Top Five Risks
When Operating in the Cloud
– And What You Can Do About It

Lookout®

The cloud brings significant benefits but also a new set of risks

Most organizations today operate in the cloud. By taking advantage of the scalability and ease of operation of cloud services, you can enhance productivity and collaboration while reducing operational costs. And when you're using someone else's infrastructure, you don't have to worry about upkeep, which means you can more easily expand capacity and recover from a disaster incident.

While the cloud simplifies operations in many ways, it comes with its own set of risks that can impact your bottom line. In 2021, the average cost of a public cloud breach was $4.8 million, and the cost of a hybrid cloud breach was $3.61 million.[1] As your organization continues to operate in the cloud, you need to be aware of these risks and take appropriate steps to mitigate against them.

$4.8 million, the average cost of a public cloud breach in 2021

1. Reed, Jonathan, Security Intelligence, "The Cost of a Data Breach Goes Beyond the Bottom Line," November 2021

Lookout®

Table of contents

Top five risks when operating in the cloud

This list is not meant to be an exhaustive rundown of all the risks related to the cloud, but it covers the major areas you need to understand. Remember, just as no cloud sits on an island, these risks are not mutually exclusive and can overlap with or affect each other.

Risk 1: Hybrid and diverse clouds

Cloud configurations are tremendously flexible and can be tailored to your exact requirements. You can operate completely in a public cloud, like Amazon Web Services, Microsoft Azure or Google Cloud or build a multi-cloud configuration that includes two or more of these providers. You may want to also maintain some operations on premises with a hybrid cloud configuration.

With customization comes complexity. And if you are not equipped to manage it, this can lead to misconfigurations. Along with stolen or compromised credentials, cloud misconfigurations were the leading causes of breaches in 2020, resulting in an average breach cost of $4.41 million.[2]

Unlike classic hacking scenarios, where the target is chosen before the attack vector, cloud breaches occur because the attacker found the quickest way to the largest payout. This is often done by setting up automation to quickly discover vulnerabilities.

Often, the path of least resistance is a misconfigured cloud resource, which has become commonplace due to the disjointed nature of cloud service deployment. With multiple cloud systems, you have to manage a patchwork of operations and security controls that likely have different rights, capabilities and requirements. In an attempt to secure this disjointed infrastructure, organizations will often deploy specialized tools as new use cases arise. But with multiple agents, consoles and processes, these disparate products often add more burden to already stretched teams and leave operational and visibility gaps that can be exploited.

Cloud misconfigurations were a leading cause of breaches in 2020

2. IBM Security, "Cost of a Data Breach 2020," July 2020

Risk 2: Shortcomings of access management solutions

Because the cloud gives you options to configure to your exact needs, it also multiplies the number of human and service identities that need to be managed. Human identities are your end users, and service identities are permissions and entitlements that control what the service can access or perform. Every resource in your cloud, such as virtual machines, containers and data stores, has a service identity.

A good access management solution can help reduce this complexity with single sign-on (SSO) that provides users access to system apps with step-up authentication. The problem is that this is quite binary, where users get access if they provide the right authentication. The tool doesn't protect the data in those apps and doesn't monitor or control actions a user can take once they enter your environment.

The COVID-19 pandemic resulted in a dramatic increase in the number of remote workers, a trend that will continue into 2023.[3] This means that you will continue to encounter endpoints and networks, such as smartphones and home Wi-Fi, that are not under the direct control of your IT. You will also need to balance security control and productivity, as your remote workers are likely not accustomed to the strong security procedures and habits necessary to keep your networks secure.

Implementing virtual private networks, or VPNs, for on-premises access can introduce basic authentication protection. But because VPNs provide network-wide access, if a user's login credential is compromised or they decide to go rogue, their account can easily be used to move laterally and compromise data. VPNs also have no visibility into data activities and aren't architectured to scale.

Your enterprise cloud could be managing thousands of identities and have thousands of policies and configuration settings. Access management alone will not be able to authenticate users or make sure that data protection policies are enforced correctly across all these apps.[4]

The pandemic has resulted in a dramatic increase in remote work, which will continue into 2023

3. "Remote Work is Here to Stay and Will Increase into 2023, Experts Say"
4. Faatz, Donald, Carnegie Mellon University, "Best Practices for Cloud Security," March 2018

Risk 3: Lack of cloud-relevant skills and expertise

Fueled by remote working needs, cloud usage is steadily increasing. But this is stretching the capacity of IT and security teams, which are already faced with a shortage of skilled workers. Organizations cite a lack of skilled personnel as one of the biggest barriers to securing their workers, devices, and corporate apps and data. Across the security industry, there is an estimated shortage of 3.1 million professionals as of November 2021.[5]

In a 2020 survey, only 27% of organizations said they were confident in their ability to address cloud security alerts, while 92% said they needed to enhance their cloud security skills. When it comes to the lack of skills, 84% said they needed to add staff to close the gap.[6]

The risk that comes from understaffed or inexperienced personnel is exacerbated by organizations' tendency to deploy multiple point solutions that require extensive day-to-day management. This mundane task results in overworked teams that don't have the opportunity to focus on career development and strategic initiatives, which results in high job dissatisfaction and turnover.

Using a cloud-delivered model will alleviate pressure by removing the unnecessary and tedious labor that point products require. This equips your IT and security teams with the visibility and control they need, as well as the time to focus on the projects that matter to their personal development and the protection of your organization.

Only 27% of organizations were confifident in their ability to address cloud security alerts

5. Hwang, Vince, Cloud Computing, "Breaking Through the Cloud Security Skills Gap," November 2021
6. Ovcharenko, Dmytro, N-iX, "7 risks in cloud migration and how to avoid them," April 2020

Risk 4: Reliance on traditional appliance-based tools

Whether you have a simple cloud implementation or a multi-cloud environment, not having a clear strategy from the beginning can result in wasted resources, inefficient operation and poor user experience due to multiple logins and processes.

Security gaps can often manifest themselves in appliance-based security tools. These products, such as VPN, on-premises secure web gateway (SWG) and data loss prevention (DLP) were traditionally deployed in stand-alone configurations. As a result, their policies are defined separately, have different management paradigms and do not integrate well with each other. Appliance-based solutions have their uses, especially when most entities reside inside perimeters, but in the cloud, they can be difficult to scale and don't provide the visibility and control you need.

By contrast, a cloud-delivered security platform approach enables you to consolidate multiple point solutions and simplify your IT security. In turn, you're equipped to enforce adaptive data protection policies that don't hinder productivity.

VPNs don't provide protection against credential stuffing or password spraying

Risk 5: Rapidly evolving modern-day threats

Cloud-based cyber threats are exposing critical shortcomings in many existing security solutions and methodologies. Today, attackers don't simply access a system. They probe around and move laterally throughout your environment, searching for sensitive data or other high-value assets.

Appliance-based tools are expensive, difficult to scale and have limited visibility into cloud-based threats. VPNs, for example, don't provide adequate protection against credential stuffing or password spraying. Identity and access management (IAM) have rigid configurations and policies that can't continuously assess a user's risk level when providing access.

Distributed denial-of-service (DDoS) attacks have become easier with the availability of new DDoS-for-hire services. And do-it-yourself (DIY) and home-grown policies are minimally effective and require a lot of additional security personnel.

There is also a new generation of malware, such as ransomware, that is easily distributed via phishing messages. These malwares have signatures that change frequently and are not always detected by appliance-based web proxies whose threat intelligence engines are often outdated.

Cloud-based solutions, on the other hand, are constantly updating, and don't require additional investment in security personnel. They are also scalable and more effective in protecting against a DDoS attack.

Cloud-based cyber threats are exposing critical shortcomings in many existing security solutions and technologies

What you can do to mitigate cloud risk

There are a near-infinite number of steps you can take to mitigate the risk of a data breach. To get you started, here are a few of the most critical ones:

Do your due diligence

One of the most important things you can do to ensure that your cloud performs to your requirements and is adequately secure is research. Don't rush to the cloud because it's the trend or the statistics look good on an analyst report. Some of the items you need to understand include operational costs, onboarding procedures, security, disaster recovery, terms of service, location of data centers, and off-boarding terms and procedures. You also should make sure that the cloud service is deployed and configured correctly.

Consolidate IT and security operations

The complexity of cloud operations requires that organizations change their security methodology from appliance-based to platform-based. A single cloud-delivered security platform that is seamlessly integrated can centralize your policy enforcement and provide a single place to manage and monitor systems. This ensures that you can efficiently protect data while providing users with what they need to stay productive.

Go beyond access management

You need to go beyond binary access management by ensuring that zero trust is enforced in a precise and dynamic manner. Take the time to configure precise access management programs and policies that protect your data while also enabling users to get access to what they need. Pay particular attention to edge devices, but don't stop there. Access management tools alone can't guard against insider threats or compromised credentials. You need a platform that can understand the context surrounding that user and detect malicious or risky behavior.

Continously monitor

Although working in the cloud is a shared responsibility model, you are ultimately responsible for the security of your environment and data. Continuous monitoring of your system behavior, both in the cloud and on premises as well as across all of your endpoints, will help mitigate risky incidents and outright malicious threats. This must include real-time monitoring of user and device risk and the dynamic enforcement of zero trust.

Protect your data

When it comes to mitigating cloud risks, you have to go beyond app-level policies. Regardless of whether you have apps on premises, in private clouds or public clouds, what matters is the protection of your sensitive data, such as sensitive intellectual property or regulated information. You must go beyond simple access management with policies that dynamically change based on the sensitivity level of the data. This means that users are given access that is appropriate to the risk levels of their behavior and endpoint.

Secure your cloud operations with a unified platform

Working in the cloud helps organizations be more productive and reduce costs. But it will add complexity and new security risks. The **Lookout Security Platform** provides protection against these and other risks in a single, easy-to-configure, integrated solution. By understanding the risks and taking steps to mitigate them, you can reap the benefits of the cloud while mitigating the potential for problems.

If you'd like to get a free evaluation of your risk, we can help.

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit www.lookout.com and follow Lookout on its blog, LinkedIn, and Twitter.

Lookout®