6 KEY TRENDS

RESHAPING DATA NETWORKING FOR BUSINESS

Telia

INTRODUCTION

Digital technologies are reshaping our private and business lives. Professional organizations are in a continuous competition to grow their businesses and improve their efficiency. In these organizations, digital technologies are acting as enablers for innovations. Data networking services that communication service providers offer to the organizations, ie. data networking services for businesses, are a focal point in this development.

Digital transformation is an on-going development in the organizations where innovations based on digital technologies are harnessed for growth and efficiency. A recent example of an area of rapid digital transformation is Work From Anywhere. The pandemic lock-down forced organizations to reshape their ways of working supported by digital solutions. Digital transformation covers the whole ecosystem of an organization emphasizing the customer value creation and organizing parties to create value on a shared digital platform.

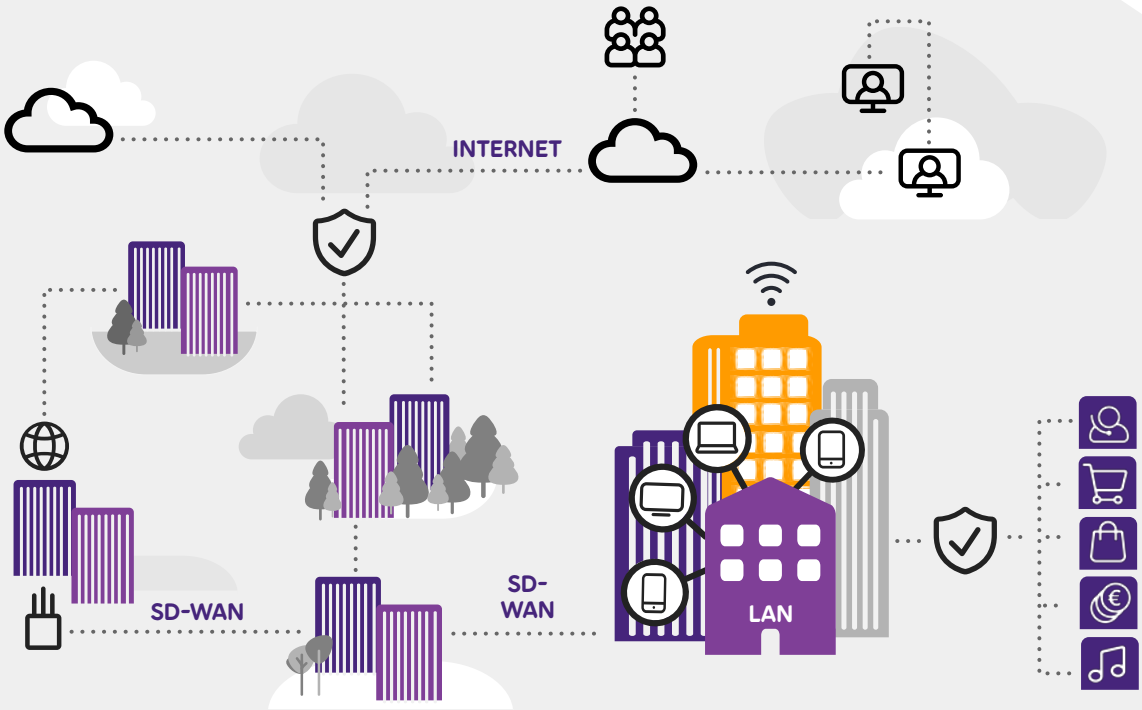
The total amount of data created, captured, copied, and consumed in the world is increasing exponentially. The opportunities for data-driven value creation are emerging as new value pools, new business models, richer stakeholder experiences and better decisions.

Hyperconnectivity is a term that is used to define the connectivity that exists in digital environments and the interaction between information systems, data and devices, all of them related to each other through the Internet. The more connected systems, devices and data there are, the more there are opportunities to create value through digital transformation for organizations individually and in digital business ecosystems. Conversely, the innovations on digitalization put pressure on connecting even more devices, systems and data.

One of the emerging branches of hyperconnectivity is Tactile Internet. It is the next evolution of the Internet which will enable the control of the IoT in real time with all human senses interacting with machines. It will enable humans and machines to interact with their environment in real time, while on the move and within a certain communication range.

Cyber security and its subcategory network security are heavily impacted by the digital transformation development. The more organizations are using digital technologies, the bigger the exposure to system vulnerabilities. The attack surface increases when the number of users, devices, applications, services and data increases. Because of the ecosystem development, the amount of 3rd party employees in the organization IT landscape increases thus adding to the risks.

The services enabled by digitalization can accelerate sustainable growth. As an example, the digital sector has the potential to directly reduce fossil fuel emissions 15% by 2030 and indirectly support a further reduction of 35% through influence of consumer and business decisions and systems transformation (The Exponential Roadmap Initiative, 2020).



TREND 1:

DIGITAL TRANSFORMATION BOOSTS DIGITAL BUSINESS ECOSYSTEMS

Digital transformation is the process of using digital technologies to create new or modify the existing ways of doing business. Digital transformation is a broad process impacting not only the actual deliverables of an organization, but also strategies, leadership, people and processes.

Netflix represents a great example of digital transformation. At first, Netflix disrupted the video rental business by introducing mail-order DVD discs. Then, digital technologies enabled wide-scale video streaming. Today, Netflix's business covers broadcast networks and production studios capable of providing on-demand content with low prices and great user experience.

A business ecosystem is the network of organizations - including suppliers, distributors, customers, competitors, authorities, and so on - involved in the co-creation of value through both competition and collaboration. The ecosystem members are in interaction with each other, creating a constantly evolving relationship in which each entity must be flexible and adaptable to survive.

In the digital business ecosystems, the emphasis is on customer value creation and in highlighting the role of digital technologies and organizing parties to create value on a shared digital platform. Digital platforms enable ecosystem members to share resources, increase knowledge sharing and relationship building which then leads to value creation. One of the main motives for organizations to participate in digital business ecosystems are business model innovations, creating new revenue streams and building competitive assets for the future. Examples of orchestrators of digital platforms are technology leaders like Amazon, Google and Microsoft, but there are many emerging leaders in their own niches.

Software defined connectivity services and enablers like APIs, Artificial Intelligence (AI), Machine Learning (ML) and Analytics are essential in supporting digital transformation and digital business ecosystems.

Software defined connectivity services enable digital business ecosystems

Software defined connectivity services contribute to the digital innovations to boost digital business ecosystems. First, software defined connectivity services support dynamic and flexible networking needs of the business ecosystems and secondly, they enable new digital innovations.

Because of the dynamic nature of digital business ecosystems, they need to be created and closed rapidly. In addition, the changes in the connectivity services are required to take place with no delay. Typically, access links need to be added on-fly or more capacity needs to be allocated to a new ecosystem member. The software defined networking services come with customer portals, which enable the organizations to request the services on-line or through APIs, which are then automatically enforced in the service provider production.

The digital platforms are typically run in public clouds. The software defined networking services can be used to dynamically allocate resources to the chosen public cloud applications that support the digital business ecosystem.

The digital transformation of networking services makes it possible for the connectivity services providers and the public cloud providers (specifically AWS, Google and Microsoft) to introduce new services combining the strengths of both parties. As an example, a communications service provider can offer an end-to-end automated connectivity service starting from the user device and ending at the workload on the public cloud.

The digital transformation of communication service providers enables also enables them to join in digital business ecosystems. With the software defined networking services, including 5G, the other digital business ecosystem members can utilize the connectivity services as part of new innovative connected products.

Analytics, AI/ML & APIs improve the resiliency of data networking services

The intent-based network captures business intent and uses analytics, machine learning, and APIs to align the network continuously and dynamically to changing business needs.

Advanced analytics improves resiliency of the networking services thus improving the resiliency of network dependent digital business services. In network analytics, data is collected from sources such as network devices, servers or probes providing traffic-flow information. Analytics can be utilized to adapt the networking services to the actual user and application requirements at a given time. As an example, network analytics may find a bottleneck on the data path, which then could even automatically be fixed by adding network resources.

The exploitation of AI/ML technologies further improves the quality and performance of network analytics. AI brings in the capability of making human-like decisions and ML the ability to learn without requiring explicit programming. ML is used to find the probability of a certain outcome using analytical experimentation. The more streaming telemetry and other data from network events we have, the more accurate the estimate will be.

Within the communication service provider industry, MEF has a strong position in defining the standards for network service APIs. Service providers implementing the MEF APIs will guarantee system-level interoperability with each other thus adding on the resiliency. This is a prerequisite for the digital business ecosystem of the service providers, materializing e.g. as automated connection deliveries from several service providers through one service provider.

TREND 2:
WORK FROM ANYWHERE IS HERE TO STAY

In response to the Covid-19 pandemic, the results of a research study (Freeform Dynamics/Cisco, July 2020) showed 4.7 times more employees are working from home now compared to before the pandemic. After the current pandemic people start to return to the offices, but it's highly likely that flexible work arrangements are here to stay. A forerunner in this area is global streaming giant Spotify who closed down its office early March 2020 during the first phase of the pandemic. In February 2021, Spotify announced their distributed-first workplace model under the name of Work From Anywhere (WFA) giving total flexibility to employees regarding where and when the actual work is performed in order to maximize productivity and creativity and to attract talent (Spotify press-release, February 2021)

The IT departments are challenged to support business continuity and resiliency and maintain remote employee productivity. The employees are expected to be able to work as productively remotely as they would be working in the office. In addition, they need to have a seamless access to all the applications and systems to manage their daily tasks. A new requirement for IT is extending enterprise-class IT operations and governance to the remote worker location.

The immediate IT responses to the increased remote working have been to scale up existing VPN capacity, scale up remote worker broadband capacity, improve remote worker security measures and to scale up video collaboration capacity (TechValidate/Cisco, September 2020).

At the same time, the necessity to rapidly adapt to the large-scale remote working situation has speeded up the digital transformation initiatives in the organizations and sometimes even resulted in entirely new business models.

From a networking service perspective, two technology domains – cloud and security - are

paramount in the remote-access solution development. The rapid adoption of cloud-based solutions to provide communication and collaboration tools has proven to the organizations the true value of cloud computing. It's not about cutting the operational cost but being able to quickly respond to changing demands. At the same time remote working makes every user a potential source of security vulnerability. According to a recent study among IT professionals (TechValidate/Cisco, September 2020), security was named as the number one challenge when enabling the remote workforce.

Cloud delivery model is the key to agility

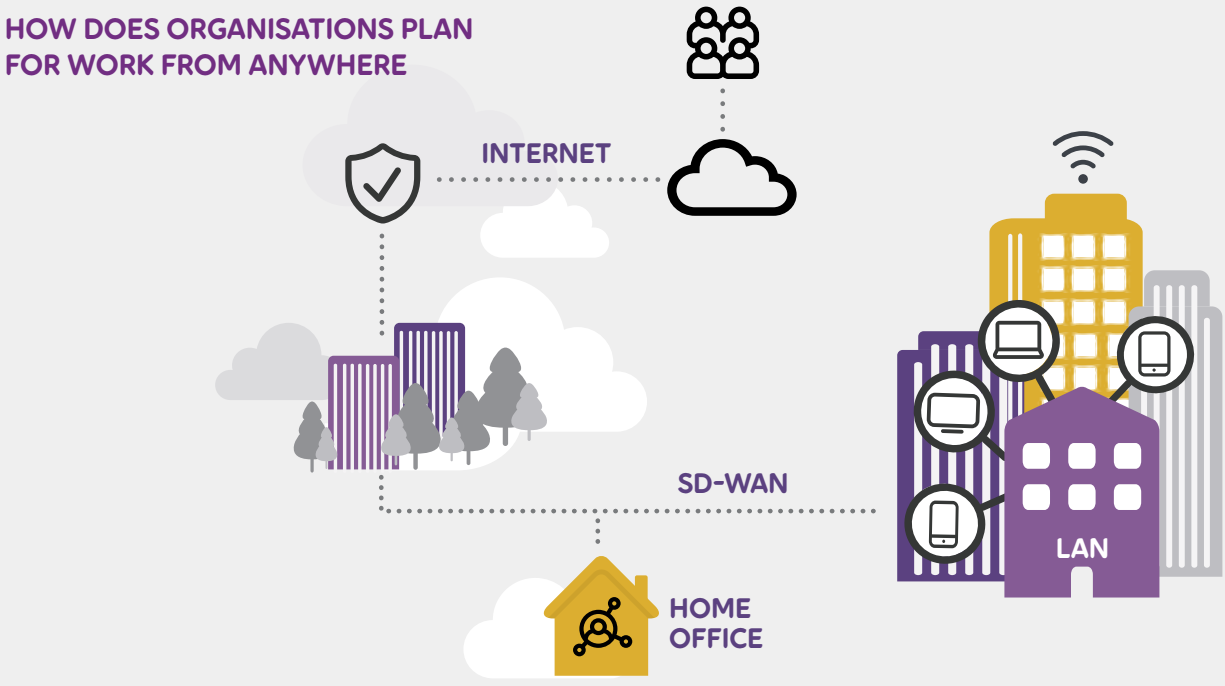
Cloud-first IT architectures have been the key success factor in responding to the flexibility and scalability requirements set by the WFA explosion during the Covid crisis. As an example, the virtual meeting application Zoom had 300 million daily meeting participants in October 2020 compared to just 10 million in December 2019.

The cloud delivery model needs to be expanded to the networking services to support the cloud-first IT approach. Organizations need to have the ability to connect their users, devices or IT resources to the cloud applications at any time with any connection.

The cloud business applications are typically run on top of the public clouds (e.g. AWS, Google Cloud, Microsoft Azure). The direct connectivity to the key public cloud services, without backhauling the network traffic via a central location is a key topology requirement.

Users at the organization premises typically connect using the organization's LAN and WAN connections. Virtually the organization LAN and WAN could be stretched to a user's home environment utilizing various tunnelling mechanisms. The WAN connection varies from a plain Internet access to an SD-WAN connection, where even the Internet access should contain SD-WAN capabilities to deliver the cloud networking flexibility promise for cloud accesses.

Traditional Organization VPNs where the network traffic is backhauled to the organization central site are still a valid solution for remote workers in case most of the network traffic is destined to one cloud, either private or public. In a multi-cloud access setup Secure Access Service Edge (SASE) services will improve the scalability, flexibility and affordability of the remote work service. SASE services also enable extending the remote work services easily to partner or other third-party remote users.



Security is the number one challenge when enabling the remote workforce

The remote working security challenges are not restricted to the network connectivity alone. Only a company managed end-device with the required security functions should be used for business purposes. Among other things, attention should be put on secure usage of Web cameras and videoconferencing applications. Additionally, the home network with WLAN access points, home routers and all the connected devices should be secured appropriately.

Enterprise VPNs continue to deliver one of the most effective and rapid ways to extend enterprise-level control and protection to remote workers. However, the benefits from the cloud delivery model regarding supporting remote working apply to security services as well. The evolving SASE services provide security services like secure web gateway (SWG), cloud access service broker (CASB), firewall-as-a-service (FWaaS), data loss prevention (DLP) and zero trust network access (ZTNA).

TREND 3:
THE IMPORTANCE OF DATA FOR BUSINESS

The total amount of data created, captured, copied, and consumed in the world is forecast to increase rapidly, reaching 74 zettabytes in 2021 and continuing the exponential growth in the coming years (Statista, 2021). 84% of S&P 500 value comes from intangible assets, including data (IP Closeup, June 2019).

World Economic Forum suggests (WEF, A New Paradigm for Business of Data, 2020) emerging opportunities for data-driven value creation: new value pools, new business models, richer stakeholder experiences and better decisions.

New value pools consist of new revenue streams, products and services as well as richer insights for a broader range of stakeholders. These results can be achieved through data insights and enabling technologies like AI and ML. The organizations utilizing this opportunity are exchanging and combining data sets, codifying and selling analytical capabilities, and engaging with new types of customers, providers and other actors to create new value on the market.

New, collaborative business models are addressing core needs of customers by augmenting their data sets with external data, creating ecosystems for new opportunities and delivering a broader range of products and services. As an example, a consortium of 10 pharmaceutical companies is pooling data to train ML algorithms and help develop new antibiotics. At the same time drug discovery, development and go-to-market times are accelerating, while development costs are reducing (WEF, A New Paradigm for Business of Data, 2020).

To sustain trust and engagement, organizations are using data to better understand the needs of their customers, employees and other stakeholders, offering personalized products, tools and services with a seamless experience. Organizations are also orchestrating ecosystems, collaborating with or acquiring other actors to connect their customers with other service providers and offer a richer experience.

Analytics-based insights are helping organizations make better decisions in areas ranging from business process optimization to supply chain management, go-to-market strategies and more. Many use cases depend on partnerships and ecosystems on data that go beyond the organization boundaries.

The data-driven value creation within and between the organizations sets continuity and scalability requirements for the networking services of business. These requirements are met with managed software defined connectivity services.

Managed service provider services for business continuity

The more important data is for business, the more crucial is the availability and performance of the networking services. The path the data needs to travel from where it's created to where it's consumed may consist of several connectivity services from several providers.

To secure the availability and performance, the network connectivity needs to be end-to-end managed. Network management contains the tools to get the required information from the managed objects and the people, processes and systems to act on the information.

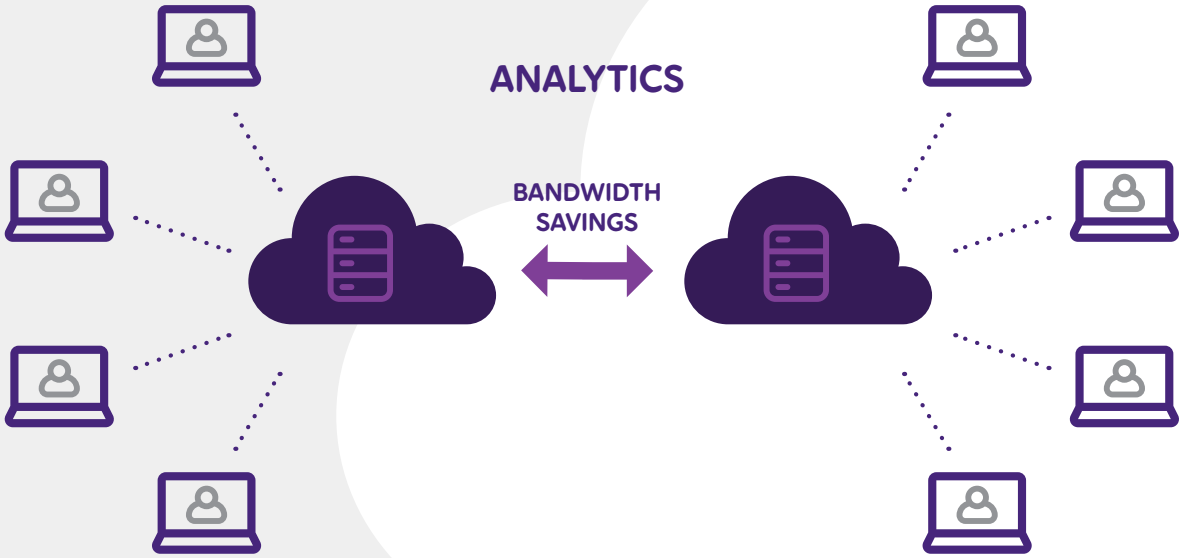
The network elements building the connectivity collect information on availability and performance, which is sent to the service provider systems. While the amount of information is huge, the collected big data needs to be analysed with the help of ML and AI to get a fast resolution to potential problems.

Connectivity is about technology, so it may break down. The pro-active service provider management will notice e.g. performance deteriorations early enough to activate the maintenance process to replace the malfunctioning technology thus securing the business continuity of the customer organization.

Software defined networking services are scalable by definition

The amount of data required by the organizations for data-driven value creation increases exponentially. This increase sets huge scalability requirements for carrying the data from the locations where it's created to the locations where it's processed.

Rapid elasticity is listed as one of the characteristics of cloud computing in the original National Institute of Standards and Technology (NIST) definition. The same characteristic also applies to cloud networking. Software defined WAN (SD-WAN), software defined LAN (SD-LAN) and a combination of those two, software defined branch (SD-branch) have been developed with the cloud-era scalability principles. The substantial increase of data needed to be collected can take place suddenly and unplanned. In this case, the requirement is the ability to scale the networking services accordingly, with no delay. The modern software defined LAN and WAN services are capable in responding to that need.



TREND 4:

HYPERCONNECTIVITY – CONNECTING EVERYTHING WHICH CAN BE CONNECTED

Hyperconnectivity is a term that is used to define the connectivity that exists in digital environments and the interaction between information systems, data and devices, all of them related to each other through the Internet. It's estimated that there will be 29.3 billion networked devices by 2023 (up from 18.4 billion in 2018) out of which half will be IoT devices (up from one third in 2018). (Cisco Annual Internet Report (2018–2023), March 2020) An example of a novel approach to support hyperconnectivity is the global satellite Internet service Starlink provided by the company SpaceX. Starlink satellites are over 60 times closer to Earth than traditional satellites, resulting in lower latency and the ability to support services typically not possible with traditional satellite internet.

IoT, the biggest driver in the hyperconnectivity is expanding from connected industries, smart cities and connected homes to even new domains. One of the emerging branches of hyperconnectivity is Tactile Internet. The International Telecommunication Union (ITU) has defined Tactile Internet as an Internet network that combines ultralow latency with extremely high availability, reliability and security. It will enable the control of the IoT in real time with all human senses interacting with the machines. It will enable humans and machines to interact with their environment in real time, while on the move and within a certain communication range. It will unleash the full potential of the fourth industrial revolution, Industry 4.0.

Tactile Internet is applied in human-to-machine and machine-to-machine interaction, with examples found in industry, robotics, virtual reality, augmented reality, healthcare and road traffic. Tactile Internet sets tight bandwidth, latency, jitter, availability and security requirements to the networking services. Ubiquitous networking services are the prerequisite for hyperconnectivity to take place. Specifically, 5G networking services combined with Edge Computing model will support a large amount of the common Tactile Internet use cases integrated with augmented reality (AR), Virtual reality (VR) and AI capabilities.

Ubiquitous data networking services are required for hyperconnectivity

IDC has defined three primary locations where digital content is created: the core (traditional and cloud data centers), the edge (enterprise-hardened infrastructure like cell towers and branch offices), and the endpoints (PCs, smart phones, and IoT devices).

The IoT devices represent the highest number of endpoints which most often are connected through short-range technology e.g. Bluetooth, ZigBee and Z-Wave, but the usage of cellular technologies is increasing rapidly. PCs and smart phones typically are connected through cellular or WLAN access and, in static environments, wired access like ethernet. The core and edge connectivity typically utilize communication service provider services like fibre access, Wavelength services, Ethernet services, IP-VPN services, Business Internet services or SD-WAN services.

The system-to-system connectivity represents by far the biggest volumes of data transferred globally. Inside the data centers, the transferred data is 5 times that of the Internet traffic, and between the data centers it is about the same level as the Internet traffic. The data center internal connections are typically based on LAN technologies using both physical and virtual switches with the automation, orchestration, management and security built in.

A deep understanding of the capabilities and restrictions of different connectivity services is required to choose the right solution. Often several different services are needed for an end-to-end solution, which emphasizes the compatibility requirements. Also, aspects like end-to-end security and service levels need to be considered.

5G and Edge computing are the key architecture components for Tactile Internet

5G networks, composed of the Radio Access Network (RAN) and Core Network (CN), are expected to meet the key requirements in realizing the Tactile Internet vision. 5G RAN implements an efficient support for various radio access technologies such as millimeter-wave and massive MIMO. It supports quality of experience aware scheduling and radio resource management for tactile applications among other things.

The key functionalities of the 5G CN relevant to Tactile Internet are dynamic application-aware QoS provisioning, edge-cloud access and security. Network slicing is required to provide a network on-demand functionality. Network Function Virtualization (NFV) and Software Defined Networking (SDN) inherited from the Internet infrastructure are critical technologies in shaping such an architecture in the cellular CN.

The very low end-to-end latency and high bandwidth requirements of Tactile Internet call for a distributed service platform architecture based on edge computing. High volumes of data generated by IoT devices are more efficiently collected, stored and processed at the network edge, rather than in the cloud or on-premises data centers.

Multi-access edge computing (MEC) is one of the key architectural concepts for 5G. MEC enables an open Radio access network (openRAN) as well as being able to host applications and content at the edge of the network. It's considered to be a key enabler for IoT and mission-critical, vertical solutions.

The public cloud providers (AWS, MS and Google in the forefront) are engaging with the communication service providers to extend their infrastructure to the communication service provider networks. They are embedding their compute and storage services in the communication service provider data centers, at service access points on the edge of the 5G network. The result is that the traffic reaches applications running in the public cloud without leaving the mobile network. On the other hand, the public cloud providers are extending data processing and ML to the devices so they can act on the data from their sensors in real-time.

TREND 5:
CYBER SECURITY IS A MAJOR CONCERN IN DIGITAL TRANSFORMATION

According to a Nominet report 'Cyber security in the age of digital transformation', cyber security was the top concern among the IT decision makers interviewed on their journey to digital transformation. The Exposure of customer data was the biggest risk, which is understandable just because of potentially significant financial sanctions caused by breaching GDPR regulations.

The more organizations are using digital technologies, the bigger the exposure to system vulnerabilities. The attack surface increases when the number of users, devices, applications, services and data increases. The fact that they are increasingly often outside of the organizations rather than inside, adds to the cyber security challenges. Because of the ecosystem development, the amount of 3rd party workers in the organization IT landscape increases thus adding to the risks. Digital transformation including digital business ecosystems, the importance of data for business and WFA are the trends in this white paper emphasizing the change needed in how cyber security is implemented in organizations.

Cyber security needs to be an inherent component of digital transformation projects. It's not enough for digital transformation initiatives to open growth opportunities for business or increase competitiveness, but they also need to answer to

the questions ‘will it be secure, and will it increase trust in our business?’.

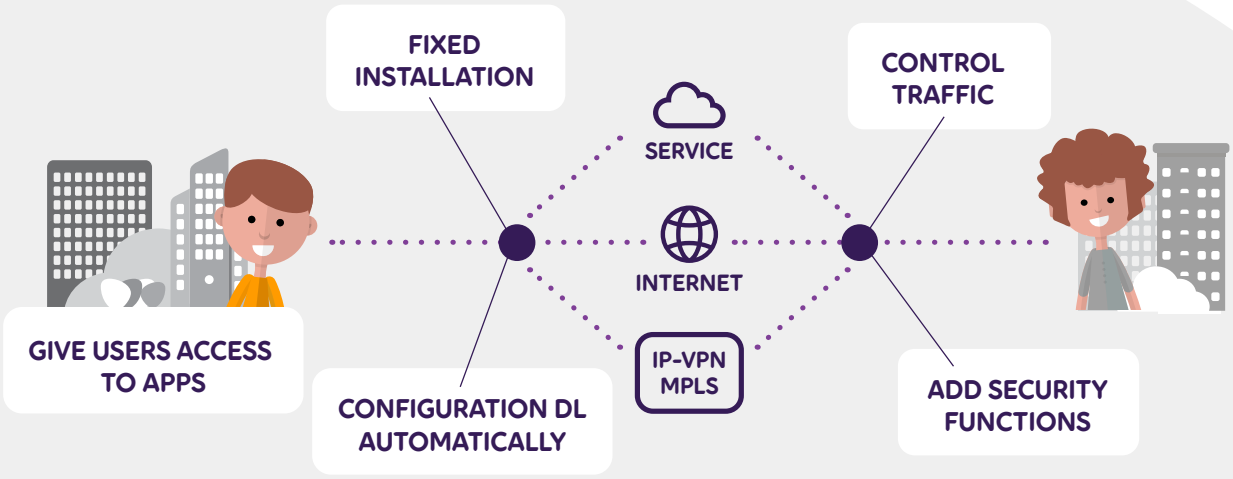
Network security as a subcategory of Cyber security is heavily impacted by the digital transformation development. More users work outside of the organization network than on the organization network. More workloads, applications and organization data are in public clouds and in edge clouds. Digital transformation requires information access anywhere and anytime with speed and agility.

SASE for dynamic secure access needs of digital organizations

Gartner defines secure access service edge (SASE) as an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions (such as secure web gateway, cloud access security broker, firewall-as-a-service and zero trust network access) to support the dynamic secure access needs of digital enterprises. Hereby we focus on the network security functions of SASE.

The identity of the user/device/service has a central role in SASE. The SASE security functions are delivered based on the identity and other relevant context information and considering the organization security and compliance policies. Identities are not only associated with people, but to branch offices, devices, applications and services. Gartner describes SASE as an intelligent switchboard which connects identities to networked capabilities via the SASE vendor’s worldwide fabric of secure access capabilities.

SASE will provide network security services in a consistent and integrated manner to support the needs of digital business transformation. SASE will enable organizations to make their applications and services available to 3rd parties with the same practices as their own employees. The leading SASE providers will have a global coverage of SASE points of presence (POP) next to the main public clouds. This is especially valuable with latency-sensitive applications. SASE should be implemented with a single agent or device to provide access policy without requiring user interaction. This results in a consistent access experience for users, regardless of where the user is, what they are accessing and where it is located.



Machine learning provides dynamic response capabilities to data network security threats

ML is a system that can recognize patterns by using examples rather than by programming them. If a system learns constantly, makes decisions based on data rather than algorithms, and changes its behaviour, it's ML.

Machine learning means solving certain tasks with the use of an approach and methods based on available data. Examples of such methods are regression to predict the network packet parameters and compare them with the normal ones, classification to identify different classes of network attacks such as spoofing and clustering for forensic analysis.

Machine learning can detect malware in encrypted traffic by analysing encrypted traffic data elements. Without decrypting, ML technologies discover malicious patterns in data hidden with encryption. ML can predict hostile environments online to help prevent people from connecting to malicious websites. ML analyses Internet activity to automatically identify attack infrastructures staged for current and emergent threats.

Applying ML technologies in network security has created new solutions called Network Traffic Analysis (NTA) aimed at in-depth analysis of all the traffic at each layer and detect attacks and anomalies. NTA solutions continuously analyse network telemetry and/or flow records. When abnormal traffic patterns or irregular network activities are detected, these tools alert the security team to respond to the potential threat.

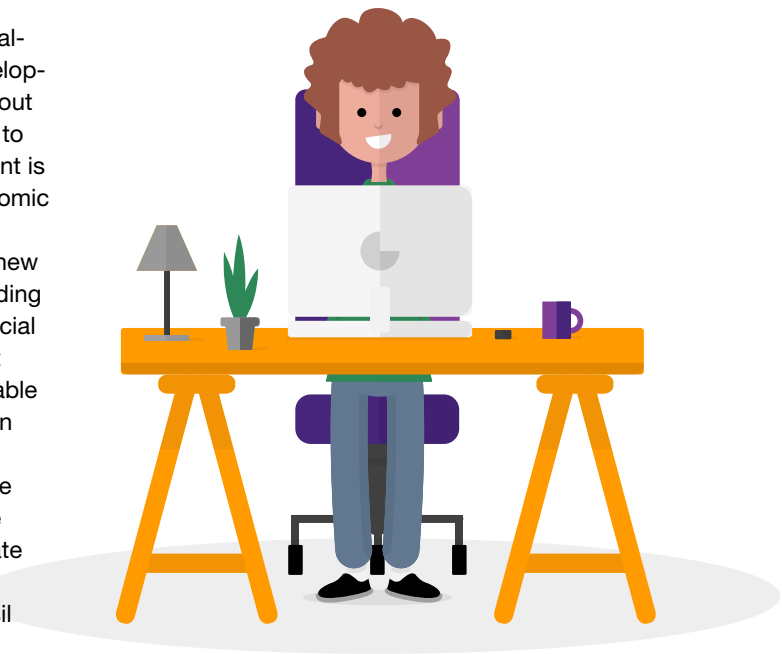
Although ML provides a great set of technologies to strengthen network security, it's worth noticing that those technologies are as well used by the hackers for sophisticated cyber attacks.

TREND 6:
SUSTAINABLE DEVELOPMENT IS THE NEW NORMAL

The concept of sustainable development was already defined in late 1980's by the UN as development that meets the needs of the present without compromising the ability of future generations to meet their own needs. Sustainable development is typically considered from environmental, economic and social perspectives.

Sustainable development has become the new normal in the development agendas of the leading organizations. The evidence like the IPCC Special Report on Global Warming (October 2018) just emphasizes the importance of getting sustainable development targets to guide the daily decision making in organizations.

The Exponential Roadmap published by The Exponential Roadmap Initiative shows that the services enabled by digitalization can accelerate sustainable growth. As an example, the digital sector has the potential to directly reduce fossil



fuel emissions 15% by 2030 and indirectly support a further reduction of 35% through influence of consumer and business decisions and systems transformation (The Exponential Roadmap Initiative, 2020). This target is supported by networking services applying the sustainability best practices of cloud computing and wide-scale deployment of IoT solutions in the societies.

Data Networks will follow cloud computing principles

Using cloud computing to provide ICT services can support sustainable development by reducing the capital spending, increasing the flexibility of business operations and supporting the innovativeness of organizations. The characteristics of cloud computing, like self-service on-demand, resource pooling and rapid elasticity are being implemented in the networks as well. The result is that the sustainability effect of cloud computing will apply to the networks too.

The network functionality is increasingly implemented as distributed virtual network functions. Data Centers are the natural locations to run the network functions, but often e.g. the application latency, like in Tactile Internet use cases, or data security requirements presume the network functions to be distributed to the edge of the network or at the customer premises. The distribution of the network functions will utilize the best practices inherited from cloud computing in a form of a cloud-native service-oriented architecture. The network functions will be run as modular micro services in containers whereas the underlying IT and network infrastructure will be run following the infrastructure-as-code practice. As a result, most of the networking services will be run, offered and consumed as any ICT services.

IoT – connectivity of information

IoT has the potential to offer new sources of economic growth and at the same time to support the decoupling of economic growth and environmental degradation through increased process efficiency.

As discussed earlier in this white paper, IoT is continuing to expand exponentially in the coming years. The number of IoT devices will count in ca. 15 billion in 2023 according to Cisco (Cisco Annual Internet Report (2018–2023), March 2020). The huge amounts of data provided by the devices need to be processed close to the endpoints. The requirements the IoT devices and systems set for the networks will vary vastly. Cyber security has a more important role than ever because of the potential impacts of data security breaches with IoT.

The networks are challenged to provide secure, flexible and highly distributed ways to collect and process the IoT data to be then consumed as information. IoT connectivity provided by the networks should be broadly understood as the connectivity of information.

COMMUNICATION SERVICE PROVIDERS SERVICES ARE THE PLATFORM FOR DIGITAL BUSINESS INNOVATIONS

This white paper has discussed six key trends reshaping data networking for business. The relevance of these trends varies per recipient, but all of them are present in the organizations touched by digital technologies. Existing and evolving data networking services provided by communication service providers have a central role in the realization of the six trends through digital business innovations.

For more information, see
Företagsnätverk – Säkra & flexibla företagsnät – Telia.se Företag

Telia