maincubes
SECURE DATACENTERS

# Customer Case Study

## Spike Reply chose connectivity by maincubes to extend its global service footprint

REPLY SPIKE

**Spike Reply, a company in the global Reply Group specializing in IT security, is using European data center operator maincubes' data centers and its secureexchange® digital marketplace. Now it is part of an ecosystem providing global connectivity with other service providers to Spike Reply and allowing it to extend its own security services footprint.**

### About Spike Reply

Spike Reply is the IT security specialist in the Reply Group. It primarily focuses on It security and personal data protection. The company has built a comprehensive, integrated and consistent portfolio of services to maximize protection that covers all aspects of IT security risk identification and minimization. The service portfolio extends from the identification of threats and vulnerabilities to the planning and implementation of appropriate technical, legal, organizational, insurance-related, and risk-mitigating measures.

Spike Reply provides manufacturer-independent security services via an extensive network of partners. Spike Reply has genuine expertise on the most widely used security technologies in the market and is able to provide sound advice on the selection of the most suitable technology. It gained this expertise through numerous projects which have demonstrably reduced IT-related business risks and costs.

The company provides support in APT & malware defense, application firewalling, data leakage prevention, database security, governance & risk management, SIEM & security intelligence, either on premise or as a managed service.

### There's no getting around e-commerce

The German e-commerce market has been continuously expanding for many years. According to the German Retail Federation (HDE) e-commerce revenue was 53.4 billion euros in 2018, which represents 9.1 percent year-over-year growth. It's high time for retailers who want their expansion plans to be successful to jump on the e-commerce bandwagon. At the same time, however, this move is associated with a number of challenges.

Even established German retail SMEs operating an online shop alongside several high street stores are faced with the task of modernizing their business to bring it in line with today's market and security requirements. Many of them are still managing the IT environments of corporate units such as Finance, HR, Property, Marketing and Logistics via a central office and have on premise digital infrastructure solutions. Although they have registered an increase in the number of online customers, noticed how cloud solutions are becoming more attractive and seen competitors introducing comprehensive and innovative digital (marketing) strategies, many of them are still hesitant to make a move.

How is it possible to find a strategy for expanding your own digital presence while at the same time combining all aspects relevant to security and availability?
After all, the threat to data and entire systems should not be underestimated.

In many cases the reasons for this hesitance are security concerns and high expectations from the public sphere – especially with regard to data protection laws and specifically the GDPR – which puts them in a dilemma.

**The SME sector is strong, but it makes an attractive target for cyber criminals**

The saying "Opportunity makes a thief" not only applies to the analogue world, but also to the digital universe. Sadly, this vulnerability is regularly confirmed by the German Federal Office for Information Security (BSI). In its most recent report on 'The State of IT Security in Germany 2019' the security experts registered another increase in the quantity and quality of cyber-attacks. The lengths to which criminals will go in committing perfidious acts have been revealed by the coronavirus crisis. The BSI had to issue a warning about fake government aid application websites stealing personal or corporate data. Cyber criminals often target the SME sector, which is not just the foundation on which the German economy is built, but also the key to the success of the social market economy model. The more sophisticated the attacks become, the more difficult it is for SMEs to adequately protect themselves.

Many companies face a dilemma: On the one hand, growth, change and digitalization are essential in the modern, smart economy. On the other hand, these Processes enlarge their IT systems' attack surfaces and increase the complexity of the infrastructure being protected. For example, automated attacks on unsecured systems in the cloud can, if successful, soon spread through the corporate network, infecting critical systems or intercepting confidential data. Just one security flaw can compromise an entire organization.

The potential for damage is enormous. For example, competitors could profit from the publication of confidential company information, or the company may face high GDPR fines for the loss of financial or personal information. Ultimately, the company's reputation is damaged and that kind of damage takes a long time to repair. Moreover, a successful cyber-attack on an online shop effectively puts a stop to all the retailer's sales via that channel.

**Practical cybersecurity measures**

Unsecure passwords, outdated software and ineffective update management are serious mistakes to be avoided at all costs. Merely by avoiding these basic mistakes a company can achieve an effective level of security at an affordable cost. In terms of the Pareto Principle, that's 80% of security for 20% of the cost. The remaining security gap can then be closed by the company itself at a (relatively) high cost or with the assistance of external service providers. The measures to be taken, which are also in the Spike Reply service portfolio, include baseline security solutions for SMEs, web application firewalls or proxies/load balancers and SIEM systems for intrusion prevention.

For high street stores closed as a result of the coronavirus pandemic, the loss of online business can be potentially devastating.

**Baseline security solutions**

These are interesting alternatives to comprehensive all-in solutions for SMEs. They include functions such as ID/IP (intrusion detection and intrusion prevention) that divide the network into local areas in accordance with the company's zoning concept or harden the system by disabling superfluous software components and functions. The advantage is that security-enhancing functions can be specifically selected without driving up costs excessively.

**Web application firewalls or proxies/load balancers**

These solutions are ideal for the protection of an online shop that is exposed to continuous access from the outside. They control access by distributing requests and restrictively enabling functions, and with the help of AI (artificial intelligence) they can detect anomalies and therefore potential attacks.

**SIEM (Security Information and Event Management) systems**

SIEMs improve a system's prevention capabilities. By collecting and analyzing security-relevant information in the entire infrastructure, a SIEM system can identify potential security incidents and respond appropriately – ideally before operations are impaired in any way. It makes sense to partner with an external service provider because these systems are expensive to buy and operate.

**In the public and private cloud – security is the bedrock of any infrastructure**

On premise IT, infrastructures are no longer able to cope with escalating requirements of security, reliability and scalability. Retail SMEs with proprietary solutions for both admin tasks and online shops risk being left behind by the competition.

Alternatively, cloud solutions, such as those hosted by maincubes' data centers, provide an infrastructure that can meet any requirements. In combination with Spike Reply's security tools and services, customers achieve additional security, enabling them to avert threats and ensure permanent compliance with statutory requirements.

## ADVANTAGES

### Public Cloud

**High flexibility and scalability**
Resources can be added or removed as required.

**Fast availability**
Available in just a few minutes if necessary – and the entire infrastructure can be added.

**Simplification**
Offers many basic functions ex-works and management is simplified by central orchestration.

**Lower HR costs**
Only some and at times no in-house personnel is required for administration and technical support.

**Low initial investment**
No hardware procurement.

### Private Cloud

**Full data control**
Compliance and security governance (security management) are simplified.

**Needs-oriented implementation**
Guaranteed high level of service.

**Long-term cost reduction**
Provided that IT resource requirements are static and can be transparently billed.

**Maximum security**
Internal security measures ensure a high degree of internal control over systems. The physical network can also have 'secure zones'.

**Independent structures**
No dependence on cloud providers (e.g. Microsoft, aws, Google) means transparent processes and an advantageous legal position.

The cloud model that the customer chooses – public or private – depends on the importance of the respective advantages. Luckily, it isn't an 'either/or' decision.

In many cases a hybrid model which combines the public and private cloud is the best choice. Here are two retail customer examples to illustrate this:

EXAMPLE 1

*Sensitive information such as customer master data or business-critical administrative data records such as HR files or accounting documents, which have to be archived for lengthy periods of time and/or require a high level of protection, are stored and processed in the private cloud.*

*The frontend for customer access to the online shop is in the highly scalable public cloud infrastructure because it has to be used and managed very flexibly. Retailers can respond promptly and at low cost to peaks in demand during special promotions (e.g. Black Friday) and scale back their resources just as quickly to maintain costs at an appropriate level.*

EXAMPLE 2

*To guarantee maximum security, the entire infrastructure is hosted in the private cloud. Resources are only scaled or relocated to the public cloud when there is an immediate need – such as hardware failure or maintenance – and returned to the private cloud afterwards.*

*This allows retailers to fully utilise their local resources in the secure private cloud yet still access the needs-oriented benefits of the public cloud as required.*

**Spike Reply security tools and cloud management via secureexchange®**

Retail enterprises wishing to operate their infrastructure in a hybrid cloud model can access their public cloud directly via one of maincubes' high-security data centers. The data center provider's secureexchange® platform offers global connectivity to public cloud providers worldwide. The scope of connectivity offered by the carrier-neutral data center operator via the platform is the reason why the security experts at Spike Reply decided to become part of the ecosystem. Members have access to a comprehensive IT security service portfolio including APT and malware defense, application firewalling, data leakage prevention, database security, governance and risk management, SIEM and security intelligence as a managed service or on premise solution.

The combination of hosting and connectivity services that maincubes provides, plus the access to Spike Reply's security solutions, delivers the flexibility, reliability and security that SME retailers need to build their online business successfully.

**maincubes' solution**

maincubes offers SMEs, such as retail enterprises, a high-security and high-availability infrastructure at its data centers with a 100% uptime guarantee for their private cloud, as well as global connectivity for access to all popular public cloud models. Customers also have direct access to Spike Reply's comprehensive security solutions via maincubes' proprietary secureexchange® platform. The IT security specialist Spike Reply is now part of maincubes' global ecosystem.

Tilsiter Straße1 | D-60487 Frankfurt am Main +49 69 6976 810-0 info-de@maincubes.com maincubes.com