



Remote Connectivity Platforms Enable Secure and Resilient Business Operations

JUNE 2023

Author:
Romain Fouchereau

An IDC InfoBrief, Sponsored by



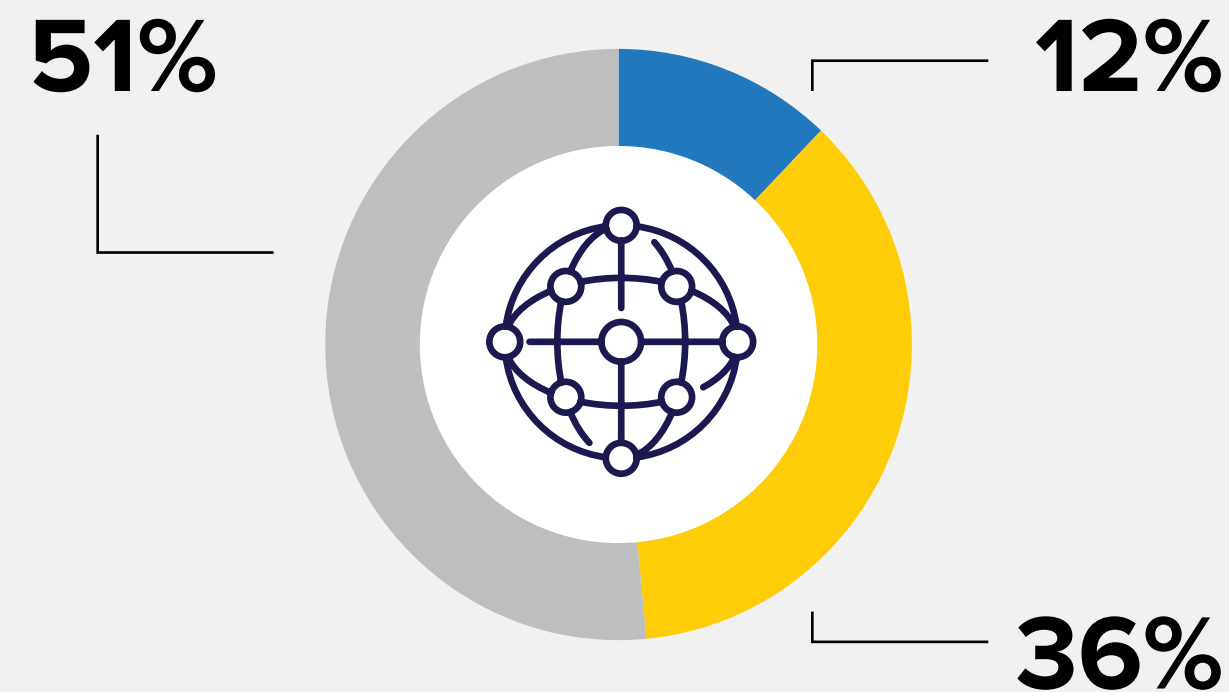
In this InfoBrief

Executive Summary	3
Market Drivers: Digital Strategies Have Disrupted Business and Workplace Structures	4
The Cybersecurity Reality	5
Organizations Face Many Challenges: Navigating Through the Storms of Disruption	6
Deploying Secure Remote Connectivity for Agile and Productive Operations	7
Achieving a Robust Cybersecurity Posture to Drive Business Outcomes	8
From Remote Access to Secure Remote Connectivity	9
Get the Most From Your Connectivity Platform With Extended Remote Management Capabilities	10
Remote Connectivity Platform is a Crucial Component of the Security Ecosystem of Products and Solutions	11
Essential Guidance: The Benefits of Adopting a Secure Remote Connectivity Platform	12
TeamViewer: Message From the Sponsor	13

Executive Summary

Digital-First Adoption

To what extent do you think your organization is a digital business?



87% of enterprises have adopted digital-first strategies or are in the process of transforming their businesses to become more digital, with 36% adopting it as a priority across the entire organization, acknowledging that we are now in a digital business era.

- To a large degree:** we have a digital-first strategy, and digital technologies have been deployed at scale
- Somewhat:** we have a digital strategy and are in the process of transforming the business
- Not at all:** we are still figuring out how to transform our business

Security and Remote Access

technologies are viewed as some of the most challenging to integrate into new project deployments and initiatives, requiring significant changes to both operating models and organization models, with:



29%

of the integration difficulties attributed to Security (including data and systems security)



29%

attributed to Remote Access and collaboration (including video/audio, file/app access, and cloud storage)

Secure Remote Connectivity



Digital transformation and cloud-first strategies mean that connectivity has expanded beyond the traditional perimeter to enable access for employees, customers, and partners from anywhere and at any time. Furthermore, the shift to a hybrid workforce has led IT teams to depend heavily on remote access and control solutions.

Deploying a secure remote connectivity solution will make work and teams more flexible and organizations more agile and competitive in the marketplace.

Digital Strategies Have Disrupted Business and Workplace Structures

Digital transformation and hybrid work models have forced businesses to innovate to adapt and to demonstrate their ability to grow and thrive in new business environments. Businesses have changed their workplace structures to adapt to the extended enterprise, moving beyond the traditional enterprise perimeter to address new imperatives such as cloud, remote users, applications, and IoT/OT use cases.



Cloud architecture adoption/investment

Planned investment in technologies aims to enhance enterprise value, with 28% of the investment allocated to infrastructure, including cloud

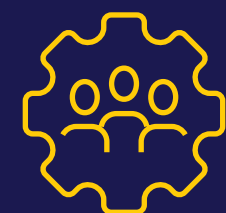
Source: Future Enterprise Resiliency & Spending Survey - Wave 7, IDC, August 2022, N=829



Hybrid work and work from anywhere

To support a hybrid work model, 36% of organizations deployed remote support software in their infrastructure

Source: Future Enterprise Resiliency & Spending Survey - Wave 6, IDC, July 2022 n=816



Proliferation of devices, complexity of IT applications and user management

Enterprise applications are key investment areas for 85% of organizations

Source: Future Enterprise Resiliency & Spending Survey — Wave 1, IDC, February 2022 N =798



IoT and the convergence of IT and OT


36% of organizations cited secure remote access as a critical cybersecurity issue in their organization when it comes to the integration of IT and OT

Source: IDC EMEA, European IT Security Survey, 2022 n=222



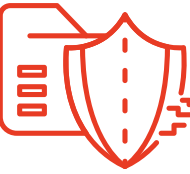
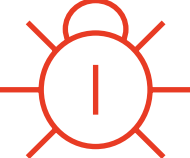




The Cybersecurity Reality







The combination of the current threat landscape and the enormous digital transformation that has taken place over the past few years, together with the shift to digital-first business models, means that protecting the network and ensuring continuous operational capability has become a priority.

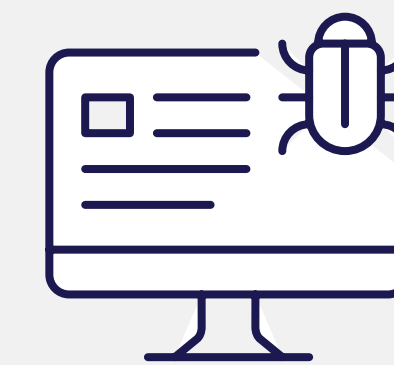
 **50%** of organizations have experienced an increase in attacks in the past 12 months

Diversity of threats

- | | |
|---|--|
|  SQL injection |  Spyware |
|  Phishing |  Zero-day attacks |
|  Supply chain attacks |  Fileless |
|  Ransomware |  Man-in-the-middle |

-  **Expansion of attack surface**
-  **Legacy systems**
-  **Shadow IT**
-  **IoT/OT**
-  **Data privacy**
-  **Regulatory compliance**

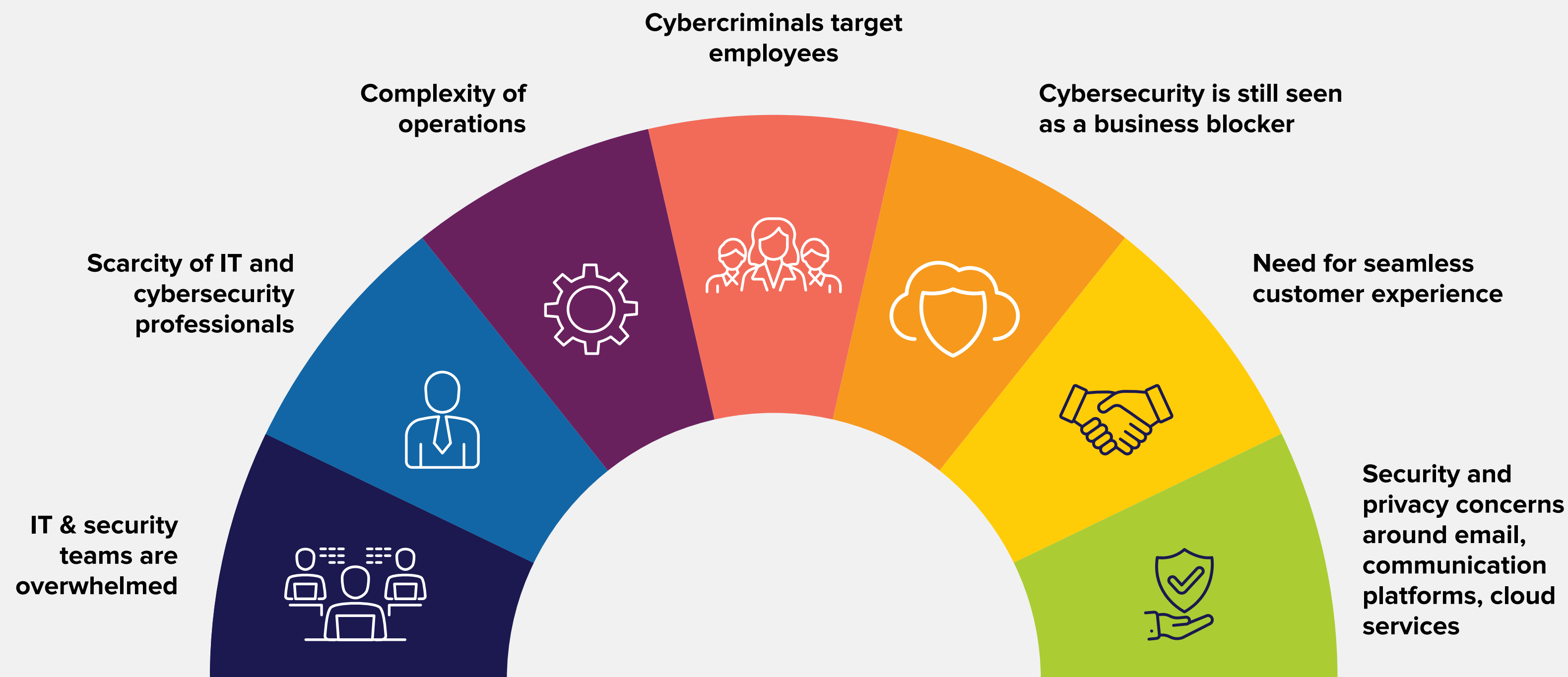


Cyberattacks are very frequent, and each one can result in extremely high cost and disruption. This affects company finances but also brand

image and data confidentiality. The volume and variety of threats facing our organizations continues to reach new heights.

Organizations need a seamless support experience across the value chain. Remote connectivity platforms are the connectivity tissue that can enable companies to ensure their operations remain agile, their employees remain productive, and business thrives in a hypercompetitive marketplace under challenging market conditions.

Organizations Face Many Challenges: Navigating Through the Storms of Disruption



Concerns around security and privacy are often the main challenge for strategic innovation and the adoption of new technologies, resulting in a delay in implementation. For example, the move towards cloud strategies and market demand has shifted perceptions: **95% of organizations now see cloud environments as more secure or as secure** as on-premises deployments.

Technology goes from a stage of innovation to majority adoption and finally reaches maturity. Workforce and talent is more distributed, collaboration and digital workspace (as a concept) has matured, and security frameworks around these technologies are now implemented by design, creating a more robust security posture.

Deploying Secure Remote Connectivity for Agile and Productive Operations

81%

see connectivity programs as a top priority investment for their organization



36%

deployed remote support software to support a hybrid work model



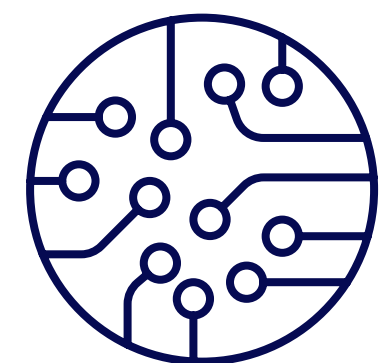
25%

are investing in remote access and collaboration technologies to improve enterprise value

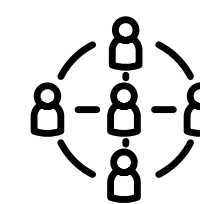


The work environment in connected enterprises is constantly evolving and organizations see the benefits they will achieve from investing in remote connectivity solutions. As enterprises are increasingly becoming complex ecosystems of identities (humans and machines), processes, and workflows, there is an urgency for the enablement of secure remote management.

Source: Future Enterprise Resiliency & Spending Survey - Wave 6, IDC, July 2022 n=816

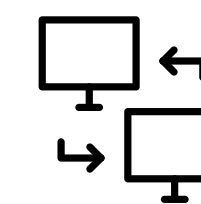


Top three technologies and services where organizations will increase investment to enable technology parity for all members of the workforce, regardless of their physical location:



1st

Content sharing and collaboration



2nd

Remote access to enterprise files and resources



3rd

Remote desktop management

Organizations Need a Robust 360-Degree Security Posture to Achieve Business Outcomes

Organizations strive to elevate their security posture. With better and more efficient security, the organization can deliver measurable business outcomes: boosting productivity, reducing costs, increasing trust in clients and partners, or reducing downtime.

Roadmap to enhance your organization's security posture



The new workforce challenge:

Gen Z employees will make up a third of the workforce by the end of the decade. They are interested in getting their work done without being slowed down or delayed because of technical issues. **Remote connectivity delivered in a secure manner at scale** becomes of paramount importance for organizations wanting to retain their qualified workforce inhouse.

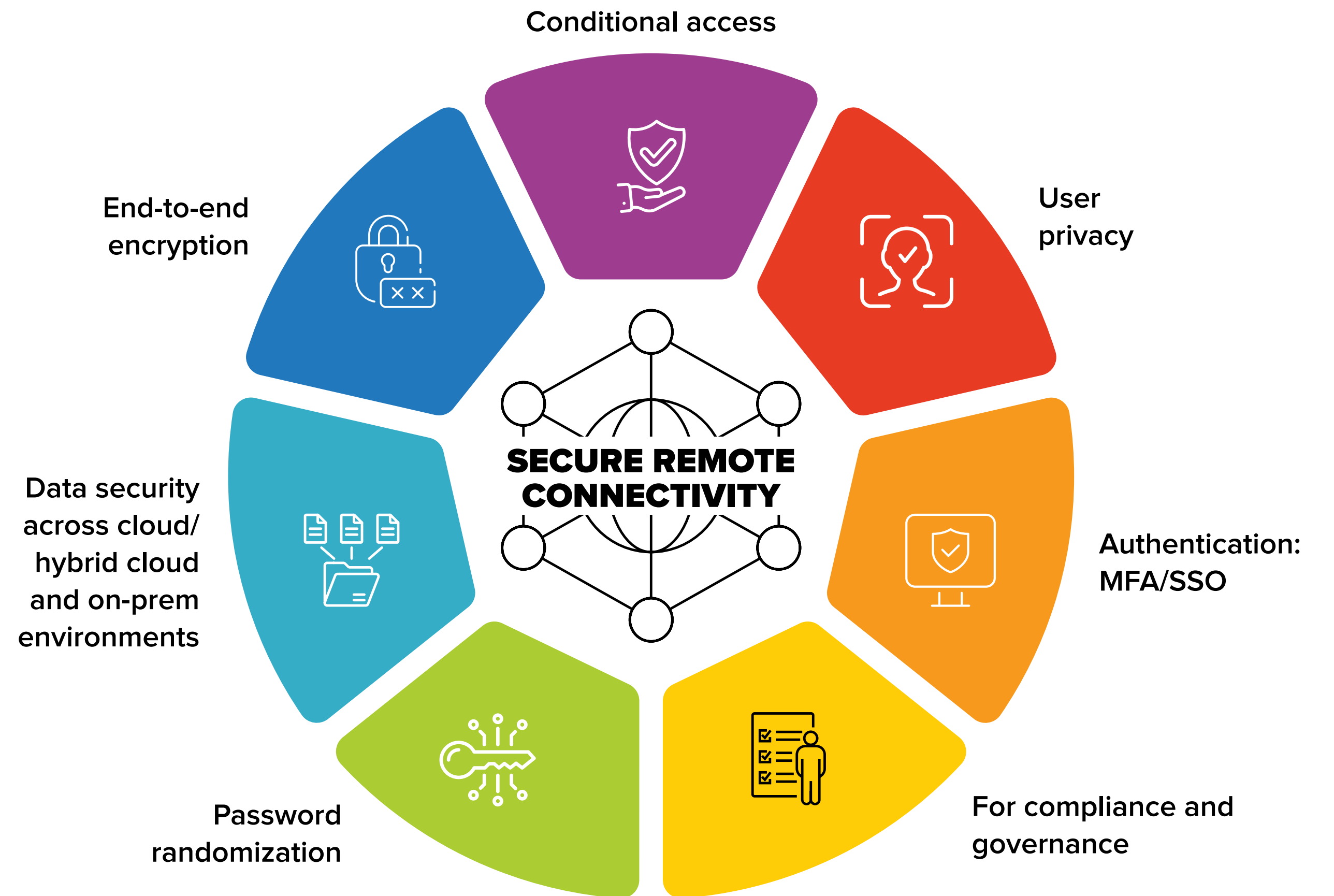


Work happens where the employee is, whether they are remote, mobile, in the office, at home or on the move. Employees prefer flexibility, and businesses want agility. Both sides favor systems that remove some of the operational complexity. Employees want a seamless and transparent experience when it comes to cybersecurity measures and are not interested in solving issues that are best handled by a support agent or a technician.

From Remote Access to Secure Remote Connectivity

Deploying a secure remote connectivity platform enables organizations to manage interactions and communications across personnel, systems, processes, and workflows. **These sessions must be carried out in a secure and privacy-conscious environment**, where only the intended actors can share and access content.

It is crucial to select a solution that has built-in security, privacy, and reporting capabilities such as:



Get the Most From Your Connectivity Platform With Extended Remote Management Capabilities

Remote management capabilities from a single dashboard enables organizations to get more visibility from devices and proactively keep their IT infrastructure healthy, stable, and secure. Remote connectivity ensures an improvement in efficiency and for IT organizations to centrally manage, monitor, track, patch, and protect computers, devices, and software, from a secure, scalable platform.



Remote Device Monitoring to monitor all critical aspects of devices, get alerted, reduce downtime, and anticipate potential issues with increased speed



Patch Management for automatic vulnerability detection and patching of outdated software, OS, and third-party applications



Asset Management to gain visibility and track IT systems and assets from a single dashboard



Endpoint Protection with partnership integration in the platform to protect users from malware such as ransomware and detect and remediate zero-day threats

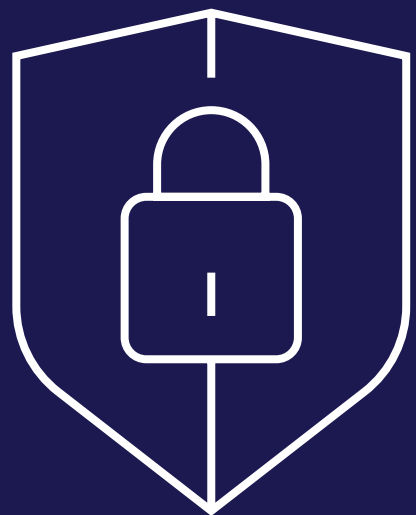


Deploy and use a network-agnostic solution, with end-to-end secure systems that bring a **more reliant connectivity than VPN** for remote access use cases

Deploying a Remote Connectivity Platform is a Crucial Component of the Security Ecosystem of Products and Solutions

Remote connectivity and remote infrastructure management platforms have a strong role to play in the security ecosystem. They offer a built-in range of security and monitoring functionalities from two-factor-authentication, to granular access control, to individual allow-and-block lists or detection of suspicious activities.

To further enhance the security posture of the organization and the remote office worker, the connectivity platform can become the place to deliver security capabilities, such as endpoint protection platforms (EPP) and endpoint detection and response (EDR), or firewall that comes integrated in the platform to deliver security operational excellence.



In the context of future of work programs, **60% of organizations are planning to deploy further network security** (access control, virus and antivirus software, application security, network analytics, VPNs, etc.) in the next 18 months.

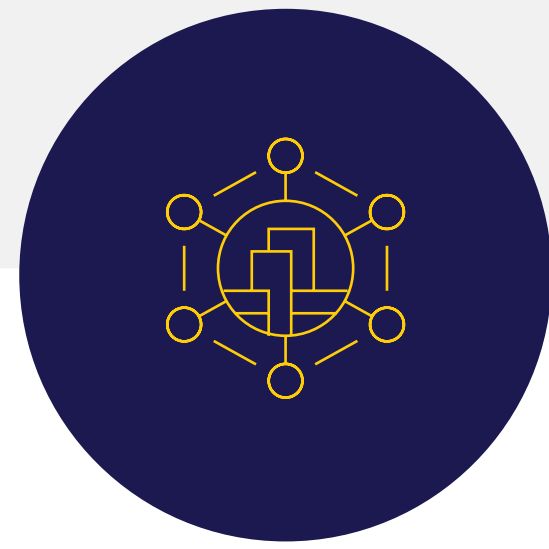


Remote connectivity is a way to accelerate the resolution of end-user issues while ensuring the support experience is secure and focused on privacy.

Having a dedicated and direct support channel (that doesn't require an end user's input, such as a chat bot, IM, or telephone call) leveraging remote connectivity can reduce the downtime an end user working remotely or on the move can face and might need support with.

Essential Guidance

The benefits of adopting a Secure Remote Connectivity Platform



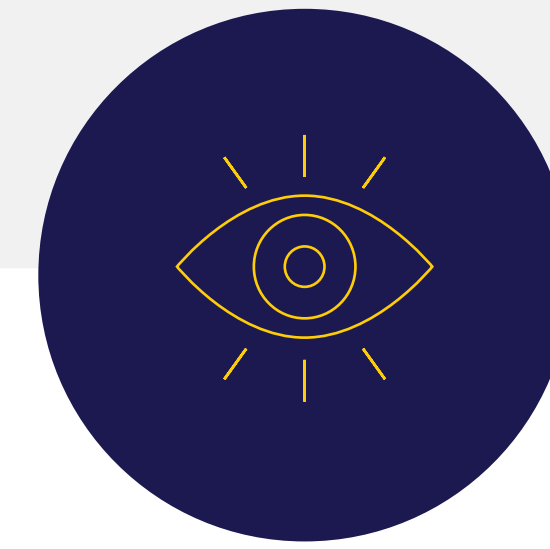
Increase the overall security posture of your organization



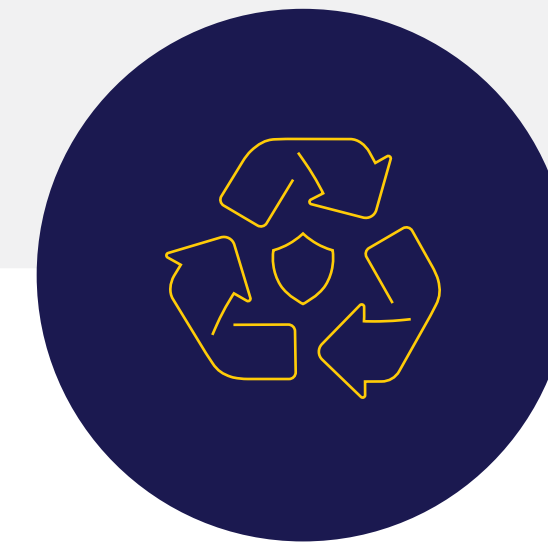
Enable hybrid workforce programs



Simplify employee work experience for more efficiency



Improve visibility and better understand your assets on the network



Integrate with the security ecosystem

Message From the Sponsor

As a global technology company, TeamViewer offers a secure remote connectivity platform to access, control, manage, monitor, and support any device — across platforms — from anywhere. With more than 630,000 customers, TeamViewer is free for private, non-commercial use and has been installed on more than 2.5 billion devices.

TeamViewer continuously innovates in the fields of Remote Connectivity, Augmented Reality, Internet of Things, and Digital Customer Engagement, enabling companies from all industries to digitally transform their business-critical processes through seamless connectivity.

Founded in 2005, and headquartered in Göppingen, Germany, TeamViewer is a publicly held company with more than 1,400 global employees. TeamViewer SE (TMV) is listed at the Frankfurt Stock Exchange and belongs to the MDAX.

Learn more:

<https://www.teamviewer.com/>



About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data and marketing services company.



This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

© 2023 IDC Research, Inc. IDC materials are licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.



IDC UK

5th Floor, Ealing Cross, 85 Uxbridge Road, London, W5 5TH, United Kingdom
T 44.208.987.7100



© 2023 IDC Research, Inc. IDC materials are licensed [for external use](#), and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

[Privacy Policy](#) | [CCPA](#)