2020 Global Networking Trends Report

Trends in network technology

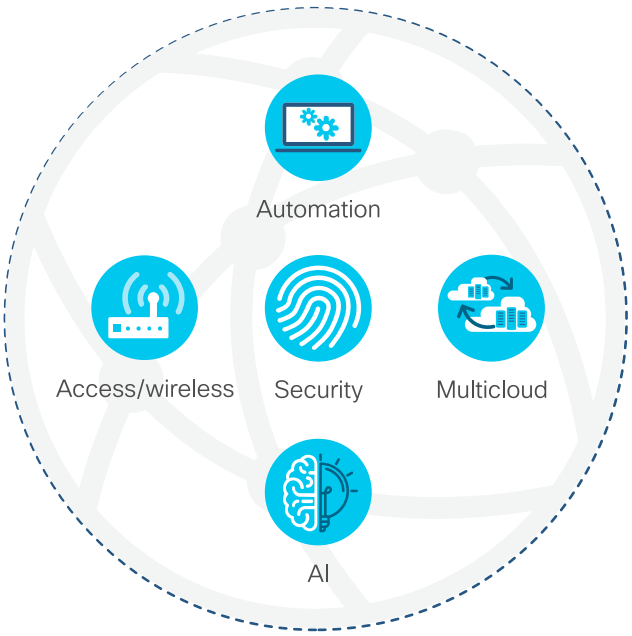
Five technologies that are shaping the new network

At this very moment, a number of major networking technology developments are coalescing to form the foundation for a new networking model. Advances in five technology areas in particular—**automation, AI, multicloud networking, wireless**, and **network security**—promise to power the biggest wave of network transformation seen in decades. These technologies will support the market's needs for increased scale, agility, and security and, by doing so, will enable the emerging trends that are changing the world as we know it.

"Organizations across the globe realize the need to digitally transform themselves to keep pace with the market and satisfy the demands of employees, partners, customers, and constituents," says Brandon Butler, IDC senior research analyst, enterprise networks. "IT leaders also realize that without a more robust, secure, and agile network, their organization's digital transformation is at risk, spurring the simultaneous refactoring of multiple aspects of their networks."

A closer look at the state of each of these technology areas provides insight into how they are reshaping the network, their current state of adoption, and the changes we can expect in the near future.

Figure 6 Five technologies enabling network transformation



Network automation at scale

Section summary

Key takeaways

- Together, software-defined networking (SDN), intent-based networking (IBN), network virtualization, programmability, and open-platform network controllers are making automated alignment of network services to business needs and IT processes a reality.
- IBN augments the automation capabilities of SDN with the ability to translate intent into policy, gather data, provide visibility, remediate problems, and assure that policies are actually doing what was intended.
- The goal of IBN is to continuously apply and assure service performance requirements, security and compliance policies, and IT operations processes across the whole network.
- Application programming interfaces (APIs) on an open-platform controller allow the controller to integrate and exchange intelligence with adjacent network and IT services, other IT domains, business applications, and heterogeneous infrastructure.

Key findings

- According to IT leaders, network automation (25%), SDN (23%), and IBN (16%) are among the technologies that will have the most impact on networking over the next five years.
- 27% of IT leaders identified a siloed design and operational approach across access, WAN, data center (DC), cloud, and security domains as causing an obstacle to their adoption of advanced network technologies.
- 34% of IT leaders identified better network coordination and integration with other IT teams as an important area for improvement.
- While only 4% of IT leaders and network strategists classify their network as an intent-based network today, 35% plan for their network to be intent-based within two years.

Section summary (continued)

Essential guidance

- IT leaders should assess their network readiness to deliver network services at a pace that the business needs.
- Explore building a roadmap that delivers on a strategy of closed-loop intent-based networking across each network domain in incremental steps that each deliver the best ROI to the organization.
- Identify and prioritize the IT processes and business applications that will benefit most from integration with an open-platform network controller.

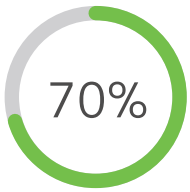
Top prediction

"The long-held vision of end-to-end intent-based policy enforcement will start to be a reality by 2025. Networking teams will be able to automate dynamic segmentation and service optimization polices at scale across domains (access, WAN, DC, multicloud, IoT) all the way from client to application and between distributed workloads."

– Ronnie Ray, VP of Customer Experience for enterprise networking, Cisco

Network automation at scale

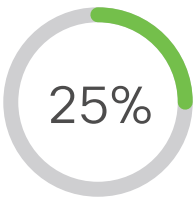
Network automation, of course, is the process of automating the configuration, management, testing, deployment, and operation of physical and virtual devices within a network. Even network optimization itself can be automated to create continuous service enhancements.



According to Gartner, "Approximately 70% of data center networking tasks are performed manually, which increases time, cost and likelihood of errors and reduces flexibility."[15]

Automation can improve network availability and relieve network operations (NetOps) teams from time-consuming daily tasks, so it's not surprising that when asked which technologies would have the biggest impact on networking over the next five years, 25% of IT leaders pointed to network automation.[14]

Innovations in the areas of SDN, IBN, virtualization, programmability, and open platform controllers are making automation a reality for networks today.



25% of IT leaders believe automation will have the biggest impact on networking over the next five years.[14]

Software-defined networking: Just the beginning

Over the last few years, SDN has offered a big step forward in enabling networkwide automation. SDN allows networking teams to manage networks as end-to-end systems, making management more efficient and flexible by separating the control and forwarding planes.

As a result, the control plane is directly programmable. It abstracts the underlying devices and infrastructure from applications and network services. Network intelligence is logically centralized through programmable SDN controllers.

SDN was initially introduced to simplify complex data center environments that needed to support portable, dynamic workload migrations and server-to-server traffic. The same principles underlie software-defined access (SD-Access), which helps secure user and device access more effectively, and software-defined WAN (SD-WAN), which can enable better user experiences accessing applications and cloud services.

Intent-based networking: Closing the loop

The primary objective of network teams is to continuously deliver application and service performance and protection for the business. So while SDN offers important advances in automation, it is only part of the solution. Organizations also need continuous network monitoring and optimization to support increasingly dynamic and digitally driven business models.

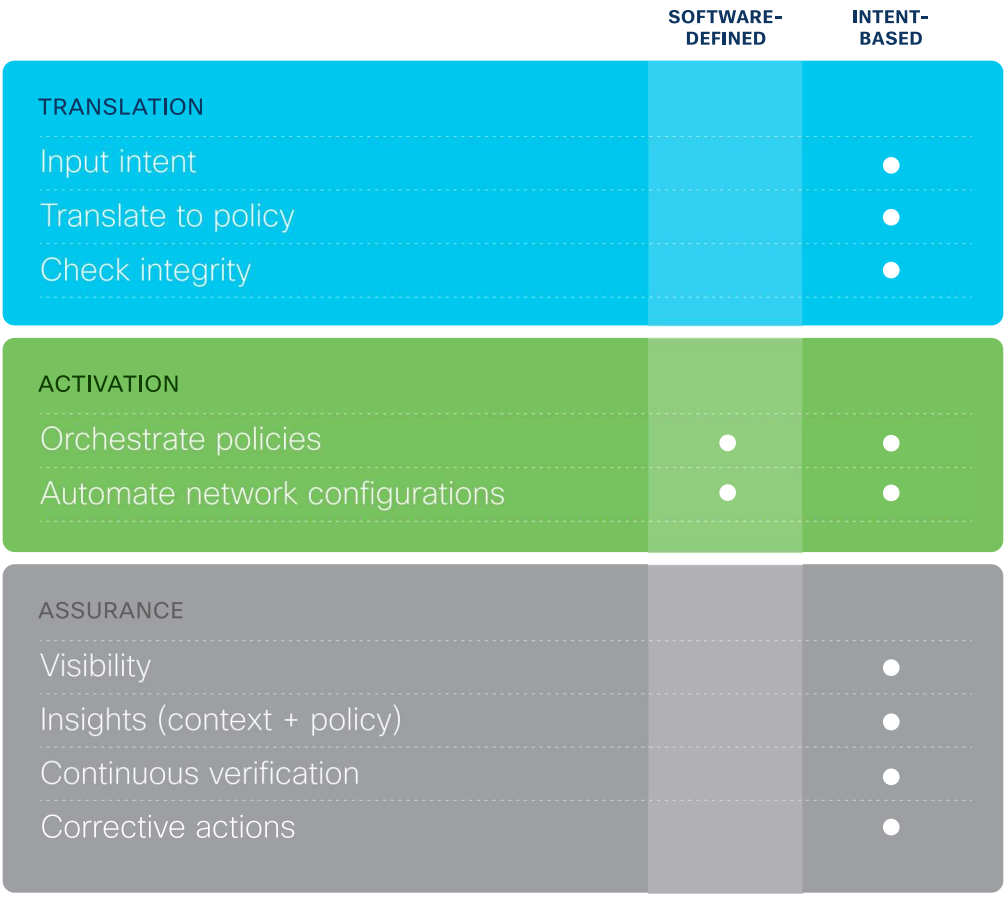
To achieve this, networks must understand the changing intent of the business and monitor dynamic network conditions so they can continuously accommodate that intent. According to an Internet Engineering Task Force (IETF) draft, "Intent constitutes declarative policy with a networkwide scope. A human operator defines 'what' is expected, and the network computes a solution meeting the requirements."[16]

Intent-based networking is a relatively new networking model that was first introduced to the market in 2017 and has since been adopted broadly by the networking industry.

To be of use, the system also needs to continuously verify that the intent is being met,

and if not, provide guidance on how to rectify it. Gartner states that "policy-based configurations will transition to intent-based networking (IBN) solutions with automation that will self-monitor, ensuring that the network actually meets the intent of the policies set at configuration time."[15]

Figure 7 IBN: Building on SDN fundamentals



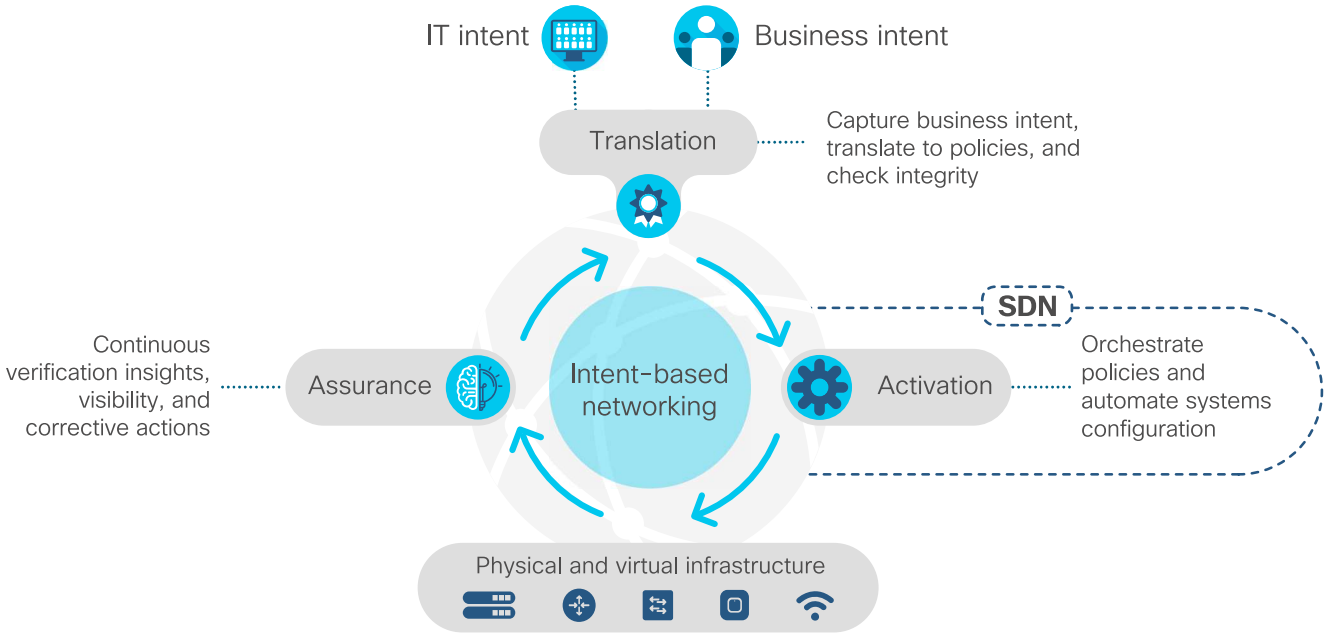
In our *2019 Global Networking Trends Survey*, we found that 26% of network strategists identified deploying intent-based networking in one or more domains as a technology priority for achieving the ideal network. And while only 4.3% of respondents class their network as an intent-based network today, 35% plan for their network to be intent-based within two years.[14]

John Apostolopoulos explains that an IBN controller expands on SDN to deliver a more complete system for continuously adapting the network to achieve the desired business intent. It augments the automation capabilities of SDN with the ability to translate intent into policy, gather data, provide visibility and relevant insights, and then assure that the network is actually doing what was intended. The closed-loop feedback provided by IBN is fundamental to achieve the desired benefits.[17]

An intent-based network captures business intent and uses analytics, machine learning, machine reasoning, and automation to align the network continuously and dynamically to changing business needs, as well as adapt to changing network loads and other environmental effects. That can mean continuously applying and assuring service performance requirements and user, security, compliance, and IT operations policies across the whole network.

How does intent-based networking work? Cisco's definition of IBN involves three functional building blocks: translation, activation, and assurance.[18]

Figure 8 Elements of an intent-based network



IT leaders are pressed to deliver services faster and more efficiently in collaboration and competition with cloud services. From a technology perspective, the compute, processing power, and AI expertise required for IBN are becoming more readily available.

IDC's Rohit Mehra says, "Intent-based networking is a significant development for the networking industry. It encompasses not only advanced levels of visibility, automation, and assurance, but it is the platform on which new machine learning-based network management functionality will be built."[19]

Network functions virtualization

The virtualization model that has radically altered compute services has been adopted in networking in the form of network functions virtualization (NFV). It allows NetOps to quickly deliver or change network services and deploy and administer them remotely. In addition to IT agility, NFV delivers substantial physical consolidation, saving space and power and creating fewer points of potential failure.

Programmability as a network foundation

For IBN controllers and systems to be scalable and achieve their full potential, they need to build on a programmable physical or virtual network infrastructure. Programmable devices and interfaces and programmable application-

specific integrated circuits (ASICs) form the underlying foundation for an intelligent network.

To adopt more efficient, automated systems, IT teams continue to move away from traditional command line interface (CLI)-based manual management approaches. Instead they are adopting data model-driven interfaces (DMI). These standard model-based interfaces provide consistency, openness, structure, and efficiency.

Leading the way toward a sustainable operational model that offers consistency and ease of use, IETF standard models like YANG provide a full set of northbound programmatic interfaces.

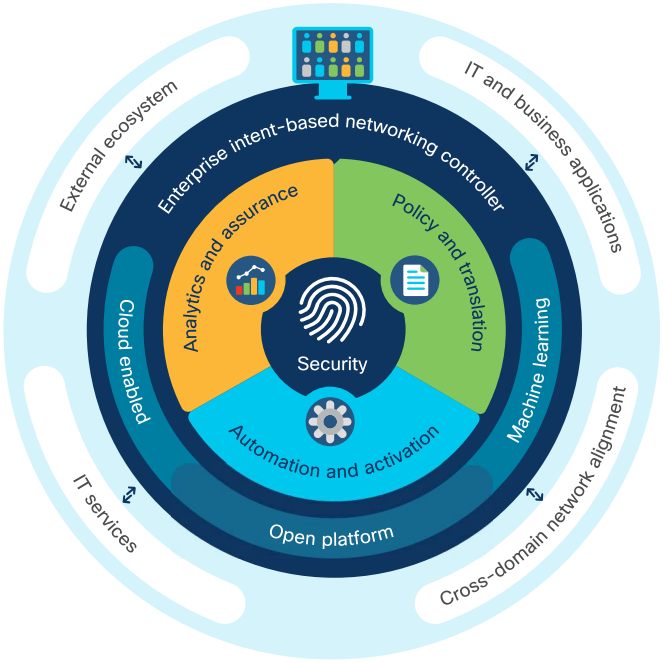
Open-platform IBN controllers: IT process and business integration

Application programming interfaces (APIs) on the controller allow the controller to integrate and exchange intelligence with adjacent network and IT services, other IT domains, line-of-business applications, and heterogeneous infrastructure.

This turns the network into an open platform that can accept policy specifications from applications and devices, take advantage of centralized cross-domain policy automation, and verify that the system is meeting the needs of the business. This improves IT service delivery by streamlining workflows across network domains, IT systems, and line-of-business processes that used to be managed independently.

In our *2019 Global Networking Trends Survey*, 34% of IT leaders identified achieving better network coordination and integration with other IT teams as an important area for improvement.[14]

Figure 9 Open-platform controller for integration with business applications, IT services, and network domains



With API and software development kit (SDK) network extensibility, IT can better align to the needs of business and IT apps, streamline operations, and ensure investment protection.

Cross-domain policy and assurance alignment: Client to workload

Networking teams need to work together to achieve end-to-end network alignment to business intent. That means creating a seamless link from wherever the client or "thing" is connecting to the network to wherever the service or application is hosted.

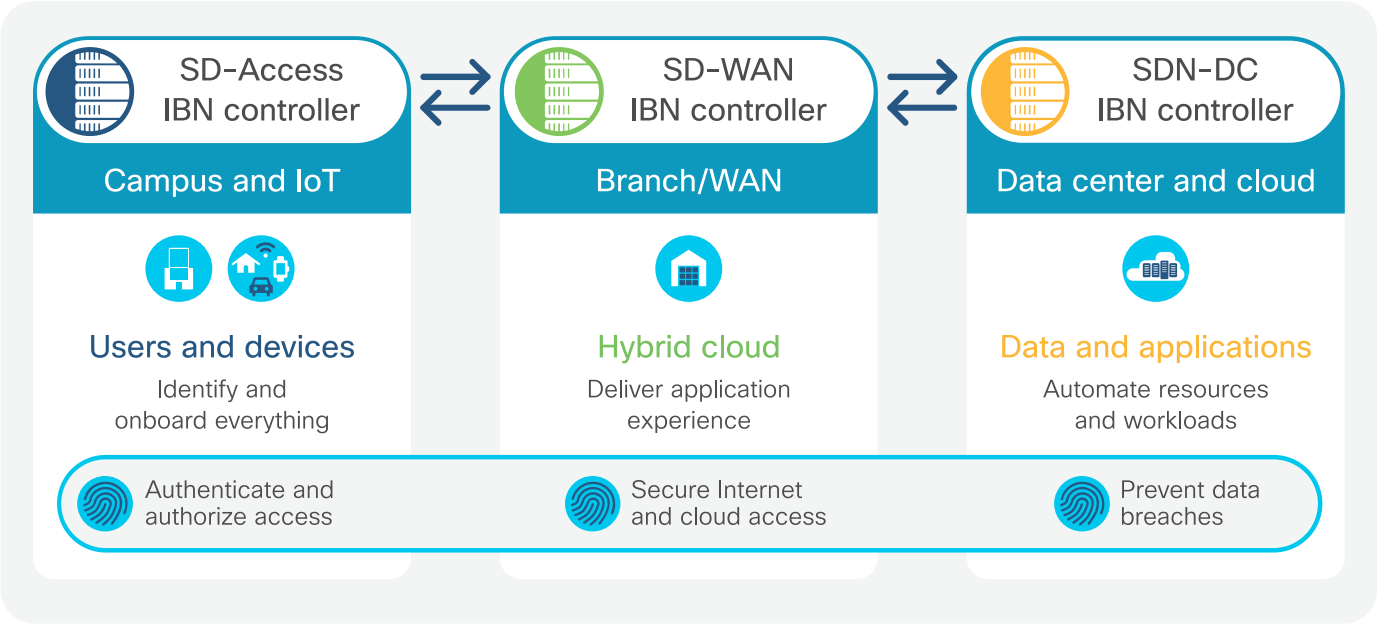
Current Analysis: For an enterprise to be successful with intent-based networking, it needs to fully embrace automation in the data center, the campus, the wide area network, and in the branch.[20]

However, in many cases that's not easily achieved. In our *2019 Global Networking Trends Survey*, 27% of IT leaders identified a "siloed design and operational approach across access, WAN, DC, cloud, and security domains" as causing an obstacle to their adoption of advanced network technologies.[14]

For good reason, the network is normally split into domains that are generally organized around the domain's primary objective. However, to achieve true end-to-end visibility, control, and validation of business intent, policy and assurance capabilities need to be orchestrated across domains.

IT leaders are taking measures to achieve this, with 26% of IT leaders identifying "integrated multidomain network policy enforcement and assurance" as a top priority for increased investment.[14]

Figure 10 Policy and assurance: Alignment across all IBN domains



AI-enabled assurance

Section summary

Key takeaways

- The use of artificial intelligence (AI) is becoming critical for operations, service delivery, and network assurance, where AIOps—the combination of AI capabilities and operations—is becoming a well-established category.
- The explosive growth in traffic volume, connected mobile and IoT devices, interconnected applications and microservices, and ever-increasing security threats is overwhelming network teams.
- Massive amounts of data, telemetry, and events generated by networks supporting increasing numbers of devices and services are exceeding the ability of human operators alone to take action.
- Fundamental to an intent-based network (IBN) model, AI uses the voluminous network-sourced data to explore the complexity of the environment and dynamically propose network adjustments.
- Machine learning and machine reasoning complement each other to deliver complex event processing, correlated insights, and guided remediation.

Key findings

- Over 50% of network strategists identify AI as a priority network investment.
- Only 17% of network strategists believe a lack of maturity in AI technologies poses an obstacle to network modernization.
- Only 22% of networking teams are using any AI for network assurance today, possibly because the availability of genuine AI-enabled tools is still quite new.
- 72% of network strategists project using AI-enabled predictive insights or prescriptive remediation within the next two years.

Essential guidance

- Take advantage of cloud-based AI learning: In some cases, changes in corporate data policies will be required to take advantage of the benefits of cloud-enabled AI tools.
- Human and AI interlock: Progressively define how far AI can go in making decisions or taking action before a human operator needs to get involved to monitor, approve, or make a change.

Section summary (continued)

- AI knowledge: Expert networking knowledge will be a premium skill set needed to verify that AI is achieving IT and business objectives as intended.

Top prediction

"By 2025, AI-enabled network assurance tools will fully automate several well-defined, specific tasks very well. However, the majority of operational tasks that demand more flexible and contextual decision making will still require the expertise and intervention of human operators."

– JP Vasseur, Cisco fellow, Cisco

AI-enabled assurance

AI is driving powerful transformations across a variety of industries and is now becoming critical for IT operations, where AIOps is becoming a well-established category.

What are AI, ML, and MR?

Simply put, AI is a field of study that gives computers human-like intelligence when performing a task. Two of the most important categories of AI are machine learning (ML) and machine reasoning (MR). Machine learning can be described as the ability to "statistically learn" from data without explicit programming. Machine reasoning uses acquired knowledge to navigate through a series of possible options toward an optimal outcome.

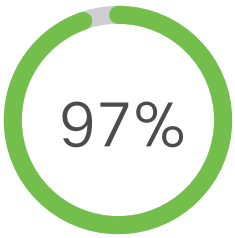
As such, ML enables a system to scrutinize data and deduce knowledge. It goes beyond simply learning or extracting knowledge to utilizing and improving knowledge over time and with experience. In essence, the goal of ML is to identify and exploit hidden patterns in "training" data.

MR is well suited for solving problems that require deep domain expertise. Humans need to explicitly capture all the knowledge a priori in order for a machine reasoner to be able to operate on new data. MR is a wonderful complement to ML because it can build on the conclusions presented by ML and analyze possible causes and potential improvement options.

Network complexity fuels AI adoption.

A number of factors are fueling the drive to AI-enabled networks. With unprecedented increases in network complexity and scale, AI is becoming increasingly necessary to help IT teams deliver consistent network and service levels.

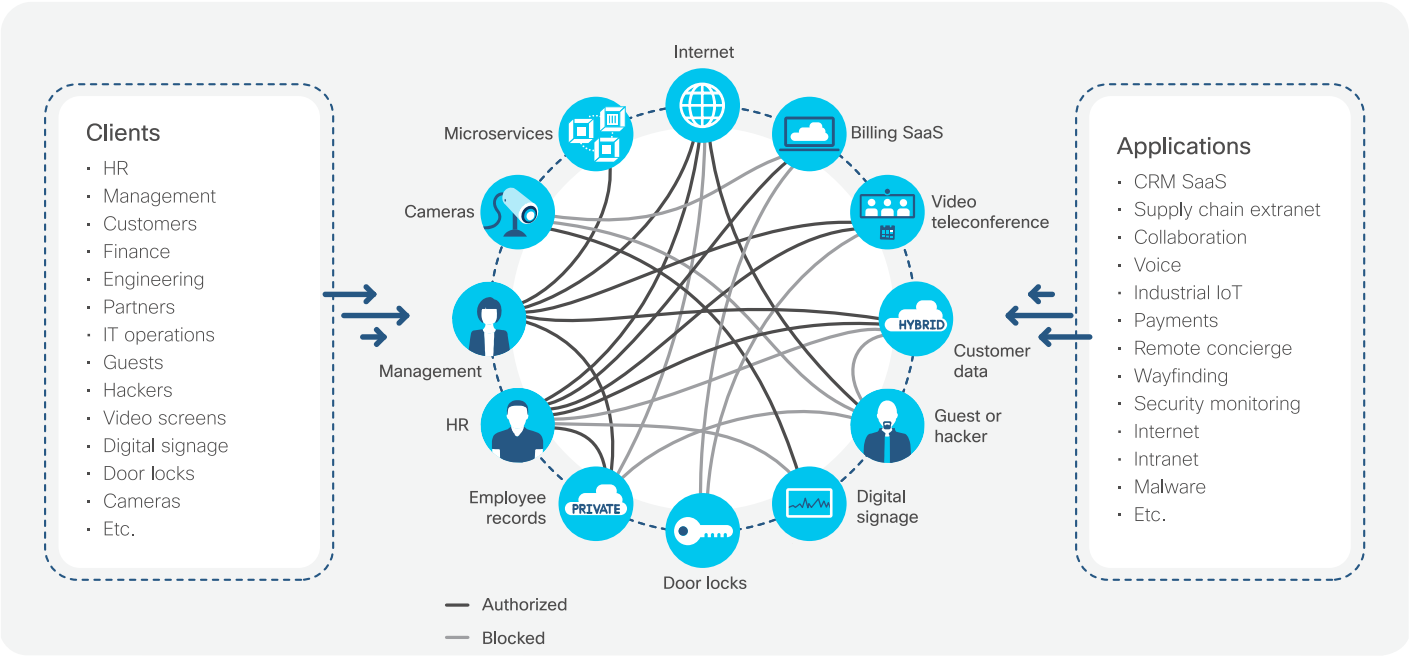
Networks are supporting explosive growth in traffic volume, connected mobile and IoT devices, and interconnected applications and microservices. Today's networks are also generating massive amounts of data that exceed the ability of human operators alone to manage, much less understand, in a timely manner.



The cost of network outages

97% of global IT leaders surveyed said they'd had performance issues related to business-critical applications in the previous six months. The average cost per network outage? US$402,542 in the United States and US$212,254 in the United Kingdom.[21]

Figure 11 Network complexity of hyperconnected organizations



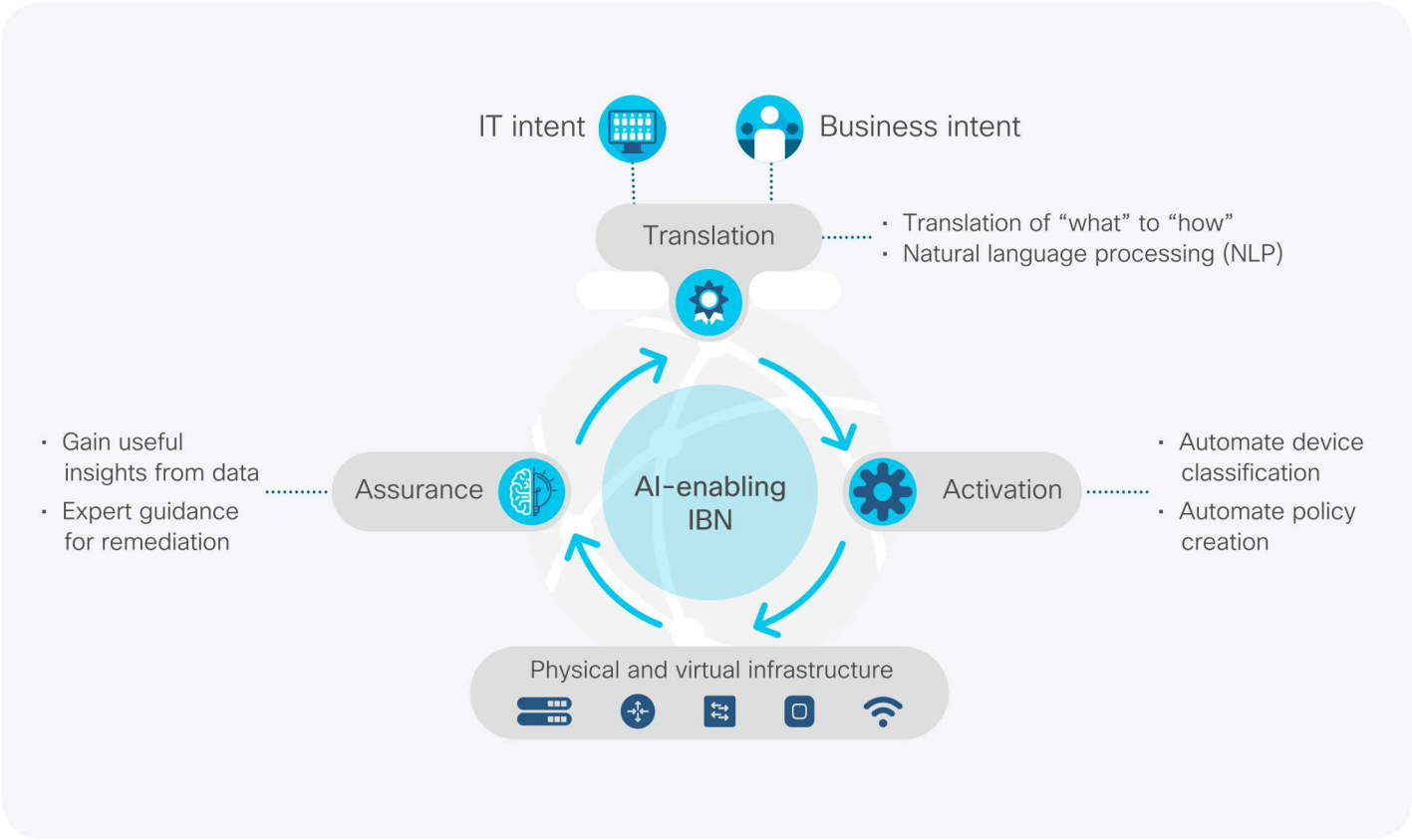
AI offers the potential for network teams to better use this data to ensure that their networks run effectively and in continuous alignment with business needs. For example, it can help create better baselines, accurately predict problems, and help with troubleshooting of complex systems.

Network strategists already acknowledge this fact. More than 50% identify AI as a priority investment needed to deliver their ideal network,[14] while only 17% believe that a lack of maturity in AI technologies poses an obstacle to network modernization.[14]

Using the voluminous network-sourced data, AI learns the complexity of the communications and networking environment and can dynamically propose adjustments to the network. This capability makes AI fundamental to an IBN model.

AI and advanced networking technologies like IBN are clearly disrupting how things are done, especially for networking operations. Testing of new applications can happen in minutes instead of weeks. Troubleshooting network issues gets significantly easier when an assurance engine identifies root causes and recommends fixes. In fact, when armed with powerful dashboards that offer actionable insights, a future network operator may only need to look in a handful of places, as opposed to plowing through heaps of possible causes.

Figure 12 Intent-based networking powered by AI



How are ML and MR applied in a network context?

As noted above, an important element of network operations and intent-based networking is network assurance, which is the continuous verification that the network state and behavior are coherent with the desired intent. Machine learning and machine reasoning offer unique capabilities that operators can use to assure required network performance, especially around the following three main assurance areas (see Figure 13 below.):

Complex event processing: When applying ML to network telemetry, it is possible to establish dynamic baselines of what constitutes normal operating conditions for a given intent.

Correlated insights: ML can provide deeper insights and visibility into the operation of the network and even help predict when an anomalous condition is likely to occur in the future. MR enhances the power of ML by applying preloaded expert knowledge captured from troubleshooting workflows of similar issues.

Remediation: Remediation allows for constant alignment to intent by identifying the most appropriate corrective actions using knowledge bases provided, for example, with MR.[22]

Current and future state of AI for network assurance

Data from our *2019 Global Networking Trends Survey* sheds light on where organizations are in their adoption of AI-enabled network assurance.

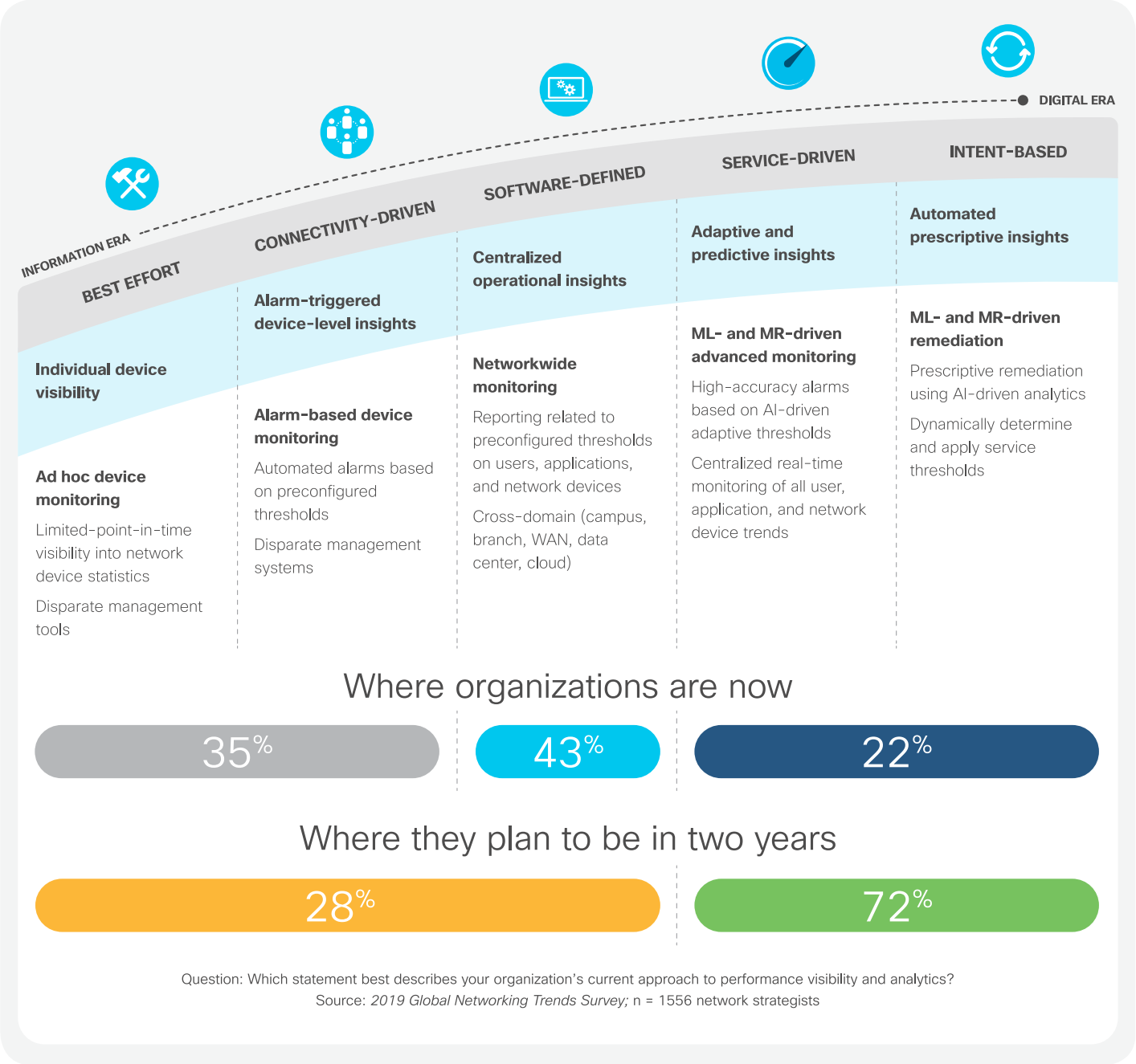
Using our standard five-stage readiness model to measure estimated state of readiness,

Figure 13 ML and MR use cases for network assurance

	Machine learning	Machine reasoning
Technology approach	Mathematical model from large data sets	Capturing human knowledge, symbolic logic
Applicability	Predictive analysis, anomaly detection, classification, regression	Mechanizing decidable workflows
Network assurance function	• Dynamic baselining and issue identification • Insights and visibility • Predictive analytics	• Automatic troubleshooting • Automatic remediation

only 22% of network strategist respondents reported utilizing any AI capabilities for network assurance today. This can be attributed to the fact that genuine AI-based network assurance solutions are still relatively new. However, 72% of respondents do plan to achieve AI-enabled predictive insights or prescriptive remediation within the next two years.[14]

Figure 14 AI-enabled assurance readiness



Question: Which statement best describes your organization's current approach to performance visibility and analytics?
Source: *2019 Global Networking Trends Survey;* n = 1556 network strategists

Considerations for going forward with AI

According to Cisco fellow JP Vasseur, when evaluating the use of AI in the network infrastructure, the following items need to be considered:

1. **Create operational best practices:** Knowing what AI **cannot** and **should not** do is just as important as understanding what it **can** do. When determining which areas of the business could benefit the most from AI, be sure to also identify areas that present the highest risk and exposure.

2. **Defining a clear objective function:** There is no algorithm capable of extracting interesting facts from a data set without the ML team clearly specifying the objectives. Being able to clearly state the goal and performance metrics before starting the ML journey is of the utmost importance.

3. **Human and AI interlock:** Defining how far AI can go in making decisions or taking action before a human needs to get involved to monitor, approve, or make a change is critical for the business and for the network team's ability to stay in control.

4. **AI knowledge:** An increasing reliance on AI has the potential to create knowledge gaps, so expert networking knowledge will be a premium skill set needed to verify that AI is achieving IT and business objectives as intended and to help operators make the right choice out of options recommended by the AI system.

5. **Data dependency:** Get better at collecting data. AI is dependent on mathematical computations for creating actionable insights, and those computations are only as good as the quality of the data they are using. Networking experts will need to work across functions and domains to ensure that data quality can be trusted for AI initiatives.

6. **Where do you apply AI:** Where AI gets applied depends on the performance, security, data capacity, and privacy of an application and data. Although there are some instances of on-premises model training, the most common application today is cloud-based machine learning. Cloud provides the compute and storage capacity to learn and execute ML from huge amounts of aggregated, anonymized data from multiple sources. In some cases, this can raise privacy concerns in terms of who has access to that data and even in which geography that data is stored. Also, be aware of latency implications that might affect real-time insights for large data sets, which could occur, for example, with video sensors that produce huge amounts of data.

7. **Changing the corporate paradigm:** Aligning your company's data policies to take advantage of cloud-based AI is ideal. By tethering millions of systems to a single AI analytics engine, a data sample size can be reached that can provide exponentially better results than the same technology that is fed by data from a single network experience. IT teams can be key in planting the seeds today that will lead to the cloud-friendly policies that will support the deployment of AI.

Networking for data and applications in multicloud environments

Section summary

Key takeaways

- All companies will need cloud-based services, but there will always be a need to keep some data and workloads on-premises.
- Monolithic applications are in many cases dissolving into interconnected microservices that are delivered via a variety of virtual and physical workloads located in containers, on-premises, in the cloud, and at the enterprise's network edge.
- A distributed data center does not work like a traditional one, so IT organizations need to adapt to meet the increased application and network connectivity demands of this new architecture.
- SD-WAN, direct cloud access, colocation facilities, and cloud exchanges, along with more affordable high-bandwidth broadband and 5G services, are emerging as important new architecture elements to ensure that cloud services can effectively and affordably deliver on business requirements.

Key findings

- SDN/NFV is already transporting 23% of traffic within enterprise data centers, a number that is expected to grow to 44% by 2021.
- 29% of IT leaders and network strategists believe that within two years, they will have intent-based networking capabilities across their on-premises, hybrid, and multicloud environments.
- Increased reliance on cloud is driving increased WAN traffic, with global business IP WAN traffic expected to grow twofold by 2022 and reach 5.3 exabytes per month.
- Over 58% of organizations globally have already deployed SD-WAN in some form, and over 94% of respondents believe they will have a basic or more advanced intent-based SD-WAN deployed within the next two years.

Essential guidance

- Identify the most mission-critical cloud-based applications and services, and prioritize any SD-WAN plans to access and protect those applications first.
- Extend consistent policy-based automation across hybrid and multicloud, being careful to consider any platform, any hypervisor, or any container framework across any location and any workload (cloud native, bare metal, hypervisor, container, and serverless).

Section summary (continued)

- Map application services, workloads, and service components to the "expanded" network to gain a better understanding of what applications, services, and microservices are on the network.
- Data center, cloud, and network teams should collaborate to develop service consistency across campus, branch, data center, edge/IoT, and public cloud/SaaS provider domains.
- Applications and services will require continuous integration and delivery between on-premises and cloud workloads, and enterprises that implement the operational processes to interconnect and support this model will reap the speed and flexibility promised by the cloud.

Top prediction

"By 2025, I expect to see 20% of workloads distributed at the edge of networks outside of enterprise and multicloud data center environments. That means one-fifth of traffic that would have generally been confined within a data center will now need to be assured and protected across the enterprise and multicloud network."

– Vijoy Pandey, vice president and CTO of Cloud Platform and Solutions Group, Cisco

Networking for data and applications in multicloud environments

The need for speed and innovation is pushing IT organizations to modernize existing apps and rapidly develop new apps that enable access to information on any device at any time. Today's app developers and business users appreciate the agility, scalability, and self-service of the cloud.

However, while 85% of IT organizations are evaluating or already using public cloud, the move to the cloud does not tell the full story.[23] In fact, the phrase "the move to the cloud" has not proven to be completely accurate. Vijoy Pandey, vice president and CTO of the Cloud Platform and Solutions Group at Cisco, says, "Over the last few years, as valuable workloads attempted to migrate to the public cloud, it became apparent that it wasn't a binary situation and there were some workloads, and critically, some data, that needed to be local."[24]

Of organizations that are using public cloud today, 85% are pursuing a multicloud strategy, increasing to 94% within 12 months.[25]

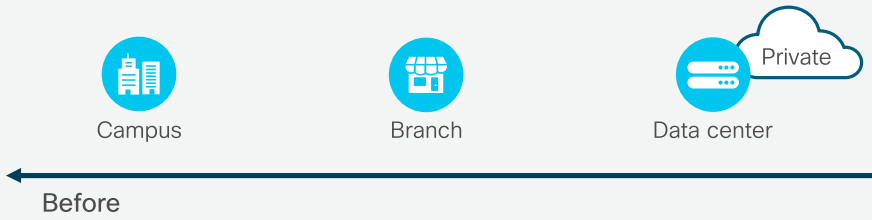
Pandey also notes that the decision to keep data on-premises derives from a number of concerns, including regulations and data protection: "Another concern is if you need a lot of insight from your data, you need to do a lot of data crunching. For all those workloads, you need local compute and local networks. While there will be a need for cloud-based services for all companies, the need for on-premises will never disappear. That's why I think making the bet on multicloud and hybrid is the way forward."

The network impact of changing application models

Traditionally, a network's performance focused on two main elements:

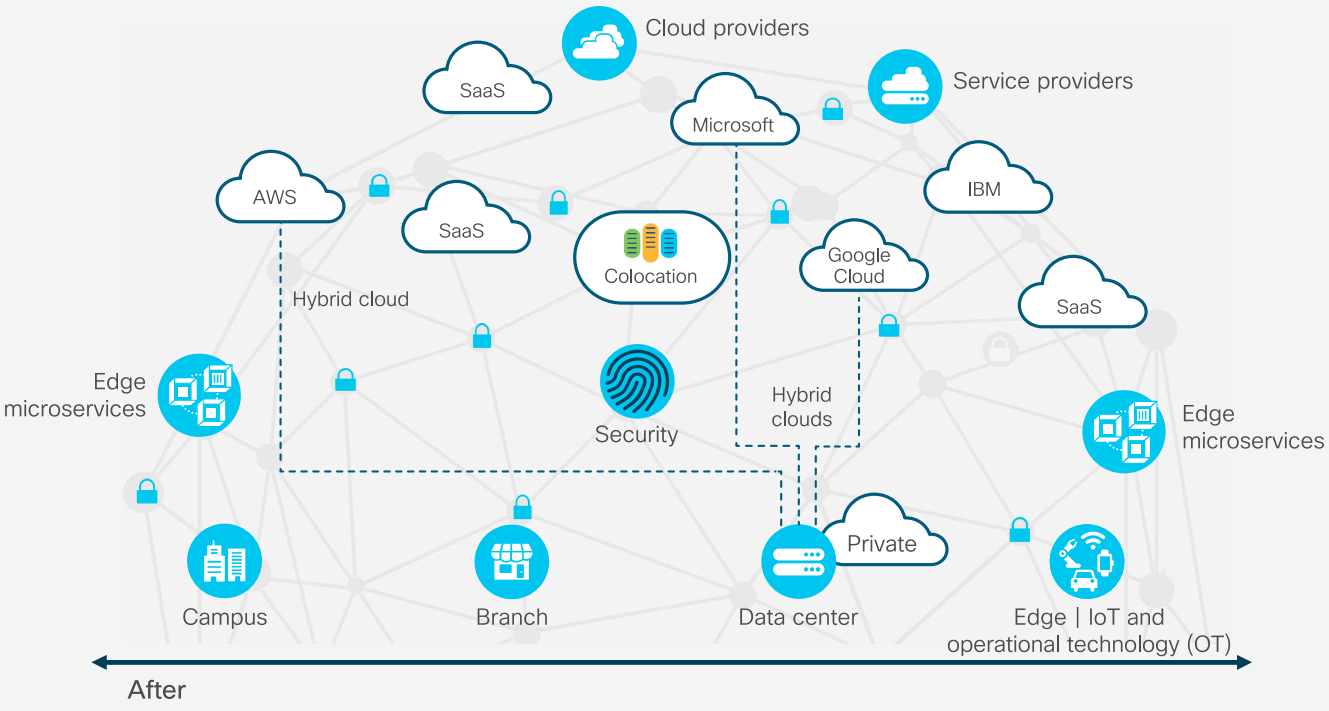
- The communication between the client and the monolithic service or application, typically hosted in a central data center
- The intra-data-center communication between servers and networked storage

Figure 15 Before: Client to service and interworkload communications



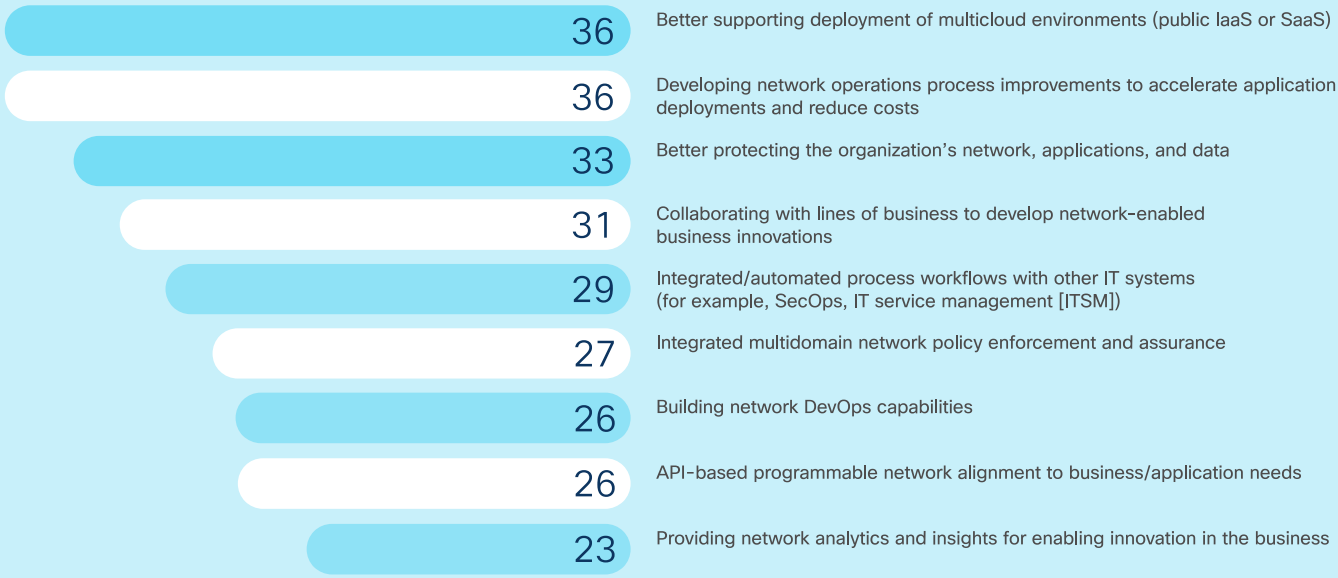
But this approach is no longer sufficient as application teams continue to adopt more agile application models that are less monolithic and composed of multiple workloads or service components that are not always colocated, but rather distributed, beyond the data center and on-premises environments.

Figure 16 After: Client to service and interworkload communications



While some IT teams may believe that a move to the cloud means the network becomes less of a consideration, nothing can be further from reality. Data center and cloud teams can no longer work separately from networking teams, a fact that IT leaders have already recognized. They now identify network investments to support multicloud environments (public, infrastructure as a service [IaaS], or SaaS) as one of their highest priorities.[14]

Figure 17 IT teams prioritize investment in networking for multicloud environments



Question: If you were able to reduce the time spent on maintaining status quo activities, on which of the following value-added services would you put more focus?

Source: *2019 Global Networking Trends Survey*; n = 505 IT leaders

According to Tom Edsall, Cisco's CTO for data center and emeritus advisor, "As applications, workloads, services, and data become more distributed across the entire edge-cloud continuum, there is an added responsibility on IT as a whole to ensure that services are delivered securely and reliably and with the desired performance, irrespective of their physical location. Data center professionals must now collaborate more closely than ever with teams responsible for branch/edge, WAN, and campus networking."

Given these ongoing changes, where do IT and networking leaders need to focus their efforts today?

Expansion into the hybrid and multicloud world means managing ever-changing variables (apps, data, users, and devices) that span every domain of the enterprise. As a result, infrastructure and operations (I&O) and networking teams must work together to tackle everything from the networking implications of public cloud and SaaS providers to the impact on their on-premises environments.

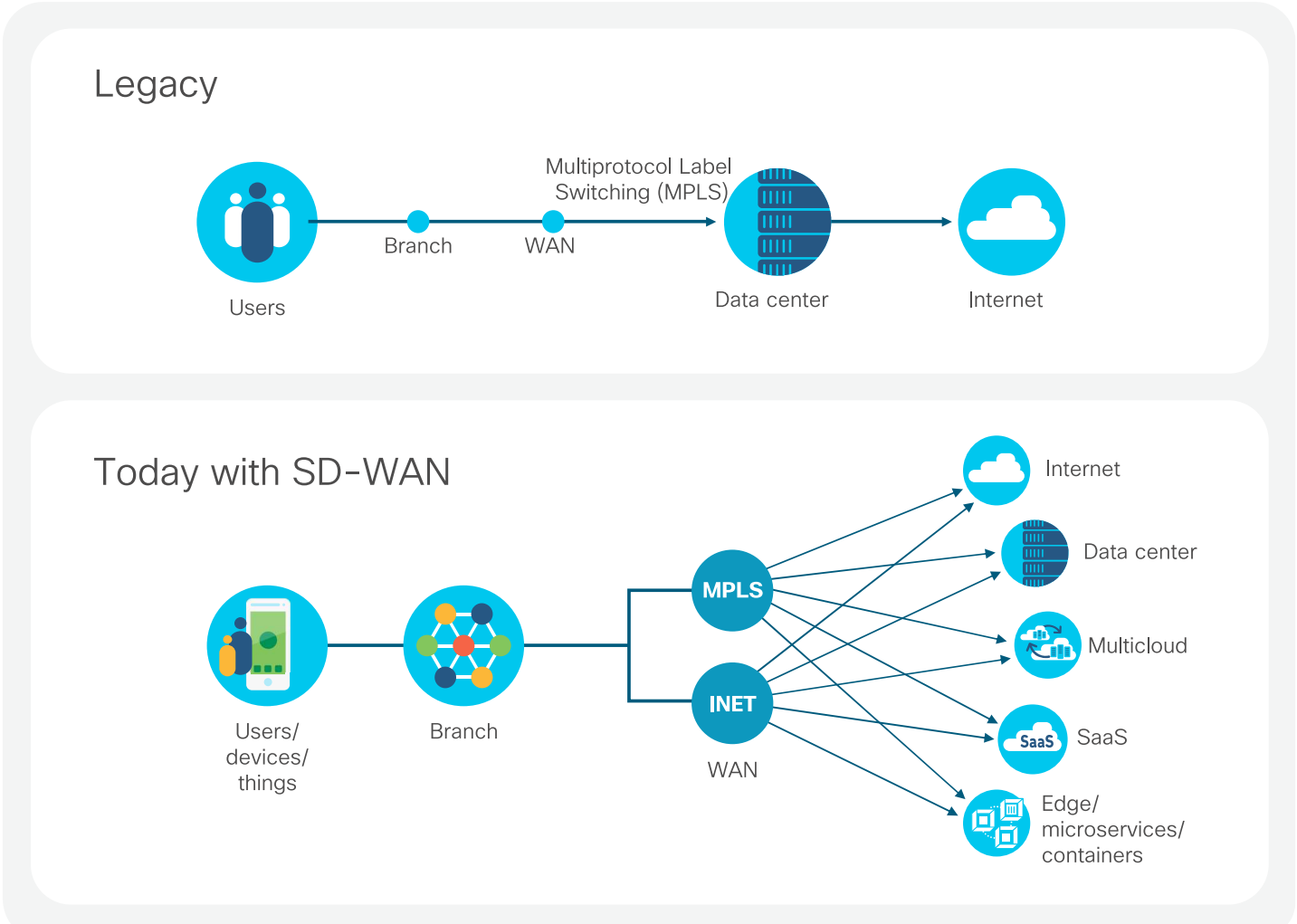
To help understand the challenge, we will look at networking requirements through two lenses:

- Optimizing user-to-multicloud connectivity
- Networking for an anywhere data center

Optimizing user-to-multicloud connectivity

The emerging predominance of cloud services means that remote connectivity to those services becomes more critical than ever. It also means that traditional wide area network architectures that focused on connecting remote sites to centralized data centers are no longer optimal.

Figure 18 The changing WAN landscape



Now that SaaS, IaaS, and distributed edge services can be hosted anywhere there's a network connection, a legacy hub-and-spoke WAN architecture can hold organizations back.

↑2X The increased reliance on cloud is also driving increased WAN traffic, with global business IP WAN traffic expected to grow twofold by 2022, reaching 5.3 exabytes per month.[12]

SD-WAN, direct cloud access, colocation facilities, and cloud exchanges, along with the availability of affordable, high-bandwidth broadband services, are emerging as important new architecture elements to ensure that cloud services can affordably deliver on business requirements.

IT teams need the same control in multicloud environments as in their own networks so they can continue to deliver the service that the business expects.

SD-WAN

SD-WAN is a software-defined approach to managing the WAN that allows a centralized controller to optimize the multicloud application experience and greatly simplify WAN operations.

The recent rapid adoption of SD-WAN indicates that it provides many answers to the growing demands of the cloud. And in fact, the cloud is the biggest driver for this SD-WAN adoption. Nearly 75% of respondents in IDC's SD-WAN survey stated that SaaS/cloud services are important (or very important) to current WAN technology choices.[26]

This is not surprising, as traditional options and services used for connecting to the virtual private cloud provided by cloud service providers leave enterprise networking teams with limited control in a multicloud scenario.

According to our *2019 Global Networking Trends Survey*, over 58% of organizations globally have already deployed SD-WAN in some form, and over 94% of respondents believe they will deploy some form of basic or more advanced SD-WAN implementation within the next two years.[14]

Also, as 5G services become more widely available, SD-WAN will seamlessly integrate them into a transport-independent framework for maximum flexibility and performance, improved always-on backup, and reduced cost.

Figure 19 WAN for multicloud readiness

Question: Which statement best describes your organization's current approach to designing, deploying, and managing your WAN architecture?

Source: *2019 Global Networking Trends Survey;* n = 1556 network strategists

Direct cloud access

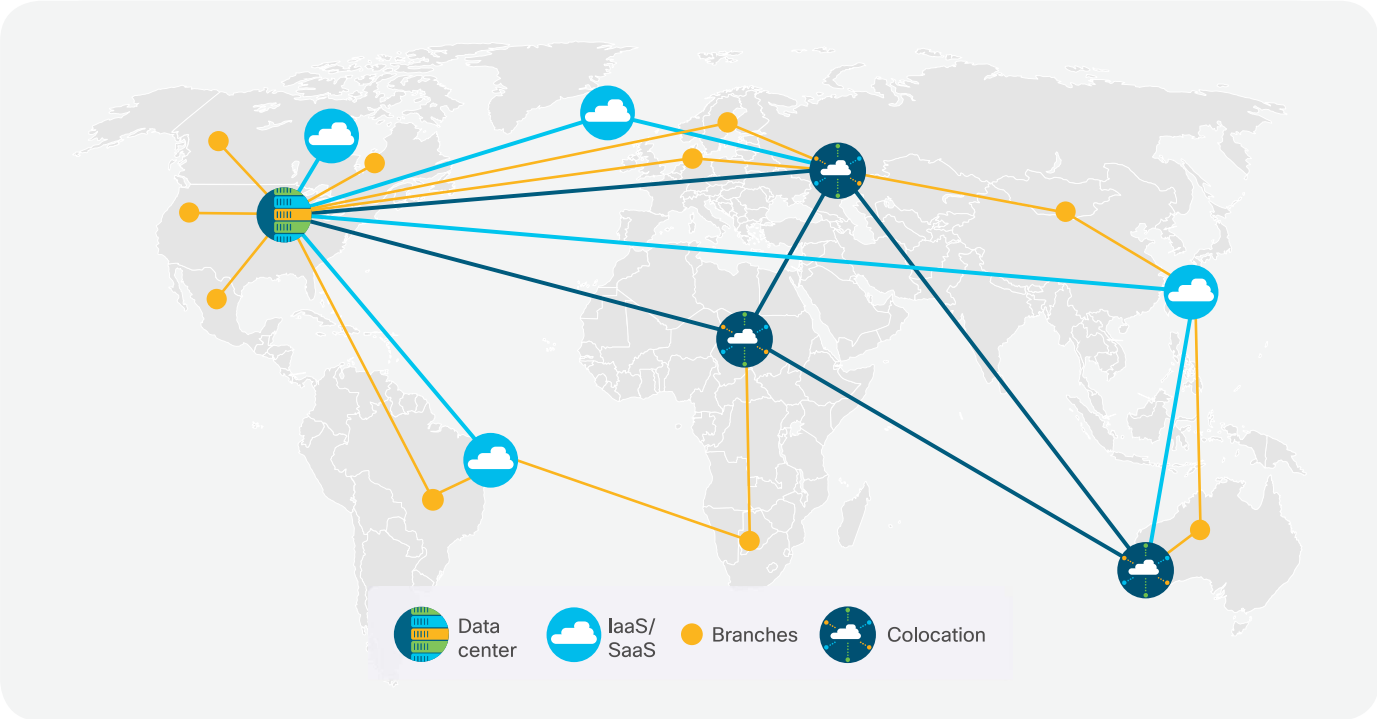
The traditional approach of backhauling branch traffic over expensive WAN circuits to the data center or a centralized Internet gateway via a hub-and-spoke architecture can hinder a transition to cloud services. It also adds expense and introduces latency that degrades the user experience.

Until now, network architects have been stuck with this approach because of the cost and complexity of the alternative, which requires deploying and managing distributed security capabilities such as firewalls, URL filtering, and DNS protection at each branch router.

Now, however, "direct cloud access" or "direct Internet access" capabilities can securely connect users directly from the branch to cloud

services. This simplifies policy management across remote sites and automates provisioning of new network services in minutes while enforcing multilayer security, including encryption, authentication, segmentation, firewall, and DNS enforcement.

Figure 20 Secure SD-WAN with direct cloud access and colocation hubs



Colocation and cloud exchange

While carrier-neutral colocation (colo) facilities are not new, they take on a much-expanded role in the age of multicloud and are a critical component of the new cloud-optimized WAN architecture. In essence, colo facilities like those provided by Equinix and other interconnection services become an extension of the enterprise WAN, providing visibility, high-performance access, and centralized security to multiple SaaS and IaaS providers. (See Figure 20 above.)

Networking for an anywhere data center

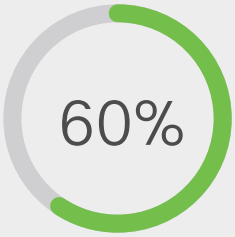
Today's data centers are no longer single locations. The emerging "distributed data center" is a result of applications and data that live both on- and off-premises in hybrid, multicloud, and edge environments. But a distributed data center doesn't work like a traditional one. IT organizations need to adapt and shift their technology and operations to meet the increased application and network connectivity demands of this new architecture.

An anywhere data center requires IT teams to ensure technology and operational consistency on-premises, across the enterprise edge, and in hybrid and multicloud environments.

Automation

The growing scale, complexity, and workload portability within data centers is forcing network administrators to replace manual processes and apply automation tools to managing network policies and connectivity.

The adoption of software-defined networking, automation, and NFV for Layer 4 to 7 services puts data center networks in a viable position to support an agile on-premises cloud environment.



Almost 60% of IT leaders and network strategists state they have already deployed some form of SDN in their data centers.[14]

This allows workload-centric orchestration of the network together with compute and storage services. In fact, you could consider a data center network that has not yet adopted a controller-based, API-driven DevOps model as behind the times.

Almost 60% of IT leaders and network strategists state they have already deployed some form of SDN in their data centers.[14] SDN/NFV is already transporting 23% of traffic within enterprise data centers, a number that is expected to grow to 44% by 2021.[23] Those data centers without SDN will struggle to support agile and flexible application models.

Intent-based networking for the data center

Building on SDN fundamentals, intent-based networking lets data center teams achieve a holistic closed-loop validation architecture that analyzes data center behavior in real time against defined policies and enables an efficient and reliable method to make changes in the network. This allows IT teams to keep up with dynamic workload changes and continuously align to the application needs of the business.

In a data center scenario, it is also very important to validate policies before activating them. With IBN, this can be achieved through continuous, automated, and networkwide verification, including compliance policies.

Extending IBN to multicloud environments

To ensure desired service levels and security for today's organizations, data center teams need to extend control and visibility beyond on-premises environments. IT teams can extend IBN policy-based automation and enforcement to multicloud environments so that they can deploy policy consistently to workloads regardless of location.

Within two years, 29% of our *2019 Global Networking Trends Survey* respondents plan to have intent-based networking capabilities that maintain business-intent alignment by assuring automated network actions across multicloud environments.[14]

Tom Edsall, Cisco's CTO for data center, explains that "IBN is the boldest and most all-encompassing effort by the networking industry to create a system-wide networking model that addresses all the latest technology trends and fast-changing needs of agile organizations."

The key to a successful on-premises, multicloud, or hybrid implementation is to keep it simple. To achieve this, network architects should consider:

- No overlay network in the cloud
- No agent dependency, which allows broad applicability for any workload
- Adaptability to the scale of the cloud

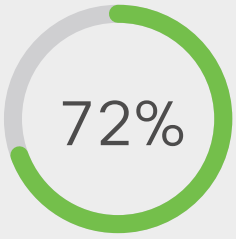
> "Intent-based networking is the boldest and most all-encompassing effort by the networking industry to create a systemwide networking model that addresses all the latest technology trends and fast-changing needs of agile organizations."
>
> **– Tom Edsall, CTO for data center and emeritus advisor, Cisco**

Underlying network infrastructure

In the data center, the underlying network infrastructure needs to provide open programmability and telemetry to support the automation and analytics that are central to IBN systems. Data center network infrastructure also needs to keep up with massive increases in traffic. Global data center IP traffic will grow threefold over the next five years. Overall, data center IP traffic will grow at 25% (compound annual growth rate) through 2021.[23]

3X Global data center IP traffic will grow threefold over the next five years.[23]

Network infrastructures need the flexibility and capacity to support both high-performance client-to-application (north-south) traffic and, increasingly, server-to-server or VM-to-VM (east-west) traffic. Today, this is typically done with a flat "spine-and-leaf" architecture supported by one or more control-layer overlay protocols.



By 2021, traffic within the data center will account for 72% of all data center traffic.[23]

According to the *Cisco Global Cloud Index*, by 2021, traffic within the data center will account for 72% of all data center traffic and will far exceed data-center-to-user (15%) and data-center-to-data-center (14%) traffic.[23]

Ongoing increases in Ethernet switching performance will be required to support the increased needs of compute traffic as well as file-based and even some block-based storage traffic.

With switched 400 Gbps now becoming mainstream, and IEEE specifications for 800 Gbps and even 1.6 Tbps in the works, the attractive capital and operational benefits of Ethernet make it inevitable that it will become an alternative to the more traditional fiber channel switching for some workloads.

Considerations when architecting your network for multicloud

In this expanded, more distributed application environment, network and cloud architects, data center executives, and infrastructures and operations teams need to develop a network strategy that will optimize the application experience. Here are some initial things to consider when doing so:

1. **Look to the organization's application strategy:** It begins with the application. IT and network strategists should have a good understanding of the organization's expanding workload and data footprint.

2. **Collaborate to bring consistency to multicloud:** Organizations need their multicloud environment (including on-premises) to work as one. Amid all the complexity, the data center and network teams should collaborate to develop consistency across their campus, branch, data center, edge/IoT, and public cloud/SaaS provider domains in order to gain optimized cost, performance, visibility, security, and user experiences.

3. **Extend policy-based automation consistency across hybrid and multicloud:** Teams should consider implementing policy-based automation across any platform, any hypervisor or container framework, any location, and any workload (cloud native, bare-metal, hypervisor, container, and serverless).

4. **Map application services and workloads and service components to the expanded network:** Network strategists and practitioners need a good understanding of what applications, services, and microservices are on the network.

5. **Prioritize application performance in your SD-WAN strategy:** Identify your most mission-critical cloud-based applications and services, and prioritize your SD-WAN plan to support those applications first.

6. **Bridge access policy and application policy across network silos:** To deliver policy-based secure segmentation everywhere, consider how IBN systems can map groups and policies between different network domains, such as WAN and data center.

7. **Build out NetDevOps skill sets:** As workloads and services require on-demand network services, not just within a data center but between remote locations, they will need to make their needs clear to the network. This will require NetDevOps skill sets that understand how to bridge application requirements to network policies.

8. **Augment SDN with AI advances:** Use AI capabilities to accelerate troubleshooting, enhance change management, and assure compliance.

Network access and wireless

Section summary

Key takeaways

- Emerging capabilities such as OpenRoaming will provide seamless, always-on, and secure global roaming between different Wi-Fi 6 networks and public 5G networks.
- Networking teams need improved analytics and AI-enabled capabilities for wireless planning, health monitoring, troubleshooting, and remediation.
- IT teams need to manage, administer, and propagate consistent access policy automatically across different access networks to better protect applications, data, users, and devices.
- Wireless networks will need to identify and dynamically support the demands of new immersive media applications and IoT devices.

Key findings

- Globally, wireless devices will account for 43% of all networked devices by 2022.
- IoT M2M devices will account for 51% of all networked devices by 2022, with the majority being wirelessly connected.
- 35% of network strategists recognize troubleshooting networking issues as the most resource-intensive and time-consuming activity for network operations today.
- 34% of organizations still use a manual approach to managing access across wired and wireless networks.
- 40% of organizations provide policy automation and segmentation for reducing the threat surface, with another 15% leveraging AI-enabled access solutions.
- Within two years, 27% of organizations plan to have an intent-based networking access model in place.

Essential guidance

- Consider how Wi-Fi 6 and 5G will affect your organization's future business requirements, and shape your wireless strategy accordingly.
- Build a roadmap for automating the secure onboarding and segmentation of all mobile and IoT devices.
- Explore the use of automated device classification to enable secure, large-scale onboarding of all types of IoT devices.
- Evaluate how location-based services and network analytics can deliver business benefits to your organization.

Section summary (continued)

- Explore how any specialized wireless technologies required for unique or demanding use cases (such as Bluetooth, Zigbee, and Thread) can be managed through a common management layer.

Top predictions

"By 2025, wireless federations such as OpenRoaming will be pervasive, allowing IT organizations and service providers to use zero-trust access systems, safely share identity credentials, and enable end users to seamlessly and securely roam on any wireless access network—both private and public. The user experience will be frictionless and policy-enforced, offering the best experience for users anywhere they connect."

– Matt MacPherson, CTO for wireless technologies, Cisco

"Through 2025, Wi-Fi 6 networks based on the IEEE 802.11ax standard, together with planned Wi-Fi 6 extensions, will become the predominant form of Wi-Fi everywhere. Only in about 2024 will the next generation of Wi-Fi based on the developing IEEE 802.11be standard (probably to be marketed as Wi-Fi 7) start appearing on the market."

– Andrew Myles, director and former chairman, Wi-Fi Alliance, and technical lead, Cisco

Network access and wireless

Globally, business IP traffic will reach 63.3 exabytes per month by 2022, a threefold increase from 2017.[3] Wired access, born from the relatively humble beginnings of shared wired local area networks like Ethernet (10 Mbps), token ring (16 Mbps), and FDDI (100 Mbps), has benefitted from ongoing innovations in silicon and optics to become the switched 400 Gbps Ethernet core network for LAN and metropolitan area network environments that customers can deploy today.

Ongoing innovations promise Terabit Ethernet and new advanced capabilities like Time-Sensitive Networking (TSN) for deterministic IoT applications in the not-too-distant future. However, in today's mobile-first world, wireless access is where a lot of the attention is focused. Wireless network access over either wireless LAN (Wi-Fi) or public mobile networks continues to change our lives in ways few could have imagined.

"We find that digital business innovation requires and drives advances in wireless innovation, while at the same time advances in wireless innovation themselves are opening up possibilities for new business innovations. It's the virtuous cycle."

– Guillermo Diaz, SVP of customer transformation, Cisco

> "Today 'experience' is the currency of business, and advances in wireless connectivity will be the enabler of many next-generation experiences. By combining the best of Wi-Fi 6 and 5G, network teams have the potential to make these experiences a reality."
>
> – Matt MacPherson, CTO for wireless technologies, Cisco

Globally, wireless devices will account for 43% of all networked devices by 2022, with smartphones accounting for 24% (6.7 billion) of all networked devices. At the same time, the number of IoT M2M devices will increase to 14.6 billion and account for 51% of all networked devices by 2022, with the vast majority being wirelessly connected.[12]

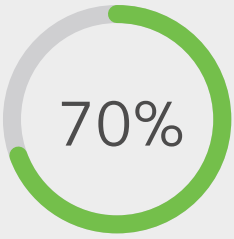
Delivering a delightful mobile user experience

People around the world have become accustomed to mobile applications such as Uber, Waze, and Webex® that make a significant difference in their work and private lives. They want their mobile experience to be an immediate one—always available, untethered, and ubiquitous—as well as a satisfying one that provides uninterrupted access to jitter-free 4K video, super-fast browsing, and crystal-clear voice over IP.

Just as importantly, wireless networks need to support new business innovations. As businesses increasingly adopt immersive media applications such as high-definition video, AR, and VR, leaders want to know that the network has the performance, capacity, coverage, and security to support new digital initiatives so they can move quickly when opportunities arise.

"Imagine if a shopper can receive a personalized and relevant experience powered by location services and AR," explains Matt MacPherson, Cisco's CTO for wireless technologies. "Or a warehouse can be outfitted with millions of sensors to allow autonomous electric robots and vehicles to fulfill orders and ship products."

New Wi-Fi 6 and public mobile 5G networks both promise dramatically better performance to support such requirements. Wi-Fi 6 brings higher data rates, lower latency, increased device density, and much better overall performance. Likewise, by 2022, public mobile 5G networks, slated for commercial rollout in the 2020 timeframe in a select set of countries, will offer speeds over four times faster than those experienced on 4G.[12]



Wi-Fi is widely used as a mobile offload mechanism and will be even more necessary in the 5G era. It's been forecasted that 5G will offload over 70% of its traffic, up from the 59% that 4G networks offload.[27]

Mobile users also want a transparent experience when accessing enterprise, cloud, and public Internet applications. That includes onboarding and roaming across networks.

By complementing 5G with Wi-Fi 6, users will get a transparent and always-on experience in private and public areas, both indoors and outdoors. This includes support for new data-hungry apps that could easily stretch the limits of many users' mobile data plans.

To help bring that vision to life, OpenRoaming builds on the Wi-Fi Alliance's Passpoint technology.[28] While still in an early stage, the OpenRoaming Foundation, a consortium of Cisco and several wireless leaders, is making the ambitious goal of seamless, secure roaming across private and public wireless networks a real possibility.

It allows users easy and secure global roaming between different Wi-Fi 6 networks and public 5G networks via a cloud-based federation of access networks and identity providers—including mobile carriers. OpenRoaming was demonstrated successfully at a recent Mobile World Congress.[28]

Using dual-mode devices such as smartphones and tablets, users will be able to switch seamlessly between private home or business Wi-Fi networks, public Wi-Fi hotspots, and the public 5G network.

"With OpenRoaming, mobile users will never have to guess which Wi-Fi network to use, suffer through a pop-up captive portal, or use an insecure username and password again. They will be connected wherever they go and can download, stream, video chat, game, and even work to their heart's desire."

– Matt MacPherson,
CTO for wireless technologies, Cisco

Preparing IT for wireless success

Network operations will need to get ahead of these emerging business requirements to deliver the desired mobile user experiences, as traditional approaches for deploying and maintaining wireless networks will not be sustainable.

In particular, troubleshooting wireless networks has traditionally been a reactive, complex, and resource-intensive activity for most networking teams. Not surprisingly, troubleshooting networking issues is recognized by network leaders as the most time-consuming activity for network operations today.[14]

Further complicating things is the fact that, in addition to emerging Wi-Fi 6 and 5G networks, IoT devices can communicate over multiple niche wireless protocols, including BLE, Zigbee, and Thread. The IT challenge will be to ensure that network management efforts are not split across these different networks.

Many IoT use cases will converge onto the mainstream Wi-Fi 6 and 5G networks, but IT teams should consider how they can manage more specialized wireless technologies required for unique or demanding use cases through a common management layer.

To get ahead, NetOps teams need a more proactive approach to wireless planning, monitoring, troubleshooting, and remediation. This requires much better visibility into wireless performance and health using analytics and AI-enabled monitoring.

Current and future state of network access readiness

IT cannot rely on traditional manual-access network operations to support mobile users. Instead, organizations need a software-driven approach that spans all network domains.

The network management system needs to be able to manage, administer, and propagate consistent access policy automatically across different access networks, even as users and workloads continue to move. It needs to unlock data and insights that will enable IT to support the business in real time and to employ AI to better predict problems and automate routine tasks. And in light of the growing prevalence of IoT applications, the network needs to automatically recognize and classify IoT devices and apply relevant policies.

Together, these capabilities will allow employees, customers, and business leaders to take full advantage of what Wi-Fi 6 and 5G offer. At the

same time, they will allow IT to not only survive the wireless deluge, but also ensure security and the best user experience in a mobile world.

In our *2019 Global Networking Trends Survey*, we asked network strategists where they are in their adoption of a secure access architecture related to the five-stage readiness model. 72% of respondents plan to deploy AI-enabled or intent-based access within two years, up from just 18% who do so today. Doing so will allow them to dynamically create and change policies and eventually consistently align access policies to business intent end to end, between users and services, wherever they roam or are located.[14]

Figure 21 Secure access readiness

Question: Which statement best describes your organization's current approach to network security?
Source: *2019 Global Networking Trends Survey;* n = 1556 network strategists

Considerations for enabling access and wireless for the digital era

1. **Wireless assurance tools will be a necessity:** In most industries, access connectivity is becoming predominantly wireless for both clients and things. Network strategists need to have advanced wireless assurance systems and tools in place to be able to deliver consistent wireless experiences across all IT and IoT access networks.

2. **Policy-based wired and wireless segmentation will save a lot of headaches:** Policy-based automation across the access, core, and branch networks allows segments and microsegments to be dynamically created and managed based on user and application groups so that networks form a dynamic zero-trust barrier to attacks and threats.

3. **Use AI-driven device classification before deploying IoT too broadly:** It doesn't make economic sense to protect inexpensive IoT sensors, monitors, and other devices with costly security solutions. However, using automated device classification and policy-based automation, IoT segments and microsegments can be dynamically created and managed based on IoT device and application groups.

4. **Prepare for Wi-Fi 6, 5G, and OpenRoaming:** Network leaders should make sure their wireless roadmap takes into account how Wi-Fi 6 and 5G will complement each other and work with devices, Wi-Fi operators, and service providers to deliver OpenRoaming capabilities.

5. **Consider location-based services:** Many business executives in retail, healthcare, and education are already taking advantage of the benefits of indoor location-based services for improved customer experience. According to our survey, 51% of respondents are already using location-aware wireless to enable a more personalized customer experience through mobile applications. Another 40% are evaluating the opportunity.[14]

6. **Prepare for microservices running on edge network devices:** With Kubernetes and other management and orchestration capabilities for container-based workloads, it is becoming increasingly attractive for application teams to start hosting network or application service components on workload-capable network devices at the edge. Consider how this will impact the network policy, performance, security, and segmentation requirements of your network.

Changing role of network security

Section summary

Key takeaways

- As applications, data, and identities move to the cloud and network edge, perimeter-based security alone cannot effectively protect against today's threats.
- The mix of many different types of devices and mobile users connecting from anywhere to networked applications everywhere results in new challenges, such as loss of visibility and control.
- Integrating security with intent-based networking capabilities results in a powerful combination that streamlines effective policy enforcement, protection, and remediation across the network.

Key findings

- Network strategists identified security as a top investment area, second only to AI.
- 43% of network teams identified improved embedded network security capabilities as a priority.
- In 2019, 48% of CISOs identified "time to remediation" as a main key performance indicator (KPI), up from 30% in 2018.
- Almost 75% of network leaders were confident they will have AI-enabled adaptive or automated policy definition and enforcement in two years.

Essential guidance

- Develop network security capabilities in five key areas: visibility and threat detection, zero-trust access, continuous protection, trustworthy network infrastructure, and integrated SecOps and NetOps workflows.
- Make sure a zero-trust security strategy is included with any network automation and assurance plans to effectively manage security threats regardless of where they exist across the distributed network.
- When upgrading infrastructure and processes, networking teams should take into account trustworthy requirements to help ensure that the network itself is tamper resistant.
- SecOps and NetOps teams need to consider how to share data, and should integrate tools to streamline threat prevention, detection, and response workflows.

Section summary (continued)

Top predictions

"By 2025, some leading-edge IT organizations will have deployed a limited set of fully automated network-enabled security workflows that will help accelerate remediation and reduce the workload on the SecOps team. The increased maturity of IBN platforms, AI/ML technologies, and integration between security and network tools will enable automation of some well-defined use cases that don't carry risk to the organization's security posture or network."

– Wendy Nather, head of the Advisory CISO team, Cisco

"In 2025, quantum computing will still be in its infancy. However, there will already be efforts to address the new danger of quantum computing being used to overcome current encryption methods."

– David McGrew, Cisco fellow, Cisco

Changing role of network security

The adoption of mobile, multicloud, and IoT models is creating new challenges and opportunities in network security. The traditional enterprise network perimeter is now just one element of a more distributed model where the identity of all users, things, and applications must be questioned, regardless of whether they are in the campus or branch, on a VPN, on the public network, or in the cloud.

IT teams need to leverage the combined powers of the network and security to be effective at tackling cybersecurity challenges. Network strategists readily recognize the importance of investing in network security. When asked how network teams can better meet business needs, respondents in our *2019 Global Networking Trends Survey* identified security as the number two area to invest in after AI, with 43% identifying improved embedded network security capabilities as a priority.[14]

The convergence of security with an intent-based networking model enables organizations to apply and enforce business role policies and respond faster to threats across all network services.

In this new reality, NetOps teams and the networks they control have a vital security role to play in five key areas:

Visibility: CISOs are concerned about maintaining visibility in this new distributed application and data model.

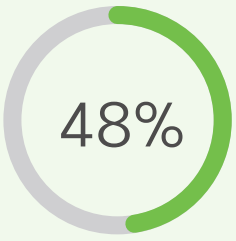
Zero-trust access: The network is an integral element for implementing a consistent trust model where all users, devices, and applications are equally suspect, regardless of where they access the network.

According to Forrester Research, a zero-trust network model must do three things:[29]

1. Segment networks in order to apply granular controls as well as prevent lateral movement.
2. Provide granular network analysis and visibility for threat detection and response.
3. Offer consolidated network security manageability and lay the foundation for automation.

Continuous protection: The network needs to act as both a distributed detection agency and an enforcement agency that can automatically and quickly take action to contain infected devices.

Trustworthy network infrastructure: With the growing threat of malicious actors looking for privileged information or trying to disrupt network operations, organizations must secure the network system and the individual network devices against attack.



In 2019, 48% of CISOs identified "time to remediation" as a key performance indicator, up from 30% in 2018.[30]

Seamless SecOps and NetOps workflows: CISOs see their SecOps and NetOps teams as working together, with 95% saying they are either very or extremely collaborative.[30] However, both teams still tend to use separate data, workflows, and tools to collect and analyze data. SecOps and NetOps teams need to rethink how they can streamline workflows, share data, and integrate tools to achieve a common goal of automated threat prevention, detection, and response.

According to Gartner Research, "for SecOps, access to network traffic supports retrospective analysis of traffic flows, identification of exfiltration attempts, network forensics, and microsegmentation workflows."[31]

Challenges with network security

Increased scale and complexity

IT must protect the organization and its data in the face of larger, more complex, and rapidly changing mobile-first and cloud-first environments and security threats that are increasingly difficult to defend against.

Workloads: As applications, data, and identities move to the cloud or Internet, the IT model continues to extend past the traditional organizational perimeter. This rise in hybrid and multicloud computing and microservices hosted at the edge requires a shift in how we secure workloads. Perimeter-based security alone cannot effectively protect against today's threats.

Clients: Additionally, the mix of many different types of devices (user devices and interconnected IoT devices) as well as different types of users (employees, contractors, third parties) connecting from anywhere to networked applications everywhere introduces even more complexity.[30]

Infrastructure: Finally, as the sophistication of threats evolves, attackers increasingly seek to subvert the underlying switching and routing infrastructure in order to eavesdrop, steal, or manipulate data and launch attacks against other parts of the network.[32]

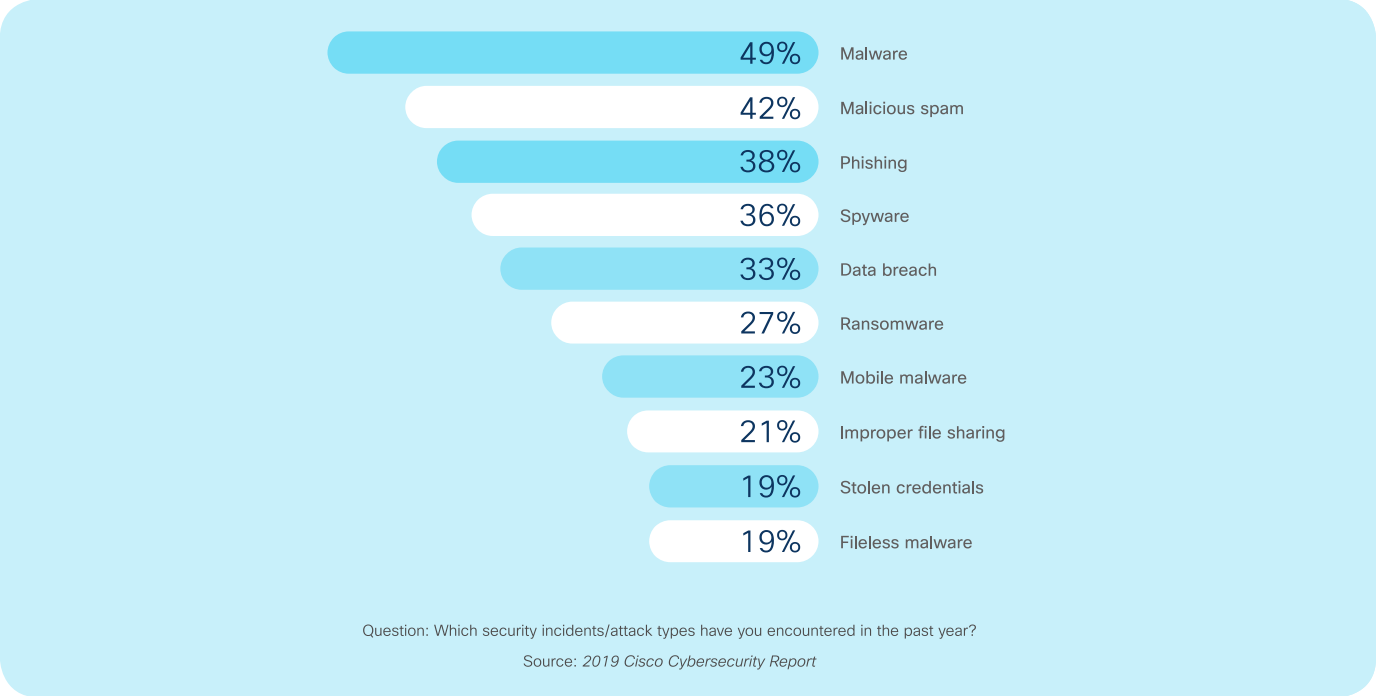
> "Like any other large organization, we need to deal with complexity at scale. We inspect 47 TB of Internet traffic, analyze 28 billion flows, and log 1.2 trillion security events daily."
>
> – Marisa Chancellor, director of infrastructure security, Cisco

The threat landscape: Continuous attacker innovation

As the potential payoff for cybersecurity attacks continues to become more attractive, the nature of attacks continues to become more sophisticated. Some of the more worrying threat trends include:

- Self-propagating, network-based ransomware
- Encrypted malware attacks, hidden within encrypted traffic, which made up an incredible 70% of all malicious attacks in 2017[4]
- IoT botnets deployed on unpatched and unmonitored IoT devices

Figure 22 Today's cybersecurity threats



For the latest information on the evolving threat landscape, see the current Cisco Cybersecurity Series Threat Report.[33]

Compliance

Security teams are also faced with adhering to new and emerging regulations. This means ensuring and demonstrating that effective security policies are in place.

The European Union's General Data Protection Regulation (GDPR) went into effect in 2018, requiring a proactive approach to data privacy. Also, healthcare, financial services, retail, federal government, and other sectors are requiring additional compliance standards, with the risk of heavy fines for noncompliance.

IoT device proliferation: Increasing the attack surface

Connected IoT devices continue to proliferate without adequate security, largely because they are often unknown or undetected by IT. Every connected device expands the attack surface for an organization. For IoT devices, network-level attacks may include distributed denial-of-service (DDoS) attacks, radio frequency identification (RFID) spoofing, and password-targeted and malicious software threats.

Gaps in visibility

The proliferation of new cloud apps and microservices can introduce gaps in IT visibility and control over their attack surface. Users can now install and self-enable applications that may be insecure or demand excessive access permissions.

> "Many IoT devices have little intrinsic security, rarely use digital certificates or credentials, and can be easily compromised. So automation of device recognition, classification, and network access policy activation become paramount in preventing or containing security breaches."
>
> **– Tim Szigeti, principal engineer, Cisco IoT**

The number and range of mobile devices (corporate and personally owned) will continue to grow, and the bring-your-own-device trend means more personally owned smartphones, laptops, tablets, and so on are accessing critical applications—resulting in further lack of visibility and control.

Tackling security challenges with an intelligent network

A NetOps team empowered with an intelligent network provides a powerful ally to SecOps in the ongoing fight to keep the organization and its data safe. By embracing an intent-based networking model where security capabilities are foundational, IT can enlist the network to automatically and effectively determine what is new, what is important, and what is unusual, regardless of where it exists across the distributed network.

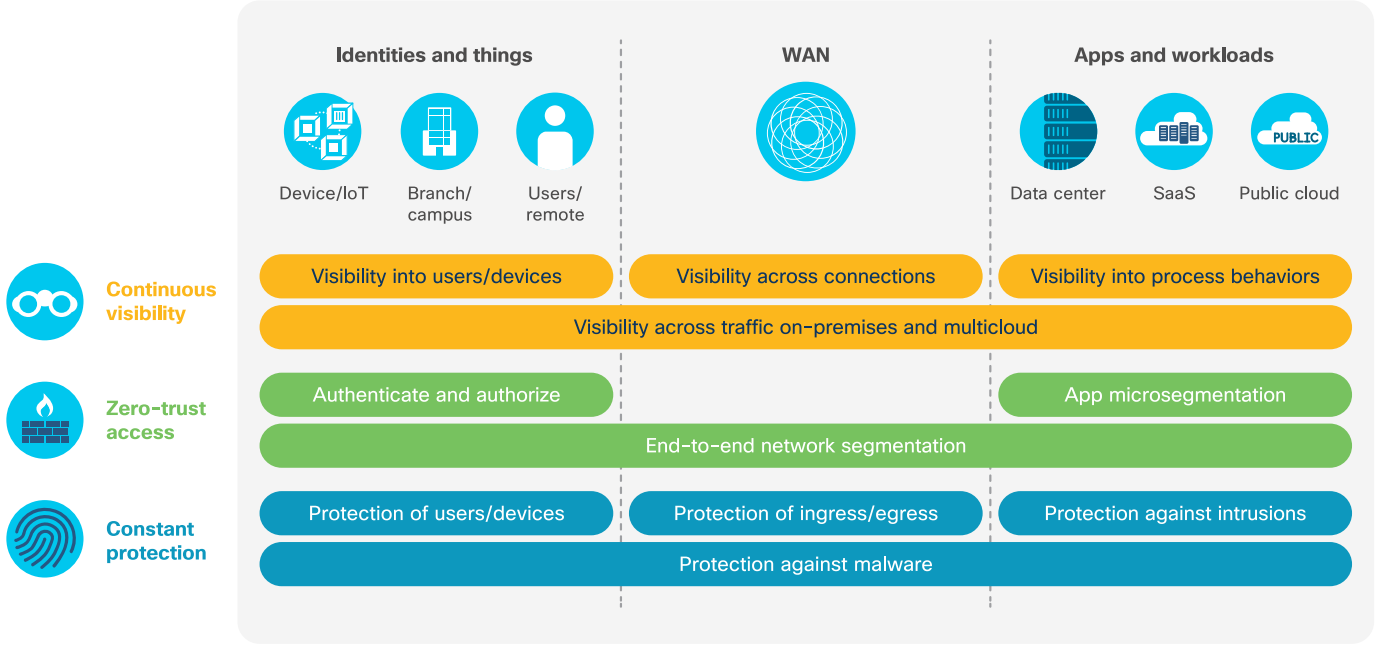
Ultimately the combination of intent-based networking and security provides continuous visibility and control into who and what is on the network. It also contributes to a complete zero-trust access model and builds threat prevention, detection, and rapid response into, not onto, the network for constant protection everywhere. (See Figure 23 below.)

Network visibility and threat detection

It has never been truer that you can't protect what you can't see. Visibility is fundamental for IT teams to protect network assets and information. This includes visibility into users, devices, apps, and things, wherever they are, in order to monitor anomalous activity and set policy.

> "We're dealing with large-scale movement to SaaS and are losing the traditional visibility and control that we've had in the past."
>
> **– Marisa Chancellor, director of infrastructure security, Cisco**

Figure 23 Integrated network security model



A full view across access, WAN, data center, multicloud, and IoT networks allows the mapping of every flow that traverses the network so that teams can determine a dynamic baseline of normal network behavior. With an intelligent network that provides full visibility, the network team has an invaluable resource to help the security team detect and remediate threats faster and more accurately—even in encrypted traffic.

Zero-trust access

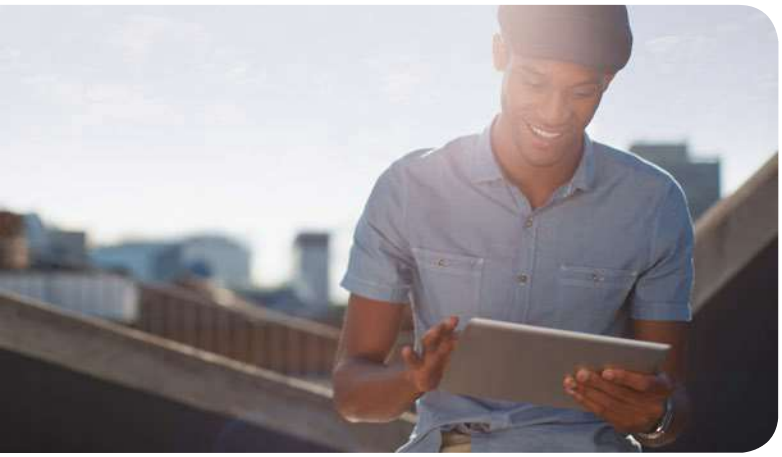
Building on an advanced visibility foundation, a holistic zero-trust security model enables NetOps teams to manage access regardless of the type and location of the devices and workloads in question. Applied suitably, it can protect workloads and data within the private or public cloud and the workforce, even when users are off network. The key capabilities of a zero-trust model include:

Securing network access: In a zero-trust access model, IT applies precise controls over who, what, when, where, and how user and IoT endpoints are allowed on the wired and wireless network. They can also apply a zero-trust approach by using group-based policy controls and end-to-end, client-to-application segmentation to restrict the access to resources on your network.

Proactively containing application breaches: IT staff can mitigate unauthorized lateral movement between workloads within or beyond the data center, which can help reduce the attack surface in the event that an attacker is already inside.

Mitigating the risk of unauthorized application access: When any type of user (employee, contractor, third party, etc.) logs into any on- or off-premises application, they need to verify their identity with two-

factor authentication (2FA) and verify the security of their device, mitigating the risk of unauthorized access to applications and data due to stolen or weak passwords.



Constant anywhere protection

To provide protection to all enterprise users and systems, the network needs to move with the times by extending protection beyond its traditional perimeters. Intent-based architectures like SD-WAN provide a centrally controlled platform for deploying and managing a full edge security stack that extends protection to every network ingress or egress. For full protection, this stack should include network segmentation, firewall, secure web gateway, malware protection, and DNS-layer security.

For any malicious files that manage to get through, malware detection can rapidly instruct the network to automatically move infected devices into a restricted or quarantined network segment. And by continuously updating threat intelligence to block malicious files and extending that intelligence to the endpoints and up to the cloud, the system can block such threats if they occur again.

Building a trustworthy network infrastructure

As organizations digitize and threats escalate, there is an increased need to verify the security and integrity of the network infrastructure and the individual network devices.

Building a "trustworthy" network infrastructure requires that security be implemented holistically across the entire product lifecycle. This helps protect against tampering and manipulation during manufacture, distribution, deployment, and continuous operation, which is especially important because third-party resellers, system integrators, or managed service providers are often involved in these processes.

When upgrading equipment, networking teams should look for a number of important capabilities, such as hardware-anchored secure boot, secure unique device identifiers, and the ability to destroy keys and activate factory reset.

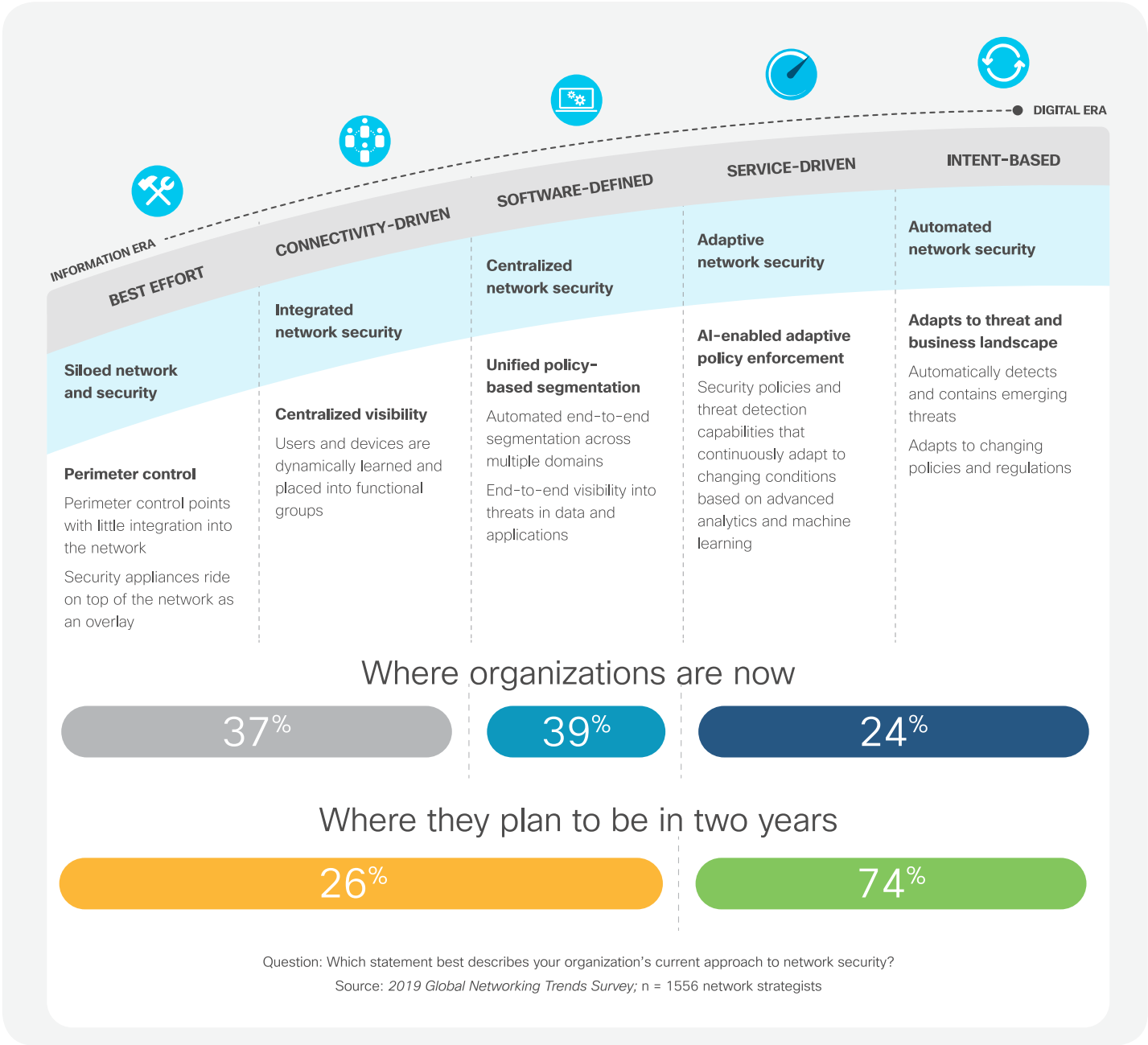
In summary, networks are becoming increasingly adept at addressing current and future threats. It's up to NetOps and SecOps to take steps to build these advanced security capabilities into their network designs and operations so they can work together toward achieving continuous visibility, protection, and trust.

Current and future state of network security

So where do organizations stand today in building out their overall network security model to achieve continuous protection?

In our *2019 Global Networking Trends Survey*, we asked network leaders how they would assess their current approach to network security vis-à-vis our five-stage readiness model. While organizations currently are distributed fairly evenly across all stages, almost three-quarters were confident they'd have some form of AI-enabled automated security policy definition and enforcement within that period.[14]

Figure 24 Intent-based network security readiness



Question: Which statement best describes your organization's current approach to network security?
Source: *2019 Global Networking Trends Survey;* n = 1556 network strategists