White paper

Locking down private cloud security

Introduction

In study after study, security is noted as a top concern in moving to the cloud.

- 81% of respondents say security is top cloud challenge.[1]
- 23% of IT professionals say protecting sensitive data is the top organizational weakness, and 21% say the second greatest weakness is the need for improved third-party product integrations across all product categories.[2]
- 59% of IT professionals say they are most concerned with the visibility and control of data.[3]

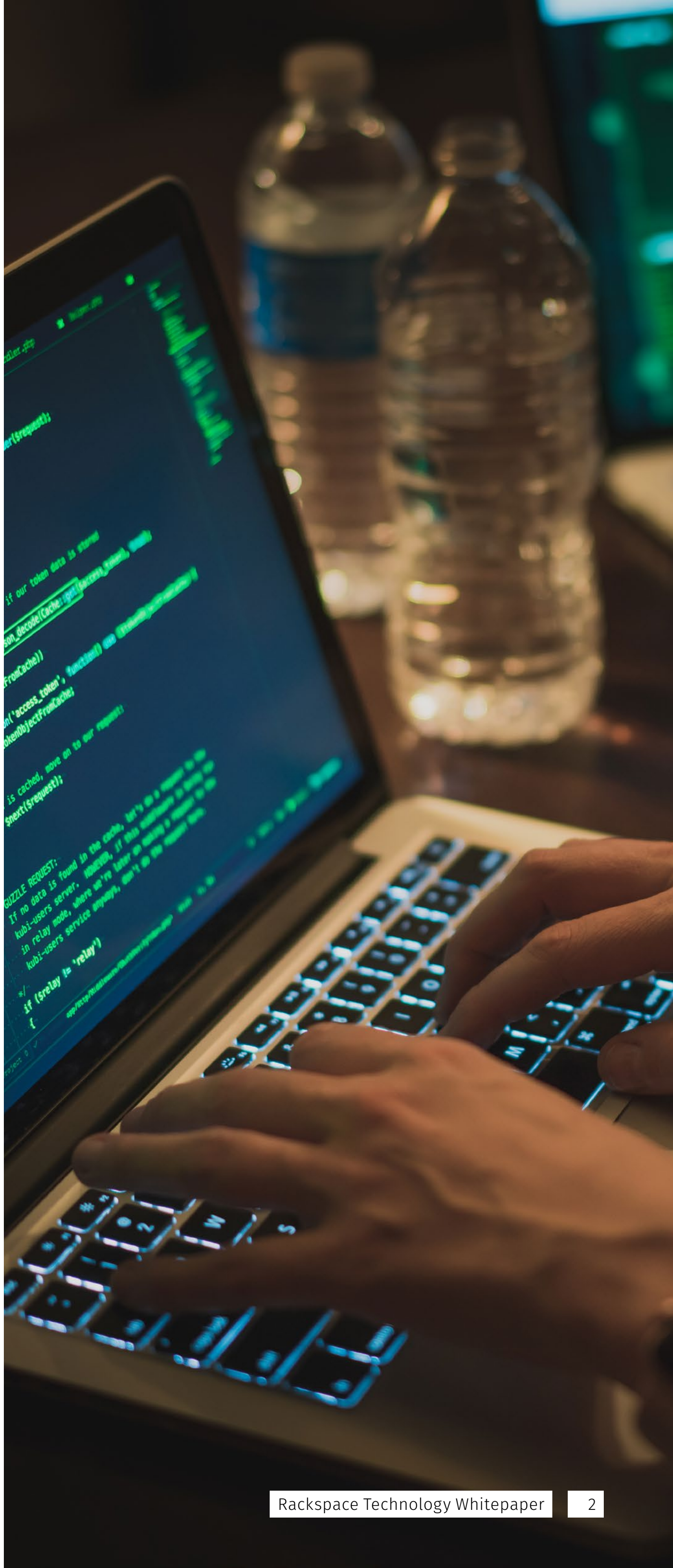
Despite the widespread concerns, security can be one of the core benefits of moving to the cloud. According to the AlertLogic Cloud Security Report, in a cloud environment you're actually safer from incidents like Trojans, brute force attacks and other suspicious activities.[4]

Flexera's 2021 State of the Cloud reported that over 90% of businesses operate in a multicloud environment. For over 80% this is a combination of public and private cloud. Private clouds play important roles as part of the multicloud infrastructure that most organizations have adopted. Organizations are using, planning to use or experimenting with a range of private cloud technologies, including VMware Cloud, AWS Outpost and Microsoft® Azure® Stack.

Enterprises are running applications on an average of 2.7 private clouds and experimenting with an additional 2.2 private clouds.[5]

Those applications carry sensitive company information, personally identifiable information (PII) and, in highly regulated industries like banking and healthcare, information that is also governed by industry and governmental regulations. Single-tenant environments with physically isolated networks and compute and storage layers can provide more security, with the added benefit of better performance.

This white paper compiles industry data and expert insights to discuss the opportunity to leverage private cloud while maintaining — or exceeding — your data security requirements.



Private cloud security challenges

As businesses move to the cloud, they're faced with new methodologies for approaching security in the midst of an ever-evolving threat landscape. This two-fold trend presents the following challenges:

Untangling the security spaghetti

Many enterprise IT shops are running multiple security appliances and a myriad of security tools throughout their environment. Whether as a result of shadow IT or bad planning, multiple security tools can create compatibility issues and generate multiple streams of siloed data, obscuring a clear view of the entire security picture. On top of that, limited expertise and understanding of new platforms and methodologies hinder a business's ability to protect itself in the cloud or on-premises.

New approaches that embrace standardization and automation are needed. But without the right talent, time and tools, transformation projects to implement cloud, DevOps and new security frameworks risk being botched or scratched altogether.

Dodging advanced security threats

If you arrive at work on a Monday morning and the storefront windows are broken, it's easy to see that you've been robbed. Unfortunately, most companies don't even know they've fallen victim to a security breach. In 2020, 82% of IT security and C-level executives believed that they experienced at least one data breach when implementing new technologies and expanding their supply chains. There could have been more security breaches that were not detected.[7]

In 2020, another study found that the dwell time, the period between a threat entering and leaving an environment, averaged 207 days.[8] That's 207 days that the bad guys have to poke around looking for your prized data and compromising your systems. Once detected, you not only have to deal with the damage of the breach, but also initiate a remediation process — or a kill chain — to identify and remove the threat.

Cyber risks

As the use of cloud increases it is presenting challenges. As stated earlier in this white paper security is the number one challenge for 81% of respondents, followed by managing cloud spend for 79%, while another three challenges were cited by 75% of respondents: governance, lack of resources/ expertise and compliance.[9]

Security expertise is essential as cyber threats are constantly evolving. For example, hackers are now using ransomware to target enterprises with unpatched servers. They freeze the target's environment until a ransom is paid.

Throughout 2019 and the first half of 2020, there were more than 380 publicly reported ransomware attacks on public U.S. organizations. In November 2019, cybercriminals added a new element to their ransomware schemes which involved creating copies of each victim organization's data before encrypting it. Next, they threatened to publish portions of the data and sell it to other criminals or simply give it away if the ransom wasn't paid.

Ransomware itself continues to be offered as a stand-alone software product, and also sold as a service (RaaS). It's an organized crime with close-knit ransomware gangs recruiting affiliates who work with them to launch attacks.

As the number of cyber threats continues to rise, feelings of "no confidence" in cyber resilience are increasing in three critical areas:

- Understanding and assessing cyber risks — from 9% to 18%
- Preventing cyber threats — from 12% to 19%
- Responding to and recovering from cyber events — from 15% to 22%[10]

In 2019, 79% of respondents ranked cyber risk as a top concern more than any other major business risk ahead of economic uncertainty at second. But less than 30% conducted management training or modelled cyber loss scenarios.[11] This is further exemplified in another study that shows only 29% of respondents can address system downtime, cybersecurity attacks, and data breaches.[12]

The root of this problem can be seen in budgets as 64% would increase cyber risk spending in response to a cyber-attack on their organization.[13] However, having a proactive rather than reactive approach is always preferable.

Evolving from perimeter defense

Once upon a time, you only had to protect the fortress walls. Not anymore. New technologies are opening up new avenues for malicious activity. And no one is safe, not big businesses nor highly regulated industries. According to Forrester, more than half of IT leaders (58%) still suffered a data breach in the past 12 months, 33% were hit by infrastructure outages and 29% were struck by ransomware.[14] Those attacks didn't come from the sophisticated hacks you'd expect from curious coders.

Social engineering has been the root cause of many recent breaches. In a survey by SANS Institute, half of the respondents who had been victims of breaches or incidents stated that account and credential hijacking played a role. The motives ranged from purely monetary gain to corporate espionage to politically charged causes.

Security must now account for new, less-sophisticated attacks in addition to advanced persisitent threats (APTs) that circumvent the perimeter. Businesses need strategies that look for and respond to anomalies within the environment to detect and mitigate breaches before valuable data and credentials are lost. One such strategy is the Zero Trust approach of "never trust, always verify" which applies behaviorial analysis through machine learning to identify anomalies across endpoints and services. If anything in the ecosystem, services, data or devices changes, the system can rewrite and automatically apply new actions based on pre-defined security policies.

In the same SANS Institute survey, 45% of respondents cited the difficulties of multi-tenancy as the second biggest challenge faced in adapting incident response and forensic analysis to the cloud. With single-tenancy and customizable security controls, private clouds can help you better address your perimeter and anything that passes into your environment.

Balancing innovation and security

People move to the cloud to accelerate the pace at which they can build, test and launch new applications. And as companies adopt the agility of DevOps, they are iterating, testing, launching and re-launching in a less linear fashion than ever before. This increases the number of opportunities for security to become an issue. Imagine multiple developers working on the same code, across multiple platforms, in multiple clouds. As systems advance in complexity, so too must the security approach. Undertaking a transformation or DevOps implementation project inevitably will demand building standard playbooks to govern security controls and reap the full benefits of new frameworks and processes.

Managed security benefits

Expertise
Specialized talent to protect existing environment

Better ROI
Eases budget constraints in supporting security initiatives

Choice
Tons of vendors with lots of solution options

Innovation
Supports increased adoption of cloud

Governance, risk management and compliance
Evolving compliance requirements

Private cloud security opportunity

Private clouds allow organizations to retain the governance and hosting of corporate data in trusted environments, while transitioning those environments to take advantage of cloud benefits, like reduced costs and better performance. Private clouds also allow you to customize security controls to meet your unique needs. As you approach the private cloud decision, security-specific considerations should include the following considerations:

Expertise

Because experienced private cloud providers have generally hosted differing and complex environments, they bring robust security experience to the table. Chances are that they already have experience dealing with the complex security challenges you're facing. In addition to protecting your assets, these experts are also available to help you understand your security options.

Capabilities

Leveraging multiple security tools across an organization creates data silos and hinders a holistic view across the entire environment. All cloud platforms come with a set of security features built-in. With access to best-of-breed tools and the experts who know how to use them, you're able to tailor security to your business needs. So, whatever you're doing now, you can replicate in a private cloud. However, you'll most likely find that the security measures already in place can be tuned or augmented to satisfy or exceed your current security needs.

Costs

Optimizing cloud costs is the 2021 top initiative (61%) across all cloud users.[15] Pre-packaged, pre-tested security configurations eliminate chasing single-license apps and ongoing maintenance for multiple security tools. Best practices and expertise in implementation also save you from the growing cost and bad publicity of a major breach. A good private cloud provider will already have done the legwork to select the right tools and security strategy for your environment.

Manpower

A McAfee report[16] places the median cybersecurity salary at 2.7 times the average IT FTE wage with some estimates recommending approximately 2.5 FTEs per 100 full-time IT employees. In the U.S., that averages out to $6,500 more than other IT professions. However, the right private cloud provider will have more hands on deck with more certifications than most organizations can find or afford. These experts are also empowered with tools and resources to strictly adhere to best practices without having to cut corners as often happens on resource-constrained, on-premises teams.

Responsiveness

Breaches are no longer a question of if, but when. Security can no longer be a reactive activity. Your provider should have a defined approach, including firm timeframes to detect, respond and contact you. Be sure you understand the difference between an alert and response function. Most providers will tell you that there's an issue, but still leave you holding the bag to figure out how to respond and mitigate it.

Managing private cloud security: DIY or MSSP?

So how do businesses tackle these many challenges? The options are a DIY approach with an array of tools and the right expertise to manage and respond to alerts, or a Managed Security Service Provider (MSSP) for a fully managed approach. As you approach private cloud adoption, you'll have to balance its security characteristics with those of your public cloud services to comprehensively secure your business.

But there is no such thing as "set it and forget it" options for security. It's a partnership with your provider. The cloud is inherently built with security in mind. Providers include security functionality for the network, storage and compute layers of a given cloud platform. However, the customer must ensure the apps and data that are running on the cloud are secure. This is the customer's responsibility.

An MSSP fills the gap between the inherent security built into a cloud, and the additional security needed to completely secure the platform and the data and applications running on it. As an MSSP, Rackspace Technology™ constantly monitors activity, and is ready to respond to alerts as soon as a breach happens. And unlike many private cloud providers, who only capture alerts and pass the remediation on to you, Rackspace Technology, remediates the breach based on agreed upon actions, then lets you know what's happened and that it's taken care of.

How they did it

Here are a few examples of how Rackspace Technology has helped customers in various industries solve private cloud security challenges:

Financial services — Accuity

Accuity identifies fraudulent activity for businesses. By partnering with Rackspace Technology a scalable infrastructure was implemented enabling the screening of its clients' big data. Leveraging Rackspace Managed Hosting and various security features, Accuity is now delivering anti-money laundering and compliance solutions while also enhancing customer experience with its reliable security services.

Software and Technology — DevonWay

When the continuous improvement software company DevonWay wanted to meet its clients' stringent cybersecurity requirements, it partnered with Rackspace Technology. As Chris Moustakas, DevonWay President and CEO explained: "The certifications, SSAE 16 Type 2, were very important to us to be able to hand over to our customers and prospects to prove beyond a shadow of a doubt that we knew what we were doing and that we took security extremely seriously,"

The managed security solution includes Rackspace Private Cloud powered by VMware and has provided DevonWay with a secure hosted environment. "We've added the managed security offering on top of our already secure environment. It allows us to have more breadth and more around-the-clock monitoring," said Robert Lentz, VP Technical Operations, DevonWay.

Healthcare – National Kidney Registry

Technology powers the National Kidney Registry's (NKR) donor match functionality. Responsible for placing 30 to 40 kidneys a month, Sincore says, "Without technology, none of this could happen. We could never have done this 20 years ago. But, because of technology, we can find the best matches for patients in need who have donors, getting them matched and transplanted as quickly as possible. Having a partner like Rackspace Technology allows us to have the infrastructure behind the scenes to do that."

Rackspace Technology has been a key partner in providing a managed hosting solution for NKR, furnishing a stable logistical management infrastructure, with support for systems and back-office capabilities. Rackspace Managed Security protects the NKR environment from APTs and other cyberattacks. "The database and the website that front-ends the database, and the database that offers connectivity to all the transplant centers, is all housed at Rackspace Technology in a highly secure data facility, which is critical to our operations. We have been able to install a HIPAA-compliant server that allows us to manage the security of the data, to protect it and to measure potential outside threats from hackers."

Summary

As businesses continue to adopt cloud-based initiatives to support AI, IoT, big data and more, they may feel apprehensive about the ability to protect critical assets in the cloud.

Historically, public clouds have been perceived as less safe for compliance or security sensitive workloads. But public cloud options have matured along with private and hybrid options that give you the same — or a better — security posture than on-premises environments. The right private cloud provider brings a more comprehensive approach to security that goes beyond standard perimeter defense with added layers of security, often out of reach for most organizations because of cost or skills gaps.

Though many professionals still point to security as a barrier to the cloud, using a strong MSSP to lock down your hosted private and hybrid cloud can put to rest any security issues that might be keeping you awake at night.

How Rackspace Technology can help

When it comes to your cloud security journey, our team of experts are here to help you every step of the way. We work as an extension of your security staff, helping you rapidly migrate to the cloud, and stay ahead of cybersecurity threats before they impact your business.

Our modern, full-service security operation defends your business against cybersecurity threats with 24x7x365 support from certified security analysts in our global SOC. Our global team of 400+ network and security experts have earned 500-plus industry certifications — including CCNAs and GIACs in cyber defense, penetration testing, digital forensics and incident response. We couple this with best of breed security tools, and add value with purpose-built automation and multicloud management through a single pane of glass.

Learn more about how Rackspace Technology can help achieve your private cloud security goals. Visit us at: **rackspace.com/security**

Sources

1. Flexera 2021 State of the Cloud Report: https://info.flexera.com/CM-REPORT-State-of-the-Cloud
2. “The State of Cloud Security: Results of the SANS 2020 Cloud Security Survey”, Thomas (TJ) Banasik, SANS Institute Information Security Reading Room: www.sans.org/reading-room/whitepapers/cloud
3. “The State of Cloud Security: Results of the SANS 2020 Cloud Security Survey”, Thomas (TJ) Banasik, SANS Institute Information Security Reading Room www.sans.org/reading-room/whitepapers/cloud:
4. Alert Logic Cloud Security Report: https://go.alertlogic.com/rs/239-ZBX-439/images/CSR_2015_Web.pdf?mkt_
5. Flexera 2021 State of the Cloud Report: https://info.flexera.com/CM-REPORT-State-of-the-Cloud
6. Flexera 2021 State of the Cloud Report https://info.flexera.com/CM-REPORT-State-of-the-Cloud
7. 2020 Ponemon Digital Transformation & Cyber Risk: https://ponemonsullivanreport.com/2020/07/digital-transformation-cyber-risk-what-you-need-to-know-to-stay-safe/
8. 2020 Ponemon Digital Transformation & Cyber Risk: https://ponemonsullivanreport.com/2020/07/digital-transformation-cyber-risk-what-you-need-to-know-to-stay-safe/
9. Flexera 2021 State of the Cloud Report: https://info.flexera.com/CM-REPORT-State-of-the-Cloud)
10. 2019 Global Cyber Risk Perception Survey, Marsh & McLennan Companies with Microsoft: www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html
11. 2019 Global Cyber Risk Perception Survey, Marsh & McLennan Companies with Microsoft: www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html
12. Digital Transformation & Cyber Risk: What You Need to Know to Stay Safe, Sponsored by CyberGRX independently conducted by Ponemon Institute LLC, June 2020: Source: https://ponemonsullivanreport.com/2020/07/digital-transformation-cyber-risk-what-you-need-to-know-to-stay-safe/
13. 2019 Global Cyber Risk Perception Survey, Marsh & McLennan Companies with Microsoft: www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html
14. Zero Trust Security Workbook from Rackspace Technology
15. Flexera 2021 State of the Cloud Report: https://info.flexera.com/CM-REPORT-State-of-the-Cloud
16. Mcafee Report: www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

About Rackspace Technology

Rackspace Technology is the multicloud solutions expert. We combine our expertise with the world’s leading technologies — across applications, data and security — to deliver end-to-end solutions. We have a proven record of advising customers based on their business challenges, designing solutions that scale, building and managing those solutions, and optimizing returns into the future.

As a global, multicloud technology services pioneer, we deliver innovative capabilities of the cloud to help customers build new revenue streams, increase efficiency and create incredible experiences. Named a best place to work, year after year according to Fortune, Forbes and Glassdoor, we attract and develop world-class talent to deliver the best expertise to our customers. Everything we do is wrapped in our obsession with our customers’ success — our Fanatical Experience™ — so they can work faster, smarter and stay ahead of what’s next.

Learn more at www.rackspace.com or call 1-800-961-2888.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS A GENERAL INTRODUCTION TO RACKSPACE® SERVICES AND DOES NOT INCLUDE ANY LEGAL COMMITMENT ON THE PART OF RACKSPACE.

You should not rely solely on this document to decide whether to purchase the service. Rackspace detailed services descriptions and legal commitments are stated in its services agreements. Rackspace services’ features and benefits depend on system configuration and may require enabled hardware, software or additional service activation.

Except as set forth in Rackspace general terms and conditions, cloud terms of service and/or other agreement you sign with Rackspace, Rackspace assumes no liability whatsoever, and disclaims any express or implied warranty, relating to its services including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, and noninfringement.

Although part of the document explains how Rackspace services may work with third party products, the information contained in the document is not designed to work with all scenarios. any use or changes to third party products and/or configurations should be made at the discretion of your administrators and subject to the applicable terms and conditions of such third party. Rackspace does not provide technical support for third party products, other than specified in your hosting services or other agreement you have with Rackspace and Rackspace accepts no responsibility for third-party products.

Rackspace cannot guarantee the accuracy of any information presented after the date of publication.

Rackspace-White-Paper-Locking-Down-Private-Cloud-Security-White-Paper-SEC-TSK-4349 :: April 22, 2021