KuppingerCole Report

EXECUTIVE VIEW

by Matthias Reinwarth | February 2019

R&S®Trusted Gate by Rohde & Schwarz Cybersecurity

Reliable control and monitoring of sensitive information stored in public clouds and collaboration tools (SharePoint, Office 365) through virtualization, encryption and fragmentation of data while enabling the safe and convenient cooperation with protected documents. Transparent, data-centric security for cloud, on-premises and hybrid storage environments.

by **Matthias Reinwarth**
mr@kuppingercole.com
February 2019

Content

Related Research Documents

Leadership Compass: Cloud Access Security Brokers - 70614

Advisory Note: Big Data Security, Governance, Stewardship - 72565

Advisory Note: Cloud Services and Security - 72561

1 Introduction

Cloud services offer many benefits, including the ability to meet changing demands and the flexibility to deliver new business solutions faster. Office 365 and SharePoint as Software as a Service (SaaS) offerings from Microsoft are the tool of choice in many organizations and industries for office collaboration, daily document work, and secure information exchange with extended supply chains and partners. However, many organizations today also have a hybrid IT environment in which some IT services are delivered on-premises in the enterprise data center, some are delivered via the cloud, and some are hybrid in both the enterprise data center and multiple clouds. These factors pose significant challenges to information security and regulatory compliance.

The digital transformation that businesses and public institutions alike are facing, requires a new type of IT environment. This requires more agile approaches and the ability to efficiently and securely translate departmental and business requirements into new software models and offerings. As a result of this, today's cybersecurity is undergoing substantial changes. Traditional cybersecurity typically focuses on protecting networks, systems, applications, servers and endpoints in general. So, when we look at the protection of the actual data as the key asset of the process of safeguarding information, traditional security mechanisms are still often used for data during transmission (data in motion, e.g. HTTPS) or in its stored state (data at rest, e.g. hard disk file system base encryption).

The question of how to secure data in an increasingly perimeter-less IT between on-premises environments, the cloud and anywhere in between is getting more and more important. Business boundaries are dissolving as the requirements and the ability to share information continuously increase. For example, in agile and collaborative working environments, information has to be shared efficiently and securely between various internal and external business partners, mainly via cloud services and with mobile devices. This requires extensive access to what is often considered to be critical content by a variety of stakeholders.

Modern, data-centric security approaches move their focus away from infrastructure and network boundaries and look rather at the transmitted payload. This modified paradigm of protecting data is key, especially when traditional IT infrastructure is replaced or augmented with cloud services. Data-centric security typically looks at the processes of

- Identifying and discovering sensitive data;
- Classifying data (from public to confidential and regulated);
- Managing and protecting (especially sensitive) data, encompassing its full lifecycle using methods such as encryption, hashing, and access controls ;
- Data loss prevention (DLP) methods and techniques;
- Monitoring and auditing of access to classified data, to provide evidence of successfully implemented measures and controls to regulators, to internal audit, senior management and the business.

Organizations are increasingly adopting a hybrid model for the delivery of IT services and this requires a consistent approach to govern and secure data on-premises, in the cloud (including multi-cloud approaches) and when shared with external parties.

Above all, ease of use and a transparent application of the above given processes are of high importance to provide security and efficiently enable business with all involved parties.

Classification, access control and technical enforcement of security measures allow to implement risk-based approaches for data-centric security. This is often required by auditors and the business to make sure that sensitive data can be identified and processed, transferred and stored with adequate safe guards. Data subject to special requirements, such as mandatory data locality or industry-specific regulatory requirements, can be appropriately isolated. This allows for them being treated individually and adequately.

That does not mean that data-centric security is the single, new solution to security challenges replacing everything that has been done before. Traditional security mechanisms (e.g. firewalls or endpoint security) continue to represent an initial layer of protection that must first be overcome and protect individual aspects and security dimensions of hybrid environments. Whenever applicable, e.g. when establishing segments of hybrid environments on premises, these measures will be valid and efficient components as parts of a so-called layered security approach, covering multiple dimensions of cybersecurity.

2 Vendor and Product Description

Rohde & Schwarz Cybersecurity is an IT security expert offering a broad portfolio of security solutions, especially in the area of data-centric security. They are a member of Rohde & Schwarz, their parent group of companies, a German electronics corporation specializing in offering services and products in the fields of measurement technology, broadcasting, radio monitoring and location as well as radio communication for mobile, broadcasting and electronics industries, aviation, defense and critical infrastructures.

After several strategic acquisitions of companies in the security sector, existing cybersecurity expertise has been bundled within a single, specialized subsidiary Rohde & Schwarz Cybersecurity GmbH in 2016.

One of the flagship products of Rohde & Schwarz Cybersecurity is R&S®Trusted Gate, a product that provides a specialized solution in the area of data-centric security. It is designed to enable organizations to transparently leverage the benefit of collaboration platforms (with the current product focus on Office365 and SharePoint) and public cloud platforms (e.g. AWS, Google Cloud or Microsoft Azure) while maintaining a high level of security and compliance at the same time.

This is achieved by integrating the R&S®Trusted Gate functionality into the shared platform of choice (collaboration services, public cloud services and custom applications). End users (employees, partners, communication partners of all kinds) continue to interact with the native cloud or collaboration platform without any friction. R&S®Trusted Gate intercepts communication with the actual platform storage and allows to apply additional levels of security, i.e. encryption and partitioning of data. The actual cloud platform will only work with a stub version of the actual file (e.g. a Word document, an Excel sheet or a

PowerPoint presentation), a "virtual file" containing a rather limited set of meta data, but no actual document content. The actual file (the "payload") is encrypted by R&S®Trusted Gate, subsequently cut up into so-called chunks and stored in potentially multiple storage systems as defined by the individual admin of the organization. These storage systems might be on-premises, or in any kind of Software-Defined Storage (SDS) as required by business, legal or governance requirements.

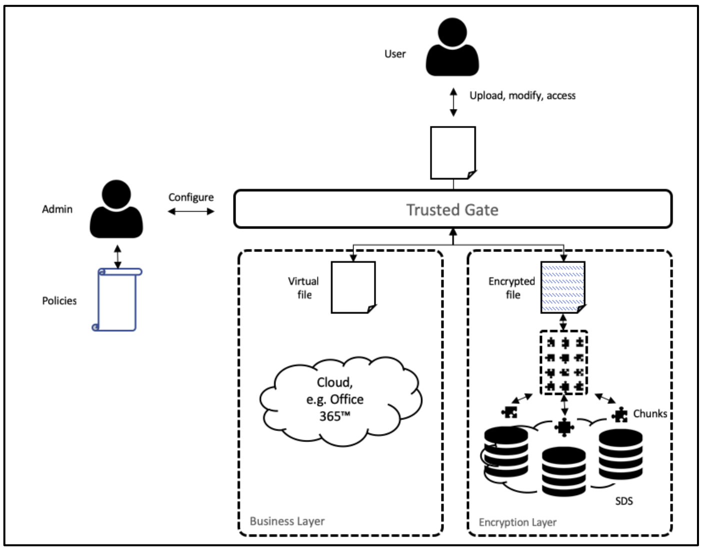

Figure 1: R&S® Cybersecurity Trusted Gate operating model

This enables configuration scenarios, where globally available public cloud services, like Office 365, can be leveraged for transparent collaboration. The native storage, e.g. SharePoint or Office365 only contains blank stub files and basic metadata. The actual document content can then be encrypted with group keys and the encrypted and fragmented data is held at e.g. AWS storage within defined regions or in storage systems on-premises. Cutting up encrypted content in slices or chunks finally means, that even compromising a single SDS would not lead to a data breach. All chunks need to be recombined before actual decryption and access can take place. This re-assembly and the decryption is under full control of R&S®Trusted Gate, so that the end user organization determining the actual configuration is in full control of keys, key stores, policies, access control, software-defined storage and auditing. Multiple instances and configuration scenarios can be managed from a single point of administration to reflect individual architecture challenges (e.g. multinational organizations and/or multi-tenant service providers).

Actual use cases are manifold: These include compliance with regulatory requirements (GDPR requirements for the storage of personal data of EU citizens in the EU), implementation of corporate requirements for the protection of intellectual property or implementation of a multi-cloud strategy for achieving resilience. Original files (encrypted and partitioned) can stay in specified regions while the workflow can be executed worldwide. Administrators can flexibly define access rights for users and groups for each file. The solution is compatible with all common file formats. When accessing a file, it is transparently decrypted for authorized users, while end users work consistently in their familiar environment.

From a technical perspective R&S®Trusted Gate can be configured in two alternative scenarios: Either as a reverse proxy, transparently enabling full functionality for Office 365 or SharePoint. Alternative scenarios can be covered with an add-in, which explicitly shows R&S®Trusted Gate features like “secure search”, depending on existing infrastructure landscapes and individual requirements. Storage systems can be added, removed or configured at runtime.

Organizations looking into securing their own applications can do so by deploying the R&S®Trusted Gate APIs. There are two options available: They can do this directly by deploying specific SOAP and REST APIs directly talking to R&S®Trusted Gate. They can choose to use standard Cloud APIs (like AWS S3 or Azure BLOB) and use the R&S®Trusted Gate Reverse Proxy. Both approaches give access to high security key management, encryption, partitioning and software-defined storage approach for individual enterprise applications (Commercial Off-The-Shelf or custom-developed).

Currently developed architecture scenarios include fully containerized deployment models, aiming at higher scalability between multiple cloud service providers and on premise for critical building blocks. This allows for larger multi-cloud concepts, with e.g. the workflow and collaboration processes running on Microsoft Azure (e.g. SharePoint or Office365) and the actual software-defined Storage running shared on AWS, on-premises and/or on Google Cloud Services, with the key servers for encryption being secured in the enterprise data center.

The solution is made available either directly through Rohde & Schwarz Cybersecurity directly or through partners like Microsoft. Additionally, fully cloud-based scenarios can soon be licensed online through the Microsoft Azure Marketplace.

3 Strengths and Challenges

Strong encryption with various key management alternatives, the partitioning of data across a growing variety of potential, software-defined storage backends, policy-based and individual assignment of access control to files, users and user groups, while keeping the actual workflows in their native collaboration tool are a unique combination of features of R&S®Trusted Gate as an innovative data-centric security solution.

Rohde & Schwarz Cybersecurity has not yet achieved comprehensive visibility as a cybersecurity vendor. However, a large number of representative customers, especially in the public sector, and the backing of a strong parent company make this appear to be of little relevance for the future. R&S®Trusted Gate as a software solution is a young solution as well but has proven successful in various customer scenarios.

A specific strength of the solution is the fact that it avoids a typical shortcoming of traditional encryption solutions: R&S®Trusted Gate implements a full text search in encrypted documents. A dedicated search engine is supplied for this, creating a secure index. This allows to interact transparently and securely even with large amounts of data. R&S®Trusted Gate acknowledges existing document classifications and treats and encrypts documents accordingly during upload already.

R&S®Trusted Gate is also designed to be a cost-saving factor for organizations that have extensive requirements for protecting their document storage. Especially when data location requirements or a reliable separation of tenant information is required, this can be achieved just by configuration alternatives within the Software Defined Storage. In the first case the storage of the data in own on-premises systems is feasible, in the second case a client separation (without the necessity of multiple

Office365 or SharePoint systems) can be achieved by physical or cryptographic separation on an otherwise shared infrastructure. Several end user organizations are reported of having already leveraged R&S®Trusted Gate for this type of infrastructure optimization.

KuppingerCole acknowledges the unique approach Rohde & Schwarz Cybersecurity has chosen for data-centric security. We recommend including R&S®Trusted Gate into the evaluation process when designing and implementing reliable protection, access control and governance for sensitive data in public clouds and collaboration environments like Microsoft 365 and SharePoint.

Strengths	**Challenges**
● Innovative data-centric security solution that helps overcome the supposed contradictions between the use of public cloud solutions and legal, regulatory and compliance requirements. ● Software-defined storage as an abstraction layer between the frontend application and the actual backend allows a wide range of storage options (public clouds, on-premises) depending on individual criteria (cost, availability, sensitivity, etc.). ● Transparent integration into existing workflow and access scenarios in Office 365, SharePoint and Public Clouds. ● Various key management alternatives, including key servers on-premises (hold/bring your own key) or in the cloud. ● Portal-based single point of configuration. ● Support for all major cloud platforms with standard solutions. For AWS, Azure and Google the product supports also special APIs and functionality for deploying R&S®Trusted Gate as backend to COTS or custom applications. ● Easy initial onboarding and global availability through Microsoft Azure Marketplace licensing.	● Yet limited visibility of Rohde & Schwarz Cybersecurity as a vendor in the market, but currently working on developing an adequate partner ecosystem. ● Benefits beyond improved security and privacy (implementation of regulatory and legal requirements, platform consolidation) need to be well-communicated.

4 Copyright

All conclusions, recommendations, and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaims all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole does not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

The Future of Information Security – Today

KuppingerCole Analysts supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company KuppingerCole Analysts provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole Analysts, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole Analysts stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com