DTS

DTS
Cloud Security

Cloud Security

The cloud is the future? But only if it is secure! The cloud simplifies many IT processes and tasks while offering great flexibility – now, not just in the future. However, cloud and multi-cloud environments require special protection because they bring new security issues and risks. Over 80% of companies use cloud environments in some way, and the same number rate the cloud as essential and ground-breaking. At the same time, 99% of all errors and problems in securing cloud environments are caused by the companies themselves and are therefore avoidable. Through our concepts, solutions and services, we want to help you make the most of the potential of the cloud and at the same time provide comprehensively secure environments and platforms – our DTS cyber security expertise for your protection in the cloud.

- Comprehensive protection for your cloud environment
- Comprehensive assessment of the security stack
- Individual solutions tailored to your company
- Design, implementation, operation & security in the cloud
- More thane 20 years of cloud infrastructure expertise
- 24/7 support in German and English
- Focus on your core competencies with the help of DTS managed services

The crucial term is “shared responsibility”, a correct understanding of responsibilities for applications and data in the cloud. The two parties – the company or customer on the one hand and the cloud operator or provider on the other – are jointly responsible at all times for different aspects of security when using the cloud. Only effective collaboration between the two parties can achieve the maximum possible protection. In this context, it is the type of cloud model used that fundamentally determines who is responsible for which security tasks. It is becoming clear, however, that the responsibilities of the company are greater and are tending to increase.

A secure path to the cloud

Modern cloud security solutions support the consolidation of your cyber defenses and promote business flexibility. When companies migrate to the cloud, their IT security experts are faced with two important questions: How can users be given secure access to the cloud? And how can applications hosted in the cloud be protected effectively? In the past, the answers to these questions generally took the form of a combination of different, isolated solutions. This in turn implies additional costs and complexity and unnecessary additional risks. DTS offers you the possibility of an integrated platform to reduce complexity and to maximize the level of protection, with the following objectives:

- Governance and compliance in the cloud
- Protection of data, identities and applications (identity as the new perimeter)
- Control of the complexity of the multi-cloud
- DevOps security and DevSecOps processes

Die Bausteine für ene sichere Cloud-Umgebung

We offer the following building blocks for a secure cloud:

- Next-generation firewall (VM series)
- Cloud access security brokers (CASB)
- Compliance and workload protection (Prisma Cloud)
- Authentication (SAS)
- Device identity as a service (DIaaS)

Palo Alto Networks VM-Series virtual firewalls provide comprehensive visibility and control over multi-cloud and hybrid cloud environments. They replace the concept of multiple isolated IT security solutions. They can be deployed for public clouds such as Azure, AWS, GCP, software-defined networks and virtualized environments, and can be managed centrally. They are therefore an essential security tool for consistent control in the multi-cloud.

The ability to use virtual firewalls for segmentation also reduces the area for cyber attacks on your infrastructure. The standard security feature set across all Palo Alto Networks firewalls ensures that threats are detected and blocked before any damage is done.

Moving to the cloud can make your business more agile, flexible and efficient. At the same time, this step is associated with various risks in terms of data security and compliance. With a CASB, these risks can be minimized and the digital transformation can be safeguarded. Cloud security starts with protecting applications, i.e. SaaS applications such as Microsoft 365, Google G Suite, Salesforce, Box and others. But it requires an integrated, people-centric approach that correlates threats and enforces consistent DLP policies across email and cloud applications. CASB protects your accounts from being compromised, accidental data disclosure, configuration errors in IaaS and PaaS resources and compliance risks. Our agentless solution gives you people-centric threat visibility, customizable access control, automated responses and comprehensive data security with DLP.

As organizations modernize their development processes and move to cloud-native architectures, managers quickly discover that an approach to security based on discrete solutions does not provide the level of consistency and control needed to protected the cloud and the applications, data and infrastructure deployed there. Palo Alto Networks’ Prisma Cloud is a comprehensive cloud-native security platform that protects applications, data and cloud-related technologies with industry-leading compliance and workload protection throughout the lifecycle in the multi-cloud and hybrid cloud. Prisma Cloud’s core functions include:

- Cloud security posture management (CSPM), i.e. a complete overview of all resources used and absolute confidence in their configuration and compliance: Prisma Cloud uses a proprietary approach to CSPM that goes beyond compliance and configuration management. Threat data from over 30 sources provides clear information about acute risks, and security measures in the development process ensure that unsafe configurations do not reach production in the first place.
  - Transparency, compliance & governance
    - a directory of cloud resources
    - Real-time configuration check
    - Compliance monitoring & logging
    - Scans of Infrastructure-as-Code configurations (IDE, SCM and CI/CD)
  - Threat detection
    - User & entity behavior analytics (UEBA)
    - API-based network traffic visibility, analysis & anomaly detection
    - Automated investigation & response
  - Data security
  - Data classification
  - Malware scans
  - Data governance
- Protect cloud workloads by using Prisma Cloud to safeguard the entire lifecycle, in the public cloud, in the private cloud and on-premises: easy integration with leading CI/CD workflows, registries and stacks
  - Host security
    - Vulnerability management
    - Runtime protection
    - Compliance management
    - Access controls
    - Container security
    - Vulnerability management
    - Runtime protection
    - Compliance management
    - Access controls
    - Git repository scanning
  - Protection of serverless environments
    - Vulnerability management
    - Runtime protection
    - Compliance management
    - Access controls
  - Protection of web applications & APIs
    - Protection from the OWASP top 10
    - API protection

- Network security in the cloud, meaning consistent policy enforcement: Prisma Cloud detects and prevents network anomalies by enforcing micro-segmentation at the container level, examining traffic log files and using advanced cloud-native capabilities for application-level (Layer 7) threat prevention
    - Network transparency & anomaly detection
    - Micro segmentation based on identity
    - Cloud-native firewalls
- Management of infrastructure access rights in the cloud: Prisma Cloud continuously scans IaaS and PaaS environments for identity and access management (IAM) risks and remedies them automatically
    - Finds all user & machine identities in all cloud environments and analyzes their rights, roles and policies
    - Overview of access rights
    - IAM governance
    - Automated response
    - User & entity behavior analytics (UEBA)

Multi-factor authentication (MFA) procedures become more important in the cloud: as companies increasingly outsource their systems to the cloud and users no longer necessarily use the same physical corporate network to access applications and data, this security factor diminishes. Other security measures must be put in place to ensure that only authorized users can access confidential resources. Since the cloud is available to different users at any time and from anywhere, MFA can be used to request additional proof of identity credentials that is difficult to forge or crack by means of a brute force attack. This makes it possible to check whether a user is who they claim to be. With the DTS SafeNet Authentication Service (SAS) we offer two-factor authentication with a wide range of authentication options, which is easily and universally available for a wide range of applications and devices. By providing a self-service portal for end users and allowing DTS to operate the platform, you benefit not only from significantly increased security, but also from much lower operating costs.

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de