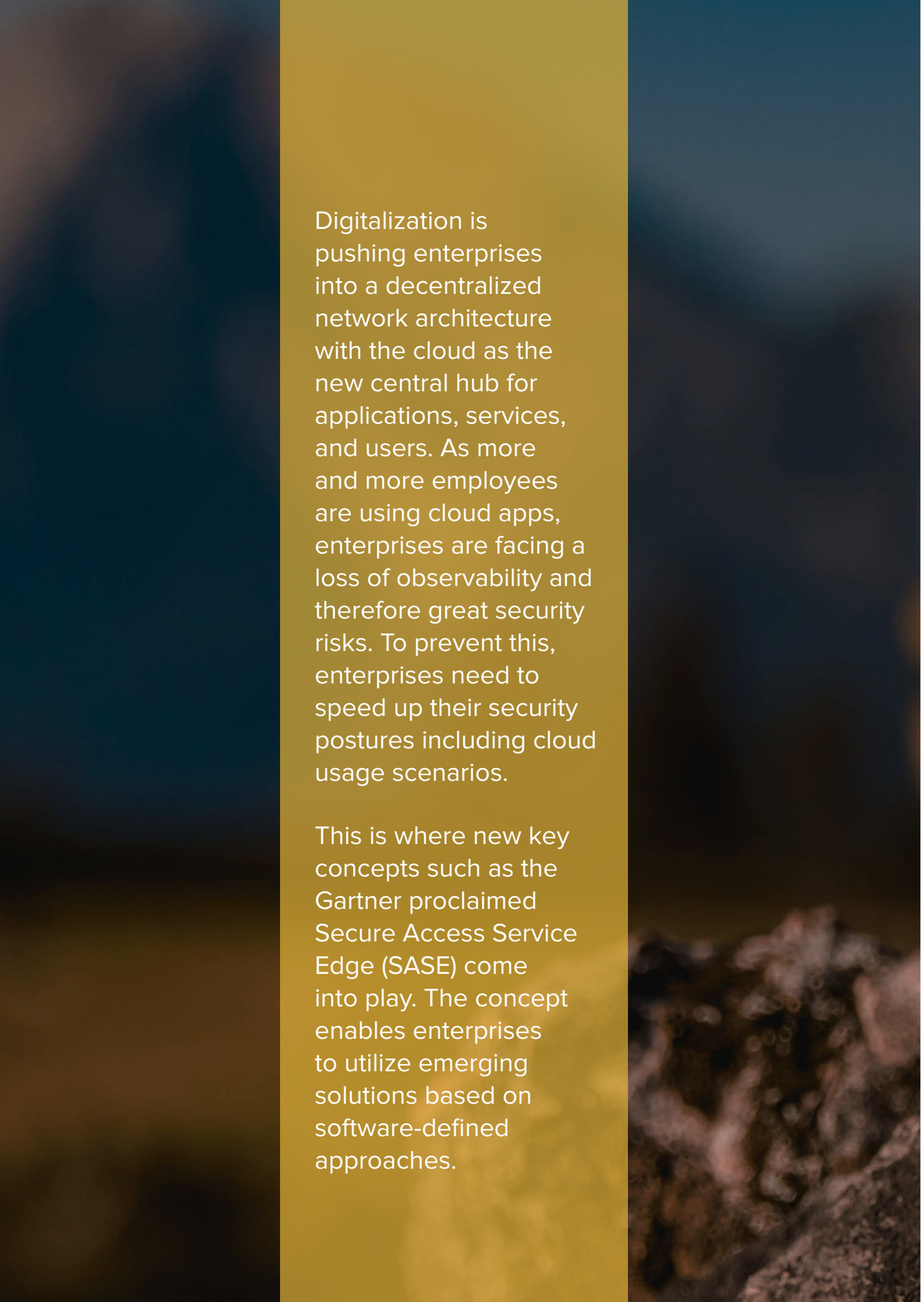
REPLY
SPIKE

SECURITY FOR AN UPSIDE-DOWN NETWORK

How to use the Gartner concept Secure Access Service Edge (SASE) for secure cloud network migration

SPIKE REPLY is the specialist for IT security within the Reply Group. Spike Reply specializes in secure IT and the protection of personal data. Spike Reply has created a comprehensive, integrated and consistent offering to identify, minimize and maximize all aspects of the risk associated with an information system.
These range from the identification of threats and weak points to the planning, design and implementation of the corresponding technological, legal, organizational, underwriting and risk-limiting countermeasures.
Spike Reply provides vendor-independent security services through a broad network of partnerships. Spike Reply can therefore provide in-depth knowledge of the most widely used security technologies on the the most appropriate technology.

www.reply.com



Digitalization is pushing enterprises into a decentralized network architecture with the cloud as the new central hub for applications, services, and users. As more and more employees are using cloud apps, enterprises are facing a loss of observability and therefore great security risks. To prevent this, enterprises need to speed up their security postures including cloud usage scenarios.

This is where new key concepts such as the Gartner proclaimed Secure Access Service Edge (SASE) come into play. The concept enables enterprises to utilize emerging solutions based on software-defined approaches.

CONTENT

THE NETWORK UPSIDE DOWN

Year by year, the proportion of corporate infrastructure that is moved to the cloud increases significantly. While the initial focus was on private cloud deployments, concerns about using the public cloud to implement significant workloads in the enterprise infrastructure are diminishing.

Gartner research states: “[...] Cloud will serve as the glue between many other technologies that CIOs want to use more of, allowing them to leapfrog into the next century as they address more complex and emerging use cases.” (Forecast: Public Cloud Services, Worldwide, 2019-2025, 1Q21 Update.)

When companies move to the cloud, this doesn’t simply mean an expansion of the computing capacity of on-premises-setups in a flexible way. In fact, the whole process of deploying, developing and operating IT applications changes dramatically. For example, the operation of a server cluster previously operated on-premises will not necessarily be worthwhile in the cloud under the same financial circumstances (compare lift-and-shift).

However, if the migration is used to automate provisioning, implement automatic scalability, automate backup processes and more, the business goals associated with cloud migration can be achieved. Then it becomes possible to even go a step further and migrate the application to a serverless application to free IT employees from operational tasks such as patching or resource provisioning.

A DEEP DIVE INTO THE KEY ELEMENTS OF SECURE CLOUD

Users make use of cloud apps
When considering the applications that employees use in an enterprise environment, they are not limited to those on the corporate network. Software-as-a-Service (SaaS) applications have long been an efficient driver in the enterprise. Attractive and flexible subscription models make it easy to choose SaaS applications for project management, file sharing, messaging and more.

In order to stay aware of associated risks, companies need to know which applications are being used and which data is being processed by them. This means enterprises need to establish ways to retain control over the application used by employees, with the same level of control as if it were an on-premises application managed by the enterprise itself.

The network traffic is changing to API’s
When cloud services are used, there is a dramatic change in network traffic. Cloud services, no matter if Infrastructure-as-a-Service or Software-as-a-Service, are typically consumed via API. Traditional interfaces for web traffic built on GET and POST are being displaced by encrypted API endpoints. If these traditional perimeters are not able to understand APIs, it leads to a loss of control.

However, APIs can be used to implement granular authorization concepts. Each service, resource and executable action can be limited and logged. This new granularity even represents improved access protection often seen with classic exposed services in the on-premises world. From the user perspective, single sign-on implementation can be used to link authentication to the user’s own identity provider.

THE RISE OF SASE

As enterprises increasingly move applications to the cloud and users intensively use these cloud applications, it is becoming clear that traditional enterprise networks are no longer sufficient for this task. The Secure Access Service Edge (SASE) concept describes the architectural changes at the so-called “service edge”. It was first defined by Gartner in mid-2019 in a report called “The Future of Network Security in the Cloud”.

Following the SASE concept, the access to services is direct. Access to external cloud services should therefore explicitly not take place via on-premises perimeters. The reasons for this are twofold. First, the data center is a bottleneck, and second, the cost of scaling increases dramatically. Not to mention the operational challenges of maintaining this without disruption.
To manage this transformation, this functionality must be applied directly to the “service edge” and can include both, cloud endpoints and on-premises.

According to the Gartner report, there are three component categories for SASE: Core, Recommended and Optional. Core functionality includes functionalities that are critical to the applicability of the architecture, also referred to as by the term Security Service Edge (SSE). Recommended functionalities represent additions but do not necessarily need to be used in every infrastructure, and optional functionalities refer to functionalities that go hand in hand with the products that are deployed in the field.

THE CORE FUNCTIONALITIES OF A SASE ARCHITECTURE

- Zero Trust Network Access (ZTNA)
- Software Defined Wide Area Network (SD-WAN)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)

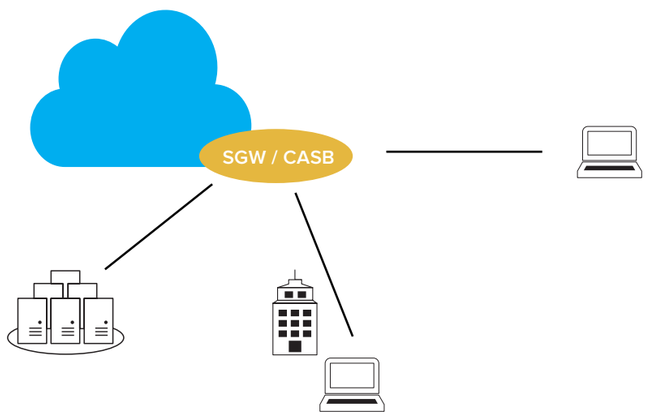
Trust nobody – verify everything
The Zero Trust Network Access (ZTNA) concept represents the first dramatic change in the approach to access control. ZTNA architectures follow the principle “trust nobody - verify everything”. This is achieved by the granularly configurable APIs described above and by principles such as “must-know” or “principle-of-least-privilege”. Thus, no user (and no device) is considered trusted without proof.
ZTNA is based on the concept of Software defined Perimeter (SDP). There are three actors: SDP Client, SDP Broker/Controller, and the SDP Gateway.

The process is as follows:
1. An SDP Client authenticates with the SDP Controller and asks for a session.
2. The SDP controller authorizes this to the SDP gateway and refers the SDP client to the SDP gateway.
3. The SDP Client is establishing an encrypted session to the SDP Gateway.

As a result, access to a particular service is not dependent on which network a user is connected to, but each session must be re-authorized. Approach allows access to be granted based on contextual information about the user and the device being used, such as location, roles, device status, security status and more.

Increase efficiency on WAN level by utilizing SD-WAN
Software Defined Wide Area Network (SD-WAN) represents the second pillar in the SASE framework. Like other virtualization technologies, SD-WAN establishes virtual WAN architectures that are flexible and independent of transport services. These transport services can range from high-priced services such as MPLS to standard broadband internet connections. SD-WAN can be used to address different service transparencies and establish cost- and performance-optimized communications.

Prevention against threats – as-a-Service
When it comes to inspecting traffic for unwanted content, an equivalent for on-premises firewalls must be found in a SASE architecture. These roles are performed by Secure Web Gateways (SWG) and Cloud Access Security Broker (CASB). Both have the goal of protecting the data and eliminating threats.
A Secure Web Gateway (SWG) is a proxy which detects threats, for example, through TLS interception and web filtering, and prevents them based on policy.
On the other hand, Cloud Access Security Broker (CASB) have a clear focus: SaaS applications. A CASB is integrated via the API of the application and offers far-reaching possibilities in the control of data traffic or processed data. In addition to granular policies that can be reduced to API actions (upload, download, share), CASBs are also operated with Data Leakage Prevention (DLP) functionalities. This allows policies to be extended to include data patterns worth protecting or malicious file detection.



COMPARING TRADITIONAL NETWORKS AND HYBRID CLOUD SETUPS

Traditional networks are usually all structured in a very similar way when it comes to network security: either one or multiple firewall clusters fulfill various security features such as access control, IDS/IPS, botnet detection, Remote Access VPN and so on. The list of possible features offered by modern next-generation firewalls is long and largely responsible for their success in recent years. Yet, with the continued upward trend in the use of the cloud for various use cases and the transition to decentralized enterprise networks accelerated by Covid-19, enterprises are faced with the challenge of a new network architecture, and thus also a new security architecture.
It is no longer sufficient to build up a well defended walled garden within data centers but also take advantages of cloud concepts. As a result, clients may no longer need to dial into a central office via a corporate VPN connection but connect directly to the cloud. This shift does not necessarily mean that classic network vendors such as Cisco, CheckPoint or Fortinet are out of business with the onset of the cloud era. These vendors still have their place in the cloud, but it looks different than in the classic on-premises world.

This overall change towards a software-defined world will keep challenging enterprises in 2021 as the mentioned prominent hardware vendors announced their shift towards a software company. Cisco Chief Executive Officer Chuck Robbins noted a “strong performance” in a statement. “Our teams are executing incredibly well, aggressively transitioning to a software model and accelerating our pace of innovation”. Companies therefore face the challenge of keeping pace with the transition to more software-defined solutions than ever before in history. However, from a customer perspective, no single vendor is able to deliver the entire IaaS/SaaS portfolio needed, forcing customers to once again adopt a multi-vendor strategy. Spike Reply has seen a strong stream within enterprises to consolidate the security and network vendors they use, but with the move to cloud-based solutions, this consolidation cannot continue without missing certain features. This leads to increased costs and, yet again, the issue and challenge of interoperability between different vendors.

A transition to flexible subscription-based services

The general business model of the classic network providers is shifting towards being a supplier of software. In traditional networks, customer companies bought a box with a service for a certain period. After the deadline has expired, they need to purchase another license and support extension from the vendor, always at fixed terms such as one, three or five years. Due to the software-defined trend, however, providers are more likely to offer subscription-based services, which are more flexible in many respects than fixed-term contracts. This trend is a strong one, directing into a software- and subscription-based future.

No rebuilding of on-premises networks in the cloud

A common misunderstanding in terms of cloud adoption is to simply lift-and-shift data center services into the cloud and thinking the server will be better and cheaper at the same time. A hybrid cloud setup is different. Simply copying services from one location to another will not ensure that advantages of the cloud are leveraged while disadvantages are avoided. So, moving to the cloud requires a proper strategy for the architecture, which needs to be rethought or even completely redeveloped.

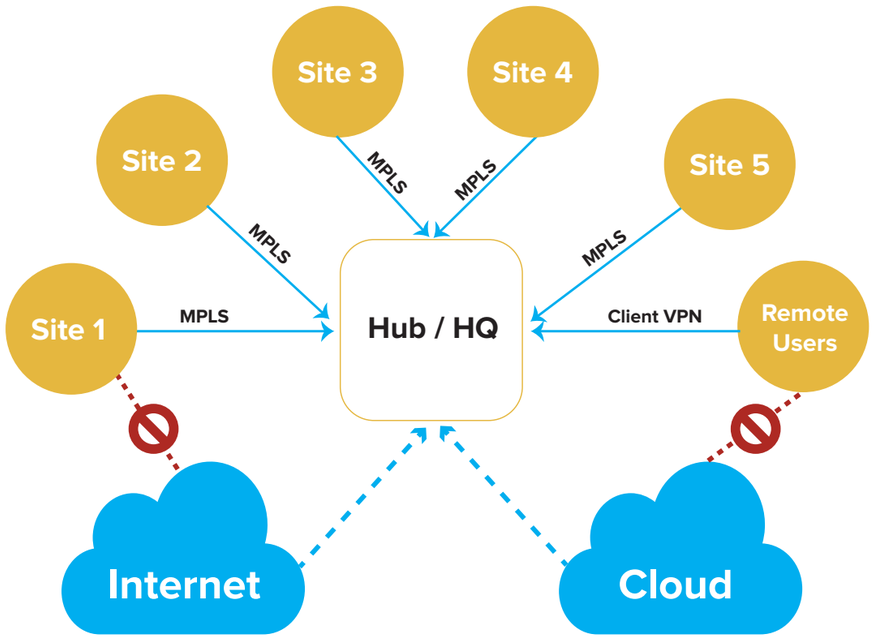
The new toolset for a hybrid cloud setup

When thinking about hybrid cloud setups, many different buzzwords around software-defined technologies emerge such as software-defined perimeter (SDP), secure web gateway (SWG), secure access service edge (SASE), software-defined WAN (SD-WAN), cloud access security broker (CASB) and so on. All those technologies are defined by a use-case including the transition to a cloud-centric enterprise network.

One example is the SWG use: An endpoint will no longer have a client on his computer with which he will connect via Remote Access VPN to a data center to build up an IPsec tunnel. In hybrid cloud setups, the client will immediately communicate with a cloud instance routing the client on the best possible way to the resources it needs. By doing so, SWG can perform multiple security functions in the cloud, such as URL filtering to ensure that the client is safe when browsing the public Internet.

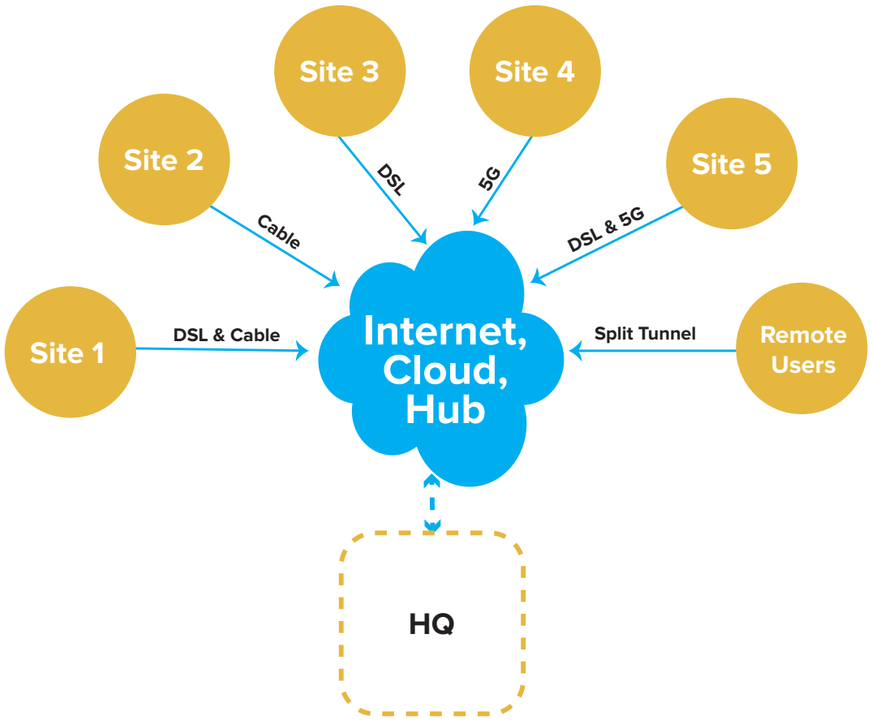
Traditional vs. modern enterprise network designs

Traditional network designs are usually based on a site to headquarter connectivity via a MPLS line. Those MPLS lines are expensive in terms of speed to cost ratio. Furthermore, applications and services are entirely centralized with barely any server on each site. This also includes the internet access as well as cloud access being centralized. In a nutshell, the headquarter or central data center is acting as a gateway to the outside world with a perimeter firewall and a broad access control set. The following figure illustrates such a traditional network design in an abstract way.



Unlike traditional network designs, modern network designs take a completely different approach to connectivity by bringing the service closer to the end user. Internet access and cloud access are therefore not tunneled to a central gateway but are accessible directly on site or from the home network. This leads to a fundamental change on how sites are connected with each other. Instead of expensive and limited MPLS lines, sites are able to use whatever technology is available at the site's location such as DSL, cable or 5G. In order to connect the sites with each other and the data center, SD-WAN or general VPN Site-to-Site connections are used to establish a tunnel for only those applications and services which are hosted centrally.

By default, the cloud becomes more and more the central hub for the remote users and therefore also the new perimeter for security features. This change requires the consideration of new technologies such as SWG, CASB and WAF to cover all the necessary security functions that were previously covered by perimeter firewalls in the data center or at headquarters.
Figure 2: Modern Network Design demonstrates how the headquarter went from being the central gateway to being any other site. Remote users split their traffic as needed and are basing routing decisions on applications and services instead of plane IP addresses.



Connect on-premises setups with clouds
To ensure the interconnectivity between clouds, on-premises or even in a Multicloud scenario there must be an abstraction layer for the network. A missing network abstraction layer is increasingly **becoming a top pitfall.** Since in **One Cloud Only** deployments it is not immediately necessary to create a comprehensive network design, **and** because we only want to start with a few services, this essential design step is often missing or incomplete. If we talk about hybrid setups or even Multi Cloud, a missing network design can become a real nightmare.

THE TOP 3 SECURITY PRINCIPLES FOR CLOUD ADOPTION

The new aspect applying perimeter functionalities when adopting cloud principles will make enterprises face the challenges outlined above. When in the process of planning the migration and taking advantage of the cloud, it's all about avoiding the top pitfalls.

1) Be aware that enterprises already use SaaS apps, and they don't know it
According to the Cloud and Threat Report by Netskope, the number of cloud apps used by companies increased by 20% last year. Most of the companies in this study cannot control the apps. Shadow IT is in fact a problem. Considering that the majority of apps receive poor compliance ratings (according to the Netskope Cloud Confidence Index), the extent of the risks currently taken by companies without realizing it becomes obvious.

2) Move security features from on-premises perimeters to the cloud
Before digital transformation moved the significant part of communication to the clouds, next generation firewalls, proxies made up the on-premises perimeter and protected all enterprise users with their security features like anti-virus, access-control, malware detection, URL filtering, sandboxing, data loss prevention, SSL interception and so on. Nowadays, users access the cloud directly and the same security features must be applied at the cloud perimeter or service edge with Secure Web Gateways (SWG) and Cloud Security Access Broker (CASB). This is necessary in order not to lose control, but also to ensure adequate performance for users. In addition, SD-WAN can help reduce OPEX significantly by eliminating the need for cost-intensive MPLS networks to be the sole service guarantee.

3) Remember not to rebuild on-premises networks in the cloud
Companies need to dive deep into sensible hybrid/multicloud network architectures. A design phase is crucial before any migration process. Each of the cloud providers has a different take on cloud networking. Within a one-cloud architecture the cloud provider also takes care that, for example, network address conflicts are not an issue. When leaving this setup, classical network planning activities have to be performed as well. Usually this means a network abstraction layer is required.