E-book

Five Cloud Security Challenges Your Business Can Face Head-On

rackspace technology®

The constant evolution of cyberthreats, and the race for more sophisticated tools to combat them, has resulted in a rapidly changing security landscape. Now more than ever, it's critical to understand your vulnerabilities and assemble the right solutions to strengthen and secure your environments. And the best way to do that is through the implementation of a cutting-edge security program focused on continuous improvement and backed by deep expertise.

In this e-book, we examine five security challenges businesses face, and how providers should rise to the occasion to defend them.

rackspace technology.

1. There is no such thing as a one-size-fits-all security solution.

Businesses undergoing digital transformation projects often encounter issues translating their existing security controls, policies and practices from one environment to the next. Expecting to move your existing workloads and security technologies to the cloud isn't an apples-to-apples proposition. Most organizations leverage multiple cloud platforms, and these platforms all have their own portfolio of cloud-native security tools that generally don't integrate with other platforms. Knowing how to architect your multicloud environments to meet your security and compliance needs with the right security technology is a challenge. The flexibility of the security tools you choose is important as your business needs change and cybersecurity threats increase in complexity. Security solutions must be fast, flexible and elastic.

And most importantly, security measures must be cloud appropriate. It's important to remember that moving your workloads to the cloud opens up new risk factors, and new security tools can be deployed to protect your apps and data. A recent study by IDC found that 79% of companies had experienced at least one breach in the past 18 months. One of the nagging issues for organizations? The lack of visibility into live cloud environments, according to the Chief Information Security Officers surveyed *(IDC Survey of 200 Security Decision Makers, 2020).*

No matter where you are in your journey of digital transformation and moving workloads to the cloud, keep in mind that you might need different security tools, policies and response plans.

2. Apps make the modern cloud architecture world go ‘round, but not prioritizing security at the start can bring that to a screeching halt.

Just like the cloud itself, threats today are dynamic. The cloud is application-centric, not infrastructure-centric. It’s built and run by developers, Site Reliability Engineers, line of business owners, and digital app managers instead of traditional network infrastructure teams. This is a change from the slower-paced governance models that many businesses are used to. Now that we are moving fast, there is more automation, speed and agility. Security needs to be more agile and adaptable as well. DevSecOps Engineers can help integrate security into the development of your cloud-native apps from the start — without slowing down your speed of development.

Why? With the cloud being application-centric, this brings a new rise in application-centric threats.

Application threats are on the rise: According to a recent Forrester survey, 33% of breaches were from external attacks, such as web application attacks, stolen credentials, and software exploits *(Forrester Analytics Global Business Technographics® Security Survey 2019)*.

Cloud misconfigurations lead to breaches: According to Gartner, 99% of cloud security failures will be the customer’s fault *(Gartner Security Report — 2025 Trends)*.

3. Today's talent shortage is a major challenge to the security industry.

According to the New York Times, there is a tremendous skills shortage. It's estimated that at the end of 2021, there will be 3.5 million unfilled cybersecurity positions. Most companies don't have the expertise or capabilities needed because their staff lacks training or experience in security to properly secure their cloud and on-premises environments. Without experienced cloud security experts on-staff, organizations will struggle to securely migrate to the cloud and transform their operational models. According to Forrester, 43% of organizations cite that competition for security talent makes it difficult to hire and retain staff *(Forrester Analytics Global Business Technographics® Security Survey 2019)*. Strong competition for security talent and demanding compliance mandates has caused many firms to invest in services rather than in more expensive and hard-to-recruit security staff.

4. A reactive security policy is not enough with ransomware on the rise.

When it comes to security breaches, it's not a matter of if, but when you'll experience one. A single security breach can devastate your organization financially, while bringing work to a standstill and harming your reputation. Many IT teams struggle being caught in an ongoing cycle of "reactive mode," which limits their ability to look ahead in a proactive manner. Waiting until after you've been affected by a security incident will be more costly in the long run and likely increase your exposure to further incidents in the future. In fact, in the past year the average cost of a breach has increased from $3.9 million to $4.24 million globally *(Ponemon, Cost of a Data Breach 2021)*.

Even with a reactive security incident response plan in place, your business could still be at risk. Cybercriminals can go from initial entry to ransoming an entire network in less than 45 minutes *(Microsoft Digital Defense Report, Sept 2020)*. This can even happen when the attack causes multiple detection alerts in security tools, such as endpoint detection and response products — signifying cybercriminals' understanding of the challenges modern IT departments face in their inability to rapidly triage, contain and respond to fast-paced attackers.

5. Security must keep pace with your infrastructure.

New threats are constantly evolving, and many companies struggle to keep up with the threats and vulnerabilities that are emerging daily. New attack techniques are sophisticated, combining overlapping techniques to breach a system, such as reconnaissance, credential harvesting, malware, and VPN exploits just to name a few. On top of that, advanced bad actors are developing unique malware in addition to openly available malicious code for mainstream online criminal activity *(Microsoft Digital Defense Report FY2020)*. Traditional approaches to security posture don't flex with cloud-first application delivery models. The benefit of the cloud is the flexibility it provides to change and meeting your business needs. While it's important to have a security partner that understands the cloud and is willing to engage and keep pace as your needs grow, it's even more important that they help you evolve your security operations.

How Rackspace Technology can help

Rackspace Elastic Engineering for Security helps you to break free of traditional reactive approaches to security with an agile, proactive, end-to-end security solution that delivers effective threat detection and incident response against increasingly sophisticated attacks.

Built on a pod structure that works as an extension of your staff, we help you meet the cloud security and compliance goals that are important to your business. No matter where you are in your cloud security journey, your pod of experts will be with you every step of the way, helping your business define and implement a security strategy that reduces risk and defends against cyberthreats. As your security partner, Rackspace Technology consolidates threat intelligence, security analytics, alerts and response services into a solution that can be easily deployed and managed across multicloud environments.

Your pod includes an engagement manager, a pod lead, lead architect, security architects, security engineers, a compliance expert and security analysts/penetration testers who work as an extension of your team and are dedicated to cyber risk remediation. Your security pod can design, build and fully manage a defense-in-depth architecture for unified protection across multicloud environments, including AWS, Microsoft® Azure®, VMware® and Rackspace Technology environments.

Our security experts have deep knowledge and experience in both IT security and cloud security and hold 800+ security industry certifications — including 100+ cloud security certifications from AWS, Azure and Google Cloud.

We remain dedicated to helping you protect your digital investments while helping to ensure security resiliency and addressing your compliance needs. We're your partner, ready to enable more predictable business outcomes and underwriting transformation benefits.

Learn more at: www.rackspace.com/security/elastic-engineering or call 1-800-961-2888

rackspace technology®

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.

Rackspace-Ebook-Elastic-Engineering-for-Security-SEC-TSK-5328 :: August 16, 2021