# Promise vs. Reality

## The operational impact of cloud solutions

REDSEAL

83%

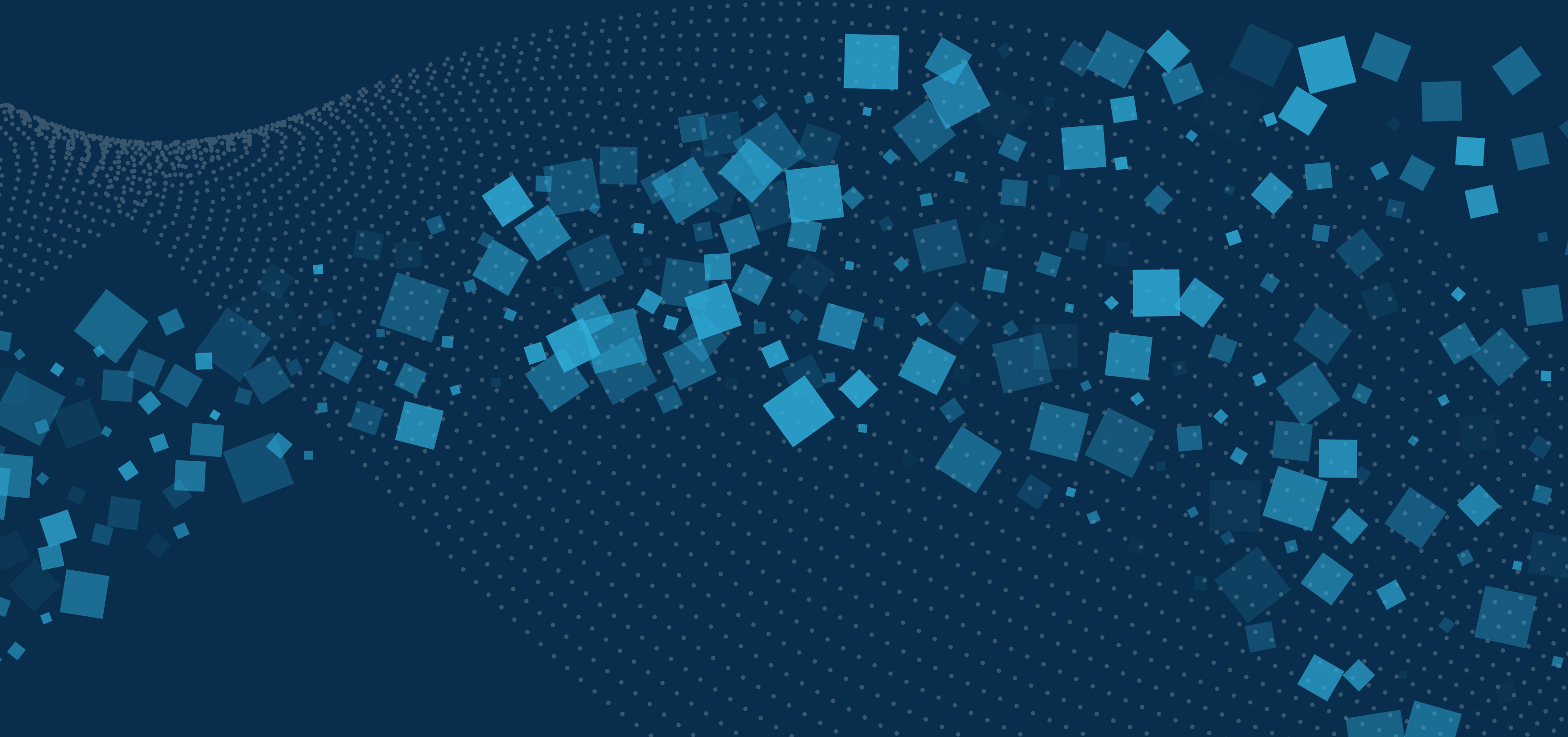
of businesses now say that “cloud is very or extremely important to their organizations future strategy and growth.

According to a recent report from Splunk and Harvard Business Review Analytic Services, 83 percent of businesses now say that “cloud is very or extremely important to their organizations future strategy and growth.” Already, 50 percent of corporate data is stored in the cloud, and predictions from research firm Gartner suggest that public cloud spending will continue to grow at least 20 percent year over year. Put simply, cloud computing has become a mainstream technology that companies can’t afford to ignore, especially as data volume and variety continue to rise. Lacking the scalable resources offered by cloud solutions, businesses simply can’t compete at scale.

The result? Cloud is now tapped for almost every aspect of business operations, from IT to sales and marketing to human resources, front-line operations, and even C-suite strategy. This broad adoption ties to the promise of cloud technologies to offer substantive benefits across all aspects of an organization.

But there’s another side to the cloud coin: Operational realities that come with deployment at scale. From increasing application and infrastructure complexity to security concerns and cost management oversight, businesses often experience a disconnect between cloud potential and practical concerns.

Here’s what that looks like in practice, what it means for operations, and what businesses can do to capitalize on the promise of cloud confidence.



# Exploring the Promise of Cloud Solutions

With public, private, hybrid, and multi-cloud environments now commonplace, cloud availability and interoperability are at an all-time high. Enterprises don't want for choice — now, they can select and deploy purpose-built cloud solutions designed to streamline critical services without breaking the bank.

## Some of the most appealing cloud promises include:

**Time Savings**

The interoperability offered by cloud services comes with the promise of easy application deployment, implementation, and use, in turn reducing the amount of time IT teams need to spend on setup, management, and maintenance. The same is true for upgrades and patches — since cloud providers handle the infrastructure and hardware upgrades, businesses don't need to schedule time for these tasks or worry about the impact of new updates on existing services.

According to recent survey data, the top two benefits of cloud solutions were peace of mind around security and version upgrades and the improved speed and accessibility that comes with cloud services.

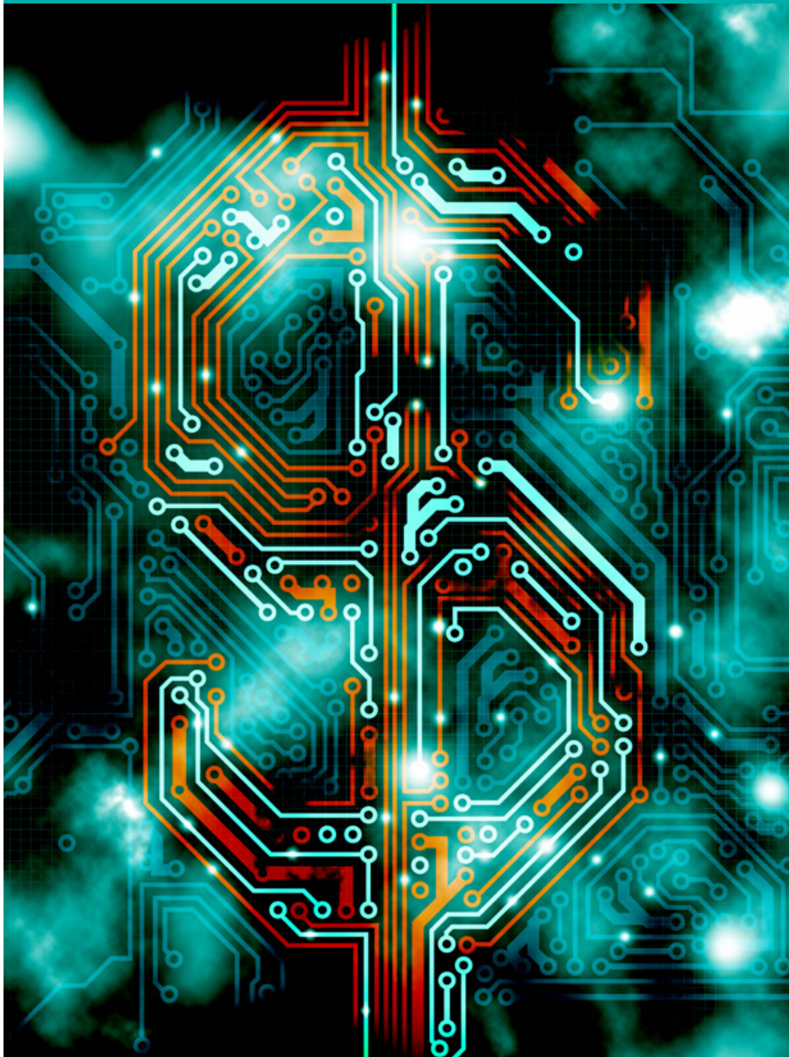
**Cost Control**

Cost is another area often tapped as a significant cloud benefit. Here's why: while on-premises servers and technologies require capital expenditure (CapEx) for the initial purchase, maintenance, and upgrading, cloud solutions use an operational expenditure (OpEx) model that sees companies paying based on service and resource use rather than for physical hardware and software licenses. As a result, businesses gain increased visibility into what they're spending, when, and how.

Cloud can also help control the costs of unplanned downtime by significantly reducing its potential. As noted by Tech Channel, 44 percent of enterprises now say that a single hour of downtime costs more than $1 million. Meanwhile, the redundant, multi-location nature of cloud services makes it possible for data to failover quickly and operations to remain on track.

44%

of enterprises now say that a single hour of downtime costs more than **$1 million**.



### IT Agility

IT teams have enough on their plate dealing with accessibility, security, and interoperability. The cloud streamlines this process by creating an environment where services and solutions naturally work together. This is bolstered by the increasing shift toward specialty cloud services that see providers excelling in key areas such as analytics or data processing and designing their solutions to work natively with other services to provide maximum business benefit.

### Service Scalability

In many ways, scalability defines the cloud. Unlike on-prem services that are naturally bound by physical space, cloud resources are capped only by what companies want to spend — and when they want to spend it. Instead of being locked into a fixed amount of processing or performance, IT teams can scale up as required and back down as needed to ensure they're not paying for the over-provision of services. Meanwhile, newer cloud models such as hyper-converged infrastructure (HCI) and metered consumption are exploring new ways to merge on-premises and cloud-based frameworks to deliver maximum scalability with minimum risk.

### Ease of Use

Authorized staff can quickly and easily create new accounts or instances on cloud services. Depending on the model used, it may be possible to spin up new solutions with IT approval or to use company credit cards for new development or application instances on-demand. In addition, the self-service nature of many cloud services means that staff members can often accomplish tasks without the need for IT support, in turn freeing up IT teams to tackle line-of-business objectives.

# Evaluating the Operational Realities of Cloud Services

While moving to the cloud offers significant potential benefits, the interconnected nature of these services creates new operational realities that don't always align with cloud promises.

## As a result, IT teams are often confronted with cloud challenges such as:

### Increased Complexity

The sheer number of cloud services and solutions available is both a benefit and a challenge for companies. Why? Because as the volume and variety of cloud options expand, so too does overall network complexity. With applications and services residing in different cloud environments — and often spanning multiple clouds — it often becomes more difficult for teams to identify IT issues and pinpoint root causes.

Recent data support this complexity concern. Almost half of companies said that cloud deployments were more complicated than they expected. Moreover, 47 percent of C-suite executives said that complexity could have significant, negative impacts on cloud ROI over the next five years.

### Expanded Attack Surfaces

More data and services in the cloud mean a bigger attack surface, giving malicious actors more avenues for compromise and increasing overall cloud security challenges. While on-site datacenters come with the risk of potential breaches leading to complete compromise, the sheer scale of the cloud makes it challenging for teams to pinpoint where attacks are coming from, what attackers are after, and what steps they need to take to limit possible impacts.

Consider the rise of cloud-based ransomware attacks. With 50 percent of companies already storing or planning to store sensitive data in the cloud, it's no surprise that more than half of all cloud threats are tied to ransomware. If attacks can compromise expanded attack surfaces to gain cloud access, they can effectively frustrate business operations at scale.

47%

of C-suite executives said that complexity could have significant, negative impacts on cloud ROI over the next five years.

### Reduced Visibility

More cloud services often mean reduced visibility, especially as adoption ramps up. The availability of self-service cloud options exacerbates this problem. If staff can quickly spin up instances and services on-demand, it's easy for IT to lose track of exactly what's running, where, and for how long.

The results range from costly to critical. If instances remain up and running long after they're needed, companies could pay far more than they should for cloud services. And if attackers manage to compromise these services, IT teams may not find evidence of attacks until it's too late. According to IBM, the average time for enterprises to identify and contain a breach is now 287 days. Consequently, cybercriminals have plenty of time to survey IT environments, establish continual access, and create a plan of attack.

### Limited Expertise

While cloud services need minimal oversight from IT individually, in aggregate, they require skilled monitoring and management. This creates an expanding IT skills gap. As noted by Information Week, 50 percent of organizations may not meet their 2022 cloud goals because they lack in-house expertise. With skilled IT pros in high demand, recruiting new talent is no easy task. Upskilling current staff can help close the gap, but this takes time and effort away from current cloud concerns.

### Changing Technologies

New networking and security technologies are continually being introduced into cloud environments. Consider the rise of next-generation firewalls (NGFWs) that leverage artificial intelligence to detect and deter potential attacks or the use of networking-as-a-service (NaaS) solutions that virtualize critical network operations to reduce resource needs. While these technologies benefit business operations, they often come with a steep learning curve for IT teams. In addition, user- and developer-facing tools often outpace security and operational solutions, creating a potential gap between deployment and defense.

# The Three-Step Cloud Journey

It's one thing to talk about cloud promises and realities generally, but what does the cloud journey look like — and how does it relate to these concepts?

## For many companies, moving to the cloud includes three common steps:

**Step 1: Deployment**

The first step in any cloud shift is deployment. This is the process of moving applications and services off on-site stacks and into the cloud and is typically handled by application developers and network engineers. The focus of this stage is functionality: Ensuring that all tools and technologies that make the jump work together and those that don't play well with cloud services — such as legacy applications or proprietary code — are left behind.

**Step 2: Security**

With cloud services up and running, businesses must now ensure that workloads are effectively managed and secured. But with multiple environments and applications to handle, misconfigurations are common: What works in one cloud may not work in another. If there's a security disconnect, it could expose sensitive client or company data.

According to the State of Cloud Security 2020 Report, misconfigurations remain the primary cause of data breaches in the cloud. Eighty-four percent (84%) of IT professionals are worried that misconfigured services have already led to undetected cloud compromise.

**Step 3: Monitoring**

Once solid security perimeters have been established, companies must continually monitor cloud environments for potential vulnerabilities. These could include unauthorized data access by internal users, new compromise points created by overlapping cloud services or overly broad access permissions.

This becomes even more complicated when it comes to security policy development and enforcement. While 82 percent of survey respondents agree that policy definitions are the responsibility of security teams, 37 percent say teams are responsible for enforcement while 45 percent argue that cloud providers are on the hook for enforcement. The result is a potential security gap as both providers and cloud customers may believe that the other is responsible for handling policy-driven security breaches.

In practice, while providers must account for security issues with their own infrastructure, companies bear responsibility for the safety and security of their data — no matter where it resides.

# Managing Cloud Security with RedSeal

Not sure how to tackle your cloud cybersecurity challenges at scale?
Cloud security solutions from RedSeal can help.

## Our hybrid cloud security framework is designed to help companies empower their cloud environments across three key areas:

### Visibility

True understanding of evolving cyber terrain and threat landscapes is critical for cloud success at scale. RedSeal's posture management solutions for hybrid environments provides complete, up-to-date visualization of cloud infrastructure, detailed knowledge of all accounts and policies for layered services such as Kubernetes, and specific identification of resources and applications exposed to the Internet at large.

### Vulnerabilities

Enhance cloud network protection with context. By understanding the relationship between applications and services across your cloud environment, RedSeal helps your team prioritize vulnerabilities and discover the best path to an effective defense. With RedSeal, you can:

- Identify undetected assets
- Discover network devices
- Visualized all reachable assets
- Create a risk-based vulnerability mitigation plan
- Reliably triage and mitigate the impact of vulnerabilities

### Compliance

Compliance is critical to ongoing cloud success. RedSeal can automate much of the compliance process, in turn streamlining the process of PCI DSS, CMMC, NERC-CIP, New York DFS, and EMEA Regulations compliance. With new regulations continually in development, ongoing assessment and automation can help reduce the risk of potential compliance missteps.

**ABOUT REDSEAL (redseal.net)**

RedSeal — a security solutions and professional services company – helps government agencies and Global 2000 companies see and secure their on-premise networks and cloud environments. RedSeal Stratus, the company's SaaS CSPM solution, gives an integrated view of cloud security posture through visualization of cloud-native and Kubernetes controls, and shows which resources are unintentionally exposed to the Internet. RedSeal's Classic product brings in all network environments – public and private clouds as well as on-premises. This award-winning security solution verifies that networks align with security best practices, validates network segmentation policies, and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk. The company is based in San Jose, California.