enticement, or other forms of manipulation.

Key Trends Driving Cybersecurity Transformation

Digital transformation has changed the IT environment drastically, introducing new threat vectors at a time when cyber-risk is already escalating. According to IDC's December 2021 *Future Enterprise Resiliency and Spending Survey, Wave 11* (n = 858), 44% of organizations reported ransomware attacks in 2021; among the victims that paid a ransom, 20% paid six-figure ransoms. Most ransomware attacks occurred after bad actors gained access to the network from normal internet browsing by users (see Figure 3).

FIGURE 3: ***Most Ransomware Attacks Required Human Interaction***

Q *For your most recent ransomware incident that blocked access to systems or data, what was the most significant source of the initial compromise?*



n = 444

Base = respondents who indicated their organization has experienced ransomware attacks/breaches

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 11, December 2021

The Business of Business Has Changed: Environments, Devices, Users, and Applications

The digital transformation trend is far more than a simple, steady cadence of emerging technologies. These technologies are reshaping how we work, which devices we use, what applications we use, and when and where we use devices and apps. Businesses are emphasizing a model of work that is "agile" and flexible, for both employees and employers, including permanent work-from-home or hybrid work options. As noted, IDC research shows that this model drives productivity. Unsurprisingly, IDC predicts that by 2023, digital transformation and business volatility will drive 70% of G2000 organizations to deploy remote or hybrid-first work models (source: *IDC FutureScape: Worldwide Future of Work 2022 Predictions*, October 2021).

However, security challenges have emerged. Users rely more on personal devices to work anywhere and at any time. The IT organization has less control over or visibility into these devices. This same "BYOD" concern was present in legacy networks as well. The concern was the lack of control IT had over these devices — personal user devices could be used to access sensitive data or systems. Today, concerns are largely about remote access, as VPN connections into flat networks are similar to the BYOD problem.

The challenge of securing data is no less complicated by digital transformation. Collaboration applications have become more powerful, user friendly, and ubiquitous, leading these applications to gain prominence in enterprise workspaces. IDC research noted a growing preference for online-first collaboration tools and cloud applications: 76% of organizations that use team collaboration applications said they have reduced email by over 20%, and some organizations reported even greater reductions. As a result, communications are now real time, asynchronous, and more conversational in tone than email correspondence. These characteristics improve productivity but also increase the risk of oversharing, unintentional data leakage, or other policy violations. The challenge is compounded when factoring in the potential for end users to access or share data via personal accounts or devices. Policies governing use of a sanctioned application will vary depending on the account type in question.

In the Digital Transformation Era, Security Must Accommodate Business Needs

As the nature of business technology continues to evolve, so too must security practices and technologies. Security vendors compete to provide best-in-class protection, spending millions in threat research to identify new vulnerabilities, block zero-day threats, and reduce time to detection.

However, security cannot exist in a silo. While threat detection must be fast and accurate, a frictionless experience is key. In turn, the underlying security mechanisms must be reliable, performant, and transparent. This is the difference between security solutions that enable digital transformation and security solutions that simply adapt to transformation.

While security practices focus extensively on factors of confidentiality and integrity, availability is often overlooked. Outages of security services may cause problems in protected systems or may force IT organizations to rely on legacy methods for protection. In a worst-case scenario, businesses may need to bypass security systems completely.

Security services must also be performant to ensure availability of protected systems because performance degradation can cause certain applications to crash or to function improperly. Outages can lead to business disruption such as work stoppages, end-user frustration, and delayed deals. Similarly, cloud service providers make extensive investments to ensure a performant user experience. But security services that add excessive latency to the user experience ultimately undermine the benefits of cloud adoption and hamper productivity. Security services lacking network optimization can add seconds to page load times for key SaaS applications, which can add up to multiple hours of lost productivity per month.

Convergence Trends in Cybersecurity

The urgency to adapt security to the digital transformation era has led to new frameworks and solutions such as secure access service edge (SASE) and SSE. These emerging models offer key benefits such as the following:

- **Security integration:** The current security architecture is currently very complex and needs to be integrated as much as possible. Integration offers benefits such as consistent enforcement of policy, comprehensive protection, and broad observability. Integrated security tools do not operate in security silos, leaving fewer gaps for attackers to exploit.
- **Security convergence:** Convergence is about business value. The limited number of point products reduces business complexity. Simplified licensing and possibility for deeper discounting also offers business value benefits. A single pane of glass for management reduces the specialization and time overhead required to use multiple disparate user interfaces for various security tools.
- **Networking and security convergence:** The SASE trend requires a visionary reevaluation of the roles of networking and network security. The current interpretation of SASE is a cumulative approach, essentially adding SD-WAN functionality to security control points. A more holistic approach to smart integration can drive business value and security outcomes.

There is no easy button in security, and SASE is proving to be a journey rather than a security "magic pill." True transformation requires reimagining security architecture and networking from the ground up rather than a simple lift and shift to the cloud. While early approaches focused on virtual form factors of familiar security appliances, these solutions require extensive manual processes that clash with the elastic scalability of cloud services.

Stated simply, enterprise-grade cloud security requires a strong cloud foundation to meet reliability and performance requirements. Therefore, security outcomes will be directly impacted by the capabilities — or limitations — of underlying cloud architecture. By taking a more cloud-native approach to security migration, businesses can adopt new and emerging business practices and use cases while minimizing or reducing business risk.

Considering Netskope

Widely known for its deep cloud access security broker (CASB) capabilities, Netskope now offers a complete SSE portfolio including secure web gateway (SWG), zero trust network access (ZTNA), and firewall as a service as well as other enterprise security solutions such as cloud security posture management (CSPM). Netskope has approached the security transformation challenge in a holistic manner, combining a data-centric approach with the guiding principle of "the network is the security." Netskope's cloud architecture is the foundation of its security solutions. The company has invested over $100 million in its NewEdge cloud with the threefold goal of increasing security efficacy, promoting the end-user experience, and improving upon the inherent technical challenges of the internet.

Key Advantages of Purpose-Built Cloud Security

Netskope SSE is a pure-play, cloud-native, integrated security service, featuring benefits that are commonly associated with the cloud. For example, cloud-delivered security offers the business benefits of evolving beyond capex-based investment cycles. Cloud services offer technical benefits as well. Cloud services do not require IT organizations to backhaul traffic from distant user devices to a datacenter for security inspection — inspection is done in the cloud. This edge security capability is ideal for distributed enterprises with many branch offices and remote users.

Currently, NewEdge cloud covers 57 regions with datacenters capable of full compute, performing all security inspections at the edge, closer to end users, to ensure that the end-user experience is secure and transparent, with minimal detour between users and SaaS applications, web, cloud, or private applications.

Cloud architecture has the potential to eliminate the performance "bottleneck" challenge that hampers on-premises firewalls and other inline security controls. The cloud offers elastic scalability to spin up more computing resources as needed to perform security inspections. For Netskope, NewEdge cloud features a microservices architecture that can perform any combination of (or all) security functions as a single-pass architecture. The microservices design leverages containerization to enable rapid addition or scale out of specific microservices as desired. This architecture allows Netskope to offer enterprises complete network protection at wire speed, with unified policy and simplified operations.

Netskope Advantages of Cloud Ownership

Netskope has a strong background in CASB, which is an increasingly data security-oriented practice. While early CASB solutions provided visibility and access control for cloud applications, IT buyers are now expecting data security capabilities such as data loss prevention (DLP). CASB also inherently requires a robust cloud presence to ensure that users can access cloud applications without interruption. Netskope quickly identified the need to build its own cloud to deliver a complete SSE portfolio that protects the user experience. This strategy provides Netskope with advantages such as:

- **True edge security:** Netskope is designed to perform security at its cloud edge, with all datacenters capable of compute, rather than access-only points of presence (PoPs). This reduces latency by performing processing in the nearest datacenter rather than centralized datacenters farther from end users.
- **Future proofing:** New services can be added by Netskope into its microservices-based single-pass architecture.
- **Routing/peering control:** Netskope uses traffic engineering and intelligent routing decisions to avoid public internet problems. Netskope peers directly with key web, cloud, and SaaS application providers such as Microsoft, AWS, Google, Salesforce, Akamai, ServiceNow, Meta, and Apple for low latency and optimal user experience.
- **Predictability:** Netskope doesn't rely on third-party cloud providers, which reduces the business risk of change, reduces the need for troubleshooting, and simplifies support.
- **Location:** Selection of ideal locations for datacenters is based on key factors that enable Netskope to maintain service levels in specific regions.
- **Uniformity:** Controlling infrastructure down to the hardware level ensures performance, uniformity, and reliability. This consistency has allowed Netskope to adopt a highly efficient "datacenter factory" approach to accelerate the cloud expansion process.

Challenges

Digital transformation is fraught with complexity, and the security transformation story is continually evolving. While the original definition of SASE includes SD-WAN, Netskope focused on building a robust cloud environment while partnering with best-of-breed SD-WAN providers. Furthermore, the hype around SASE has morphed the concept from a specific definition into a marketing checklist requirement, with dozens of security companies offering their version of SASE. These considerations will require Netskope to educate customers about its approach to SSE and SASE.

Shaping the Security Transformation Story

The Netskope approach has required time and money, and the company points to strong service-level agreements (SLAs) and third-party testing results as proof of NewEdge cloud's capabilities as an enterprise cloud security platform. Importantly, the NewEdge investment has delivered lessons learned. Netskope has streamlined the process of building its cloud, using automation to stand up new datacenters rapidly. This has driven rapid expansion of NewEdge cloud and aggressive plans for future development. Ultimately, Netskope is well positioned to shape the direction of the security transformation journey with a focus on enterprise data protection, a single-pass architecture of SSE services, and a foundation in performance.

Conclusion

Businesses must embrace digital transformation to remain competitive. However, new technologies and business practices have also introduced previously unimagined threat vectors. Digital transformation presents a new opportunity to address legacy security challenges, including the "human factor." Overall, a modernized security approach can unlock benefits of stronger security and business efficiencies.

Organizations can adopt new and emerging business practices while minimizing business risk. But user experience and network performance are critical linchpins for success.

Ultimately, true modernization of security will require a fundamental reassessment of how networking can impact security objectives. If security is done well, organizations can adopt new and emerging business practices and use cases while minimizing or reducing business risk and rejecting legacy trade-offs between security and performance.

About the Analyst

Christopher Rodriguez, *Research Director, Security and Trust*

Christopher Rodriguez is a Research Director in IDC's Security and Trust research practice focused on the products designed to protect critical enterprise applications and network infrastructure.

MESSAGE FROM THE SPONSOR

More About 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. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements. Learn how Netskope helps customers be ready for anything on their SASE journey, visit www.netskope.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com