White paper

Locking down private security

rackspace®

ALERT LOGIC

Introduction

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

- 1/3 of surveyed central IT professionals still call cloud security a significant challenge.[1]
- 52% of surveyed technology decision makers have concerns around the risk of unauthorized access, data integrity and protection in the cloud.[2]
- 62% of surveyed IT security professionals say their top cloud concern is unauthorized access to data by outsiders.[3]

Despite the widespread concern, 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]

Private clouds offer even greater levels of control over security variables. While fewer companies are using private clouds, those that do, use them more than ever. Enterprises are running applications on an average of 2.3 private clouds and experimenting with an additional 2.1 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 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

Though public cloud adoption is growing, organizations that have moved to the cloud or are in the process of implementing a cloud strategy, are most likely to use a private cloud. Current studies show that, overall, enterprises run 75% of workloads in the cloud with more in private clouds (43%) than in public clouds (32%).[6]

Private cloud is emerging as the leading cloud platform for enterprises. Nearly one in four businesses (24%) are looking to expand private cloud use this year, with Azure platform showing the most robust growth.[7]

Percent enterprise workloads in clouds

43% private cloud
32% public cloud
25% non cloud

Source: RightScale 2017 State of the Cloud Report

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, mulitiple 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.

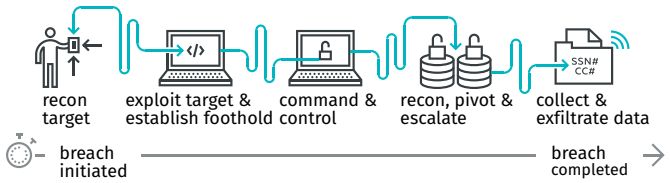
New approaches that embrace standardization and automation are needed. But without the right talent, time and tools, transformation projects to implement cloud, DevOps and new security frameworks risk being botched or scratched altogether.

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. Unfortunely, most companies don't even know they've fallen victim to a security breach. In 2016, roughly 22% of surveyed IT security professionals stated that they weren't sure if they'd been breached.[8]

According to industry estimates, it can take up to 200 days to detect a breach.[9] That's 200 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.

The kill chain



Managing more — and big(ger) data

Since 2013, the the financial impact of an incident has grown 29%. From a profit perspective, the average company loses $158 per record, with healthcare record losses costing up to $355. These costly attacks won't slow down anytime soon.

The primary reason for the rising risk of breaches is the staggering amount of data being stored and collected. Almost half (48%) of SANS Institute survey respondents are storing employee records in the cloud, followed by 41% storing business intelligence and 38% storing business financials and accounting.[10] With all of these valuable nuggets of data available, criminals are using new tactics to attack — tactics that old security techniques aren't able to quickly handle or resolve.

For example, ransomware that once focused on holding individuals' personal data hostage is now turning toward enterprises. Using spear phishing, malicious software to attack vulnerable, unpatched servers, ransomware enters and freezes up your environment until you pay the ransom. And 68% of surveyed respondents believe that traditional security techniques aren't ready for the next generation of malware.[11]

The risk arises not only from the profit motives of malicious parties, but also in the risk of falling out of compliance with industry and government regulations. Survey responses indicate that 46% of organizations are required to comply with the Payment Card Industry Data Security Standard (PCI DSS), 33% with Sarbanes-Oxley (SOX) and 35% with

Health Insurance Portability and Accountability Act (HIPAA) mandates.[12] Not having the security framework, process and expertise to adhere to these standards can result in a breach, but also, leave an organization with heavy fines, penalties and loss of accreditations needed to do business.

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. By 2020, three in 10 global businesses will be compromised. Those attacks won't come from the sophisticated hacks you'd expect from curious coders.

Social engineering was the root cause of the 2014 Yahoo hack that compromised over 500 million accounts. In a recent 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 range from purely monetary gain to corporate espionage to politically charged motives.

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. 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 cloud can help you better address the 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 to reap the full benefits of new frameworks and processes.

The prevalence of new ways to access and interact with data also opens up new avenues for attack. For example, the big Dyn DNS attack of 2016 was a typical DDoS attack in every way except one. Instead of enlisting PCs or even mobile devices as in the past, this attack commandeered the communications capabilities of millions of connected devices — think washing machines and televisions. The growing use of the internet of things (IoT), coupled with the increase in connected devices, increases the number of endpoints through which bad guys can gain entry.

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**

GRC

Evolving **compliance requirements**

DIY	MSSP
Tooling	Managed security
Staff	Compliance support
SOC	Moderate monthly operating expense
Large upfront capital expense	

rackspace

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:

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 top initiative across all cloud users (53%), and especially among mature cloud users (64%).[13] 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 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 plan of attack, 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 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 the inherent security capabililties (single-tenancy, highly customizable platform) with the conditions you need to run 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 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, 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 has helped customers in various industries solve private cloud security challenges:

Financial services – PayLease

PayLease CTO, Wade Williams, brought the company's online payments and utility management service to Rackspace Private Cloud to meet its specific use case. "We are very serious about security, and one of the main drivers for getting into Rackspace initially was to be located in a PCI Level 1 data center. You can't cut corners with security and Rackspace makes that so much easier," says Williams.

Government – CSID

When the Office of Personnel Management was hacked, it called CSID. CSID called Rackspace. "Rackspace gave us the ability to mobilize the teams on both sides to get hardware and infrastructure in place, to support something that I would characterize as urgent and unusual. It was a demanding and volatile situation driven by political and government leaders. Our technology had to respond."

Collaborating with its Rackspace Private Cloud team, the company set up infrastructure to serve the performance and stringent security and compliance needs of the U.S. government's human resources hub. "When the contract was awarded, we had only hours to scale up our front-end to service millions of government employees who were affected and notified in an aggressive timeframe," said Bloomstrand.

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 allows us to have the infrastructure behind the scenes to do that."

Rackspace 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, database that offers connectivity to all the transplant centers, is all housed at Rackspace 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."

rackspace®

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 cloud options have matured with private and hybrid options that give you the same — or a better — security posture than an on-premises environment. 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 Managed Security Service Provider (MSSP) to lock down your hosted private cloud can put to rest any security issues that might be keeping you awake at night.

Sources

1. RightScale 2017 State of the Cloud Report: http://assets.rightscale.com/uploads/pdfs/RightScale-2017-Stateof-the-Cloud-Report.pdf
2. 2016 IDG Enterprise Cloud Computing Survey: https://www.idgenterprise.com/resource/research/2016-idgenterprise-cloud-computing-survey/?utm_campaign=Cloud%20Computing%20Survey%202016&utm_medium=Press%2Release&utm_source=Press%20Release
3. Security and Accountability in the Cloud Data Center: A SANS Survey: https://www.sans.org/reading-room/whitepapers/analyst/security-accountability-cloud-data-center-survey-37327
4. Alert Logic Cloud Security Report: https://go.alertlogic.com/rs/239-ZBX-439/images/CSR_2015_Web.pdf?mkt_
5. Cloud Computing Trends: 2017 State of the Cloud Survey: http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey
6. Cloud Computing Trends: 2017 State of the Cloud Survey: https://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey
7. Cloud Computing Trends: 2017 State of the Cloud Survey: https://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey
8. Security and Accountability in the Cloud Data Center: A SANS Survey: https://www.sans.org/reading-room/whitepapers/analyst/security-accountability-cloud-data-center-survey-37327
9. IDC Intelligence-Led Security: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ASW12370USEN
10. Security and Accountability in the Cloud Data Center: A SANS Survey: https://www.sans.org/reading-room/whitepapers/analyst/security-accountability-cloud-data-center-survey-37327
11. Ransomware Surveys Fill In Scope, Scale of Extortion Epidemic: http://www.darkreading.com/operations/ransomware-surveysfill-in-scope-scale-of-extortion-epidemic/d/d-id/1327523
12. Security and Accountability in the Cloud Data Center: A SANS Survey: https://www.sans.org/reading-room/whitepapers/analyst/security-accountability-cloud-data-center-survey-37327
13. RightScale 2017 State of the Cloud Report: http://assets.rightscale.com/uploads/pdfs/RightScale-2017-Stateof-the-Cloud-Report.pdf

Alert Logic

Alert Logic® Security-as-a-Service solution delivers deep security insight and continuous protection for cloud, hybrid and on-premises data centers. Providing application, system and network protection from the cloud, the Alert Logic solution analyzes over 400 million events and identifies over 50,000 security incidents monthly for over 3,800 customers.

About Rackspace

At Rackspace, we accelerate the value of the cloud during every phase of digital transformation. By managing apps, data, security and multiple clouds, we are the best choice to help customers get to the cloud, innovate with new technologies and maximize their IT investments. As a recognized Gartner Magic Quadrant leader, we are uniquely positioned to close the gap between the complex reality of today and the promise of tomorrow. Passionate about customer success, we provide unbiased expertise, based on proven results, across all the leading technologies. And across every interaction worldwide, we deliver Fanatical Experience™. Rackspace has been honored by Fortune, Forbes, Glassdoor and others as one of the best places to work.

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

Rackspace-White-Paper-Locking-Down-Private-Cloud-Security-White-Paper-SEC-14960 :: May 24, 2019