IDC EXECUTIVE BRIEF

NETWORK TRANSFORMATION IN GERMANY 2021

Goals, Requirements, and Technologies for Network Modernization

IDC ANALYZE THE FUTURE

APRIL 2021
SPONSORED BY CISCO

Good connectivity is the basis for all business priorities

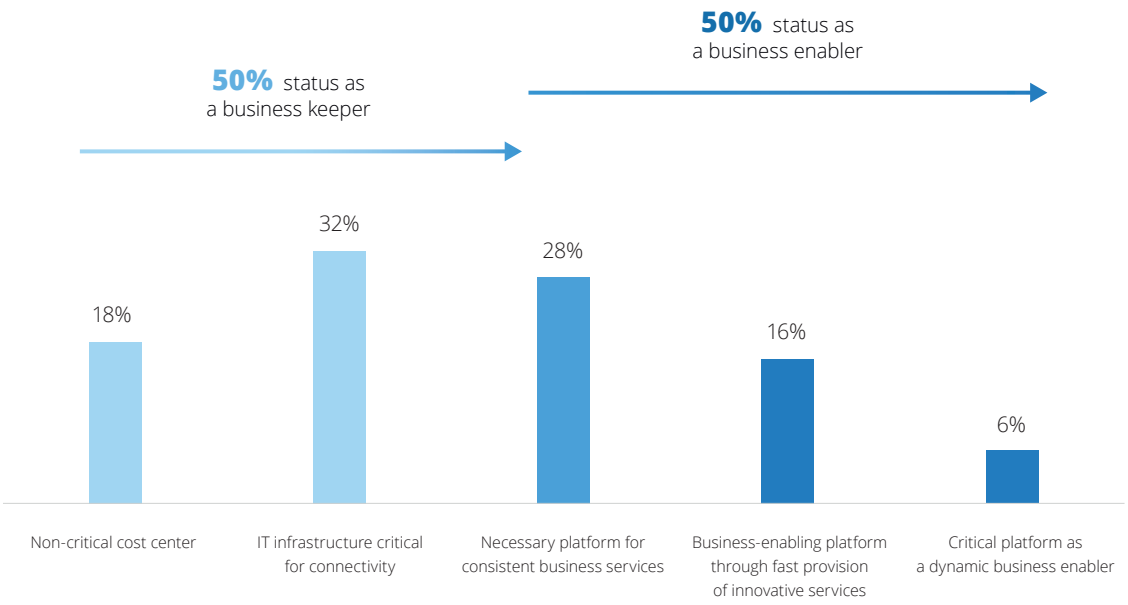
For years, many enterprises have neglected their networks, focusing instead on infrastructure topics such as the latest processors, GPUs, all-flash arrays, and cloud computing. All of them process data, but this data is mostly created elsewhere and has to be reliably transmitted to the relevant processing sites. This has prompted many enterprises to rethink the importance of networks. The COVID-19 pandemic was another wake-up call and showed many enterprises how much they depend on their networks, both in terms of employee connectivity and of service delivery with partners and to customers.

Reason enough to take a closer look at corporate networks and internal and external data flows. To gain a clearer picture, IDC interviewed IT business managers and IT specialists from 158 enterprises across all industries in Germany with 250 employees and more, and with at least five WAN connections and critical connections in public clouds, to find out how corporate networks are run and equipped for the future.

Heterogeneous perception of the network role:
Cost center vs. innovation enabler

Many enterprises are yet to fully appreciate how much they depend on their networks today and, more importantly, will do so in the future. On the contrary, in around half of the enterprises surveyed, networks are taken purely as a cost center and reduced to a connectivity role. The remaining 50% of organizations ascribe them a transformative role in which they are regarded as a basic platform for day-to-day business, as an innovation and business enabler. Equipped with their own control level and intelligence, they provide scalable, consistent, and yet agile services that enable ongoing adaptation to constantly changing business requirements and form the basis for new innovative technologies such as IoT, edge computing, and AR/VR.

Figure 1: How management views the network's role



N = 158; without "Don't know"
Source: IDC "Network Transformation in Germany 2021" survey

Modern network environments generate new requirements

Modern technologies, the data traffic they create, and the network's role as a transformative business enabler generate many new challenges that cannot generally be surmounted with today's static network architectures. The design of typical modern corporate networks has already changed dramatically.

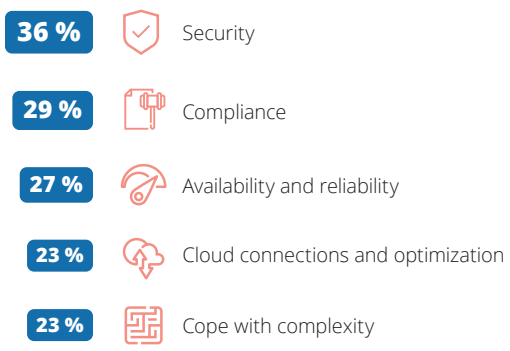
They used to be relatively manageable and largely consisted of wired client-server networks, some private site connections, and central gateways that connected internal networks to external parties such as the internet or to employees via VPN.

Most modern corporate networks are far more complex and may comprise:

- Datacenters, co-locations, datacenter providers, and hosts
- Private connections, carriers, content distribution networks (CDNs), and internet providers
- Private, public, and hybrid clouds
- Mobile peripherals, edge, and other smart devices
- Numerous wired and wireless network areas
- Partners, suppliers, branch offices, and customers who are connected to their resources by diverse means and applications

The boundaries of any given network and those of network traffic have therefore become far more diffuse, and more difficult to identify and control, creating challenges for security and compliance. Despite numerous new internal and external network components, enterprises still need to stay in control and enforce security policies. And because value creation is increasingly linked to IT, or even hinges on it, maintaining network availability and reliability is a key mission.

Figure 2: Major challenges in current network operation



N = 158; multiple answers possible; abbreviated
Source: IDC "Network Transformation in Germany 2021" survey

Network transformation for more security, flexibility, and resilience

For the respondents, the ongoing issue of security is not only a challenge, but also one of the key drivers of network modernization. Modern intelligent approaches and network technologies help to make networks and traffic transparent and to identify security risks.

Network management and network automation bring additional dynamism to the task. Manual approaches are hard put to deal with the complexity and sheer volume of data and devices while manual procedures are a security risk. Only full network transparency, the holistic approach based on it, and automatic processing of network management tasks can master this complexity.

Figure 3: Major drivers for network modernization and transformation

N = 158; multiple answers possible; abbreviated
Source: IDC "Network Transformation in Germany 2021" survey

The same applies to the growing number of applications. Configuring individual network devices, protocols, and ports to deliver individual applications can be challenging in networks that have evolved over time, and each new application adds increased cost and complexity to the challenge. To best support dynamically changing application landscapes, flexible network structures are required that can be adapted to the requirements quickly and agilely. It is not just the number of applications that cause the dynamics, but also their degree of utilization. Flexibility therefore also means being able to add external on-demand resources such as cloud or carrier services to support in-house networks during peaks in workloads.

Other key drivers, given their growing indispensability and criticality for day-to-day business, are network availability and resilience. Network teams must be able to ensure continuous availability and to deploy resilient structures and technologies to ensure that all network functions are restored as quickly as possible in the event of a failure.

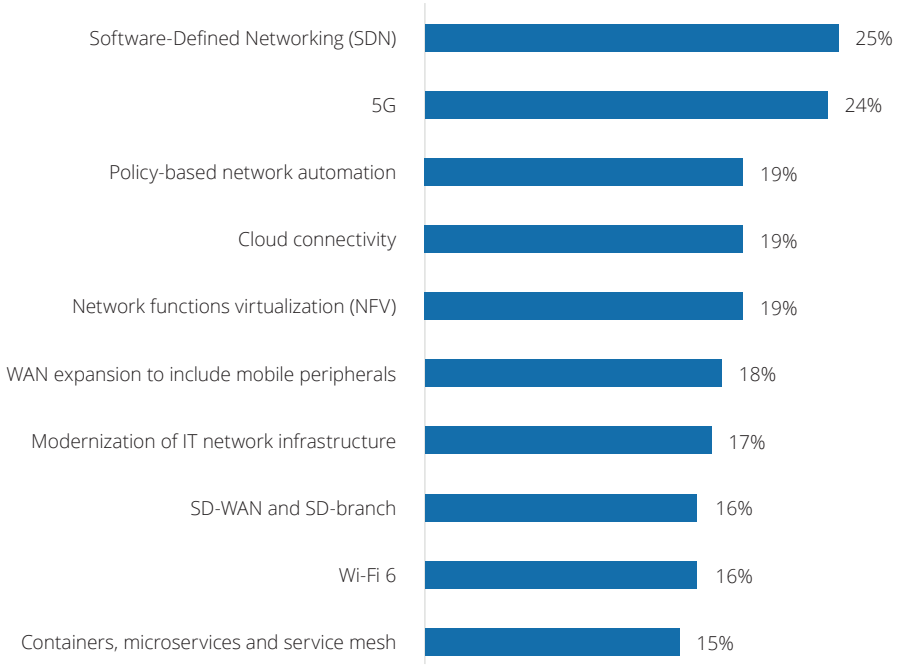
New network technologies enable integration and automation

For many enterprises, software-defined networking (SDN) is currently the most important area for network transformation. Other relevant technologies in this area, such as network function virtualization (NFV), SD-WAN, and SD-Branch, are also based on network virtualization and software-defined networks. Similarly to other virtualized and software-defined infrastructures, separating physical hardware and controlling software also offers many benefits in network operation.

Whereas previously the control level of each individual device selected the right protocol-based route for traffic, a common controller now takes charge of this task for the entire network. The benefits include a holistic view, network programmability, and network automation based on policies that specify minimum network performance requirements and so forth. Virtual resources are also much easier to configure, scale, or migrate to another location in the IT environment as required, significantly increasing flexibility and agility. Moreover, they facilitate the integration of network domains that are usually separated or operate in silos.

The new 5G and WiFi 6 wireless technologies are also important for network transformation. They can be combined with SDN to facilitate device connectivity while delivering the same high level of performance as a wired connection. This also provides a starting point for WAN expansion. The daily challenge of connecting new locations and branches to the corporate network via WAN now also extends to mobile peripherals. Using workarounds with VPNs and cloud apps to satisfy increasing security and performance requirements is becoming more difficult. The future approach in this case will also be software-defined to enable peripheral connectivity and management via SD-WAN or SD-branch solutions with an over-arching control level, irrespective of the connection type and physical connection medium.

Figure 4: Top 10 most important technology areas for network transformation in the coming 24 months

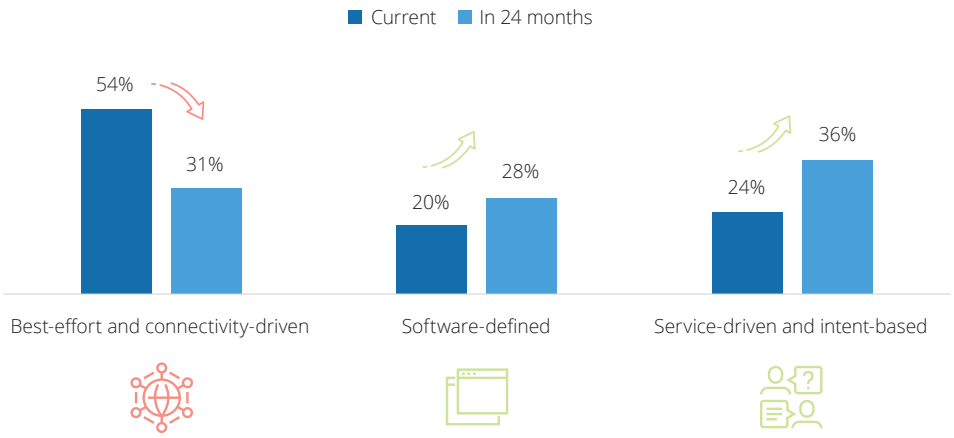


N = 158; multiple answers possible; abbreviated
Source: IDC "Network Transformation in Germany 2021" survey

Software-defined and intelligent — the network architecture of the future

Employees should enjoy the same working conditions and environments at all locations to be productive everywhere — across all the applications and services they use in their daily business. IDC refers to a "branch of one" architecture approach in this context — the entire enterprise is "one universal branch office" with consistent performance and user experience. Such requirements cannot be realized with outdated network architectures. More than half of the networks in Germany are landscapes that have evolved over time, providing only best-effort functionality or are at least connectivity-driven. While the latter ensure optimum end-to-end connectivity, scant importance is attached to the quality of connectivity.

Figure 5: Network architectures currently implemented and planned over the next two years



N = 158; without "Don't know"
Source: IDC "Network Transformation in Germany 2021" survey

Of late though, more advanced architectures are becoming increasingly prevalent. There is a growing trend towards using SDN architectures. Service-driven and intent-based architectures go a step further. Drawing on SDN and new approaches to network and performance management, they align networks to the individual needs of business units and their applications, make adjustments automatically, and continuously improve the network.

The implementation of these architectures is complex and requires advanced technological expertise as well as sophisticated AI/ML algorithms. This is not just a matter of network upgrading, but of efficient restructuring so that various end-to-end data streams can be mapped and optimized according to business requirements. Usually, this means combining corporate and third-party network infrastructures, which can be optimally achieved with software-defined architecture and case-by-case configuration. These architectures tend to be rare at the moment, but in IDC's opinion, they will become significantly more common as digitalization progresses and more ambitious real-time applications are developed.

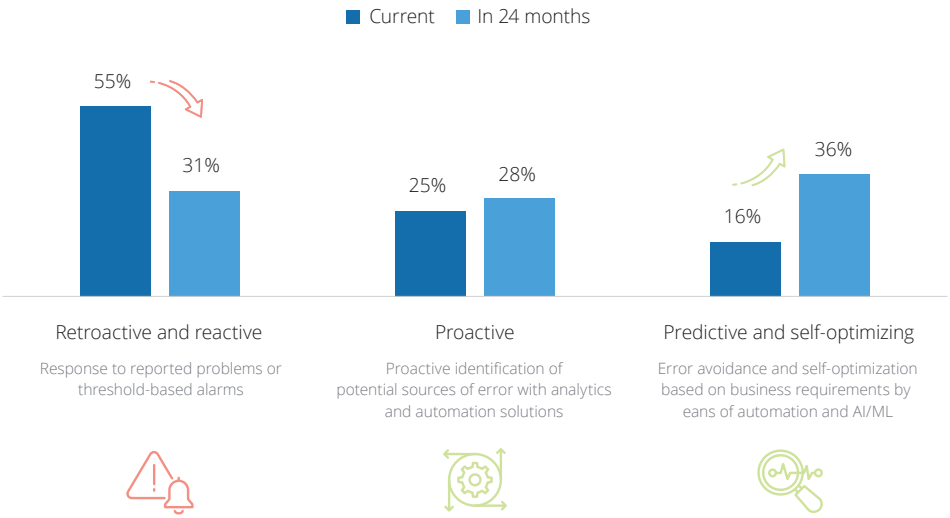
By contrast, SDN is well on its way to becoming "state of the art" for networks. Around two thirds of the enterprises surveyed already use SDN in different domains — for example, via software-defined infrastructure (SDI) in their datacenters or via SD-WAN for site connectivity. The main benefits of SDN are regarded as cost optimization (28% of respondents), more efficient application operation (26%), reduced hardware management (26%), and improved security and compliance (25%).

AI/ML and automation are becoming critical requirements for network operation

Regardless of the architecture used, day-to-day network management is an important factor in maintaining a functioning network. Not only the implementation of new technologies, but also regular tasks pose a challenge for network teams in most enterprises. More than two-thirds of the enterprises surveyed struggle with tackling routine network management tasks — from onboarding new applications and integrating new network devices, peripherals and locations, to managing contracts and providers and detecting and resolving security issues.

This is largely due to manual network management, which is still common in 55% of enterprises. These reactive and retrospective approaches usually mean that challenges are not addressed until they have become a problem. To avoid this, enterprises are increasingly opting for proactive network management approaches. They use automation and analytics to replace manual management processes, reducing sources of error while detecting problems at an early stage — at best in real time, when they can still be corrected easily. Yet automating management tasks using fixed configurations and policies will not suffice in the future, as the policies required by large IT environments easily run into the thousands. Manual configuration, management, and customization of policies is therefore not a long-term option. Proactive, self-optimizing management approaches based on AI/ML algorithms combined with SDN will be essential. They identify new IT and business requirements, derive appropriate measures, recognize potential problems and their causes at an early stage, and automatically program or optimize configurations and policies based on experience.

Figure 6: Currently used and future network management approaches



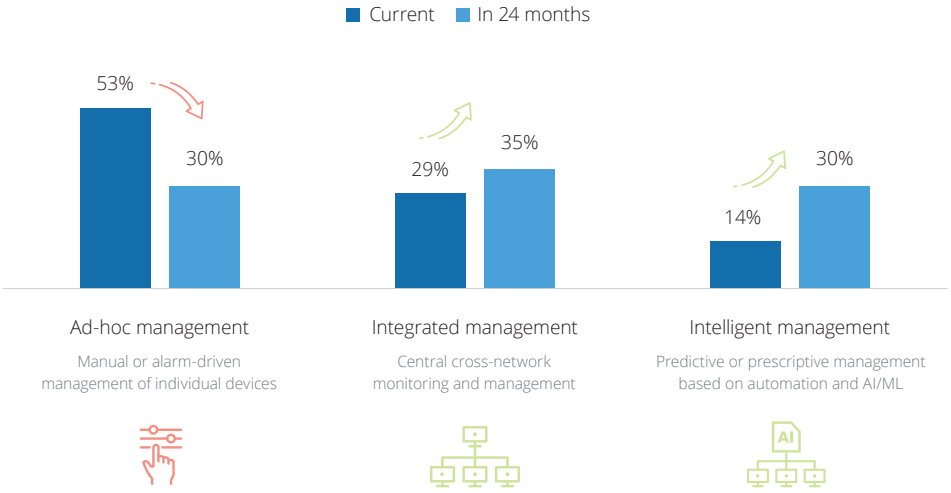
N = 158; without "Don't know"
Source: IDC "Network Transformation in Germany 2021" survey

Optimizing network quality with holistic performance management

Another common problem is performance monitoring in networks as a functioning network management and basic connectivity reveal nothing about their actual quality. If performance management is carried out incorrectly or neglected, enterprises are denied the chance to define and rate performance in the first place, and to identify and quickly remedy performance problems. Manual ad-hoc monitoring of individual devices or network silos, as practiced in more than half of the enterprises surveyed, is also problematic for several reasons. For one thing, incidents are only dealt with if they happen to occur at the time or are discovered in log files, and for another, because although problems occur in one place, their cause may be elsewhere, in another network team.

Manual troubleshooting is like looking for a needle in a haystack, given the thousands of internal and external devices, connections, and applications. For modern technologies and most usage scenarios, such as smart factories and data streaming, such delays are unacceptable and can seriously disrupt business processes. Integrated network-wide supervision and monitoring that measures different KPIs across the network, applications, and peripherals can significantly reduce these issues and, in IDC's view, should be considered a minimum standard now already.

Figure 7: Currently used and planned future network performance management approaches



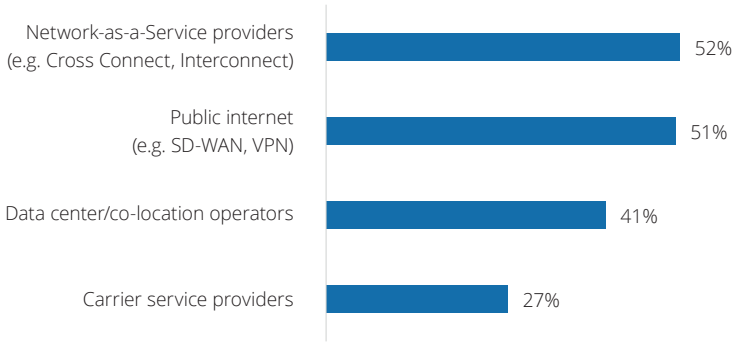
N = 158; without "Don't know"
Source: IDC "Network Transformation in Germany 2021" survey

Moreover, without comprehensive performance monitoring, comprehensive optimization is almost impossible. Applications and services not only rely increasingly on maximally fail-proof, ultra-available connections, but have other requirements in terms of data throughput, latency, jitter, and packet loss. These very individual requirements can be specified to networks for each application via the relevant performance SLA or QoS provisions. In the future, with the help of AI/ML algorithms and SDN, modern intelligent performance management will be better equipped to control traffic across networks based on these individual specifications to anticipate potential problems and adapt network capacities in line with anticipated performance or capacity changes.

Counting in the cloud as an integral part of corporate networks

Cloud adoption has a significant influence on IT in general, and on networks in particular. Applications are increasingly hosted in the private or public cloud and distributed via IaaS provider, carrier or the internet — and in some cases, by all of them together. These infrastructures, too, become directly or indirectly part of an enterprise's network and digital performance. Hybrid clouds are also becoming increasingly popular in optimizing application landscapes: this integration of private and public clouds enables the flexible movement of IT workloads between systems in line with current requirements. This has a direct impact on networks: the commands or data required to start virtual machines or containers and the generated data must be exchanged between the cloud instances and then forwarded to the destinations.

Figure 8: Types of connections used to access important external cloud services



N = 146; only enterprises with important connections to external clouds; without "Don't know"
Source: IDC "Network Transformation in Germany 2021" survey

Public cloud applications are becoming increasingly interconnected via APIs to share data and services, turning them into multicloud environments. Since enterprises do not usually maintain direct physical connections between different cloud datacenters, connectivity services are being offered increasingly for this as well. Network-as-a-service (NaaS) solutions, often called "datacenter interconnect" or "cloud interconnect" solutions, directly connect datacenter operators, cloud hyperscalers, and internet carriers, and thus offer deployment and scalability as well as other cloud services for network infrastructures.

The so-called SDN-based "cloud managed networks," which can also be purchased as NaaS, enable enterprises to globally manage and control their own and external network resources, as well as complex and distributed data streams in the cloud, without having to build and maintain their own extensive network infrastructure. Increasingly, individual network functions such as firewalls, load balancing of the IDS/IPS can also be integrated into corporate networks as cloud network function (CNF) services.

Conclusion

Corporate networks have long been neglected compared to other topics. However, there are many reasons for enterprises to take their networks seriously and to look more closely at their use. All modern technologies are based on reliable device connectivity, real-time processing, and secure connections. In other words, anyone keen to successfully apply enterprise mobility, remote working, or data analytics and to use increasingly relevant technologies such as IoT, edge computing, and VR/AR in order to support their employees, or to create new business models, will have to address the subject of networks.

To avoid losing time, the right course should be set now and appropriate framework conditions created. A key prerequisite for enterprises is to evaluate the role and importance of their network. They must clearly define their business objectives and the technologies needed for new business models and, on this basis, work out network requirements and modernization measures. Enterprises must also clearly assign responsibilities for implementing these measures. Importantly, a central department must keep track of far-reaching changes, while taking into account new business ideas and changing requirements. Enterprises must also ensure that network teams possess the appropriate expertise to apply new, virtualized, software-defined and cloud-based networking technologies, and that the necessary soft skills are promoted to understand business requirements and to translate them into IT requirements.

Building the optimum network environment and ultimately a "branch of one" is not an easy task and should not be underestimated. However, no enterprise can afford to pass up the positive effects on productivity, innovation, and competitiveness and the opportunities they unlock.

Methodology

In February 2021, IDC conducted a primary market survey to gain insights into the status of IT networks for enterprises and into the plans, challenges, and success factors of German enterprises in their handling of current and new network approaches, architectures, and technologies. Based on a structured questionnaire, in February 2021, IDC surveyed IT managers and specialists in 158 enterprises across all sectors in Germany with more than 250 employees, and with at least five WAN connections and critical connections in public clouds. The following information was supplied by Cisco.

IDC
ANALYZE THE FUTURE

CISCO

Case study: Jade University of Applied Sciences

WWW.CISCO.DE

CUSTOMER PROFILE

University with 3 campuses in Wilhelmshaven, Oldenburg, and Elsfleth with 7,600 students

CUSTOMER REQUIREMENTS

- Centralized, automated network management across the three sites
- Consolidation of legacy infrastructure
- Consistently good user experience for students and staff alike at all sites

SOLUTION MAPPING

- Central management via Cisco DNA Center
- Automated policies and access issuing via SD-Access
- Network performance guaranteed by Cisco DNA Assurance
- Network infrastructure standardization based on Catalyst 9000 series

PROJECT HIGHLIGHTS

- Improved visibility of network components, peripherals, and users in the LAN and WLAN
- Automated campus-wide distribution of policies for peripherals and users in line with access requirements
- Fully centralized life-long management of network components, including best-practice-based commissioning, configuration, and software updating
- Backed by Cisco DNA Center, Jade University's network infrastructure can be managed by one person

"With access to current and historical network traffic, access points can be reconfigured to meet future needs."

"When a user calls me with a configuration or connection issue, I have all the information I need at my fingertips and can help immediately."

HENNING BOHLKEN, LEAD NETWORK ENGINEER

CISCO

Case study: Bosch

CUSTOMER PROFILE

Bosch Group is a leading international provider of technology and services. The company employs around 410,000 people worldwide. Its corporate activities are divided into four business units: Mobility Solutions, Industrial Technology, Consumer Goods, and Energy and Building Technology. As a leading IoT company, Bosch offers innovative smart home, smart city, connected mobility, and connected manufacturing solutions. Bosch offers products "invented for life".

CUSTOMER REQUIREMENTS

- Reduce time-to-market by means of optimum datacenter operation
- Transform datacenter operation to support connected products and services
- Identify and eliminate network vulnerabilities before they affect business

SOLUTION MAPPING

- Bosch's "intent-based" network solution is based on Cisco ACI for workflow automation. It enables workflow automation and simplification, as well as proactive management of datacenter networks, and frees up time to devote to innovations and business projects.
- The openness and flexibility of Cisco's automation APIs enable seamless integration into business processes and the integration of technologies such as OpenStack and Kubernetes. With Cisco ACI and the flexible spine/leaf architecture of Cisco's Nexus 9000 series switches, services are now provided based on the zero-touch model.
- Cisco's intent-based networking solution transforms datacenter networking into a proactive model. The entire network is checked for correctness so that its Bosch operators can be sure that it is always compliant with the intent originally defined.

PROJECT HIGHLIGHTS

- Implementation of a central network platform for all datacenters
- Optimization of datacenter network operation to enable innovation
- Faster datacenter fabric delivery reducing provisioning time from days to minutes

"The openness and flexibility of Cisco's APIs for automating underlay and overlay networks tipped the scales in favor of using Cisco ACI. It enabled seamless integration into business workflows and technologies such as OpenStack and Kubernetes with full support from Cisco."

JAN HOLZMANN, SENIOR MANAGER FOR CENTRAL NETWORK SERVICES, BOSCH

"We spent most of our time on network operations, which left little time for innovations. With Cisco ACI, we can devote more time to projects that put Bosch ahead of the curve as a company."

GERO BECK, SENIOR NETWORK ENGINEER, BOSCH

Interview with Uwe Müller & Falko Binder, Cisco Systems

NETWORK TRANSFORMATION IN GERMANY 2021

At the presentation of the "Network Transformation in Germany 2021" survey findings, IDC spoke to Uwe Müller and Falko Binder from Cisco Systems.

IDC: The current situation involving the sudden need for remote working has shown enterprises how difficult it is to respond to new network requirements. How do you help users to flexibilize their networks to meet new performance requirements?

Müller: The home network, connection via a router, and optimum line, peripheral, and application protection are all part of the equation. For instance, Cisco can help customers securely connect a video terminal or laptop to the corporate network. Modern networks are no longer limited. They stretch from home workplaces into the cloud or into the corporate network and its datacenters, which in turn are connected to each other and exchange data with other datacenters.

Remote working is therefore a challenge for IT infrastructures. Demands on IT have increased because applications need to be always available everywhere, and services managed from everywhere, whether they are in the cloud or in the datacenter.

IDC: Networks are often business-critical infrastructures. That is why security is frequently a focus — both in terms of operational reliability and resilience and of IT security. What should users look out for in particular?

Binder: Users are primarily interested in their applications and high-performance, secure network connections. They should exercise the same degree of security awareness everywhere. The "famous" USB flash drive should therefore be suitably protected both within the enterprise and at home.

The administration should take two things into account: architecture, and thus the seamlessness of security from user to application and operation, and ensuring a certain level of life-long security.

The security concept should start with the end user and extend to the application. Furthermore, the underlying infrastructure must be dovetailed and not consist of a string of island solutions. For the network, that means everything, from the LAN and WAN to the datacenter must form a secure entity.

While secure operation can be implemented by deploying certified systems, it is ensured by setting up, following and constantly developing secure operating procedures.

IDC: Mobile peripherals, trends such as the Internet of Things, and external infrastructures such as the public cloud make networks increasingly complex and diffuse. How do you help your customers to stay in control and cope with this complexity?

Müller: You need to simplify the complexity. And this can be achieved by automation. A modern, intuitive network recognizes automatically what configuration it needs and adapts itself accordingly. Modern infrastructures self-configure to suit peripheral requirements in line with predefined policies.

Cisco opts for the platform concept, which is aimed at providing a controller or "single pane of glass" for all these tasks. By coordinating security, cloud, and network policies, a scalable concept is created with a unified management platform.

IDC: Cloud services are increasingly becoming an integral part of the application landscape, along with the data streams they generate. What network design aspects do you recommend customers focus on to ensure efficient use of cloud services?

Binder: Modern users communicate directly. The network must be smart enough to recognize that secure, direct communication from the user to the application is enabled in the cloud. This is achieved through SD-WAN architectures.

The services of current datacenters are enhanced by cloud-based services. It makes sense to merge the physical and cloud datacenters and manage them via a uniform set of policies. As a lot of users today use services from different clouds, connecting a network for multiple clouds to the existing datacenter network is recommended.

This newly won agility should be monitored in real time and automatically adjusted to user expectations.

Uwe Müller
Datacenter Sales Lead Germany, Cisco Systems

IDC: With new approaches such as software-defined networking (SDN), companies can make their networks intelligent and programmable. In your opinion, what should the network of the future look like and what foundations can you already lay for your customers?

Müller: Today's networks are fully automated and tomorrow's even more so. They adapt flexibly to users. They are efficient and offer lifelong security from the outset thanks to zero-touch deployment mechanisms.

They are also equipped with AI mechanisms. Trends and also errors are therefore detected proactively. These mechanisms offer network assurance, which provides a high level of service in an increasingly complex environment.

Regardless of how small or large a network is, it has to be fully automated, secure, intelligent, integrated, and predictive.

Falko Binder
Enterprise Networking Sales Lead Germany, Cisco Systems

For more details of this publication please contact:
Katja Schmalen, Marketing Director, +49 69 90502-115 or kschmalen@idc.com.

IDC CENTRAL EUROPE GMBH

Hanauer Landstr. 182 D
60314 Frankfurt • Germany
T: +49 69 90502-0
F: +49 69 90502-100
E: info_ce@idc.com
www.idc.de

IDC ANALYZE THE FUTURE