



The bridge to possible

2024

Global Networking Trends Report

Networking strategies to advance
digital business



Welcome to the 2024 Global Networking Trends Report



Jonathan Davidson
Executive Vice President
and General Manager,
Cisco Networking

Throughout my 25+ years in the networking industry, one thing has remained consistent: the network becomes more important every year. Far from being a commodity, the network is inextricably linked with respondents' business strategies. This year's research shows more advanced network environments are linked to better results.

As an IT professional, you understand that factors like artificial intelligence (AI), cloud, hybrid work, containerised applications and Internet of Things (IoT) can accelerate innovation, unless complexity gets in the way. Ultimately, you're responsible for the quality of experiences delivered across the network. Efforts to deliver quality experiences are often thwarted by increasing network complexity, legacy approaches and mismatched skill sets.

In this report, we assess the networking challenges, IT and business priorities, architectural maturity and investment strategies of 2052 IT leaders and professionals across 10 industries globally. Our goal is to provide insights into areas driving network transformation. Across these trends, three themes stand out to me and often come up in my conversations with customers: the platform, security and AI.

- **The platform.** Adopting a centralised network management platform is transformational. This approach helps IT teams attain greater visibility, connectivity and security in a world of public clouds, private clouds and on-premises workloads.
- **Secure networking.** Cybersecurity tops the list of respondent concerns. Customers across every vertical believe that AI-generated insights will help them stay ahead of the expanding threat landscape. If it's connected, it must be protected.
- **For AI, with AI.** Organisations are modernising their infrastructures for AI workloads and more sustainable data centres. And with AI, they are building better networks, predicting failures and diagnosing problems.

The 2024 Global Networking Trends Report provides a critical perspective from the IT leaders who are tasked with ensuring the network delivers secure digital experiences for all. I hope you find it as informative and helpful as I have.



Jonathan Davidson

3

Contents

4 Overview

5 Architecture transformation

- Trend: Network Platform Adoption on the Rise
- Trend: Digital Experience Assurance for Greater Reliability and Consistency
- Trend: Reliance on Partner Ecosystems and Open API Integrations

11 Security convergence

- Trend: Network and Security Convergence Bridges Consistency Issues
- Trend: Secure Multi-Cloud Networking
- Trend: Cloud-Based Security Is Top Networking Investment Area

17 AI operations

- Trend: AI-Powered Operations to Improve Efficiency
- Trend: Data Governance and AI-Enabled Analytics for Predictive Assurance
- Trend: AI-Enabled Security to Mitigate Risk

22 Data centre at scale


- Trend: Data Centre Modernisation a Priority for Scaling AI Workloads
- Trend: Data Centre Operators Adopt AI and Platforms

26 Sustainability advancement

- Trend: IT-Led, Data-Driven Strategies for Sustainability
- Trend: Infrastructure Telemetry and Visibility Requirements are a Priority
- Trend: Planning for Improved Building Infrastructure Efficiencies and Experiences

32 Conclusion

33 Methodology

 **CISCO** The bridge to possible

©2024 Cisco and/or its affiliates. All rights reserved.

Overview

On the journey to more simple, secure, scalable and sustainable networks, the 2024 Global Networking Trends Report identified important advances in five strategic areas to help drive digital business.



Architecture transformation

A network platform, integrated partner ecosystem and digital experience assurance – enabled through advanced network telemetry and end-to-end visibility – are all becoming increasingly popular to simplify operations and drive digital resilience.



Security convergence

Converging network and security technologies and workflows are now a top priority and a best practice as security concerns expand with continued cloud adoption.



AI operations

Automation through an AI-enabled approach is a much-sought-after strategy to simplify and optimise operations, assure the digital experience and mitigate risk while strengthening security.



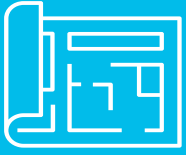
Data centre at scale

Data centre infrastructure modernisation is underway to meet AI workload and new application demands at scale while leveraging AI-native platforms to address increasing complexity.



Sustainability advancement

IT is looking to networking platform features to advance telemetry and visibility and build smart, sustainable buildings while advancing net-zero goals.



Architecture transformation

A **network platform** is an integrated system that combines software, policy and open APIs with an intuitive user interface, advanced telemetry and automation. It provides a centralised operator experience, end-to-end network management and an API-driven ecosystem that simplifies operations and enables digital experiences across one or more networking domains.

The evolution to an **AI-native network platform** equips IT teams with the continuous intelligence and automated control required to consistently deliver quality digital experiences.

IT leaders are still grappling with point solutions deployed during the pandemic that served time-sensitive needs but have left IT teams with an inefficient and complex infrastructure framework. Many are looking to be more efficient with an architectural approach that provides greater end-to-end visibility and control across all network domains.

42% of IT leaders and professionals say a network platform can greater support cross-domain management to unlock better performance, innovation and cost savings.



Trend

Network Platform Adoption on the Rise

Respondents acknowledge the growing need for the network to support their organisation's dynamic IT and business initiatives, spanning improvements in end-user experiences, network and security performance, and managing operational expenditures (OpEx). IT leaders and professionals recognise that a network platform can provide a more efficient and consistent architecture, allowing for simpler cross-domain integration and improved performance in these and other initiatives.

Today

According to the research, while one in five (21%) organisations surveyed are currently using multiple, separate management systems when managing their campus, branch, WAN, data centre and multi-cloud domains, 39% are currently leveraging a platform architecture across some networking domains. Survey respondents were strongly supportive of network platform adoption, given the alignment of benefits from that approach with the IT and business outcomes they are trying to achieve. Those outcomes include faster IT and business innovation (43%), improved network performance and security posture (40%) and cost savings (37%).

In addition to acknowledging the benefits of a network platform, respondents are also realising the importance of cloud-based management, with respondents saying 33% of their LAN, WAN and SD-WAN is currently cloud managed. When asked about the advantages of cloud management, respondents cited enhanced network security (45%), quicker network infrastructure deployments (41%) and faster access to new management features (39%).

"Organisations that take advantage of a platform approach, which can simplify management and enable advanced functionality, will be better positioned to win in the digital business era."¹

Brandon Butler, IDC Research Manager, Enterprise Networks



Two-year outlook

Adoption of the network platform is anticipated to increase, with nearly three-quarters (72%) of respondents expecting to leverage a platform architecture across one or more domains. Of those, 39% expect to scale the platform architecture across all networking domains, greatly simplifying network management and enabling a variety of business, operational, and technical benefits – from open API ecosystems to enhanced IT collaboration across functions, easier integrations and a rich pool of data. Data aggregated from telemetry across network domains provides an enterprise-wide view that can be used to generate insights from AI analytics, enhancing performance, experience, security, cost efficiency and sustainability.

72%

of IT leaders and professionals expect to have a platform architecture in place across one or more networking domains in the next two years.

 Read the [IDC white paper](#) on the network platform approach.



"The simplicity with the cloud-based platforms allows my team to show users possibilities beyond just troubleshooting with the network. We have the opportunity to be more innovative."

Jack Satterfield,
Chief Technology Officer,
Pima Community College



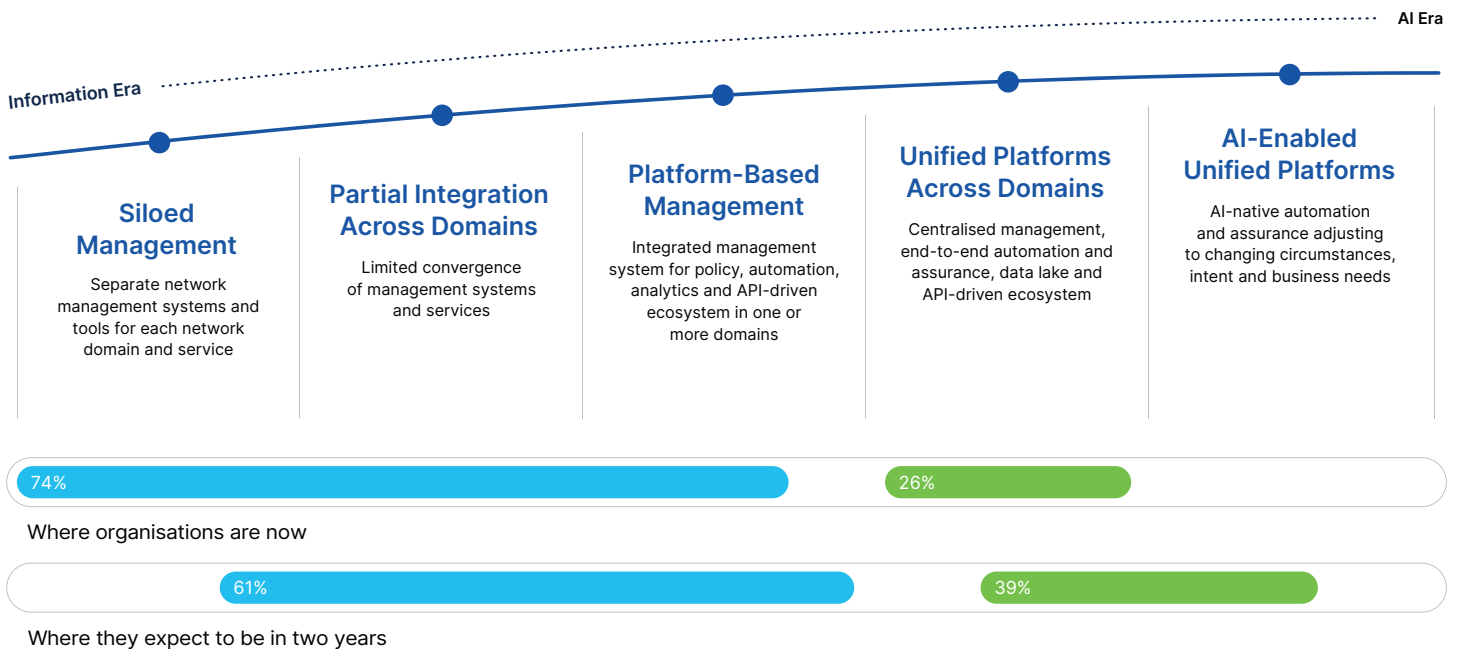


"Enriched with enterprise-wide data and guided by AI-driven insights and recommendations, a platform can deliver end-to-end visibility to inform and resolve potential performance and connectivity issues. Combined with an open and extensible developer ecosystem, IT professionals can integrate a platform deeply into their business workflows and accelerate time to value with automation."

Lawrence Huang, Senior Vice President and General Manager, Cisco Networking - Meraki & Wireless

Network architecture maturity status (today vs two-year outlook)

Network architecture refers to the enterprise network infrastructure design, life cycle management and governance across domains, including campus, branch, WAN, data centre, multi-cloud, industrial, etc.





Two-year outlook

Among all respondents, 75% plan to deploy tools that offer end-to-end visibility via a single console. Of those, 38% expect that their digital experience assurance will be AI-enabled and another 37% anticipate leveraging a single console to gain end-to-end visibility. An AI-native network platform that combines network datasets from different domains and uses artificial intelligence/machine learning (AI/ML) to analyse the data will help drive decisions that make network operations proactive and predictive instead of reactive.

75%

of organisations plan to gain end-to-end visibility via a single console to enable high-quality digital experiences within the next two years.

Trend

Digital Experience Assurance for Greater Reliability and Consistency

Digital experience assurance refers to the ability to provide consistently reliable experiences between users, devices, applications and services across all *owned* (data centre, campus and branch, WAN, and industrial networks) and *unowned* (internet, cloud provider, multi-cloud) domains. By correlating and contextualising data to provide continuous intelligence and automated corrective actions across the end-to-end network, IT teams can achieve digital resilience that assures always-on, quality experiences for employees, customers and the organisation overall.

Today

IT leaders are grounded in the principle that network experiences – for customers and employees alike – are an important driver for digital business success. However, as workforces, applications and services grow more distributed, visibility into the hops between network, cloud and internet domains has become less transparent. Many of these connections begin and end outside of the traditional corporate infrastructure. A pain point felt by over a third of respondents (35%) is a lack of visibility into complete network paths, including internet and cloud networks. Additionally, 41% said that service reliability to ensure predictable and consistent user experiences and application delivery needs significant improvement. Without it, their organisations cannot meet IT and business objectives.

The ability to provide an end-to-end approach to digital experience assurance across all owned and unowned network paths is critical to ensuring digital resilience. Yet, 39% of respondents said they currently have either limited visibility or full visibility using multiple consoles to monitor digital experiences between users, devices, applications and services.

"With how our network works, any small disruption to our operation can have a knock-on effect. It's vital that we assure our services from the very get-go."

Simon Challis, Senior Technology Manager, Platform Design, EasyJet

Trend

Reliance on Partner Ecosystems and Open API Integrations

With the need to rapidly create more sustainable IT infrastructure and buildings, IT will increasingly rely on extended partner ecosystems and platforms that enable integrations with open APIs.

Today

Currently one in five (21%) organisations in the survey have no API-driven network ecosystem integrations. Another 22% have limited IT integrations across disparate network domains.

Over a quarter (26%) said a top networking investment area over the next 12 months will be management platforms for simplified operations and API-enabled integrations. For 33%, the most important criteria when evaluating new networking investments is the ability to integrate the technology into the existing network. An extensible ecosystem with platforms that enable technology innovations through open APIs and partner integrations will better allow the network to drive IT and business success, said 29%.



Two-year outlook

A majority (64%) expect to have unified, API-driven integrations for IT and business innovation within the next two years, and 20% of this group anticipates deploying an intent-based, API-driven network. Intent-based, API-driven networks abstract low-level network complexities, allowing developers to build sustainable applications that can dynamically request and leverage network resources based on real-time requirements to promote efficient resource utilisation and reduce waste. For 40%, selecting partners to provide sustainability services is expected to lead to a significant, positive impact on their organisation's sustainability strategy.

64%

of respondents expect to have unified, API-driven integrations for IT and business innovation within the next two years.





Security convergence

"There is a certain amount of flexibility and agility that we need. But our main focus is really securing the network; understanding, deploying, establishing and managing a secure network architecture."

IT Director,
Multinational
European Bank

The continued expansion of the attack surface due to highly distributed workforces and applications has kept cybersecurity risk at the forefront of organisations' minds. Cybersecurity is the number-one concern impacting networking strategy, according to 40% of respondents. Cloud-based security management, along with the convergence of security and networking, are considered priorities for addressing the growing threat landscape.

40%

of IT leaders and professionals said cybersecurity is the number-one concern impacting their networking strategy.



Trend

Network and Security Convergence Bridges Consistency Issues

Organisations are prioritising the integration of networking and security domains and teams as both an IT and business imperative. They recognise that keeping networking and security tools, data, platforms and processes separate is no longer a viable option. Bridging capabilities and applying AI-powered analytical insights based on combined networking and security data delivers more reliable, optimised connectivity and stronger security across campus, branch, data centre, cloud and operational technology (OT) environments.

Today

In this year's survey, 42% of respondents said integrating networking and security is the area requiring the most improvement to meet IT and business objectives.

According to 44% of organisations surveyed, faster cybersecurity threat identification and response was the most important benefit expected from convergence of networking and security technologies, processes and tools. Sharing data and telemetry between networking and security domains was the second-ranked benefit for 29% of respondents, followed by providing consistent, secure access to multi-cloud applications from anywhere for 27% of respondents.

"Convergence is not merely a technical adjustment but a strategic imperative that necessitates a shift towards a powerful, unified IT framework that combines data, processes and human expertise to combat threats and deliver consistent experiences."

Omri Guelfand, Vice President, Product Management, SASE, Cisco




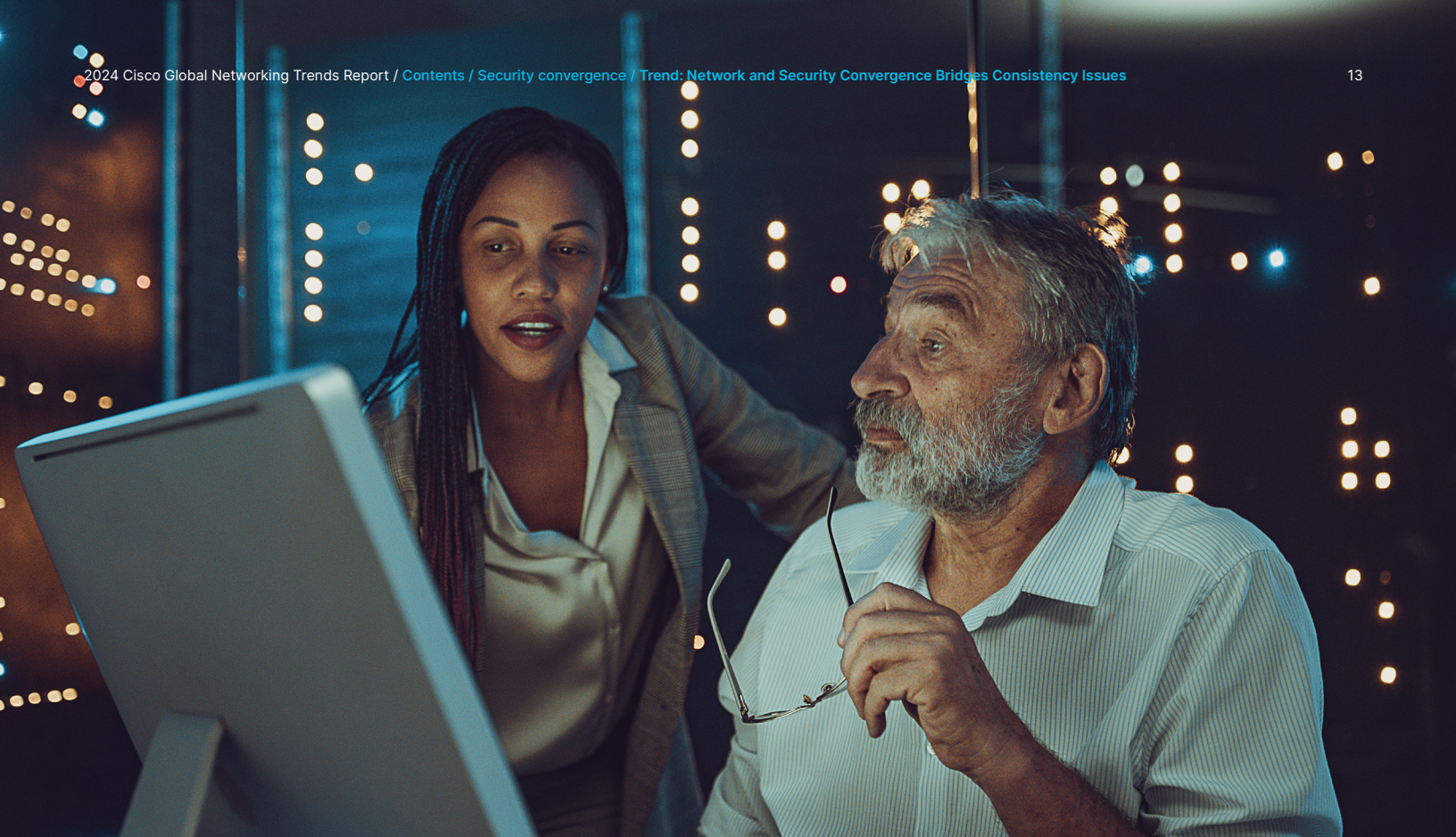
Two-year outlook

Organisations are planning multiple architectural and technology investments to help facilitate their networking and security convergence journey. When asked about their top network security priorities for the next two years, 52% said the integration of network security into broader IT security functions was their top priority. One important example of this is that 76% of those organisations plan to deploy a secure access service edge (SASE) architecture with integration of SD-WAN and security service edge (SSE) cloud security within the same timeframe.

76%

plan to deploy a SASE architecture with integration of SD-WAN and SSE within the next two years.

 Explore [secure networking](#) for people, applications and data.



Significant network security investment areas over the next years

52% Integrating of network security into broader IT security

49% Moving more security tools to be cloud based

33% Consolidating vendor management

26% Implementing a zero-trust network

23% Integrating across SD-WAN and cloud-based security for complete SASE architecture



Two-year outlook

In two years, 60% of companies expect to have an integrated multi-cloud networking and security management platform with common APIs for secure workload mobility, network and application visibility, and policy management.

Additionally, organisations on the leading edge of IT innovations plan to have AIOps-driven automation in place to optimise workload mobility with end-to-end visibility across multi-cloud, private cloud and edge networks.

60%

of companies expect to have an integrated multi-cloud networking and security management platform in place within the next two years.

Trend

Secure Multi-Cloud Networking

Organisations are moving decisively to deploy workloads across multiple public and private clouds, creating a multi-cloud environment. According to the [2023 Global Networking Trends Report](#), 92% of organisations use two or more public cloud providers to host their workloads, with 34% using more than four. However, each public cloud service provider, private data centre and hybrid cloud environment uses different network and security operational models. Organisations need to address the resulting management complexity with a strategy that enables better visibility and more consistent control of connectivity and security across disparate private and public cloud environments.

Today

Separate vendor-specific cloud network management tools are being used by 20% of surveyed organisations for data and workload integrations between data centre, edge and public cloud networks. For 17% of respondents, SD-WAN cloud on-ramp connectivity is being used to help deliver more consistent connectivity and management across clouds, and 28% have deployed a basic multi-cloud network platform that manages connectivity across two or more cloud environments.

"Multi-cloud is a reality that we must deal with ... In a perfect world, I wouldn't want to have a multi-cloud because [it] is very complex to manage from a configuration and maintenance standpoint and a cybersecurity standpoint."

IT Director, Global Automotive Technology Company

Trend

Cloud-Based Security Is Top Networking Investment Area

Cloud-based security is the biggest area of networking investment for this year, according to 38% of respondents.

Securely connecting the distributed workforce and their devices is a dominant part of future IT strategies. In a multi-cloud, work-anywhere world, a cloud-native security solution such as SSE fosters closer network and security collaboration and minimises risk by centralising access control, threat protection, data security, security monitoring and acceptable-use control.

Today

Given the increasingly distributed nature of the modern workforce, it's no surprise that ensuring robust security to support remote or hybrid workers was cited as the top networking challenge for 39% of respondents. Cloud applications and continuous updates to hosted security vulnerability engines and data-rich analytics engines were each identified as the main motivations for choosing cloud-based security by 40%. The most popular cloud-based security capabilities organisations in the survey are using IP VPN (53%) followed by secure web gateway (47%) and cloud access security broker (40%).



Two-year outlook

Over the next two years, 49% of respondents will be investing significantly in cloud-based security tools. Within that timeframe, 39% expect that more than half of their security tools will be cloud-based. This pace of growth is expected to continue, with the global cloud security solutions market expected to more than triple in size between 2022 and 2029, growing from USD 33 billion to USD 106 billion.² For 29% of survey respondents, policy-based microsegmentation to support a zero-trust network architecture for IoT devices will be another major area of IT investment.

49%

of IT leaders and professionals said they will be investing significantly in cloud-based security tools over the next two years.



Top networking investment areas over the next 12 months

38% Cloud-enforced security

34% AI-enabled networking for predictive assurance

33% Data centre network upgrades to facilitate new app and workload types (e.g. GenAI)

31% Hiring new or re-skilling existing networking staff

30% Network automation

29% Sustainability initiatives





AI operations

"I think the great power of AI, besides generating images and text, is faster correlation analysis. AI will be able to identify really quickly and alert us on when there is a bottleneck, what could be the cause, is there a mismatch into the configuration – and automatically correct it."

Group CIO,
European-Based
Private Equity Firm

This year's survey data shows that IT leaders and professionals clearly believe in the potential of AI to greatly enhance a myriad of applications, including automating operations, enforcing policy, strengthening security and assuring digital resilience.



Trend

AI-Powered Operations to Improve Efficiency

AI promises to radically improve operational efficiency. A broad adoption of AI-enabled operations will bring trusted systems that constantly learn and improve, reducing a significant amount of manual work.

Today

Fewer than 5% of respondents believe their IT teams are equipped to deliver the innovations required to help steer business strategy, satisfy customers and optimise operations. Asked about the day-to-day activities of designing, deploying and managing the network, 37% said they struggle with staff resources to manage consistent designs and deployments. Over a third said that a lack of automation to perform operational tasks is a significant issue. With increasingly distributed and complex networks and intelligence spread across different domains and networking products, reducing the administrative burden on IT is a priority.

A majority (67%) of those surveyed said their IT teams have begun adopting AI capabilities to simplify operations, automate complex tasks and accelerate remediation of performance issues. In the move to AI for network operations, 32% believe using a network platform is the right solution to aggregate network telemetry data for analytics and specialised AI applications.

"The future will involve more automation ...

The emphasis has to be on efficient operations, allowing the group to channel IT investment into revenue-generating projects."

Nicolas Gachet, Global Head of Network Special Projects, the Adecco Group




Two-year outlook

Within two years, 60% expect to have AI-enabled predictive automation in place across all domains to manage and simplify network operations. Additionally, 17% expect to integrate AI-enabled networking with AIOps in that timeframe. This will enable predictive optimisation between users, devices and apps across all network domains.

60%

of respondents expect to have AI-enabled predictive automation in place across all domains to manage and simplify network operations within the next two years.

 Explore [AI-enabled NetOps](#) service automation and assurance.

AI-enabled advancements expected within the next two years to improve network operations, security, digital resilience and sustainability:

AI-enabled predictive network automation in place across all domains to simplify NetOps

60%

AI-enabled secure access service edge (SASE) cloud architecture

54%

AI-enabled endpoint recognition and policy management

51%

AI-enabled predictive digital experience assurance

38%

AI-enabled network solutions to deliver sustainability outcomes

25%





Two-year outlook

Within the next two years, two-thirds (66%) of respondents expect to have governance policies and procedures in place to access and utilise data to support defined use cases. A third expect that those use cases will result in competitive advantages for their organisations. For 38%, those will include proactive and predictive operations with AI-enabled network and digital experience assurance. Investment in those capabilities is expected to yield the performance and experience-based results required to drive digital business.

66%

expect to have governance policies and procedures in place over the next two years to leverage data to support defined use cases – half of which expect these use cases to give them a competitive edge.

Trend

Data Governance and AI-Enabled Analytics for Predictive Assurance

IT leaders and professionals acknowledge that gaining visibility into network performance from various network domains is crucial to assuring consistent, high-quality digital experiences. They are looking at how to access both aggregated, proprietary telemetry data and performance telemetry from owned and unowned domains. Once data is aggregated, IT and business leaders can apply AI to analyse traffic and assist in performance-based decision making to improve operations and create competitive advantage.

Today

Less than 7% of respondents say their data governance practices currently provide them with a competitive advantage. Survey results show a third of respondents are prioritising the aggregation of data-driven analytics through a network platform, and another 41% believe a network platform can improve application performance overall.

Organisations realise that collecting performance data is only the first step. More than a third (34%) ranked AI-enabled networking for predictive assurance as their second most important networking investment area over the next 12 months. Applying AI training models to data for predictive and proactive remediation of network problems can help assure network performance and high-performance digital experiences. Yet today, less than 4% of surveyed organisations currently have AIOps-enabled predictive service assurance in place to manage digital experiences between users, devices, applications and services. This indicates the reactive nature of ensuring network performance today instead of a more predictive and proactive approach.

"Every organisation leverages a network to connect their users. And having the most consistent [network] experience is critical to making sure our organisation functions properly ... Without a solid network that your organisation is running on, you wouldn't have that organisation or the ability to connect its users."

Michael Kutka, Network Architect, Insight Global

Trend

AI-Enabled Security to Mitigate Risk

Organisations continue to cite cybersecurity risks as their top networking concern. Complex and ubiquitous connections, distributed users and resource constraints have organisations looking to create a security posture that is data-driven and AI-enabled to mitigate risk and overcome a cybersecurity skills gap.

Today

Security is not only a top concern, but it is also one of the most important metrics used to define the success of networking initiatives and investments for 30% of respondents. But using AI capabilities to provide a stronger and more consistent security posture is currently in its infancy among surveyed organisations.

A little over one quarter are currently using AI-enabled automation for end point recognition and policy management. Less than 4% are using AI for end-to-end segmentation to enable a zero-trust model for securing user and device connectivity.

"Identity intelligence is being built, developed and trained on current security models and billions of security events obtained from telemetry. It can then be applied to next-generation security controls like secure service edge and SASE to help IT teams make smarter zero-trust access decisions and better defend against identity-based attacks."

D.J. Sampath, Vice President, Product Management, AI Security, Cisco



Two-year outlook

The use of AI to enhance cybersecurity is expected to increase in the next two years, with 51% of respondents planning to deploy AI-enabled endpoint recognition and policy management. This will give organisations the ability to identify potential performance and security issues and proactively address them. Another 54% plan to have an AI-enabled, SASE cloud architecture in place within the next two years.

51%

of IT leaders and professionals plan to deploy AI-enabled endpoint recognition and policy management to enhance cybersecurity within the next two years.



Data centre at scale

Different AI workload types come with different data centre infrastructure needs. Organisations will need to modernise their data centres depending on the AI workload types they are prioritising for their data centres. The three workload types can be categorised as:

1. Build the model for large foundational training.
2. Optimise the model for fine-tuning a pre-trained model with specific data sets.
3. Use the model for inferencing insights from new data.

The tsunami of AI workloads being deployed in enterprise data centres alongside more traditional workloads is resulting in a renewed prioritisation of data centre modernisation. Organisations need an infrastructure capable of effectively hosting these new, demanding workloads, while also simplifying operations.



Trend

Data Centre Modernisation a Priority for Scaling AI Workloads

To facilitate increasingly data-intensive workloads from new applications like AI/ML, IT leaders and professionals are focusing their budgets on Ethernet and enhanced Ethernet to advance data centre modernisation.

Today

In addition to public and private clouds, on-premises data centres and edge environments are playing an increasingly important role in IT hosting plans. Among respondent organisations in this survey, 25% of their workloads are running in data centres, hosted clouds or collocated data centre environments. Another 17% are being hosted in edge environments with small form factor infrastructures.

A third of respondents said they are making data centre network upgrades an investment priority over the next 12 months based on the increased network demand from new applications and workloads like generative AI (GenAI). For 32% of organisations, InfiniBand is the current high-performance, high-throughput technology of choice to connect data-intensive workloads.

"While the details of your AI effort will continue to evolve, the infrastructure choices made now will determine their future success. Ethernet is the answer standing the test of time, and will once again through new standards-based innovations."

Kevin Wollenweber, Senior Vice President and General Manager,
Engineering, Data Centre and Provider Connectivity, Cisco



Two-year outlook

Over the next two years, 47% of respondents expect a moderate or significant increase in workloads hosted in data centre, hosted cloud or collocated data centre environments.

The expected expansion of AI workloads poses a major network scaling challenge. Networks must scale more efficiently than with traditional network protocols used for high-performance computing environments. This is leading to greater interest in Ethernet and enhanced Ethernet connectivity, with 89% of respondents planning to have deployed some form of AI-ready data centre clusters within two years and 56% saying they will deploy a next-generation enhanced Ethernet network to provide standardised packet lossless technology to support AI workloads.

56%

of respondents are planning to deploy next-generation enhanced Ethernet networks to meet the increasing demand of AI workloads over the next two years.

 Explore how to scale your [data centre for AI applications.](#)



Two-year outlook

Within two years, 61% of respondents plan to simplify their data centre network operations with an AI-native platform approach that facilitates predictive operational insights to support more efficient and secure data centre management of workloads and services across NetOps, DevOps and CloudOps.

61%

say they plan to simplify their data centre network operations over the next two years with AI-native platforms to facilitate predictive operational insights from AIOps and data analytics.

Trend

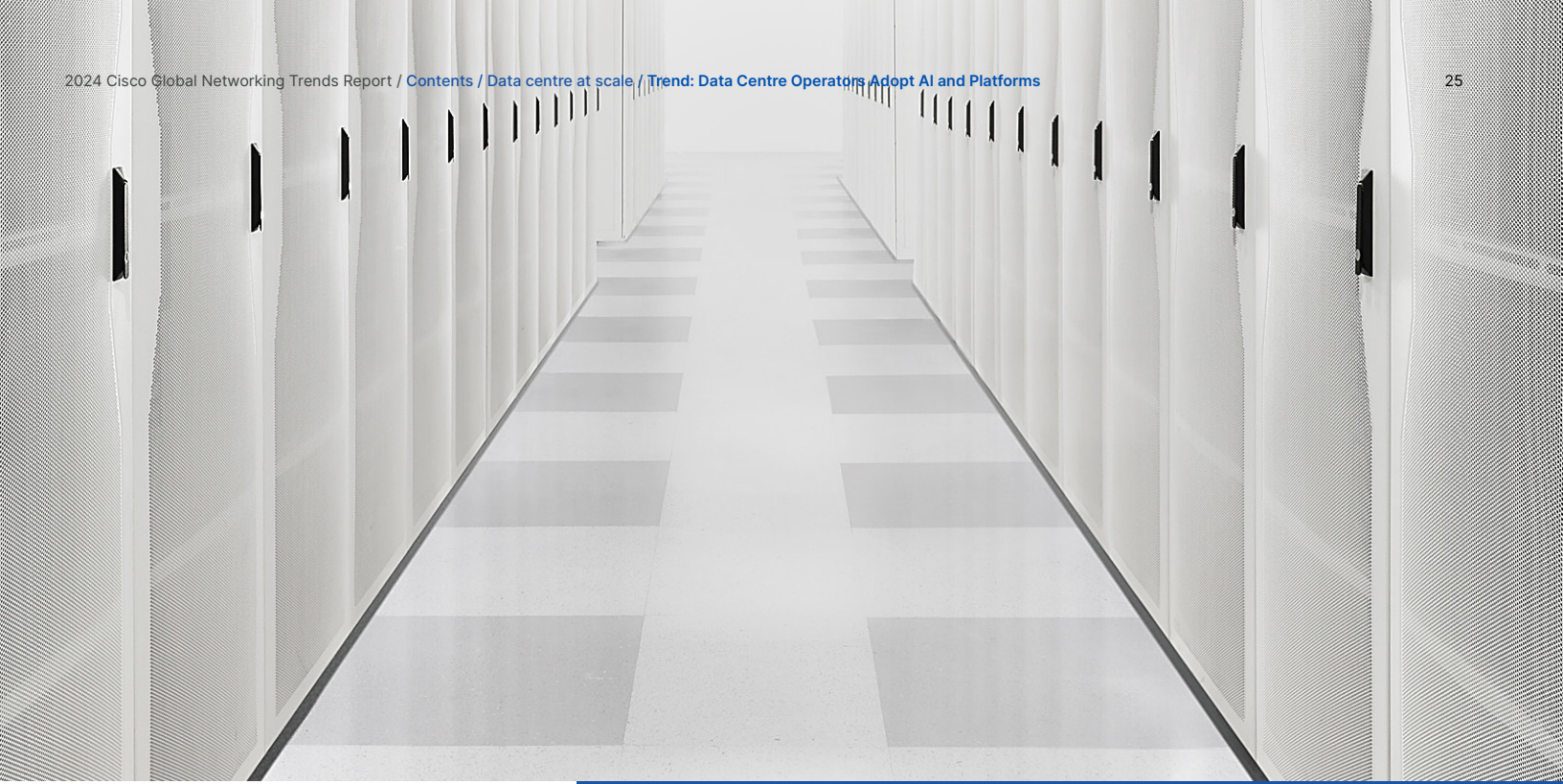
Data Centre Operators Adopt AI and Platforms

Data centre teams are turning to network platforms and AI to address the increasing complexity of data centre network operations.

Today

Currently, 38% of organisations clearly see how a network platform can support simplified data centre network management. And 32% see immediate dividends from access to aggregated network telemetry data to feed analytics and AI-native capabilities for better user and IT outcomes.

Faster IT and business innovation is recognised as the top benefit of a platform approach by 43% of those surveyed. For 42%, the top benefit is simplified end-to-end network management that facilitates cross-domain IT workflow integrations across SecOps, CloudOps and ITOps. For 41% of respondents, a major benefit of a platform approach is the ability to accelerate deployment of applications and networks.



Data centre modernisation initiatives planned within the next two years to meet increasing workload and operations demands.



47% of respondents expect a moderate or significant increase in workloads hosted in private data centre, hosted cloud or collocated data centre environments.

89%

data centre clusters deployed for running AI workloads

61%

AI-native platform approach that facilitates predictive operational insights

56%

enhanced Ethernet network fabrics for running AI workloads

43%

platform architecture across all domains, including data centre

40%

hardware modernisation to drive greater energy efficiency and sustainability goals



Sustainability advancement

"As a CIO in current days, sustainability is part of the strategy. IT needs to ensure that these [sustainability business goals] are being supported by IT solutions, and moreover, that these IT solutions are using sustainable technologies themselves."

CIO,
Private Holding Company
in Latin America

Business stakeholders continue to drive sustainability demands, often driven by mandated environmental, social and governance (ESG) compliance standards. This puts IT squarely in the lead to reduce energy consumption and minimise emissions. Hampered with lack of visibility and poor data quality, IT's focus is to advance visibility of sustainability data across their networks and to create smarter, more sustainable buildings.



Trend

IT-Led, Data-Driven Strategies for Sustainability

Organisations believe that IT can play a leadership role in their sustainability strategies. Collecting the right data and producing insights to reduce energy usage and carbon emissions is a work in progress, with many companies expecting major progress in the next two years.

Today

IT leaders and professionals said networking investments over the past 12 months have advanced sustainability goals by 19%. For 42% of organisations, sustainability is seen as one of the top areas where the network can drive digital business success, and IT is playing a major role in the formulation of sustainability strategies.

"As we collectively move toward an increasingly digital future, IT will play a critical role in helping to turn this ambition [net-zero campuses by the end of 2025] into a reality."

Rachel Higham, Global Chief Information Officer, WPP



Two-year outlook

IT anticipates being embedded in organisation-wide sustainability strategies, according to 56% of respondents. Another 55% of IT leaders and professionals expect network protocol-driven sustainability initiatives like selective powering and the use of low-power modes to positively impact sustainability goals over the next two years. According to IDC, by 2026, ESG performance metrics will be viewed as a top decision factor for IT equipment purchases and over 50% of RFPs will include metrics on carbon emissions, material use and labour conditions.³

56%

of IT leaders and professionals expect IT to be embedded in organisation-wide sustainability strategies over the next two years.

Trend

Infrastructure Telemetry and Visibility Requirements are a Priority

IT teams struggling with gaining visibility into relevant sustainability metrics expect to utilise platform dashboards to gain comprehensive visibility into real-time sustainability telemetry.

Today

The main technological obstacle to becoming a sustainable organisation is that existing IT products do not provide an adequate level of visibility into sustainability data, said 40% of respondents. Specifically, nearly a third (32%) said they don't have visibility into their IT-related energy consumption or emissions data. Another 39% said they are unsure if the data they're gathering meets the quality standards needed for measuring their sustainability performance for external reporting.



Two-year outlook

Network-driven energy management (e.g. real-time telemetry and platform dashboards) solutions are expected to have a significant, positive impact on sustainability strategy, said 60% of respondents. Another 25% expect to use network and AI solutions to deliver sustainability outcomes across the organisation that are customised to industry-specific or layout-specific needs. For example, at a large office complex, thousands of data points are generated every second to fine-tune energy efficiency for heating, cooling and lighting.

60%

of respondents said network-driven energy management solutions like access to real-time telemetry and platform dashboards are expected to have a significant, positive impact on sustainability strategy over the next two years.

"Greater infrastructure visibility allows companies to optimise future upgrades, purchasing only the necessary capacity to avoid wasting energy."

Frank Osberg, Network Architect, Solar Denmark





IT initiatives expected to positively impact sustainability strategy over the next two years:

60% IT network-driven energy management (e.g. real-time telemetry and platform dashboards)



55% Network protocol-driven sustainability (e.g. selective and low-power modes, demand anticipation)



44% Procurement transformation (e.g. partner/vendor selection, packaging, recycling)



40% Partner/vendor selection (e.g. mature sustainability services and programmes)



39% Hardware modernisation (e.g. product modularity and product efficiency)



Trend

Planning for Improved Building Infrastructure Efficiencies and Experiences

With over half of the workforce now reportedly working mainly from corporate sites, and with buildings being a major source of CO2 emissions, IT teams can now modernise buildings using data and analytics to meet sustainability and employee productivity goals.

Today

Work models are split down the middle among organisations, with 54% of respondents saying they connect to the network primarily at an office or corporate site and 46% connecting from home, in the field or working hybrid schedules. At the same time, according to industry figures, 37% of the world's CO2 emissions come from buildings,⁴ while more than 30% of a building's energy is wasted, according to estimates in the U.S.⁵ Additionally, 36% of study respondents said that connectivity, infrastructure and facilities management all require significant improvements to be more sustainable. IT teams can partner with facilities management professionals to modernise work environments for improved employee satisfaction and productivity while also improving energy efficiency and lowering their carbon footprint through monitoring, data analysis and more efficient infrastructure.

"The priority has been, particularly after the disruption of COVID-19, to create a welcoming space where people can unlock their creativity. ... We have a role to play in attracting employees back to the office. People have missed that experience."

Colin Bannon, Chief Technology Officer, BT



Two-year outlook

In the next two years, 30% of respondents believe that sustainability concerns will significantly impact their organisation's networking strategy. 31% anticipate deploying network-enabled energy visibility, and control features will be among the top smart building investment areas over the next two years.

During this time, they are also prioritising the upgrading of Wi-Fi infrastructure for improved performance and density (42%), deploying a platform for smart services (35%) and upgrading switches to support Power over Ethernet (PoE) (34%).

42%

of organisations said their top smart building initiative over the next two years will be prioritising the upgrade of Wi-Fi infrastructure for improved performance and density.

Top planned smart building investment areas over the next two years:

42% Upgrading Wi-Fi infrastructure for improved performance and density

35% Deploying platform for smart services such as location-based services

32% Upgrading switches to support Power over Ethernet (PoE, Universal POE)

31% Deploying network-enabled energy visibility and control

29% Implementing energy-efficient infrastructure

29% Enabling policy-based microsegmentation to support zero-trust network access (ZTNA) for IoT



Conclusion

At a time of economic and sociopolitical change, organisations are on a journey to create operational efficiency, secure connectivity and accelerate IT innovation for digital business advancement.

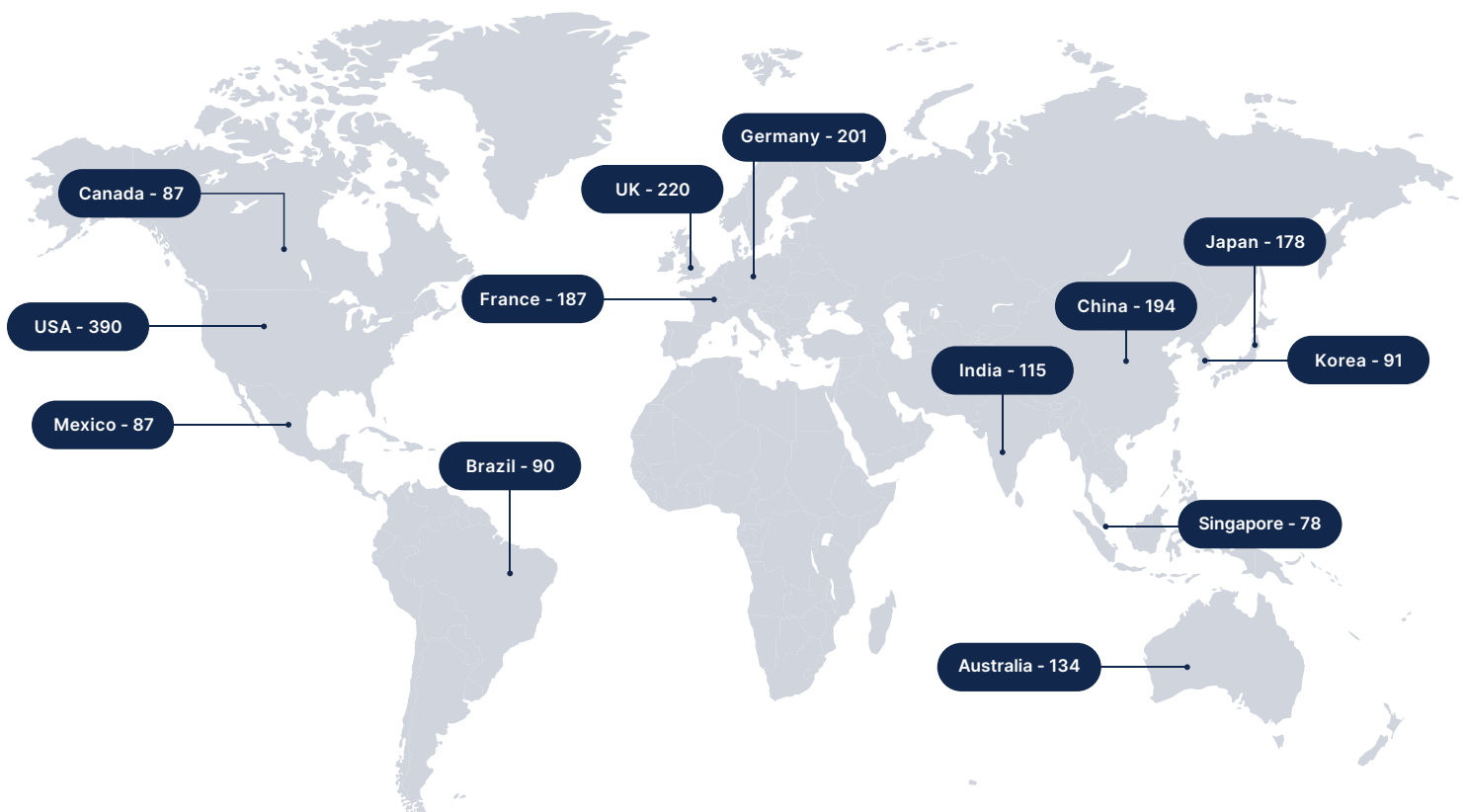
IT leaders are advancing their organisation's network journey by:

- ✓ Proactively assuring reliable, secure, connected experiences for greater digital resilience
- ✓ Ensuring a simplified and unified operational experience across domains and teams with AI-native network platforms
- ✓ Delivering the scale and flexibility to support the use cases, applications and workload demands of today and tomorrow
- ✓ Adding extensive data-driven capabilities to simplify complex cross-domain environments, achieve proactive remediation and strengthen security across users and devices
- ✓ Enabling easy access to a broad ecosystem of partner solutions via open APIs

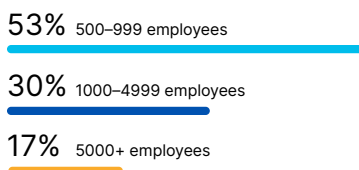
Within the next two years, many more organisations will add advanced networking architectures and capabilities to their environments, doing far more with increasingly scarce human resources and redefining how the network contributes to the bottom line.

Methodology

The Global Networking Trends study was conducted by Cisco with research and analysis by IDC, during November 2023. Responses were gathered from 2052 IT leaders and professionals from 13 countries and 10 industries. Top networking challenges, priority IT and business outcomes, architectural advances and future-looking investment strategies were assessed across a dozen criteria points critical to an organisation's networking advancement, including architecture, cross-domain security strategy and the pivotal role AI plays across all facets of networking.



Company size



Demographics

- 13 countries
- 10 industries
- 2052 respondents surveyed
 - 68% IT professionals (manager, director)
 - 32% IT leaders (VP, EVP, C-Level)

Objectives

- Assess top networking challenges
- Identify priority IT and business outcomes
- Understand level of architectural advancement
- Determine future investment strategies



- ¹ IDC Analyst Connection, sponsored by Cisco, "How A Network Platform Approach Is Becoming Imperative for IT and Business Agility," #US51420323, December 2023.
- ² "Cloud Security Market Size, Share, Trends," Fortune Business Insights, 2021.
- ³ IDC Blog, IDC FutureScape: WW Sustainability/ESG 2023 Predictions, 5 December 2022.
- ⁴ "Building Materials and the Climate: Constructing a New Future," United Nations Environmental Programme report, 2023.
- ⁵ "How Much Energy is Consumed in U.S. Buildings?" FAQ, U.S. Energy Information Administration, 2023.