PROFICIO™

CLOUDSECURITYCHECKLIST

79% of companies surveyed reported at least one cloud breach in the last 18 months*

How secure is your cloud?

As more and more organizations begin to host a portion of their infrastructure in the cloud, it is no wonder that the cloud has become a big target for attackers. Virtual servers can be infected with malware or ransomware, credentials can be stolen, and cyber criminals can exfiltrate data. Web applications are one of the most significant sources of enterprise data breaches, and public-facing web applications are often hosted on cloud platforms. Because cloud platforms are designed for easy sharing, data runs the risk of becoming unintentionally shared or exposed.

Here are 10 checks to assist you in securing your cloud environment.

*IDC Cloud Security CISO Survey

PROFICIO™

Percentage of breaches targeting external cloud assets: 90%[1]

1 Selecting the Right Cloud Provider

Before you migrate into the cloud, you need to decide which cloud provider you want to utilize. It is critical that you define your organizations requirements and expectations. There are a lot of options to choose from so take the time understand what each provider offers; this includes the basic security measures they provide, what services they offer, where they will host your data and the costs for each application. For most organizations, it's best to select an established cloud provider, like Amazon Web Services (AWS), for their broad offering and established security and support protocols.

Have you researched cloud providers to see who best aligns with your cloud strategy?

2 Proper Setup is Key

Some of the largest breaches in recent years have been a result of misconfiguration of cloud infrastructure resources, where an unauthorized user was able to elevate their privileges and compromise sensitive documents. Often, a simple mistake such as not controlling permissions to cloud accounts, restricting access to web applications, or implementing micro-segmentation, is at the root of the cause. When configuring your cloud environment, providers like AWS have best practice guides available to follow so you're setup for success from the start. After setup is complete, perform periodic auditing of your configurations and users to help optimize rules and policies that will improve security over time.

Are you able to create properly segmented applications in the cloud to mitigate the risk of misconfigurations?

3 Know Your Responsibility

Alongside proper configuration, it is important to understand what areas of the cloud you're in charge of securing. Known as the Shared Responsibility Model, cloud security vendors like AWS lay out what areas they are responsible for securing – and what you, the cloud user, are liable for. In general, the cloud platform provider is accountable for the security of the cloud (regions, storage, database, etc.) and you, as the cloud client, are responsible for security in the cloud (customer data, access management, network and firewall configurations, etc.). Often, security lapses fall on the shoulders of the customer so it's crucial to know your role.

Do you know what areas of your cloud you're responsible for securing?

PROFICIO™

Percentage of organizations that report difficulty securing the cloud: 45%[2]

4 Implement Controls for User Access

Once your cloud environment is set up, you need to start allowing your users access. It is important not to over grant access – if you are lax in this area, keeping privileges in place for too long, neglecting to expire passwords, or failing to remove access when an employee or contractor leaves, you may leave the door open for risk. Using the Principle of Least Privilege is always a good strategy, so you're only providing the minimum level of access that users need to accomplish their jobs.

Have you determined how to best control user permissions, to reduce the risks of unauthorized access to sensitive data stored in the cloud?

5 Keep On Top of Vulnerabilities

Staying on top of your current vulnerabilities is a vital part of keeping your cloud infrastructure secure. Since many cloud-based applications are integrated into the broader cloud ecosystem, it only takes is one security flaw to put your sensitive data at risk. Regular scanning of your environment will not only help you identify risks that lie within your network, but it can also help you keep track of what assets your team has in use, so you can shut down any unused access to prevent unauthorized access. Finding any out-of-date systems or known security vulnerabilities located inside your network can help you identify gaps in your infrastructure that could lead to security breach.

Do you have a process in place to help catch and patch any potential vulnerabilities?

6 Collect and Monitor Logs

Critical security events can occur at any time, but with timely detection and swift response, you can often catch attacks early and minimize damage. Make use of support tools provided by your cloud provider, such as CloudTrail and CloudWatch in the case of AWS, have logs sent to a Security Information and Event Management (SIEM) tool, such as Splunk, and enable 24/7 monitoring and threat detection of events from cloud-based appliances like virtual firewalls and WAFs. It is also important to setup proper logging and apply use cases that can detect suspicious activity.

Are you set up with proper logging and around-the-clock monitoring?

PROFICIO™

Highest ranked cloud threat: Misconfiguration[3]

7 Keep Compliance Top of Mind

Many organizations move to the cloud because it allows them the flexibility to collect and archive log data in their preferred location, for a range of retention periods. However, for organizations that must adhere to compliance regulations like PCI, HIPAA and GDPR, there are often other logistics challenges that come into play to meet specific compliance mandates. Since it can be difficult to modify the compliance policies once implemented, make sure you understand what controls and restrictions are required so you can find a cloud provider to fit these needs.

Have you reviewed your compliance requirements to ensure your cloud provider can meet them?

8 Secure your Endpoints

With more and more endpoints accessing the cloud, organizations need to have endpoint security tools in place to bolster defenses against the main endpoint threats they face. These tools can include email security solutions, firewalls, antivirus solutions, and a Cloud Access Security Broker (CASB). By combining standalone endpoint solutions or using a comprehensive endpoint security tool, such as an Endpoint Detection and Response (EDR), you'll have good visibility of your endpoints. Make sure to enable monitoring, with a SIEM solution like Splunk, and ensure your endpoint security tools are managed properly, internally or partnering with a Managed EDR provider, for the best coverage of your endpoints and network.

Do you have solutions in place to help you monitor your endpoints for threats?

9 Rapid Response and Containment

Some of the biggest data breaches occurred because nefarious activity was occurring in the background for a significant period without detection. Having the ability to automatically respond to specific alerts that trigger on your existing cloud-based tools, like a WAF, allows for faster response to high-fidelity threats so you can quickly contain attacks before they cause damage. This provides additional time for the internal teams to research the threat while protecting your environment in the interim.

Can you quickly contain credible threats using an automated process?

PROFICIO

Misconfiguration breaches by industry: 41% Tech | 20% Healthcare 10% Gov | 6% Hospitality & Finance[4]

10

Find a Trusted Partner

While many organizations want to manage their security in-house, some things are best done internally, and others best left to partners. Whether it's moving to the cloud, monitoring your cloud assets, or meeting compliance requirements, most cloud vendors have a place to find trusted resources, like AWS Marketplace. They also offer certifications or competencies to better help you select a qualified provider to partner with.

Have you selected a cloud security partner to help you on your security journey?

It's not a matter of if you will be attacked... but when.

Proficio's Managed Detection and Response (MDR) services were created to take the cloud security weight off your shoulders. Our security experts are highly responsive and understand your environment, policies, and processes, to provide more accurate threat detection. Acting as an extension of your team, we help you reduce your risk so you have peace of mind in your cloud security journey.

To Learn More Contact Proficio at info@proficio.com | Proficio.com

1/3 Verizon 2021 Data Breach Investigations Report (DBIR) - 2 SailPoint State of IaaS Cloud Infrastructure Security and Governance Report - 4 ExpertInsights.com

SOC 2 Type 2 Certification

Proficio undergoes an annual audit and is in full compliance with the American Institute of Certified Public Accountants (AICPA) controls for Service Organizations. SOC 2 requires companies to establish and follow strict information security policies and procedures, encompassing the security, availability, and confidentiality of customer data. Our audit report is available upon request.