KuppingerCole Report

EXECUTIVE VIEW

Von Matthias Reinwarth | März 2020

R&S®Trusted Gate von Rohde & Schwarz Cybersecurity

Transparente, datenzentrische Sicherheit in nicht vertrauenswürdigen Infrastrukturen. Zuverlässige Kontrolle und Überwachung von sensiblen Informationen, die in öffentlichen Clouds und Kollaborationswerkzeugen (z.B. Microsoft Office 365, SharePoint, Teams) gespeichert sind. Virtualisierung, Verschlüsselung und Aufteilung von Daten, um eine sichere und bequeme Zusammenarbeit für Multi-Cloud-, firmeninterne und hybride Speicherumgebungen und echte Datensouveränität zu ermöglichen.

von **Matthias Reinwarth**
mr@kuppingercole.com
März 2020

Inhalt

Weitere relevante Dokumente (in englischer Sprache)

Architecture Blueprint: Hybrid Cloud Security - 72552

Advisory Note: GRC Reference Architecture - 72582

Advisory Note: KRIs and KPI for Cyber Security - 80239

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

Advisory Note: Cloud Services and Security - 72561

Advisory Note: Cyber Risk – Choosing the Right Framework - 80237

1 Einleitung

Im gleichen Maße, wie moderne Unternehmen in allen Branchen ihre rasche Digitalisierung fortsetzen, wird die Notwendigkeit, die hierfür notwendigen Daten sicher zu speichern, zu verarbeiten und auszutauschen, zu einem wesentlichen Faktor für jedes Unternehmen. Dies ergibt sich aus einer Vielzahl von Herausforderungen: Regulatorische und gesetzliche Anforderungen, Business Continuity, Datenschutz für Mitarbeiter und Kunden und insbesondere die steigende Notwendigkeit des Schutzes des geistigen Eigentums.

Gleichzeitig überholen praktisch alle Unternehmen ihre Infrastrukturen in vielen Anwendungsbereichen und entscheiden sich für die Nutzung von Cloud-Infrastrukturen. Vor 20 Jahren war das kollektive Wissen von Unternehmen in der Regel in internen Datenbanken gespeichert. Heute hingegen ist es über so unterschiedliche Cloud-Dienste wie Teams, Office 365, git, Jira oder ServiceNow verteilt, während früher unternehmensinterne Systeme in der Cloud auf Infrastructure as a Service (IaaS) gehostet werden.

Cloud-Dienste bieten vielfältige Vorteile, darunter die Fähigkeit, auf sich verändernde Anforderungen zu reagieren und die Flexibilität, neue Geschäftslösungen rascher bereitzustellen. Dies gilt insbesondere für die entscheidenden Bereiche der Kommunikation, aller Arten von Workflows und den Austausch von Dokumenten einschließlich Kollaboration. Office 365 und Teams als Software as a Service (SaaS) Angebote von Microsoft sind in vielen Organisationen und Branchen das Werkzeug der Wahl für die Zusammenarbeit im Büro, die tägliche Arbeit mit Dokumenten und den Informationsaustausch mit erweiterten Lieferketten und Partnern.

Die Unternehmensgrenzen verschwimmen, da die Erfordernis und die Fähigkeit, Informationen auszutauschen, ständig zunimmt. Der Trend verlagert sich eindeutig in Richtung Multi-Cloud und hybrider Umgebungen, wobei die Kommunikation und der Dokumentenaustausch in diesen Systemen die Grundlage entscheidender Geschäftsprozesse bilden. Diese Aspekte stellen erhebliche Herausforderungen an die Informationssicherheit, die Einhaltung gesetzlicher Vorschriften, den Datenschutz und den Schutz des geistigen Eigentums dar.

Ohne von vornherein zu unterstellen, dass Anbieter von Cloud-Computing-Diensten grundsätzlich nicht zuverlässig sind, muss eine Cloud dennoch im Sinne einer Risikobewertung als "nicht vertrauenswürdig" beurteilt werden. Datensicherheit kann passiv oder im Verborgenen kompromittiert werden. Etwaige schädliche Aktionen können von innerhalb der Cloud von einem böswilligen Administrator oder Mitarbeiter durchgeführt werden. Und ohne hier allzu sehr ins Detail zu gehen, stellt die nationale Rechtsprechung einiger Staaten im internationalen Zusammenspiel derzeit eine ganz besondere Herausforderung dar, da staatlichen Stellen unter dem Vorwand einer legitimen Strafverfolgung ein weitreichender Zugriff auf Daten in Cloud-Infrastrukturen gewährt werden soll.

Ohne weitere Schutzmaßnahmen eröffnet dies ungeahnte Möglichkeiten, Zugang zu Informationen zu erhalten, die als intern und geheim zu betrachten sind und die aus Sicht des Dateneigentümers vor einer solchen Einsichtnahme geschützt werden müssen.

Geht man davon aus, dass der Trend zu Cloud-Infrastrukturen unvermindert anhält, sind traditionelle Ansätze zur Cybersecurity, die Infrastruktur und Systeme schützen, nicht mehr angemessen. Die traditionelle IT-Sicherheit konzentriert sich in der Regel auf den Schutz von Netzwerken, Systemen, Anwendungen, Servern und Endgeräten im Allgemeinen. In den heutigen Infrastrukturen decken derartige Maßnahmen jedoch nicht mehr sinnvoll die zentralen Schutzanforderungen ab. Die Frage, wie man in einer zunehmend perimeterlosen IT Daten zwischen firmeninternen Umgebungen, der Cloud und überall dazwischen sichern kann, wird immer wichtiger. Dadurch verändert sich die aktuelle Cybersicherheit nachhaltig. Dies macht einen umfassenden Paradigmenwechsel erforderlich, da Infrastrukturen, die weder selbst betrieben noch administriert werden, nicht mehr angemessen abgesichert werden können. Stattdessen liegt der Fokus auf den Daten selbst, d.h. der Nutzlast, wodurch die Infrastruktur, die diese verarbeitet, aus Sicht der Datensicherheit irrelevant wird. Unter der Annahme, dass diese Infrastruktur als potenziell gefährdet, gefährlich und von Akteuren bevölkert ist, die als feindselig anzusehen sind, müssen die Informationen selbst in einer solchen Umgebung technisch und konzeptionell abgesichert werden.

Gleichzeitig muss sichergestellt werden, dass es zu keinem wesentlichen Funktionalitätsverlust kommt. Wenn Datensicherheit dazu führt, dass weitreichende Funktionen wie die kollaborative Bearbeitung von Dokumenten oder auch nur die einfache Suche innerhalb eines Datenbestandes nicht mehr möglich sind, dann macht dies den Einsatz moderner Kollaborationsplattformen wertlos. Die entscheidende Herausforderung besteht darin, ein höchstmögliches Maß an Sicherheit zu bieten, ohne die Einsatzfähigkeit der Anwendungen zu beeinträchtigen.

Zu den wichtigsten Strategien der datenzentrischen Sicherheit gehören die Vermeidung/Reduzierung von Daten in den eigentlichen Cloud-Systemen und ein umfassender Ansatz zur Verschlüsselung und Verschleierung, der sicherstellt, dass verschlüsselte Informationen unter keinen Umständen von Unbefugten in ihrer ursprünglichen Form wiederhergestellt werden können.

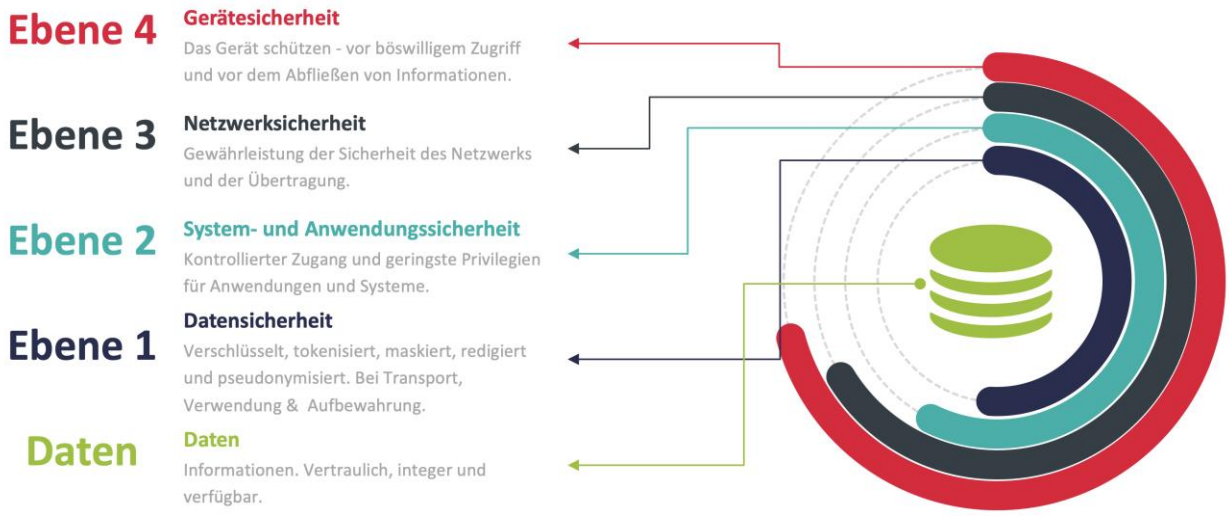

Abbildung 1: Datenzentrische Sicherheit als Zentrum eines mehrschichtigen Sicherheitsansatzes

Dies bedeutet nicht, dass die datenzentrische Sicherheit die einzige, neuartige Lösung für Sicherheitsherausforderungen ist, die alles bisher Dagewesene ersetzt. Datenzentrische Sicherheit schützt das, was wirklich geschützt werden muss, nämlich die eigentlichen Informationen als Nutzlast.

Zusätzliche Ebenen können als Teil eines mehrschichtigen Sicherheitsansatzes ergänzt werden, der mehrere Dimensionen der Cybersicherheit abdeckt. System- und Anwendungssicherheit, Netzwerksicherheit und der Schutz des Gerätes des Benutzers bleiben wichtige Schutzebenen, da auch weiterhin traditionelle Sicherheitsmechanismen (z.B. Firewalls oder Endpoint-Sicherheit) zusätzliche Schutzebenen bieten. Diese zusätzlichen Schutzebenen müssen erst überwunden werden , um einzelne Aspekte und Sicherheitsdimensionen zu schützen, insbesondere in hybriden Umgebungen.

2 Beschreibung von Anbieter und Produkt

Rohde & Schwarz Cybersecurity ist ein IT-Sicherheitsexperte, der ein breites Portfolio an Sicherheitslösungen, insbesondere im Bereich der datenzentrischen Sicherheit, anbietet. Das Unternehmen ist Mitglied der Rohde & Schwarz-Gruppe, ihrer Muttergesellschaft, einem führenden Lösungsanbieter in den Geschäftsfeldern Messtechnik, Broadcast- und Medientechnik, Aerospace | Verteidigung | Sicherheit sowie Netzwerke und Cybersicherheit.

Nach mehreren strategischen Übernahmen von Unternehmen im Sicherheitsbereich wurde das vorhandene Knowhow im Bereich IT-Sicherheit im Jahr 2016 in einer einzigen, spezialisierten Tochtergesellschaft Rohde & Schwarz Cybersecurity gebündelt.

Eines der Aushängeschilder von Rohde & Schwarz Cybersecurity ist R&S®Trusted Gate, ein Produkt, das eine spezialisierte Lösung im Bereich der datenzentrischen Sicherheit bietet. Es soll Unternehmen in die Lage versetzen, die Vorteile von Kollaborationsplattformen (mit dem aktuellen Produktschwerpunkt auf Office 365 und SharePoint) und öffentlichen Cloud-Plattformen (z.B. AWS, Google Cloud oder Microsoft Azure) transparent zu nutzen und gleichzeitig ein hohes Maß an Sicherheit und Compliance zu gewährleisten.

Ermöglicht wird dies durch die Integration der R&S®Trusted Gate-Funktionalität in die jeweilige Plattform (Kollaborationsdienste, öffentliche Cloud-Dienste und individuell angepasste Anwendungen). Die Endnutzer (Mitarbeiter, Partner, Kommunikationsteilnehmer jeglicher Art) interagieren weiterhin mit ihrer gewohnten Cloud- oder Kollaborationsplattform. R&S®Trusted Gate agiert als Zwischenebene in der Kommunikation mit dem tatsächlichen Speichersystem der Plattform und ermöglicht die Einbindung zusätzlicher Sicherheitsstufen wie z. B. der Verschlüsselung und Partitionierung von Daten. Die Cloud-Plattform erhält nur eine entkernte Version der tatsächlichen Datei (z. B. eines Word-Dokuments, eines Excel-Tabellendokuments oder einer PowerPoint-Präsentation) – eine „virtuelle Datei“, die eine limitierte Menge an Metadaten, aber keine tatsächlichen Dokumenteninhalte enthält.

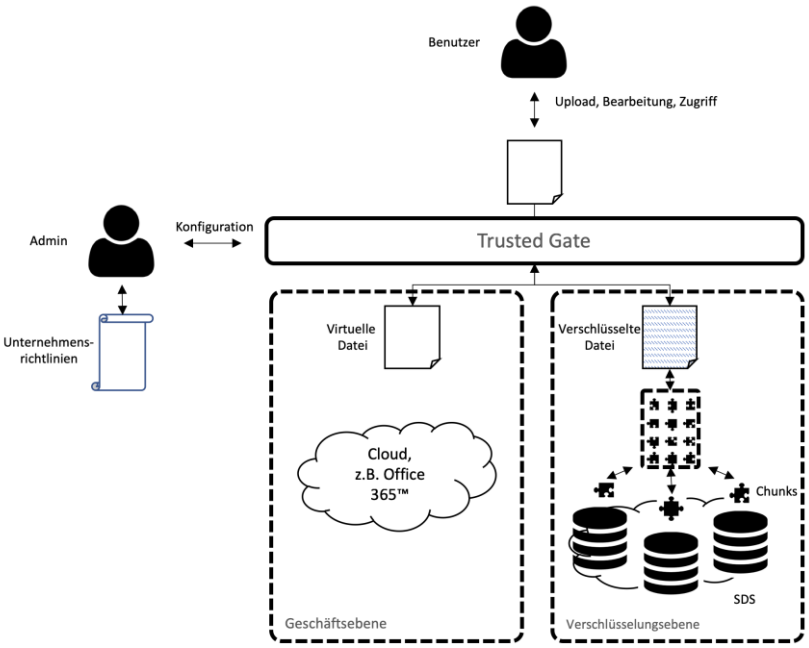

Abbildung 2: Modell der Arbeitsweise von R&S®Trusted Gate

Dies ermöglicht Konfigurationsszenarien, in denen weltweit verfügbare, öffentliche Cloud-Dienste wie Office 365 zur transparenten Zusammenarbeit genutzt werden können. Der anwendungseigene Speicher, z. B. SharePoint oder Office 365, enthält nur entkernte Dateien und grundlegende Metadaten.

Die tatsächlichen Dokumenteninhalte können mit Gruppenschlüsseln verschlüsselt und die fragmentierten Daten beispielsweise in AWS-Speichern in festgelegten Regionen oder On-Premises, im eigenen Rechenzentrum, gespeichert werden. Die Aufspaltung verschlüsselter Inhalte in Teilmengen oder Chunks sorgt schließlich dafür, dass die Kompromittierung eines einzelnen SDS nicht zu einem Datenleck führt. Denn bevor die Entschlüsselung und damit der Zugriff erfolgen kann, müssen alle Chunks zusammengeführt werden. Diese Zusammenführung und die folgende Entschlüsselung wird vollständig durch R&S®Trusted Gate kontrolliert. So behält die Endnutzerorganisation, die die genaue Konfiguration selbst festlegt, die volle Kontrolle über Schlüssel, Schlüsselspeicher, Sicherheitspolitik, Zugriffskontrolle, SDS und Audits. Mehrere Instanzen und Konfigurationsszenarien können zentral und je nach Anforderungen der Unternehmensarchitektur (z. B. multinationale Organisationen und/ oder Multi-Tenant-Dienstleister) verwaltet werden.

Die Anwendungsfälle sind vielfältig: Sie umfassen die Einhaltung regulatorischer Vorgaben (EU-DSGVO-Vorgaben zur Speicherung personenbezogener Daten von Bürgern innerhalb der EU), die Umsetzung von Unternehmensvorgaben zum Schutz geistigen Eigentums sowie die Umsetzung einer Multi-Cloud-Strategie für mehr Cyber-Resilienz. Die Originaldateien können (verschlüsselt und partitioniert) in festgelegten Regionen gespeichert werden, während der Workflow weltweit stattfinden kann. Administratoren können für jede einzelne Datei Zugriffsrechte für Benutzer und Gruppen flexibel festlegen. Die Lösung ist mit allen üblichen Dateiformaten kompatibel. Wird auf eine Datei zugegriffen, wird diese für autorisierte Benutzer transparent entschlüsselt, während die Endnutzer konsistent in ihrem gewohnten Umfeld weiterarbeiten.

Aus technischer Sicht kann R&S®Trusted Gate auf zwei verschiedene Arten konfiguriert werden: Als Reverse Proxy, der transparent die volle Funktionalität von Office 365 oder SharePoint bereitstellt, oder als Add-in, das bestimmte R&S®Trusted Gate-Features wie die „Sichere Suche“ je nach vorgegebener Infrastruktur und individuellen Anforderungen bereitstellt. Speichersysteme können während der Laufzeit jederzeit hinzugefügt, entfernt oder konfiguriert werden.

Zu den derzeit eingesetzten Architekturszenarien gehören vollständig containerisierte Deployment-Modelle, die eine höhere Skalierbarkeit zwischen mehreren Cloud-Service-Anbietern und vor Ort für kritische Komponenten ermöglichen. Dies ermöglicht die Realisierung umfangreicher Multi-Cloud-Konzepte, bei denen z.B. die Workflow- und Kollaborationsprozesse auf Microsoft Azure (z.B. SharePoint oder Office 365) und der eigentliche softwaredefinierte Speicher auf AWS, lokal und/oder auf Google Cloud Services gemeinsam genutzt werden, wobei die Key-Server für die Verschlüsselung im Unternehmensrechenzentrum abgesichert werden. Von einer einzigen Administrationsoberfläche aus können mehrere Instanzen und Konfigurationsszenarien verwaltet werden.

Datenzentrische Sicherheit, wie sie von R&S®Trusted Gate implementiert wird, kann in verschiedensten Szenarien eingesetzt werden: Ursprünglich primär für den Schutz von Daten in Cloud-Infrastrukturen konzipiert, nutzt Rohde & Schwarz Cybersecurity die Technologiebasis nun für zusätzliche Aufgabenstellungen: Das immer beliebter werdende OneDrive for Business kann mit R&S®Trusted Gate ebenso geschützt werden wie die weit verbreitete Collaboration-Suite Microsoft Teams. Im Laufe der Zeit wurden weitere Anwendungsszenarien hinzugefügt.

- Sichere, selbst verwaltete Projekträume können als Plugin in SharePoint hinzugefügt werden, ohne dass ein Administrator beteiligt werden muss.
- Szenarien zur Optimierung der Infrastruktur für einen effizienteren Umgang mit vorhandenen Ressourcen: Viele verschiedene Konfigurationsmodelle sind denkbar und werden in der Praxis eingesetzt, insbesondere die Realisierung mandantenfähiger Systeme durch eine physikalische oder kryptographische Separierung auf einer ansonsten gemeinsam genutzten Infrastruktur (z.B. für Multi-Tenant Service Provider, ohne die Notwendigkeit mehrerer Office 365- oder SharePoint-Systeme).
- Sicherer Informationsaustausch zwischen Partnern. Einfache Einsatzkonzepte können mit einer Webschnittstelle für den Zugriff auf gemeinsam genutzte vertrauliche Informationen umgesetzt werden. Permanentere und transparentere Architekturen synchronisieren hingegen verschlüsselte Inhalte unter Nutzung zweier R&S®Trusted Gate-Instanzen und einer gemeinsam genutzten, softwaredefinierten Speicherinfrastruktur.
- Konfigurationsszenarien, um individuelle rechtliche oder regulatorische Herausforderungen für multinationale Organisationen zu reflektieren. Dadurch können insbesondere die Anforderungen an den Speicherort der Daten effizient umgesetzt und erfüllt werden.
- Fortgeschrittene Anwendungsfälle nutzen R&S®Trusted Gate zur Pseudonymisierung von Identitäten, um den Zugriff auf externe Systeme (z.B. Public Clouds) über anonyme IDs zu ermöglichen.

Unternehmen, die die Absicherung ihrer eigenen Anwendungen planen, können dies durch den Einsatz der R&S®Trusted Gate APIs erreichen. Dabei stehen zwei Optionen zur Verfügung: Einerseits können sie dies direkt durch den Einsatz spezifischer SOAP- und REST-APIs im direkten Zusammenspiel mit

R&S®Trusted Gate erreichen. Andererseits können sie sich für die Verwendung von Standard-Cloud-APIs (wie AWS S3 oder Azure BLOB) entscheiden und den R&S®Trusted Gate Reverse Proxy verwenden. Beide Ansätze ermöglichen den Zugriff auf hochsichere Schlüsselverwaltung, Verschlüsselung, Partitionierung und softwaredefinierte Speicheransätze für individuelle Unternehmensanwendungen (kommerzielle Standardversion oder kundenspezifisch entwickelt).

Die Lösung wird entweder direkt über Rohde & Schwarz Cybersecurity oder über Partner wie Microsoft zur Verfügung gestellt. Cloud-basierte Anwendungsfälle können online über den Microsoft Azure Marketplace lizenziert werden.

Rohde & Schwarz Cybersecurity arbeitet aktiv daran, den zugrunde liegenden datenzentrischen Sicherheitsansatz auszuweiten. Neben anderen Integrationen und Szenarien steht eine Ausweitung der Anwendungsbereiche zur Sicherung weiterer beliebter SaaS-Angebote auf der Roadmap.

3 Stärken und Herausforderungen

Angesichts der Tatsache, dass die datenzentrische Sicherheit immer mehr an Bedeutung gewinnt, bietet Rohde & Schwarz Cybersecurity überzeugende Lösungen für eine Vielzahl von Sicherheits- und Datenschutz-Herausforderungen, insbesondere in Cloud-Anwendungen und SaaS-Szenarien. Durch die Entkopplung der Anwendung von der eigentlichen Datenspeicherung bieten diese Lösungen die Flexibilität, eine umfassende Datensouveränität zu erreichen und gleichzeitig die Vorteile moderner SaaS-Lösungen zu nutzen.

Starke Verschlüsselung mit verschiedenen Varianten der Schlüsselverwaltung, die Partitionierung von Daten auf eine wachsende Vielfalt von möglichen, softwaredefinierte Speicher-Backends, richtlinienbasierte und die individuelle Zuweisung der Zugriffskontrolle an Dateien, Benutzer und Benutzergruppen unter Beibehaltung der tatsächlichen Arbeitsabläufe in ihrem nativen Kollaborationstool sind eine einzigartige Kombination von Merkmalen von R&S®Trusted Gate als innovative datenzentrische Sicherheitslösung.

Die Einbeziehung von Microsoft-Teams als einer sehr beliebten Kooperationsplattform in die Palette der unterstützten Systeme ist eine wichtige strategische Erweiterung. Sowohl "out of the box"-Anwendungsszenarien als auch komplexere, aber leicht konfigurierbare Anwendungsfälle, die den datenzentrischen Sicherheitsansatz nutzen, zeigen die Vielseitigkeit des zugrunde liegenden Konzepts.

Rohde & Schwarz Cybersecurity verbessert zunehmend seine Sichtbarkeit als Hersteller von Cybersecurity-Lösungen durch eine große Anzahl von repräsentativen Kunden, insbesondere im öffentlichen Sektor. R&S®Trusted Gate ist eine wachsende Familie von datenzentrischen Sicherheitslösungen für verschiedene Cloud-Plattformen, die sich in einer schnell steigenden Zahl von Kundenszenarien bewährt hat. Es ist als kostensparender und effizienzsteigernder Baustein für Organisationen konzipiert, die umfangreiche Anforderungen an die Absicherung der Speicherung ihrer Dokumente haben.

Eine besondere Stärke der Lösung ist die Tatsache, dass sie die typischen Unzulänglichkeiten traditioneller Verschlüsselungslösungen vermeidet, bei denen verschlüsselte Daten während der Speicherung unbrauchbar sind: Im Gegensatz zu diesen Lösungen, die z.B. SharePoint zu einer reinen

Datenablage für verschlüsselte Daten-Blobs machen, implementiert R&S®Trusted Gate eine Volltextsuche in verschlüsselten Dokumenten. Dazu wird eine spezielle Suchmaschine bereitgestellt, die einen sicheren Index erstellt. Dies ermöglicht eine transparente und sichere Zusammenarbeit auch bei großen Datenmengen. Dasselbe gilt für die Zusammenarbeit in Teams oder SharePoint, die durch den einzigartigen Verschlüsselungs- und Daten-Shadowing-Ansatz von R&S®Trusted Gate möglich bleibt.

KuppingerCole begrüßt den besonderen Ansatz, den Rohde & Schwarz Cybersecurity für die datenzentrische Sicherheit gewählt hat. Wir empfehlen, R&S®Trusted Gate in einen Evaluierungsprozess einzubeziehen, wenn es darum geht, zuverlässige Datensicherheit, Zugangskontrolle und Governance für sensible Daten in öffentlichen Clouds und Kollaborationsumgebungen wie Microsoft 365, Teams und SharePoint zu konzipieren und zu implementieren.

Stärken	Herausforderungen
• Innovative datenzentrische Sicherheitslösung, die die sichere Nutzung von Public-Cloud-Lösungen ermöglicht. • Leistungsstarke Lösung zur Erfüllung gesetzlicher, behördlicher und Compliance-Anforderungen. • Softwaredefinierte Speicherabstraktion als Brücke zwischen Frontend-Anwendung (Geschäftsebene) und verschlüsseltem Speicher (Backend). • Große Auswahl an Speichervarianten (öffentliche Clouds, On-Premises) zur Erfüllung individueller Anforderungen (Kosten, Verfügbarkeit, Empfindlichkeit usw.). • Transparente Integration in bestehende Workflow- und Zugriffsszenarien in Microsoft Office 365, Teams, SharePoint und Public Clouds. • Verschiedene Alternativen zur Schlüsselverwaltung (z.B. On-Premises, Cloud, Hold/Bring your own key). • Portalbasiertes zentrales Konfigurationssystem. • Unterstützung der wichtigsten Cloud-Plattformen mit Standardlösungen. • Ermöglicht die effiziente Nutzung und Konsolidierung bestehender Plattformen. • Einfache Erstinbetriebnahme und globale Verfügbarkeit durch die Lizenzierung über den Microsoft Azure Marketplace.	• Noch begrenzte Sichtbarkeit von Rohde & Schwarz Cybersecurity im Markt, aber ständige Arbeit an der Weiterentwicklung des Partner-Ökosystems. • Lösungsdesign erfordert zusätzlichen Speicherplatz in der Cloud oder im eigenen Rechenzentrum für die sichere Datenspeicherung. • Das Potenzial der Lösung, das über die Verbesserung der Sicherheit und des Datenschutzes hinausgeht, ist auf dem Markt noch nicht allgemein wahrgenommen worden.

4 Copyright

Die Zukunft der Informationssicherheit – Heute

KuppingerCole Analysts unterstützt IT-Fachleute mit herausragendem Fachwissen bei der Ausarbeitung von IT-Strategien und damit verbundenen Entscheidungsprozessen. Als führende Analysefirma bietet KuppingerCole Analysts anbieterneutrale Informationen aus erster Hand. Mit unseren Dienstleistungen haben Sie einen sicheren und zuverlässigen Partner an Ihrer Seite, um essentielle Entscheidungen für Ihr Unternehmen zu treffen.

KuppingerCole Analysts ist seit seiner Gründung im Jahr 2004 eine in Europa ansässige Analysefirma mit Fokus auf Informationssicherheit und Identity- and Access Management (IAM). KuppingerCole Analysts steht für Fachwissen, Vordenken, herausragende praktische Relevanz und eine anbieterneutrale Sicht auf die Marksegmente der Informationssicherheit. Alle wichtigen Aspekte werden abgedeckt: Identity and Access Management (IAM), Unternehmensverfassung und Abschlussprüfung, Sicherheit in der Cloud und in virtuellen Umgebungen, Informationsschutz, Mobilfunk- und Softwaresicherheit, System- und Netzwerksicherheit, Sicherheitskontrolle, Analyse und Berichterstattung, Unternehmensführung, Organisation und Richtlinien.

Für weitere Informationen kontaktieren Sie bitte **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