MTG **Enterprise Resource Security**
Mastering Cryptographic Key Lifecycles

DARZ
Daten sind wertvoller als Geld

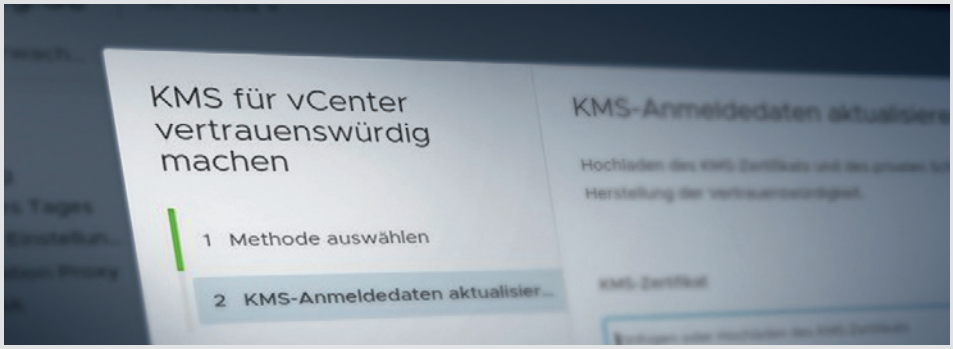
Foto: © MTG

VMware encryption – higher security with just a few clicks

Our encryption service is based on a Key Management System by MTG, which is aligned with VMware. This enables you to meet your company's growing security requirements both quickly and cost-effectively!

Virtual machines (VM) are portable and can therefore run on any server. Unauthorized internal persons or external attackers who have accessed the relevant networks are able to access the data of unencrypted VMs without any protection.

VMware has addressed this threat by allowing encryption for your VM via external key management systems (KMS). The encryption expert MTG offers a VMware-compatible KMS product. In cooperation with the infrastructure solution provider DARZ, a cost-effective SaaS service was created especially for SMEs.



vmware READY NETWORKING AND SECURITY

Once connected to vCenter, users can reliably encrypt their VMware VMs with just a few mouse clicks.

MTG KMS & DARZ Managed IT Security Services

Effective Data Protection

More security or your data – less concerns

Supports NIS 2, DSGVO, ISO 27001 and industry-specific standards

More and more legal regulations require the implementation of "state of the art" cybersecurity. These include the NIS 2 regulation that recently came into force, the GDPR, and the requirements of DIN ISO 27001. This also includes smaller companies and more industries.

With end-to-end encryption of all VMware VMs, testing steps are no longer required and process descriptions in the context of protection profiles and risk analyses can be significantly reduced.

Protection of critical data

With the encryption service, all sensitive data on the VMware VM are protected:

> Database, file system and source code repository are automatically encrypted.

> Locally stored access data (e.g., for database access, SSH keys etc.) are protected.

> Log files (e.g., from applications) and personal data for system logins, transactions, and IP addresses are encrypted anytime.

vSAN Protection & TPM

Besides encrypting VMs, VMware also offers the option of protecting so-called vSANs (virtual Storage Attached Network) with the same method.

Additionally, applications and operating systems for which TPMs (Trusted Platform Module) are required (e.g., Microsoft Windows 11) can be virtualized without any problems.

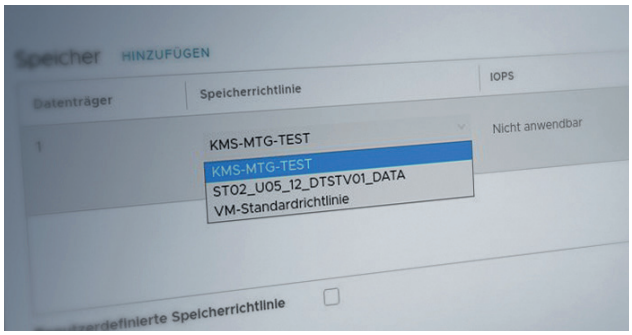
Encryption of data in any operating mode

During storage, operation, and access, data on the VMs remain encrypted. This provides comprehensive security and saves additional costs for encryption.

> **Security at rest:** When the storage medium on which the encrypted VM is located is accessed, the data can not be read. This explicitly also applies to databases running on the VM. Expensive database encryption is no longer necessary.

> **Security at work:** Protection is also provided while the VM is running.

> **Security in transit:** During transfer from the storage location to the hypervisor / ESXi host, the VM's data is also protected.



Highly secure key storage

The Key Encryption Key (KEK) is stored externally in a KMS for each VM and protected via FIPS-certified Hardware Security Modules. This logically separates the storage locations of the VM and the key.

When storing VMs on portable or removable media, the VMs are always encrypted. Loss of the data carriers is not critical. The data carriers can be disposed more easily at the end of their life cycle.

Listed on VMware Marketplace

MTG KMS & DARZ Managed IT Security Services

Easy Connectivity & Operation

Reach your goal with minimum effort and cost

Easy connectivity

The uniqueness of this offer is the possibility to encrypt the VMs completely independent from the location via the DARZ service. The MTG Key Management System is connected via the KMIP standard interface of the vCenter and is managed by our experts.

Easy encryption via own vCenter

Using the familiar user interface for managing the VM (vCenter / vCloud Director), users can encrypt any connected VM with just a few clicks. No additional software or training is required.

Back-up, redundancy and high availability

The key material is stored customer-specific and very secure. The entire system is highly scalable and is operated in a fail-safe and geo-redundant way.

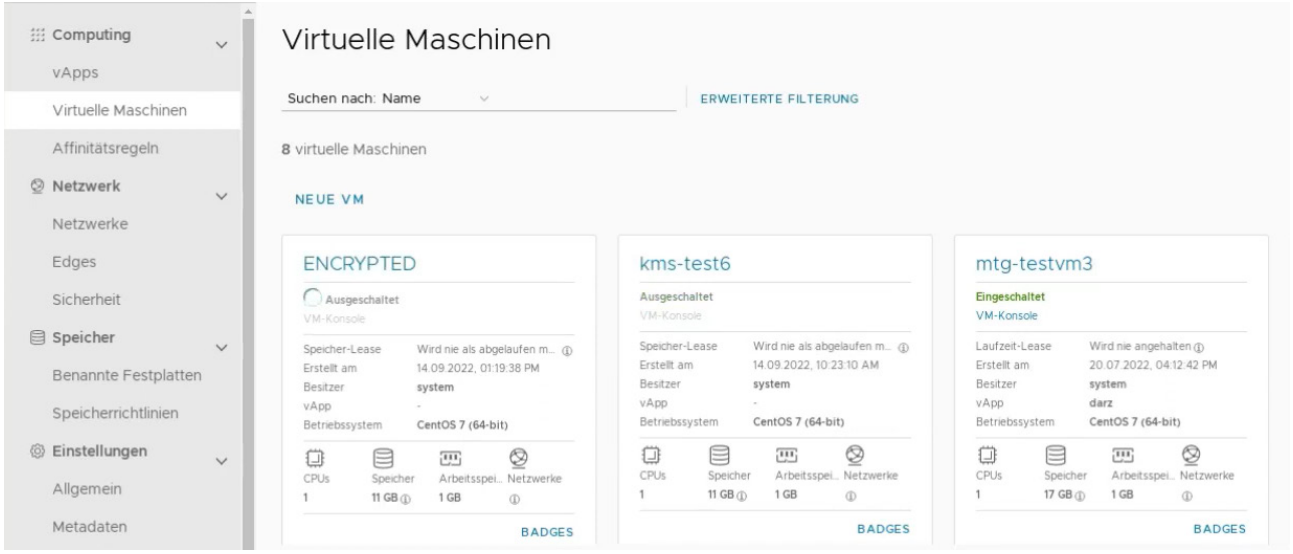
Consistent encryption processes

> With the offered solution, the user has a consistent procedure and process for encrypting all data in the VM. This reduces time, costs, and complexity.

> The vCenter provides transparency in encryption and decryption. After a one-time configuration, no further manual process is required. Password entry (pre-boot authentication) is also not required.

> Everything that runs on a VM is automatically encrypted. Encryption of the VM is possible regardless of the guest operating system (Windows, Linux, iOS, etc.). In particular, it can be enforced even if the guest OS does not support Full Disk Encryption.

> The encryption of VM can be enforced company-wide by policy. Encryption can then be centrally checked and verified in audits very easily. This policy then becomes valid for all guest systems across all platforms.



Demo Video:
Easy encryption via vCloud Director

Managed service from experienced experts

In cooperation with DARZ GmbH, a long-term partner and infrastructure provider, a new VMware Encryption-as-a-Service has been created, enabling you to encrypt your VMware quickly and easily.

DARZ GmbH

DARZ GmbH supports companies in taking advantage of the opportunities arising from digital transformation. Besides high performance, the managed services solutions offer distinct modularity, flexibility and scalability. This allows each customer to put together different services that are relevant to them in terms of quantity, quality and combination at any time.

The data center is certified to various security standards, such as TÜV ISO EN50600 CAT III, DIN ISO 27001 and BSI TR-03145. The managed services are operated in a fail-safe and geo-redundant way at two German locations.

MTG AG

Founded in 1995, MTG AG is a leading specialist for sophisticated encryption technologies "Made in Germany". The MTG ERS® product portfolio includes Certificate Lifecycle Management, Public Key Infrastructures, Key Management Systems and Hardware Security Modules.

In addition to VMware encryption, cloud solutions for Managed PKI with Certificate Lifecycle Management are also offered. All corporate processes at MTG are ISO 27001 certified.

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

DARZ
Daten sind wertvoller als Geld

DARZ GmbH · Julius-Reiber-Strasse 11 · 64293 Darmstadt
Phone: +49 6151 8762-777 · vertrieb@da-rz.de

da-rz.de

MTG

MTG AG · Dolivostrasse 11 · 64293 Darmstadt
Phone: +49 6151 8000-0 · contact@mtg.de

mtg.de