The bridge to possible

2021 Global Networking Trends Report

Business Resilience Special Edition: See the five trends driving agility and resilience in times of disruption.

Contents

An introduction – Resilience

Introduction: From business continuance to business resilience

Neither as individuals nor as businesses were we anticipating or prepared for a global, long-term disruption like COVID-19. Practically overnight, entire workforces began working remotely, while some businesses scrambled to push their goods and services online and others shifted strategic supply chains to new suppliers and geographies.

Understandably, the pandemic has been a wake-up call for every nation, municipality, and organization. But what has changed? After all, it's not the first predicament companies have faced; 7 out of 10 organizations experienced at least one severe crisis in the last 5 years, and 95% are convinced it won't be their last.[1]

Organizations experienced at least one servere crisis in the last 5 years.

Source: "PwC: Global Crisis Survey 2019"

Human-caused disruptions such as cyber attacks, regulatory mandates, and social unrest have become an increasingly common part of our landscape. Globally, we are experiencing the harsh impacts of hurricanes, wildfires, floods, and other **natural disruptions** at an increasing rate and regularity.

Successfully navigating future disruptions requires IT leaders to adopt a new mindset. One that has a renewed emphasis on the IT agility required to achieve **business resilience**, rather than the more prescriptive and reactive approach that has been the foundation of traditional **business continuity** planning**.** Different from today's business continuity efforts, business resilience positions organizations to prepare for even the unexpected.

[1] PwC, "PwC's Global Crisis Survey 2019."

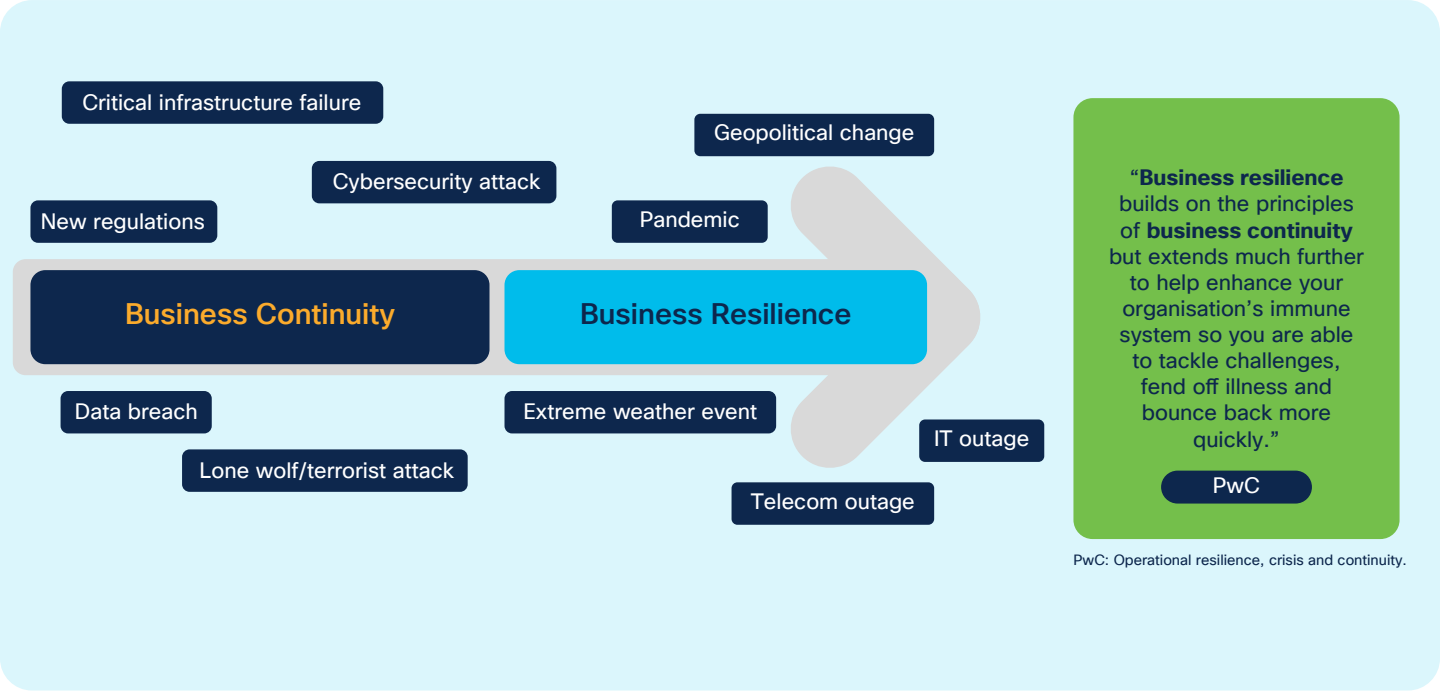
Business continuity vs. Business resilience

Business continuity: The capability of an organization to continue the delivery of products or services at acceptable predefined levels following a disruption.*

Business resilience: The ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper.**

* International Organization for Standardization, "Security and Resilience-Vocabulary", ISO 22300-2018

** International Organization for Standardization, "Security and resilience - Organizational resilience - Principles and attributes", ISO 22316-2017



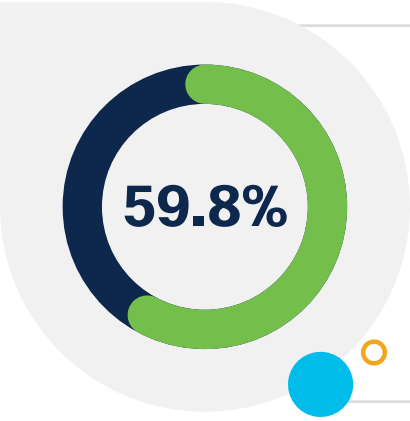
PwC: Operational resilience, crisis and continuity.

Figure 1. From business continuity to business resilience

Five networking trends

The network: 5 trends for enabling business resilience

Vital business processes are dependent on an increasingly complex web of digital technologies that provide the foundation for achieving organizational resilience.



A majority of business continuance professionals (59.8%) rate IT resilience as the most significant factor in responding to the current pandemic.

Source: BCI, "The Future of Business Continuity and Resilience"

As the sole platform that binds, protects, and enables an increasingly dynamic and distributed set of users and devices and increasingly disaggregated and dispersed applications and workloads, the network plays a central role in helping organizations build their resilience.

In other words, network resilience that maintains network connectivity and uptime is no longer enough. Companies need the resilience enabled by an advanced network platform that can respond quickly to any circumstances, enable new operating models and services, integrate with IT processes, and safeguard their employees, core activities, customers, and brand. Actually, this is the same advanced network required to support digital transformation initiatives.

Network resilience	vs.	Business resilience networking
Network resilience: The ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation of a given communications network, based on prepared facilities.*		**Business resilience networking:** Networking designed to enable organizations to respond rapidly, securely, and effectively in the face of expected or unexpected disruptions.

* International Telecommunication Union, "Requirements for Network Resilience and Recovery."

Building agility and resilience for workforce, workplace, workload, and operations

We've chosen to highlight five trends that networking leaders should consider as part of their efforts to support their organization's resiliency plans. They relate to enhancing the resilience of four key spheres: **workforce, workplace, workload,** and **IT operations.**

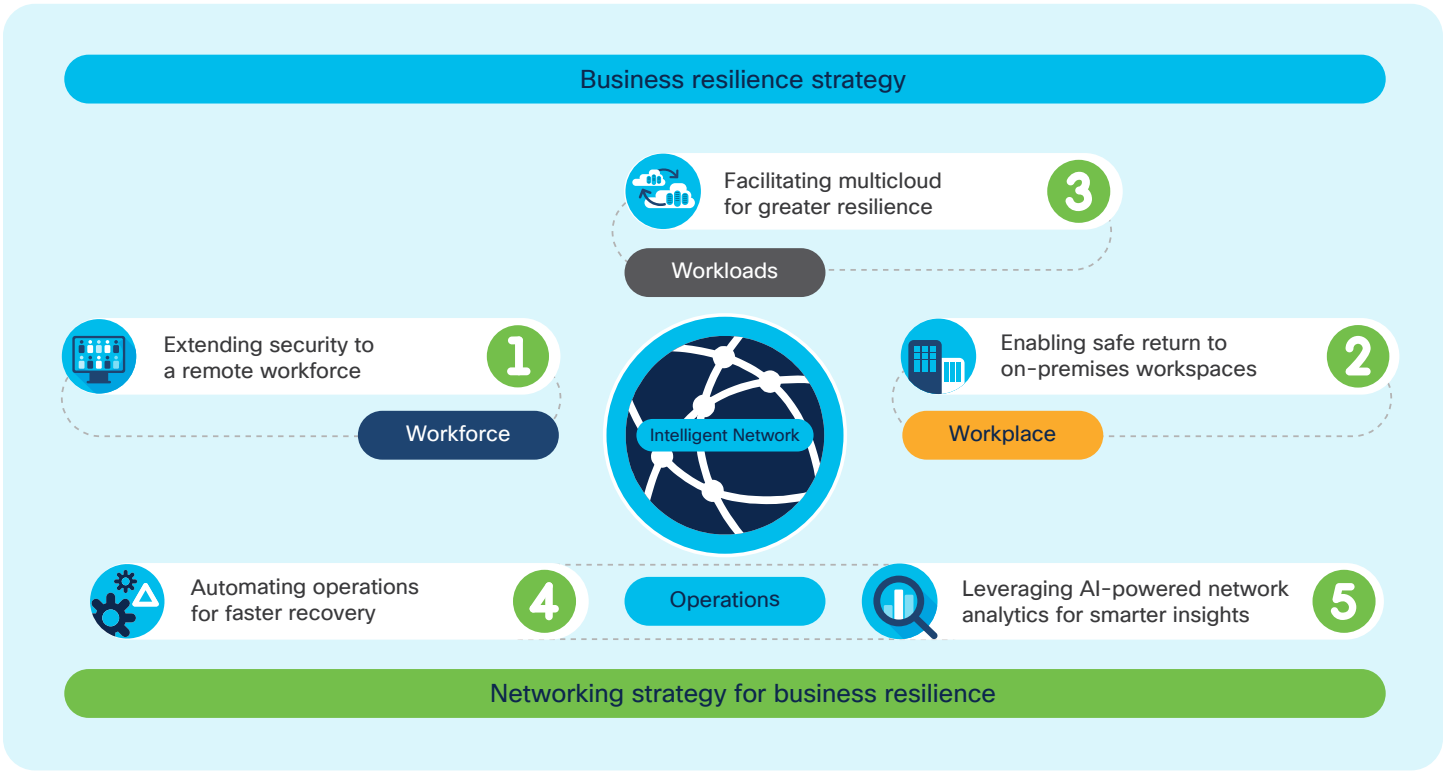
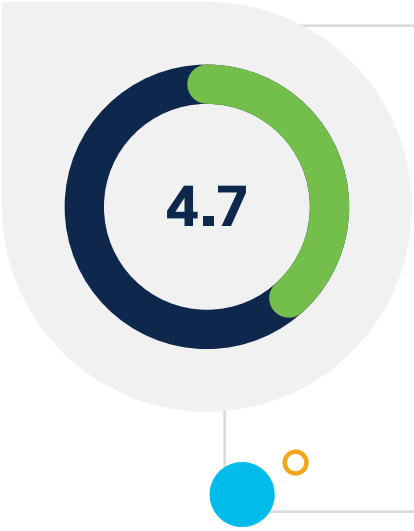


Figure 2. Network foundation for workforce, workplace, workload and operational resilience

Workforce – Remote, Secure

Trend #1: Workforce – Extending security to a remote workforce

Most organizations are coming to the realization that new, more flexible approaches to work will become a permanent reality for their employees.



An average of 4.7 times more employees are working from home now compared to before the pandemic. Many IT teams struggled with scaling to cope with the sudden demand.

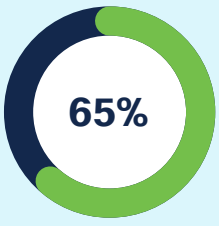
Source: Freeform Dynamics, "A New Perspective on the Modern Workplace," report sponsored by Cisco, July 2020

As a result, IT is faced with a new set of business requirements:

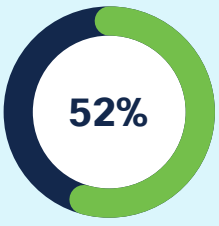
- Empowering workers to be productive and collaborative from anywhere
- Optimizing IT performance, cost, and security for each worker
- Extending enterprise-class IT operations and governance to the home

But meeting those requirements has its own challenges. In particular, remote worker security, as well as end-user behavior, continue to be ongoing concerns and challenges for the majority of IT organizations.

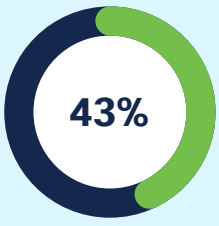
Top 4 IT challenges for enabling remote workers:



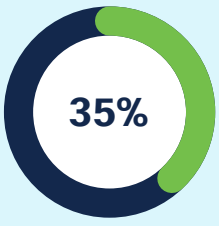
Security (65%)



End-user behavior (52%)



Application performance (43%)



IT operations (35%)[2]

[2] "2020 Cisco Business Resilience Networking Survey"

When using personal devices and connections to access corporate applications and data, remote workers are particularly vulnerable to cybersecurity attacks. Many circumvent the VPN and connect directly to services and applications in the public cloud, which remains the most difficult environment to defend.[3]

Network considerations: In enabling secure work-from-home models at scale, IT teams should adopt some or all of the following approaches:

- **Scale VPNs to protect remote workers:** Enterprise VPNs continue to deliver one of the most effective and rapid ways to extend enterprise-level control and protection to remote workers.
- **Use multifactor authentication (MFA) to protect applications:** MFA, which verifies each user's identity before allowing them on the network or access to sensitive applications and data, is critical for protecting the organization.
- **Deploy a secure access services edge (SASE) to help ensure protection for multicloud access:** Cloud-based security and SASE help defend against Internet-based threats, regardless of the connection, user device, or cloud environment.

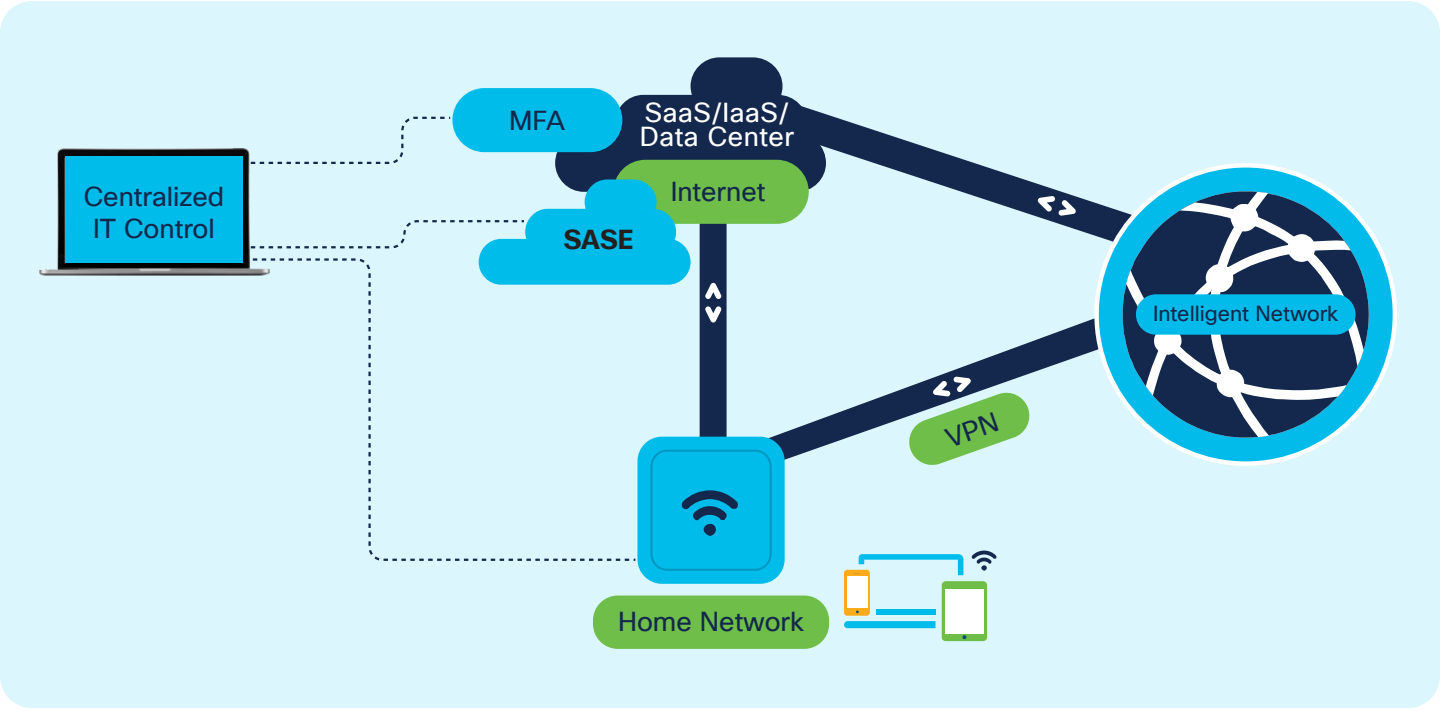


Figure 3. Secure remote workforce with VPN, MFA and SASE

Find out more about connecting and securing your remote workforce

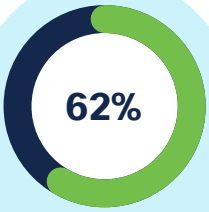
[3] Cisco Umbrella, "2019 Cybersecurity Trends."

Workplace – Safe, Trusted

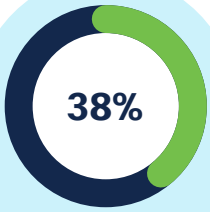
Trend #2: Workplace – Enabling safe return to on-premises workspaces

While many questions remain, it's clear that workplaces and workspaces will evolve in the wake of the current pandemic. Countless companies are in the process of boosting existing services such as video conferencing and location-based Wi-Fi. Others are deploying new services and safeguards, such as physical distance monitoring, proximity reporting, increased workplace automation, and even robots that support human productivity and communication.

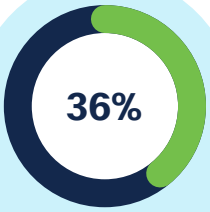
How networking teams are preparing for a safe return to the workplace



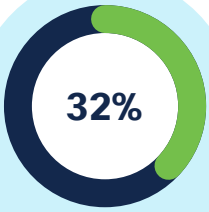
62% are deploying more pervasive video conferencing.



38% are implementing social density insights to ensure safe working conditions.



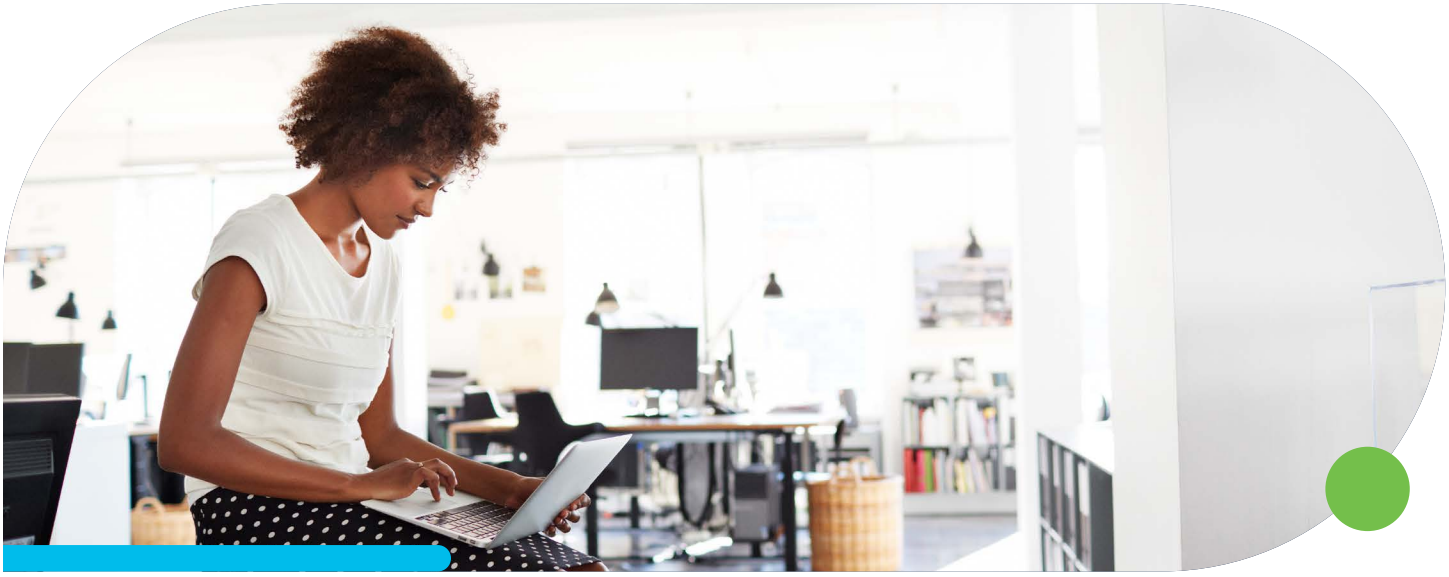
36% are focused on remote NetOps and help desk.



32% are deploying proximity reporting to maintain social distancing.

30% are establishing new workplace safety measures such as thermal cameras, advanced air filtration, and touchless elevator controls.

Source: "2020 Cisco Business Resilience Networking Survey"



Network considerations: A modern, agile network is a critical engine that facilitates the safe and seamless reintroduction of workers to the premises.

- **Stress test the network:** In many cases the network has been out of action for a number of weeks. Don't take for granted that it can still deliver the necessary wired and wireless services.
- **Automate identity-based secure access:** Organizations need the ability to consistently manage, secure, and segment user and device onboarding and access to services, whether they're connecting from on-premises, home, or public networks.
- **Enhance the safety of employees and customers via location-based analytics:** Enable workplace monitoring, alerts, and insights to help protect the health and safety of employees, partners, guests, and customers by leveraging existing Wi-Fi networks.

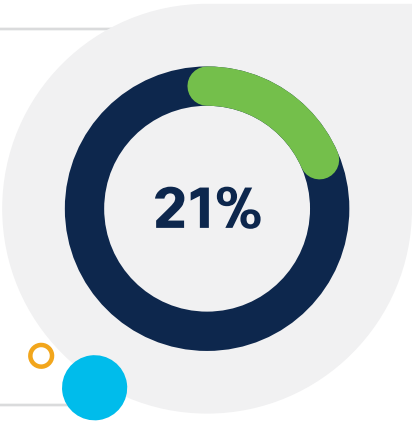
Find out more about creating a safe workplace environment

Workload – Multicloud

Trend #3: Workload – Facilitating multicloud for greater resilience

IT leaders are using cloud services as a means of improving business resilience in the wake of the global pandemic. This includes increased adoption of a multicloud model – distributing applications, workloads, and data across on-premises data centers and public cloud providers – to reduce costs, increase flexibility, and protect against and spread the risk of catastrophic failures.

> 21% of organizations are moving additional workloads to the public cloud due to pandemic-related CapEx issues."
>
> IDC, "COVID-19 Impact Survey, Wave 5," 2020



Network considerations: To ensure a consistent experience for users and DevOps teams, organizations need a proactive, multicloud networking strategy that aligns the network with cloud, security, and IT operations' priorities.

Successful multicloud networking strategies are based on three main pillars:

- **Workload:** Adopt a cloud operating model to simplify the policies, security, and management of workloads and services across on-premises data centers, multiple disparate clouds, and other computing environments.
- **Access:** Adopt SD-WAN and SASE approaches to help ensure consistently secure multicloud (including SaaS) access for users and devices across corporate and public networks from the campus, branch, or home, or on the road.
- **Security:** Reduce the risk associated with users, devices, and applications distributed across multiple clouds and other computing environments.

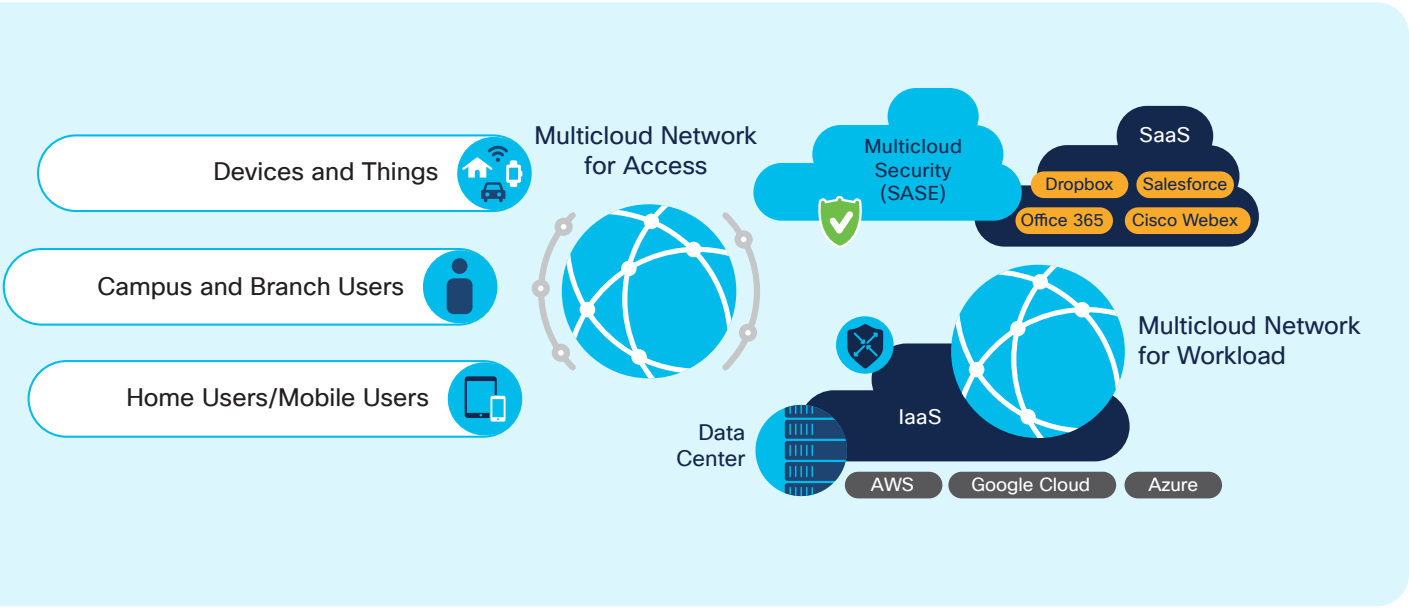


Figure 4. Multicloud network: workload, access and security

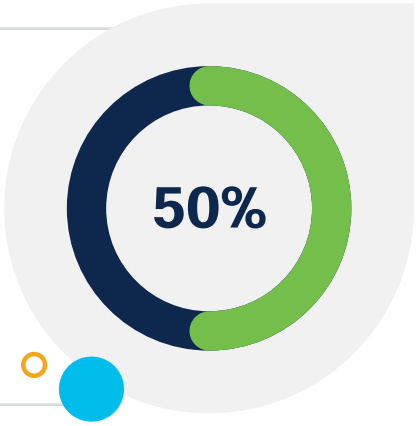
Find out more about building a secure and effective multicloud networking strategy

Operations – Automated

Trend #4: Operations – Automating operations for faster recovery

The explosion in the numbers of dispersed remote workers isn't the only thing placing an extraordinary strain on today's NetOps teams. The pandemic has also spurred unprecedented levels of steep fluctuations in client counts, application traffic patterns, and new use cases such as e-learning, video conferencing, virtual events, remote care, process automation, and other network-dependent services.

> 50% prioritize network automation for addressing disruptions today.
>
> 2020 Cisco Business Resilience Networking Survey



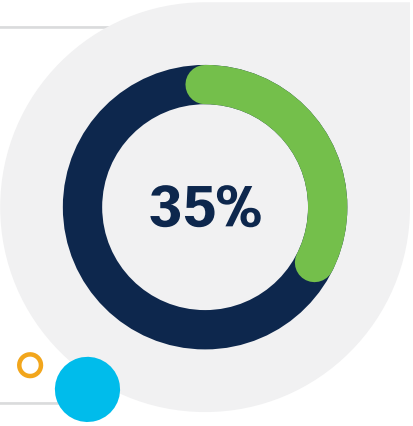
So it's no surprise that today, half of network professionals recognize network automation as a critical requirement for ensuring continued service and performance during a disruption.

Source: Cisco, 2020 Global Networking Trends Report

Network considerations: NetOps teams can achieve continuous improvement and rapidly respond to growing disruptions and threats by taking a step-by-step approach:

- **Automate repetitive administrative tasks** such as network provisioning, configuration, and image management to reduce the administrative burden and improve compliance in each domain.
- **Automate network access, onboarding, and segmentation** to protect groups of distributed users and things and mitigate the spread of cybersecurity attacks.
- **Automate network policy within the enterprise data center** with application-centric segmentation that protects apps and data and follows the workload.
- **Automate policy beyond the data center to the cloud** with a cloud operating model that delivers consistent application policy across on-premises and hybrid cloud environments.
- **Automate end-to end multidomain policy-based segmentation** to establish a consistent, end-to-end zero-trust access model from users and things to workloads.

> 35% plan for their networks to be intent-based across all domains by 2022–up from just 4% in 2019.
>
> Cisco, 2020 Global Networking Trends Report



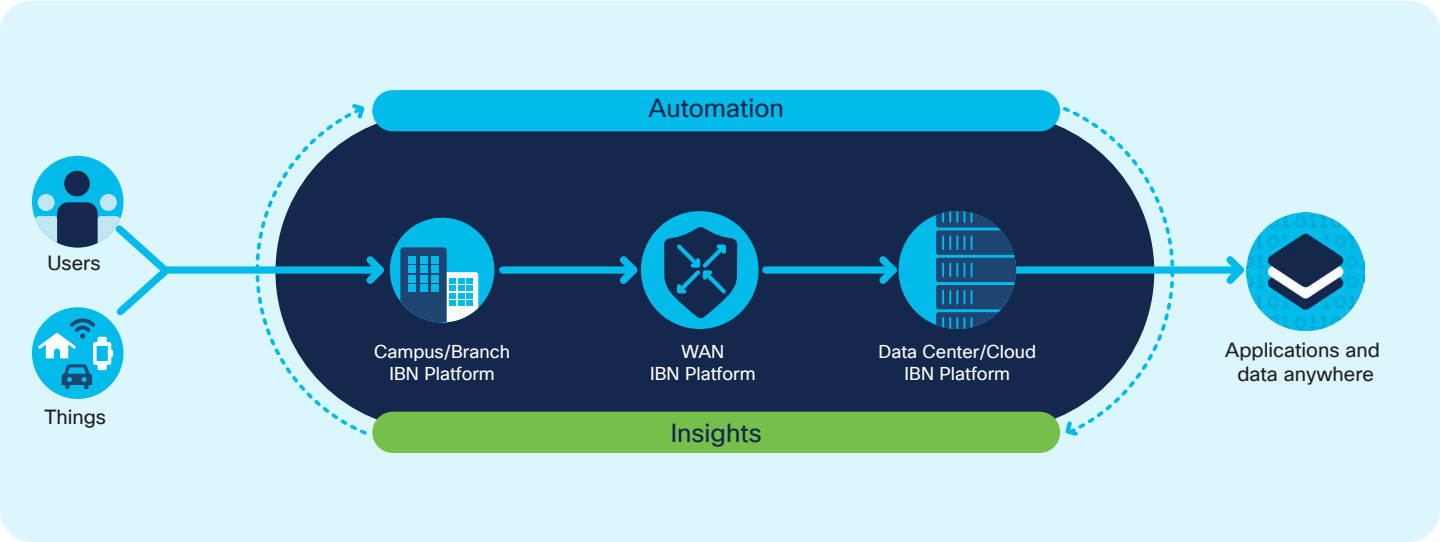


Figure 5. Automation and insights from user to workload anywhere

Find out how to automate policy across multiple network domains

Operations – AI-enabled

Trend #5: Operations – Leveraging AI-powered network analytics for smarter insights

Managing the complexity and scale of modern networks and the resulting deluge of events and issues bombarding multiple disparate monitoring platforms can be both overwhelming and ineffective, especially when a disruption hits.

> 4,400: Average number of wireless-related monthly events on an enterprise network.*
>
> Source: Cisco telemetry: Cisco DNA Center, 2020

* Based on over 600 enterprise networks. Events include onboarding failures/times, radio throughput, and DHCP response time/failures. These event numbers have already been reduced using AI-enabled dynamic baselining.

Clearly NetOps teams need the help of advanced analytics to make smart and timely remediation decisions.

By using AI-enabled network analytics and machine learning techniques, NetOps teams are achieving a much more manageable set of issues they can take action on.

> At a global level, Cisco AI Network Analytics, an application within Cisco DNA Center, resolves 2.6 million monthly “events” into 15,080 actionable “issues” – a reduction of 99.4%.*
>
> Source: Cisco telemetry: Cisco DNA Center, 2020

* Based on over 700 enterprise networks, globally.

This reduction is allowing the teams to focus all their efforts on the things that really matter and that have the potential to cause negative business impact.

And this issue is no longer limited to the enterprise network. Now that the majority of networked transactions either emanate from or terminate outside of the traditional enterprise network, NetOps teams need visibility and analytics for the public networks they are connected to as well. This is especially important during periods of unusual stress, such as the recent pandemic.

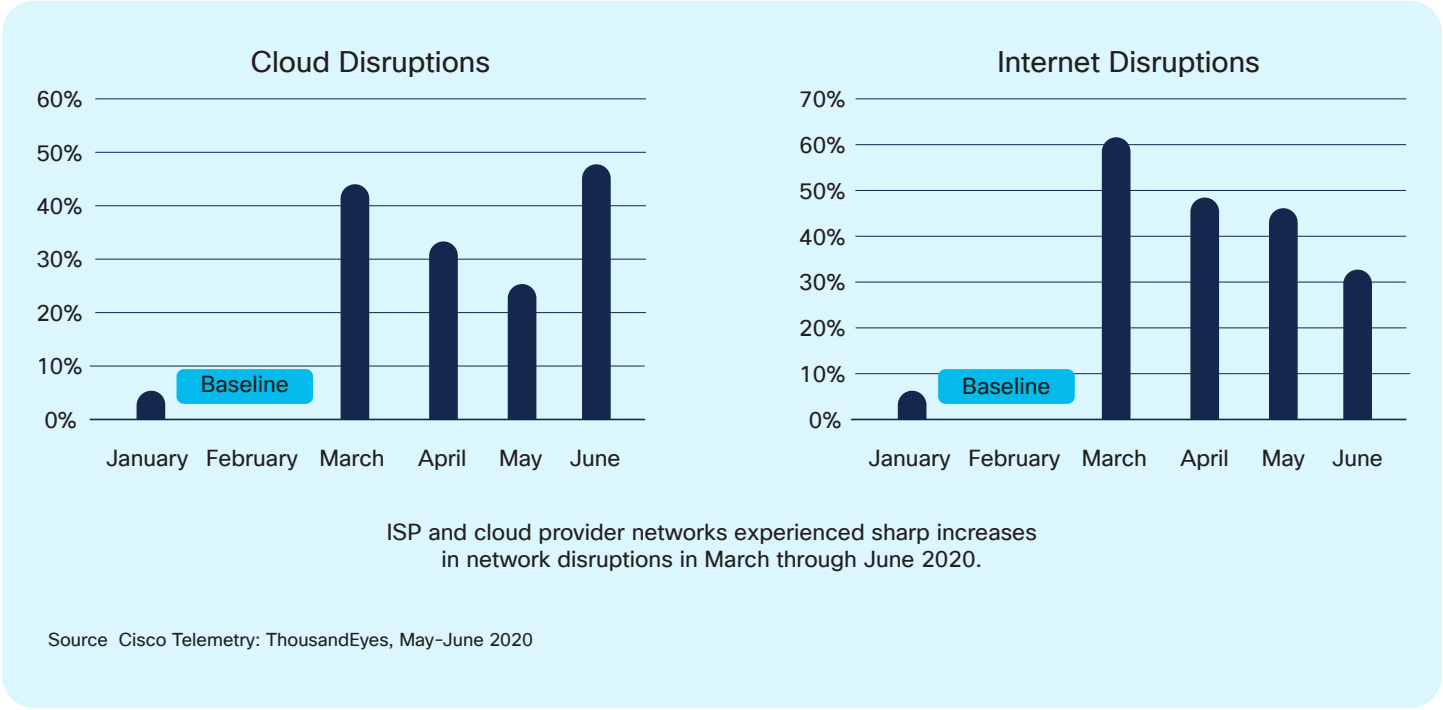
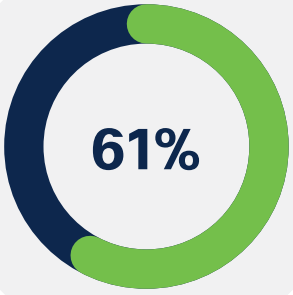


Figure 6. Cloud and Internet Service Disruption Increases During Pandemic

> Cisco ThousandEyes identified a 61% increase in the number of network disruptions across ISP networks and a 44% increase across cloud provider networks between February and March 2020.
>
> Cisco ThousandEyes, "Internet Performance Report: COVID-19 Impact Edition", 2020



Network considerations: To make sense of an event tsunami, NetOps teams should adopt AI-enabled network analytics and assurance systems to achieve:

- **More accurate detection:** Improve the accuracy of automated issue and anomaly detection within and across network domains.
- **Faster remediation:** Correlate events to detect and clearly describe the most likely root cause of issues and anomalies.
- **Automated policy management:** Identify devices, applications, and trends and offer recommended policy updates.
- **Fewer degradations:** Identify patterns and trends and provide contextual insights that accelerate proactive, corrective, and preventive action.
- **Peer intelligence:** Provide intelligence and analytics that help network administrators compare their network performance to global, industry, or regional benchmarks.

Find out how you can use AI-enabled insights to better manage your networks:

Network Insights for Data Center

In conclusion

Conclusion: Improving business resilience with an advanced network platform

Disruptive events will keep challenging us and our networks throughout our careers. It's time to rethink how your **network strategy** enables your business **resilience strategy** and prioritize the new network capabilities most necessary to stay ahead of the next big thing.

The automation and AI-enabled insights offered by intent-based networks provide a powerful platform to help you adapt to any circumstance. They deliver the agility, security, intelligence, and speed required to support resilience for:

- **Workforce:** Empowering workers with secure, enterprise-class performance and access to their applications while working from home, the office, and everywhere in between
- **Workplace:** Enabling employees to return safely to the office with Wi-Fi-enabled monitoring, alerts, and insights
- **Workload:** Facilitating multicloud resilience models and protecting data and applications wherever the workloads reside across public clouds, and on-premises data centers
- **Operations:** Automating end-to-end network policies and segmentation and simplifying administrative tasks while improving visibility, reducing alerts, and enabling faster remediation

In this next normal, it's all about having a network that can adapt to support whatever the future brings. As you think about your business resilience strategy, consider how your network can be a key enabler of that strategy.

For more information about business resiliency

Additional things you may be interested in

Business resiliency

Webinars

Cisco Digital Network Architecture (Cisco DNA)

C96-744303-00 11/20