

E-BOOK

# Secure the cloud.

---

A hacker's perspective on the dangers of ignoring cloud security and how to protect yourself.

RedSentry



**E-BOOK**

# Table of Contents

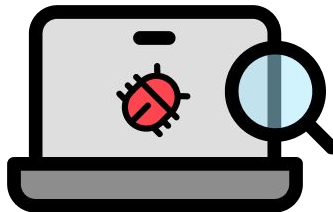
- 3** Let's talk Cloud Security
- 6** Doesn't my cloud provider provide security?
- 8** Cloud security should be as dynamic as your environment
- 9** Four biggest threats facing your cloud security
- 10** Threat #1 User-caused misconfigurations
- 13** Threat #2 Insecure APIs & Web Applications
- 14** Threat #3 Hijacking of accounts
- 15** Threat #4 Accidental Data Sharing
- 16** Cloud Security Options
- 18** Penetration Testing
- 21** Vulnerability Scanning
- 23** Red Sentry's Automated Cloud Platform
- 25** Schedule your free scan today!

# Let's talk Cloud Security



In an effort to prevent cyber attacks, most companies perform **vulnerability scans** and **penetration tests** on their internal and external assets at least annually.

This is critical. However, it's only the first step in **keeping a company secure.**

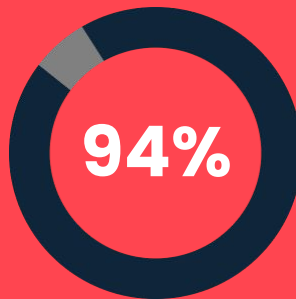




By 2025, the global  
cloud computing  
market is projected  
to be valued at an  
astonishing

**\$832 billion**

storing over  
zettabytes of data



**It's not exactly news that cloud  
computing is exploding.**

It's estimated that 94% of enterprises  
already use a cloud service, and this is  
growing exponentially.



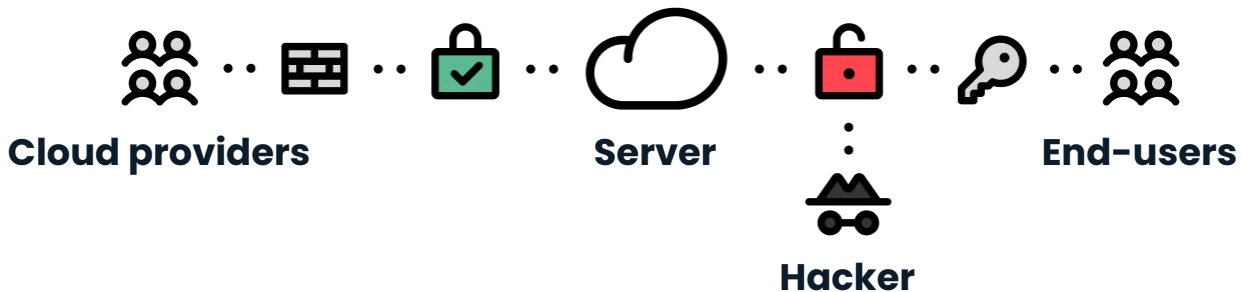
**The danger of quick technology advancement is security being left behind.**

**Just as companies move toward the cloud, security efforts must move in the same direction.**

Most IT professionals assume that their cloud provider, whether it's AWS (Amazon Web Services), Microsoft Azure, or Google Cloud, handles cybersecurity on their behalf. And they do, to a certain extent. They keep their systems updated and patch vulnerabilities daily. The technical end is handled quite well. But...

**What cloud providers can't control, are the end-users.**

**It turns out that you -yes, you- are the problem.**



**“Whether you use AWS, GCP, Azure or hosting services, you need cloud security tools to keep your company protected.”**



## **The vast majority of cloud vulnerabilities are user-caused.**



For example, cloud providers allow admins to get very fine-grained with their permissions, which is appreciated. However, admins sometimes don't understand the nuances with these permissions.



They may assume that checking a box to make a file “public” means only folks within the organization can access it, but it actually mean anyone across the globe can get it.



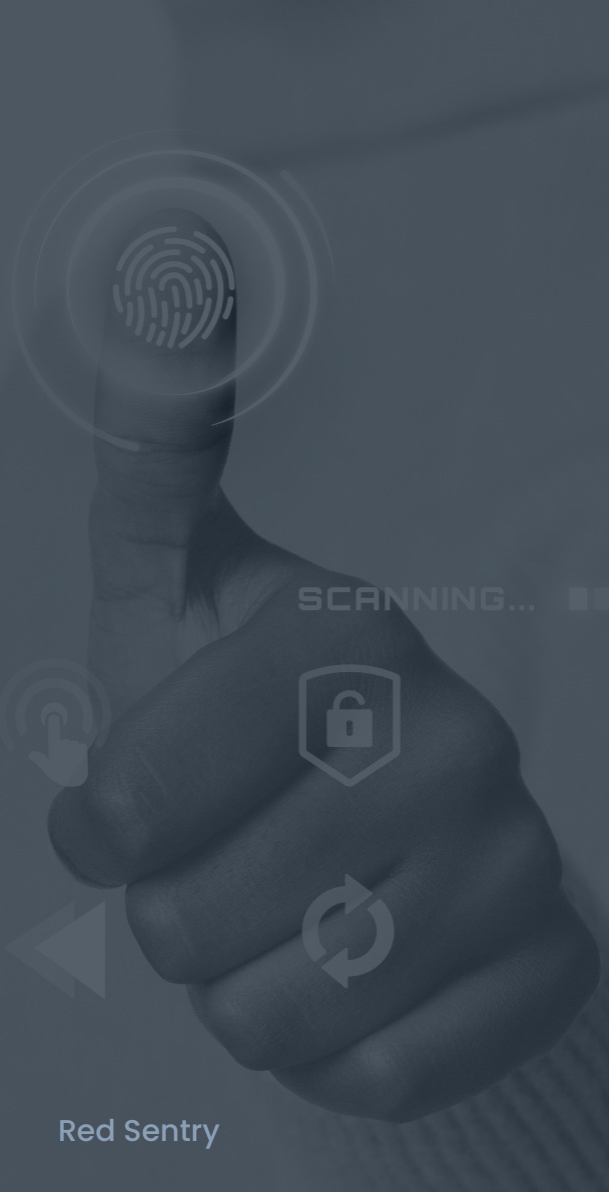
The trend of **moving to the cloud** makes perfect sense for most companies both technically and financially.

You can spin up a cloud server in mere minutes, and only pay for what you use. It's fast, convenient, and endlessly scalable. Cloud environments are dynamic, ever-changing, and unique to every company.

And while these aspects add value for your organization, they also make traditional cybersecurity efforts a thing of the past.

*"Working in the cloud requires a unique and comprehensive cybersecurity approach, with strategy and tools as fluid as your environment. The only way to keep your company and data secure is through a continuous, real-time approach to cybersecurity."*





# Biggest threats facing your cloud security

- 1** User-caused misconfigurations
- 2** Insecure APIs & Web Applications
- 3** Hijacking of accounts
- 4** Accidental data sharing

## 1- User-Caused Misconfigurations

You've likely heard of **common vulnerabilities and exposures (CVEs)**, which are caused by software and can be easily fixed by applying a patch or update. **Misconfigurations**, however, are caused by humans and don't have a CVE or Patch associated with them.



**This type of vulnerability is just as dangerous as any CVE, and can be used by attackers to hack your company.**

Sometimes these changes to your cloud may be accidental. As cloud environments become more advanced, they have more and more options for users to edit, and many employees don't know the repercussions of changing specific settings.



**“The phrase ‘pay for convenience’ becomes all too relevant, because changing settings for convenience may leave you paying ransomware in the long run.”**

**These misconfigurations may also be caused by a desire for convenience.**

For example, someone turning off multi-factor authentication may make life easier than verifying your identity every time you log in, but it also leaves your entire company at risk. Setting folders to public instead of granting individual access may expose files to the world.





## Other examples of user-caused misconfigurations

- 1 Modifying an S3 bucket policy to public
- 2 Giving every cloud user admin access for convenience
- 3 Spinning up a public MongoDB instance without authentication

## 2- Insecure APIs & Web Applications

**Applications running with vulnerabilities can be the gateway into a cloud environment.**



If a hacker compromised a web application 10 years ago, they would have probably landed on a server inside the target's network. Now, it's more common for hackers to land in the target's cloud environment.



Example: if a malicious hacker gets remote code execution on an application running on an AWS EC2 (virtual machine), they can use that as a pivot point to compromise the rest of the cloud.

### 3- Hijacking of Accounts

**To interact with the cloud, it's common for applications and developers to use **API tokens**.**

**Sometimes these tokens are embedded within applications, or if using AWS, it's common to retrieve them by sending an HTTP request to the metadata url. Once the token is exposed, **it can be utilized to hijack the account**.**



#### **Example:**

If a hacker finds a server-side request forgery (SSRF) vulnerability in a web application, it can be leveraged to retrieve AWS tokens via the metadata url. The account can then be hijacked.

## 4- Accidental Data Sharing



**In 2017, an economist found that **data is now worth more than oil**, which is why it's the first thing hackers go after.**



Credit card numbers, social security numbers, passwords, medical records, and more have all been breached at some point due to them being publicly accessible.

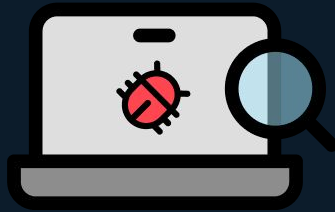


Hackers routinely probe for open S3 buckets, databases such as ElasticSearch and MongoDB, and more. Sensitive data can be stored almost anywhere. It's important to make sure it's not accidentally exposed to the internet, where it is publicly available to the world.

Now that you've seen the common vulnerabilities of cloud security,

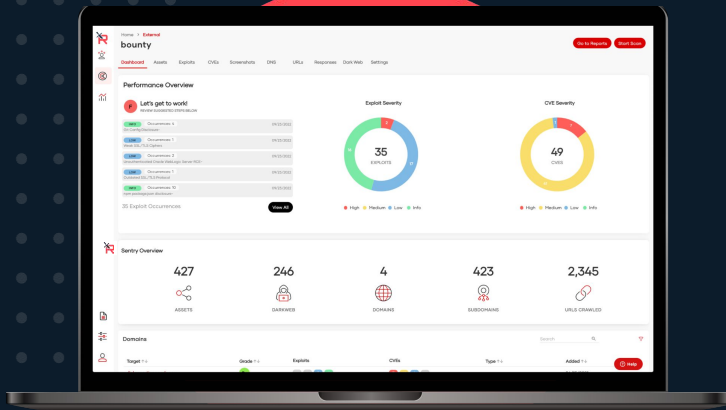
## How can you work to avoid them and keep your company and data protected?

**"At Red Sentry, we recommend a combination of ongoing vulnerability scanning and penetration testing, which both have unique benefits for your company."**





**Vulnerability scanners** look for known vulnerabilities and misconfigurations in your cloud environment and report potential exposures.

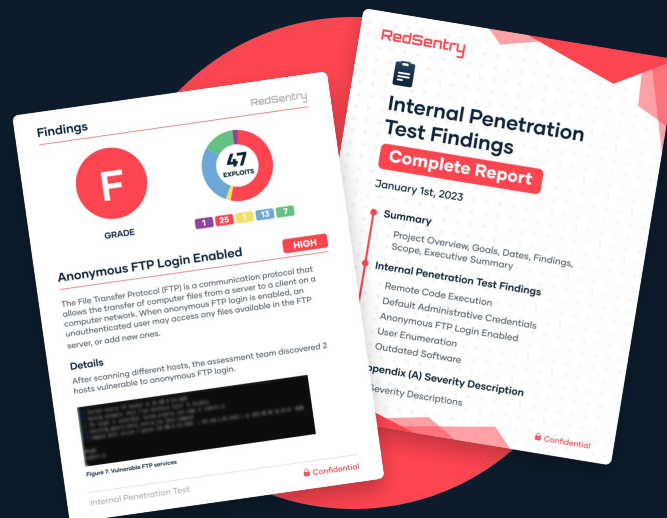


Because vulnerability scanners are automated, they are able to test a larger scope of assets. Thousands of assets can be tested, instead of just a handful.

Some scanners, like Red Sentry's, are also continuous and notify you the second a new vulnerability is found within your environment.

**Penetration tests** go a step further and exploit the vulnerabilities found to determine the degree to which an attacker can gain access to your assets.

Because penetration testers are humans and not software, they're able to **think more like malicious hackers** and dive deeper into vulnerabilities, to give you a more realistic idea of your weaknesses.





**Most companies undergo an annual penetration test on their publicly facing external assets (only).**

**What many people don't know is that penetration testing can (and should) be done on cloud environments as well.**

**It's a newer technique, so IT professionals are often not aware that it's even an option. This is not something the cloud providers do as part of their service – it's up to each cloud customer to get a penetration test of their environment.**

**Cloud penetration testing** largely works by policy-matching; that is, by checking the company's cloud permissions to make sure they're set how they should be.

---

A good cloud penetration tester will check for open S3 buckets, ensure that multi-factor authentication is turned on, attempt privilege escalation, and much more.

While performing penetration test on your cloud environments (as well as your web applications, internal environment, and external assets) will certainly go a long way toward keeping data out of nefarious hands.

*"IT experts should be intentional about what kind of cloud penetration testing expertise they engage."*



**There can be widely  
varying skill levels among  
these penetration testers.**

---

Big companies may introduce their experienced, A-list ethical hackers, but it may be someone far more junior that's handling the projects. When hiring a firm to perform a cloud penetration test, be sure to ask to see the bios of the team members that will actually be doing the work.

**If your annual penetration test doesn't find any vulnerabilities, **don't assume you're in great shape until next year.****

---

Of course, new misconfigurations pop up daily. And there's also a chance the company or the penetration tester assigned to your project **may have missed something.**

Automated vulnerability scans can run continuously, so you're notified as soon as a misconfiguration occurs. These tools are consistent among customers, so you don't have to worry about the skill of the person assigned to you.

Of course, any technology is only as effective as the team that developed it, so you should do your due diligence here too.

 **Watch a demo**

 **Try a free trial**

 **Read reviews**

 **And ask for references**

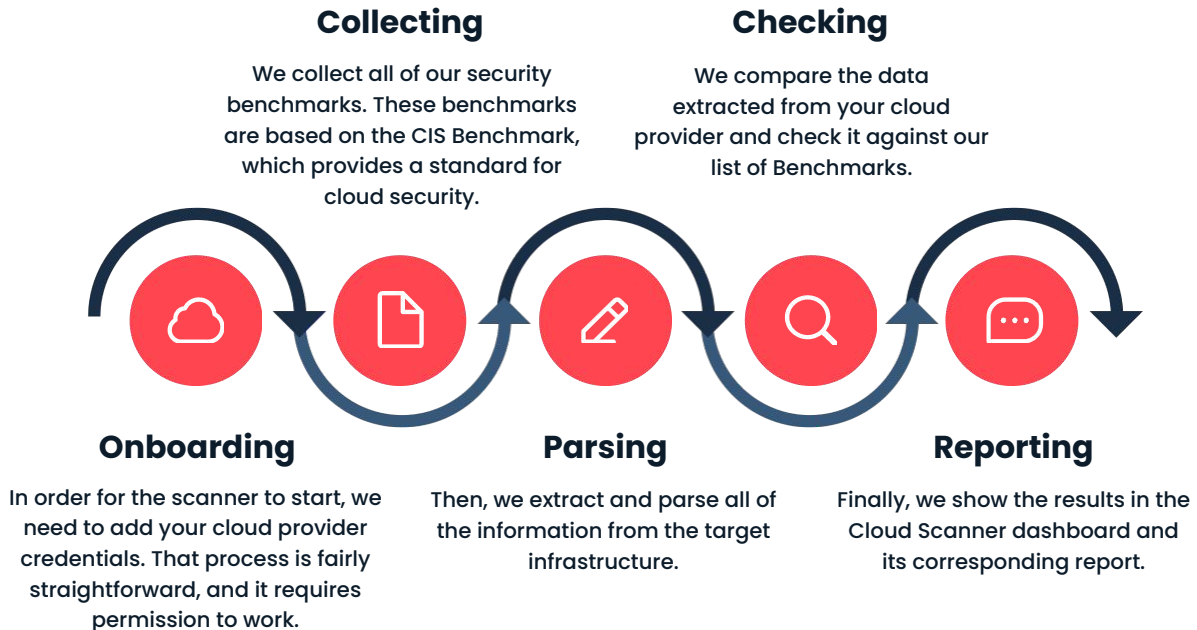


**Whether you choose a traditional penetration test or an automated vulnerability scanner (or ideally, both), adding this tool to your cybersecurity arsenal will **help ensure that user error don't jeopardize the security of your cloud assets.****

# Red Sentry's Automated Cloud Platform



Cloud scanner  
Methodology





**Have questions or  
want to learn more?**

**Get a free scan**

RedSentry

