IT Security in the Cloud Age

T Systems

Let's power
higher performance

Introduction

The pros and cons of the cloud have long been the subject of intensive discussion in Europe. In addition to the lack of cloud expertise within companies, it was the security provisos and compliance challenges in particular that forced companies to scrutinize the (public) cloud as a sourcing model.

Today, the scales have tipped in favor of the cloud, with 70 percent of all German businesses using cloud services to varying extents[1] – from IaaS to PaaS to SaaS. Business logic is consumed in the form of SaaS applications from the cloud, while infrastructures and software platforms are being dynamically and elastically moved to the cloud as IaaS and PaaS.

The cloud's economic benefits are too great to ignore. The pay-per-use principle enables IT services to be used as needed, without requiring any investments. This demand-based availability reduces business risks and allows new business ideas to be tested quickly. The cloud also offers businesses another highly attractive feature: scalability. Cloud resources and services therefore give businesses maximum agility, meaning they are able to swiftly respond to market requirements.

These days, cloud usage is a reality. It has also long ceased to be in a fledgling state. The high degree of sophistication that comes with using cloud services is evident in the fact that the discussions surrounding the cloud are now shifting. User companies are currently taking the next step and actively establishing multi-cloud landscapes. They want to deliberately position themselves as platform-independent, reduce risks and vendor lock-in, and utilize the specific advantages offered by the respective platforms.

The cloud's role as an enabler of digital business models cannot be overestimated. But although the discussion about security and compliance is now secondary to the notion of added value for businesses, **no company using cloud services can get around the need to establish a comprehensive security plan for cloud usage**. And this security plan must form an integral part of the cloud strategy.

Although cloud service providers have been continuously working on the security of their platforms in recent years, and also offer a variety of security functions, the reality is that this by no means results in a comprehensive, one-stop-shop security solution. This is because cloud usage also involves sensitive, business-critical and particularly confidential data (personal data, invoicing data, sales information, customer data etc.) leaving the company domain. Responsibility for the security of the data and applications in the cloud cannot be transferred to the cloud service provider; it continues to be held by the user company. This means the user company must ensure that uniform regulations and compliance guidelines are also implemented in multi- and hybrid-cloud approaches. Only when security and digitization go hand in hand is the path clear for future business.

Migrating to the Cloud

As recently as ten years ago, the standard model for rendering IT services was still the traditional server-based infrastructure. These infrastructures were physically located in data centers, which were sometimes run by the company itself and sometimes outsourced.

The cloud eliminates the need to assign IT services to specific hardware in controlled environments. IT services are virtualized in the best sense of the word, regardless of the infrastructure. The result are service-based integrated architectures. IT is used as a service.

A development pathway to cloud-native architectures and services typically encompasses various intermediary steps. At the start are the lift-&-shift approaches, which are used to migrate existing workloads from the data center or on-premise environments. The costs for infrastructure management are reduced and the migration results in initial scaling options for the company. In the next step, companies try to reduce the time to market. Development cycles of business-supporting applications are accelerated by using cloud services beyond compute and storage, such as through the use of platform services and development tools. “Serverless” designs are also used in isolated cases.

The re-architect phase simplifies operations in a dynamic environment. Fast development cycles are supported. Microservices, containers and “serverless” architectures become the standard, laying the foundation for DevOps, an agile culture which integrates and holistically embraces the development and operation of software. These kinds of companies release their applications in rapid cycles – sometimes even several times a day.

The accelerated application development requires resources to be used in a way that is not always under one’s own control. As a collaboration model, the cloud demands a high degree of trust in the service-providing companies – leading to a shared responsibility model. Using cloud-native approaches involves a paradigm shift, including in the way security is handled. In the past, a service’s components were known throughout its entire life cycle and its contributions were traceable. In the cloud-native world, responsibility and expertise are shared around. The way IT platforms are changing, the shift to a cloud architecture produces a new set of threats.

Matters are also rendered more difficult by the fact that, as a result of digitization, business processes are more intensively tied to IT. The importance of IT is growing, while control over it is decreasing. The combination of these two developments has a synergistic effect on the potential for risk. At the same time, user companies remain responsible for the security of data and applications. Cloud usage is posing new challenges for security – on top of the existing challenges.

New Security Requirements as Part of the Cloud Transformation

There are essentially three parameters which characterize the new set of threats posed by the cloud:

1. **Exposed position**
   The classic perimeter has served its time. The cloud means a shift in the company's external boundaries – and no one can say exactly where to. The advantages of having services provided from the cloud (convenience of sharing data, reduced response times, public accessibility of services) generate new potentials for risk. On the one hand, attackers per se may gain access to public infrastructures, and on the other, data can easily be published unintentionally. And beyond mere human error, APIs also enable unwanted non-human communication, through which data can inadvertently flow out. Cloud architectures thus require security managers to give each application its own "perimeter protection" – which is no mean feat.

2. **Cloud technology and governance**
   It is common for resources to be shared in the cloud. The platforms used are highly developed and complex to enable them to offer users high scalability and the required speeds. Users have little influence over the provision method. Typical problems resulting in such complex environments include errors caused by complex IAM structures or isolation errors between different tenants. The lack of transparency makes it difficult to enforce the company's internal compliance policy, for example regional regulations, data protection categories or password guidelines. There is also a risk that users will use "unhardened" operating system and application images, which unintentionally creates the potential for attacks.
   But the gain in agility afforded by the cloud also raises another issue. Companies that frequently and quickly roll out updates for applications in agile mode also need to establish suitably swift security mechanisms. Tried-and-tested processes and technologies for security cannot keep up with this agility. There ends up being a gap between the technical feasibility for application development and deployment, and the notion of a guaranteed appropriate level of security. In other words, the security of applications is left behind by the tremendous pace of developments and rollouts.

3. **Trust in the cloud service provider**
   Shared responsibility is the motto in the cloud. The users (when using an IaaS) are responsible for the applications and data they operate in the cloud, while the cloud provider takes responsibility for the security of the platform itself – up to the relevant service model's limits. Up to this limit, the cloud service provider's performance appears as a "black box" – and the user only has transparency beyond the boundaries of the black box, in his/her sphere of influence. He/she thus has no insights in the weaknesses of the cloud solutions used – especially when operating in complex environments. The cloud service provider also potentially has access to the cloud resources in its data center, without the user realizing this. This includes the hardware (e.g. memory dump, storage dump, network sniffing), the cloud management tools used, and the APIs. The latter can, for instance, contain unofficial backdoors only known to the cloud provider.

For many users, the cloud world is something new that has to be learned – particularly in terms of security. The cloud service providers expect their users to play their part in shared responsibility in order to protect applications and data in the cloud. But this cloud security expertise is not yet available everywhere. Gartner predicts that, by 2025, 99 percent of all errors in the cloud will be caused by users[2]. Security managers at the corporate users should thus take precautions with their own security measures. The challenge of cloud security is intensified by the fact that companies generally do not use "one" cloud, but rather that multi-cloud approaches are now common practice, i.e. user companies have to provide security expertise for various cloud architectures.

Comprehensive Cloud Security Strategy

Companies seeking to optimize cloud usage despite the security considerations need to take four aspects into account when establishing a comprehensive cloud-security strategy:

1. Concepts for risk management, business continuity management, and a long-term plan for the system development lifecycle are fundamental at a **strategic level**. Designing suitable metrics for cloud security is equally important.

2. At a **process level**, weaknesses need to be identified, and a compliance management system established. This includes cloud incident response, the integration of security aspects into the DevOps approaches, and proactive cloud threat modelling.

3. Examining **cloud architectures** is another key component of a cloud security strategy. In addition to knowing the specifics of the various service models (Iaas, Paas and Saas), security aspects need to be integrated in particular into cloud migration projects such as lift & shift or rearchitect.

4. This framework must be accompanied by correct use of the matching **tools and technologies**. The native security solutions provided by cloud service providers must first be used appropriately. Any gaps are then filled in using additional security solutions created by specialized manufacturers – especially in a multi- and hybrid-cloud environement. Finally, cloud users should also allow for machine learning mechanisms and automated responses.

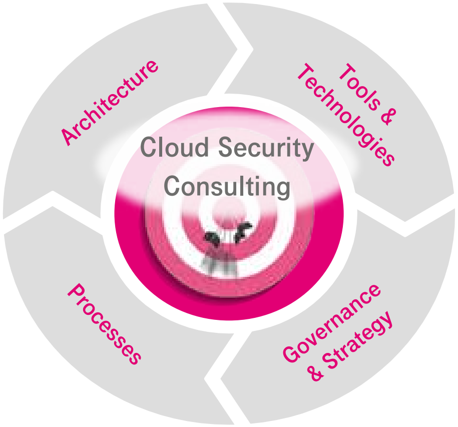

Fig. 1: Individual and comprehensive strategy for cloud security

This basis gives rise to key achievements which help ensure that an efficient cloud security system can be built. Users initially gain transparency over their data. They know where which data is, who and which application is processing it, and where the data goes. Security shortcomings in their own organization are identified and can be eliminated through suitable countermeasures. In particular, user companies can also assess the areas in which necessary expertise needs to be enhanced by suitable partnerships with security experts. T-Systems can support enterprises seeking for consulting.

Cloud Security: Combining Established Mechanisms and New Tools

The good news is that there are already suitable solutions available to address the new challenges associated with cloud security.

There are two factors which make cloud security complex. The agile approaches for application development and provision, and the resulting multi-cloud landscapes. The fact that multi-cloud use arises unplanned causes many companies quite a headache. Hyperscaler resources are not always accessed via official channels. It's no secret that the easy availability of cloud services has paved the way for shadow IT, which, given it is used outside the realms of official IT governance, creates new security and compliance risks.

A comprehensive cloud security strategy encompasses tried-and-tested protection methods and supplements these with cloud-specific security mechanisms. Many manufacturers have focused their solutions on specific security aspects. Established protection measures include monitoring network traffic using the latest generation of firewalls. Virtual next-generation firewalls provide intrusion protection and protect against advanced persistent threats. Advanced web application firewalls, which can also be provided as virtualized services, expand on this basic protection to include the application layer. Additional established technologies, meanwhile, monitor database activities.

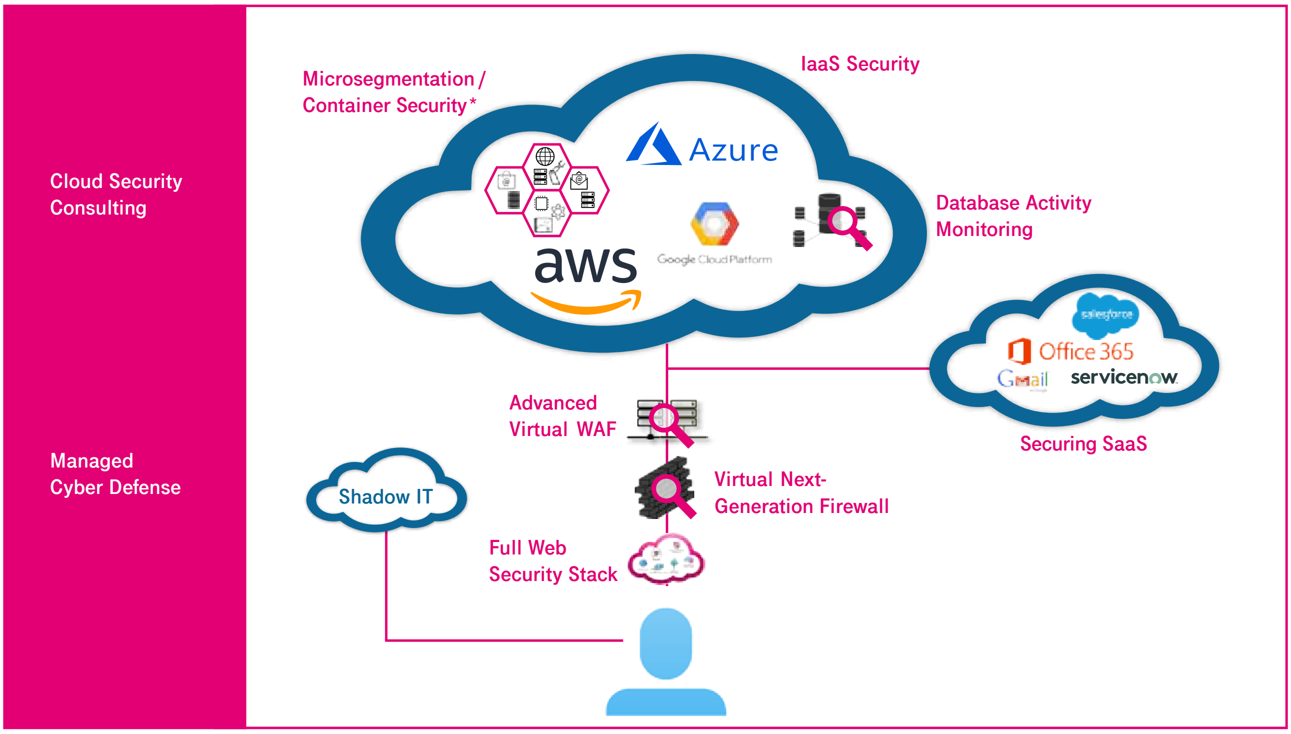

Fig.2: Secure working in the cloud era

Specific Security Solutions for Cloud Service Usage

Securing SaaS

SaaS continues to hold the lion's share of the cloud market. It is specially aimed at end users and its ease of use means it is very widespread. Solutions that can be used for malware and account protection exist specifically for the use of SaaS, such as Salesforce or Office 365. They also enable the encryption of unstructured data, offer functions for data loss prevention, and monitor compliance with regulations.

Comprehensive solutions (full web security stacks) integrate various security mechanisms, such as virus protection, advanced threat protection, web security, content/URL filtering and firewalls, as a complete service. The major advantage of cloud-based provision is the fact that the solution can monitor cloud services directly at the location where they are produced. This gives cloud service users a better user experience compared to centrally provided solutions facilitated through a corporate network.

Related example: Internet Protect Pro at a manufacturing company

A manufacturer uses a scalable Office solution in the form of Google's G Suite from the public cloud for its new branch offices and growing workforce. It is available via the Internet regardless of location and efficiently supports the company's dynamic growth. But Internet-based Office systems are insufficient in an enterprise environment when it comes to security. The manufacturer had previously relied on a central firewall at a central data center, through which all online data traffic must pass. The security solution is thus not an optimum fit for the flexible Office solution. The security architecture results in long run times when it comes to using the applications, which makes for a negative user experience, especially at the international company's more remote locations.

The company decided to replace the central approach with a localized one. While the MPLS network continues to be used for business-critical applications, the branch offices have been given their own routers, so as to enable direct Internet breakouts. This gives the international subsidiaries direct access to the data centers from which the Office services are provided.

But how should an appropriate level of security be facilitated in this new architecture? Investing in new security hardware at the respective branch locations was not a feasible option. The mechanical engineering firm now purchases its security "as a service" from the cloud through Internet Protect Pro powered by Zscaler. Zscaler runs its security solution as a cloud service at various data centers around the world. The data traffic for the Office applications initially runs through Zscaler's security functions, before accessing G Suite. Internet Protect Pro protects the respective local Internet access based on a multi-layer security concept.

Security Solutions for Cloud-Native Strategies

Other special security solutions for the use of cloud services at companies are specifically aimed at developers who use IaaS resources or develop cloud-native applications with containers. Cloud nativity denotes one of the key trends in the IT industry.

According to a forecast by IDC[3], applications will be moving further in the direction of cloud-nativity, hyperagility and architecture in 2021. 80 percent of development work will then be performed on PaaS using microservices and cloud functions, while 95 percent of all new applications will be deployed in containers.

The Cloud Native Computing Foundation[4] defines "cloud-native" as applications that use an open-source software stack to deploy applications as microservices. The parts are packed into individual containers that are orchestrated dynamically to obtain optimum resource utilization. This approach has several advantages compared to simple cloud VMs:

- Fast provision of new releases
- Easy management
- Reduced costs
- Higher service reliability
- Avoidance of vendor lock-in
- Infrastructure independence (cloud-native applications can also be run on-premises)

Cloud-native therefore combines a bundle of multiple modern technologies – beyond just the cloud: containers, microservices and orchestration. The trend toward cloud-native approaches also requires security mechanisms that are able to follow this same path.

In principle, these security solutions revolve around two approaches. One type of solution focuses on compliance issues, and is used to centrally establish security policies for the developed applications and monitor them in the relevant public clouds through the tenants used. In other words, the solution monitors whether the developed microservices, instances and workloads work in accordance with the established policies, and alerts the security team if any discrepancies are detected.

Introducing Central Policies for the Multi-Cloud

A typical policy could, for example, stipulate that data must be generally encrypted by Amazon Web Services (AWS) in the S3 Object Storage. AWS provides this security function as a platform service. If a developer forgets to implement the encryption when updating his application, the security solution detects this automatically and informs the security team, so that the error can be immediately rectified. Advanced tools can not only detect these wrong setting but automatically remediate them. What makes this IaaS security solution so elegant is the fact that – once established – this same policy can be automatically applied to various tenants in various public clouds. In other words, a compliance check can be conducted even if the entire service or specific microservices are moved to the Google Cloud, Azure or the Open Telekom Cloud. Similar policies can also be set up to store data, for example to ensure compliance with the EU GDPR. Policies are predefined according to HIPAA, EU GDPR or Best Practice and can be applied "out of the box" to various clouds. For specific demands individual policies can be introduced with the help of a policies designer. Monitoring compliance enables companies, particularly those that have applications developed and provided by third parties, to monitor whether applications have been designed in accordance with the specifications.

Checking Container Use

As already described, containers are one of the essential components of cloud-native approaches. They offer developers maximum flexibility. Monitoring container-container communication is a typical new challenge for security teams at user companies. But the containers' flexibility also gives attackers the major advantage: The attacker exploits a weakness within a container environment and can move (east/west traffic resp. lateral movement) without protection in the container to access relevant data.

In a typical “attack”, an attacker captures a container providing a publicly available website function. From here, they can access the client database in the back end via container-container communication.

Microsegmentation is one of the most efficient and cost-effective ways of preventing such attacks. It establishes “permitted” communication paths between various subservices, which can be distributed over containers or container groups. This so-called “whitelisting” facilitates ongoing checks of container-container communication. If the tool detects that containers are not abiding by the rules, communication is blocked. In the example mentioned, for instance, the (stipulated) website communication to the price list can be permitted, while further communication to protected data in the back end can be prohibited. This means the attacker will only be able to access the price list, but not the client data requiring protection for the sake of the company’s interests. Microsegmentation thus permits the introduction of zero-trust environments. Another advantage is the fact that it is software-based. It can be set up dynamically so that the regulations can migrate across centrally even if the application is moved.
Such approaches can also monitor whether developers access hardened, i.e. security-checked, images when designing containers, which means that the security team can contain any security risks very early on. The check only needs minimum efforts of the developers: These functionalities can be implemented into common developer tools via plug-ins. Weakness scans of already active containers or container images are best conducted at the container registries level, so that new weaknesses or security alerts can be identified during operation itself. Active, vulnerable containers are then patched through redeployments. With these solutions the complete container life cycle on various platforms can be protected in an overarching manner.

Conclusion

Digitization is making it necessary to use clouds and cloud-native methods so that companies can survive in a heightened competitive environment. But this paradigm shift from classic IT provision to highly agile approaches poses a challenge for companies' security managers, who are faced with a completely new situation – established security tools and processes now only have limited effect in the agile cloud world. They need to find new security solutions that can keep up with agile application provision and cloud usage. Various specialized solutions capable of supporting certain aspects of cloud usage with effective security mechanisms are already available on the market. In each case, however, companies need to thoroughly check which is the right solution for their needs.

But cloud security is more than just implementing specific security solutions. All security aspects need to be assessed holistically right from the time the cloud solutions are designed. This includes the architecture, user, role and permissions management, communication rules, the use of encryption and associated key management, monitoring, and (automated) remediation. Discussing matters with an experienced security provider can help develop a comprehensive, efficient and platform-independent security strategy for the cloud world.

As one of Europe's leading service providers, T-Systems has a comprehensive security portfolio and can assist user companies with their migration to the cloud on two levels.

We work with you to define your cloud security strategy, identify gaps, and find suitable solutions to eliminate these gaps and best prepare the company for the cloud world. As a second step, we can help you implement the relevant solutions and, on request, operate them continuously.

Sources:
[1] "Cloud-Nutzung auf Rekordniveau bei Unternehmen",
Umfrage von Bitkom Research im Auftrag der KPMG AG (German only)
[2] "Is the Cloud secure?", Gartner, Oct. 2019
[3] IDC FutureScape: Worldwide IT Industry 2018 Predictions, 2017
[4] "State of the Developer Nation 16th Edition – Q4 2018", Developer Economics, Slashdata, April 2019

Expert Contact

Andreas Pecka
Head of International Expert Sales &
Presales Cyber Security
a.pecka@t-systems.com

Published by

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
Email: cyber.security@t-systems.com
Internet: www.t-systems.com

T Systems Let's power higher performance