Forcepoint

eBook

7 Steps to Cloud Security Success

Seven steps for protecting your people
and your data at the pace of business

Table of Contents

Introduction

When it comes to the cloud, IT and security professionals have mixed feelings. While 75% of them view the public cloud as more secure than their organization's own data centers, 92% of respondents admitted their organization has a gap between current and planned cloud usage and the maturity of their cloud security program.[1]

For security teams, the prospect of protecting data in the cloud is, at the very least, unsettling. Securing data in someone else's data center—without having any physical access to the underlying infrastructure—isn't something they'd eagerly raise their hands to do.

But as business teams continue to barrel forward in their cloud adoption, security teams have little choice. They must shift their mindset from building protective walls to securing data in a complex environment.

1. Oracle and KPMG Cloud Threat Report 2020

Introduction

As security teams struggle to adapt, cloud adoption continues to accelerate. IDG reports 59% of technology buyers plan to be "mostly" or "all" in the cloud in 18 months—up from 38% who say they are mostly or all in the cloud today.[2] This is a hefty increase.

According to IDG, this steep adoption curve is less about cost savings and more about the cloud's other advantages, such as faster application provisioning and enhanced computing power.

Of course, not all organizations are enthusiastically embracing the cloud. There are still skeptics who ask, "Is the cloud secure?" But for security teams, the more relevant question is, "Are we using the cloud securely?"

Signs your cloud footprint may not be secure:

- → **Continued data loss:** 75% of cybersecurity and IT professionals have experienced data loss from cloud services more than once.[3]
- → **Misconfigured cloud services:** Led by overprivileged accounts, exposed web servers, and other types of server workloads, more than one misconfiguration results in more than 10 data loss events.[4]
- → **More products, less effective protection:** Enterprises that deploy more than 50 tools rank themselves 8% lower in their ability to detect threats, and 7% lower in their defensive capabilities, than other companies employing fewer toolsets.[5]
- → **Compromised cloud credentials:** 59% of organizations have experienced spear phishing attacks that compromised employees with privileged cloud accounts.[6]
- → **Quicker deployments:** Organizations that bring new sites online without waiting for carrier provisioning create security risks.
- → **Rising cloud costs:** Through 2024, 80% of companies that are unaware of their cloud adoption mistakes will overspend by 20-50%.[7]

2. IDG's 2020 Cloud Computing Survey
3. Oracle and KPMG Cloud Threat Report 2020
4. Ibid.
5. IBM's Fifth Annual Cyber Resilient Organization Report (2020)
6. Oracle and KPMG Cloud Threat Report 2020
7. Smarter with Gartner, "4 Lessons Learned From Cloud Infrastructure Adopters." June 30, 2020.

Seven Steps to Cloud Security Success

Step 1:
Develop a Thorough Cloud Strategy

Do you have isolated cloud initiatives scattered across your organization? Form a group with a broad range of participants to help create cloud guidelines for your entire organization. Be sure each of these guidelines connects directly to your organization's business strategy. Remember to include distinct objectives, benefits, risks, and key adoption criteria in your guidelines.

A cloud strategy is not an implementation or migration plan. Rather, it should pave the way to cloud adoption by providing a clear perspective on the cloud and its role in your organization.

Think of your cloud strategy as a living document. It will change as vendors come and go, the business landscape changes, and organizational goals shift and develop.

Step 2:
Define New Security Policies, Procedures, and Controls

Don't assume you can lift and shift your on-premises privacy and security controls because they may not be designed to protect your data against cyberattacks in a public cloud environment.

In fact, misconfiguring your cloud security controls can very well open the door to cyberattacks. Gartner predicts, through 2025, 99% of cloud security failures will be the customer's fault.[8] The first step to avoiding this outcome is to get visibility into your current state of security on-premises and across private and public clouds. Then, get a clear picture of your CSP's security practices.

Cloud security tip: Before the contract phase, ask them to fill out a Consensus Assessment Initiative Questionnaire (CAIQ) developed by the Cloud Security Alliance. This assessment will give you valuable insight into the CSP's security practices.

If you have a Cloud Center of Excellence to manage and govern cloud adoption, collaborate with this group to ensure your policies and procedures are optimizing the security and reliability of the architectures that are slated for deployment.

8. Smarter with Gartner, "Is the Cloud Secure?" October 10, 2019.

Step 3:
Draw Clear Lines of Responsibility

Because cloud security is a shared responsibility between you and your CSP, it can be difficult to nail down who is doing what. In fact, only 8% of IT security executives say they fully understand the cloud's shared responsibility model.[9]

On a very basic level, CSPs are responsible for securing the cloud environment, and you're responsible for protecting what's in the cloud—including your data and your users. You're also accountable for securing your staff and their behaviors, including compliance failures caused by their actions or inactions.

The division of specific security responsibilities will be slightly different, depending on your chosen route to the cloud. (See the chart at the right.)

- → **Infrastructure as a Service (IaaS)** involves changes to the architecture, such as lifting and shifting an existing application to be hosted in the cloud.
- → **Platform as a Service (PaaS)** involves changes in functionality, such as rebuilding an application so it can leverage the cloud to lower costs and accelerate iterative improvements.
- → **Software as a Service (SaaS)** involves changes to the ways applications are delivered, accessed, and managed, such as using the web to deliver and access third-party applications.

9. Oracle and KPMG Cloud Threat Report 2020

Cloud Security Responsibility

Asset to be protected	IaaS	PaaS	SaaS
People	●	●	●
Data	●	●	●
Apps	●	●	○
Operating System	●	○	○
Virtual Networks	●	○	○
Hypervisors	○	○	○
Servers and Storage	○	○	○
Physical Networks	○	○	○

● You ○ Cloud Service Provider

Regardless of the route you choose, it's imperative to work closely with your CSP to confirm who is responsible for which security elements. After an initial agreement is reached, continue to collaborate with your CSP to clarify your obligations as your business's cloud usage changes/evolves.

Step 4:
Review the Cloud's Configuration

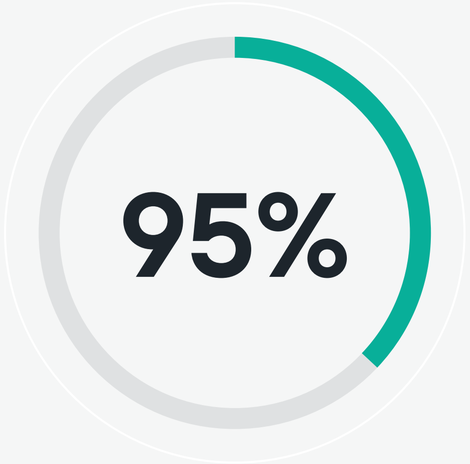
Misconfigurations are one of the errors most commonly associated with cloud security incidents. In fact, organizations with known misconfigured cloud services experienced 10 or more data loss incidents last year.[10]

Although your CSP will provide configuration guidance and controls, it's important to make sure the cloud's hardware and software details are set up for interoperability and communication across your employees' various locations. Also check your CSP's configurations to confirm they're compliant with your applicable industry and government regulations.

Need help? Cloud configuration monitoring tools are available that can help you identify misconfigurations. You can also use network traffic monitoring and user behavior analytics to identify anomalies and misconfigurations, along with their associated issues.

10. Oracle and KPMG Cloud Threat Report 2020

Step 5:
Create a Cloud-specific Security Reference Architecture



Of cloud security failures are the subscriber's fault, according to industry analysts.

Addressing these areas will help create a robust foundation for keeping your data secure in the cloud.

To safely place workloads in the cloud, you'll need to build a cloud-specific security reference architecture incorporating these components:

→ **Identity access management:** Identify and define the users who are authorized to operate in the cloud environment. Spell out what they're allowed to do. Apply Zero Trust principles to how data is accessed and used—replacing implicit trust of people inside your network with a requirement for explicit permission, every time something is used.

→ **Application security:** Establish a collective understanding of applications in use and their corresponding threats. To simplify this process, you can implement a Cloud Access Security Broker (CASB) and a Zero Trust Network Access (ZTNA) service to secure SaaS, PaaS, IaaS, and homegrown applications. As a preventative measure, you might also consider moving to a DevSecOps model, embedding security into the entire application lifecycle.

→ **Data security:** Determine the scope of encryption for data-at-rest and data-in-motion. Activate each of the cloud provider's key management services to encrypt all data and transactions, in addition to strong authentication and policy-based data loss prevention (DLP) controls for storage and collaboration.

→ **Data activity monitoring:** Log and audit all data activity at a granular level to comply with your organization's security policies and applicable regulations.

Step 6:
Accept Responsibility For Compliance

Most CSPs use third-party audits to continually evaluate their regulatory compliance. However, your CSP's compliance doesn't cover your use of the cloud environment. As a result, you should not only assess your CSP's security practices, but also develop and maintain additional controls that coincide with your security risk management framework.

With the right technologies, this can be simpler than it sounds. Using large libraries of prebuilt templates, some tools can automate your compliance specific to your region, government, and industry regulations.

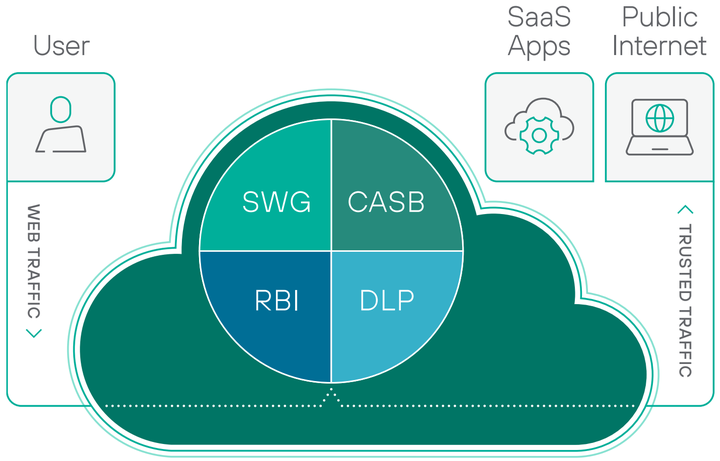
Trust program certifications—not just self-audited compliance.
Be wary of CSPs that claim certification for their entire organization, yet only include a single subset of operations in the compliance scope. Become familiar with ISO 27001, ISO 27018, CSA STAR, SOC 2 Type 2 certifications, which will help you identify potential security control issues.

Step 7:
Continuously Scan and Monitor Your Cloud Environment

Even when you've completed your cloud deployment, your work is still not done. Actually, you're just getting started. Unlike monitoring a static data center, the cloud is a rapidly changing environment. To monitor it effectively, you'll need:

- → **The ability to observe behaviors** at every level of your cloud infrastructure, including visibility into the host, container, control plane, and application layer.
- → **Deep behavioral context for alerts** so you clearly understand what happened and whether it's truly an anomaly for a specific user. This will help combat alert fatigue. You can also quickly prioritize high-risk incidents with risk scoring, which is included in some behavior analytics security solutions.
- → **A security posture assessment** of human and non-human identities to determine incorrectly provisioned or over-provisioned accounts, especially ones with high-risk privileges.

Curious about cloud-native security?
Learn more about Forcepoint Cloud Security Gateway (CSG), our converged service for securing your users and data in the cloud and on the web.



CSG delivers web, cloud, and data security in a single service. It provides Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Data Loss Prevention capabilities, all in one SKU. Remote Browser Isolation (RBI) is also available as an add-on.

Flexible protection for you in the cloud

By following the seven steps outlined in this eBook, you'll be several steps ahead of your peers in protecting your users and data in the cloud. As you develop your strategy and define new policies, be sure to explore new technologies that will help you put these plans in action. (You won't be able to rely on static security tools to protect the cloud's dynamic environment.)

At Forcepoint, we believe the best way to secure the cloud is with the cloud. To achieve flexible, scalable protection for your enterprise, we recommend **Forcepoint Cloud Security Gateway** (CSG). CSG delivers web, cloud, and data security in a cloud-based, centrally managed service. You'll be several steps ahead of your peers in protecting data in the cloud … and safeguarding your people around the world. In addition, CSG:

- → Secures your remote staff's access to on-premises data and business-critical cloud applications.
- → Stops malware, viruses, and phishing, wherever your staff is working.
- → Uncovers risky cloud apps and Shadow IT while securing cloud access across your organization.
- → Delivers complete web and data protection with uniform policies for every user everywhere.
- → Provides controls for BYOD, managed devices, and real-time compliance.

See how we can help you with your security approach today.

View Video

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.