[deft]

Cloud Security

Best Practices Checklist

v21.9

Founded in Chicago, Deft offers data center, network, cloud, consulting, and business continuity solutions to such clients as Cars.com, Basecamp, FreshBooks, Metra, New Relic, SAP, and PicsArt. We're a dedicated team of engineers and innovators who love nothing more than solving business problems with technology. Deft is an Advanced AWS MSP Partner and proud to be an 8-time Inc. 5000 Honoree.

As trusted technology advisors and implementers, we can offer a rich set of best practice recommendations across cloud security management:

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Understand your cloud provider's shared responsibility model.

The key to a successful cloud security implementation is understanding which security responsibilities are yours and which responsibilities are your cloud provider's. While you can't control how your provider secures their portion, you do have the right to access your cloud vendor's audit reports to verify that they adhere to your service level requirements.

Get creative about teaching cloud security to your organization.

An employee population of 1,000 means a minimum of 1,000 unique points of vulnerability for the cloud and cloud-based applications. It only takes one person to unknowingly log into a fake website to compromise the system. That's why any corporate cloud security strategy must include a plan for educating stakeholders about what they need to do to maintain a high level of vigilance when operating in the cloud — and what might happen if they don't.

As you develop your educational plan, consider including the following:

- **Explicit security and privacy guidelines**, such as those outlined by the National Institute of Standards and Technology (NIST). It may be wise to have staff sign an agreement stating that they've read and agree to those guidelines.`
- **Plain-English explanations about why the guidelines are important.** Most of your cloud end-users won't be IT professionals, so it's crucial to translate potential security risks into terms lay users can understand.
- **Notifications about security issues as they arise.** This doesn't have to mean that every employee gets constant security system notifications, but regular communications about threats targeting users are helpful for keeping security top of mind.
- **Interactive components aimed at building awareness and creating a culture of security.** Education is important, but it's only the beginning of maintaining a secure environment. The kind of training that can change behavior over the long term requires participant engagement and needs to be recurring — a "one and done" approach won't suffice.

These efforts will likely be most successful if you work with other parts of the organization to get the word out. For example, could you put together a mini quiz everyone must pass by some deadline?

Creativity in communication is crucial to drive engagement and, ultimately, adoption of security best practices.

Empower your internal team to ask security questions.

Few IT leaders have led a cloud migration in the past — so if you have questions about how cloud security works, you're certainly not alone. Consider this an opportunity to get security training for yourself and your team from the cloud provider you're working with. Ask for detailed recommendations about necessary infrastructure changes to prepare for the cloud, as well as future maintenance guidelines. Empower members of your team, who will be responsible for various components, to ask questions during the migration so they understand how to protect the new environment.

Maintain control over which cloud apps your departments can use.

Gartner predicted that a third of all successful security attacks in 2020 would be on shadow IT resources. During the contract negotiation process, make sure that there's a method to control which cloud applications your departments can use. This is important both to control costs and to minimize security threats.

One option available to IT administrators for the highest level of cloud security: ask department heads to consider recommending a cloud service approved by the government's Federal Risk and Authorization Management Program (FedRAMP). FedRAMP reviews cloud services for adherence to security best practices and puts vendors on an approved list. By directing users to FedRAMP-authorized apps, IT admins provide some freedom while improving the odds that their cloud remains secure.

Pay attention to third-party audits but understand their limits.

Third-party audits can be useful to verify that your cloud provider is adhering to the security standards established in your contract. For example, it's a good idea to ensure that your cloud provider complies with the standards of the SOC 2 audit. SOC 2 audits validate that a third-party is adhering to core security principles including defined and documented security processes, availability, processing integrity, confidentiality, and privacy of a cloud network. These are not one-size-fits-all efforts, though, so be sure that your cloud provider is being measured on metrics that matter for your organization.

Another thing to be aware of is that your cloud provider passing a particular audit for a particular certification does NOT automatically mean that you are also certified. For things like payment card industry (PCI) data standards, you need to undergo your own PCI audit to say you are PCI-certified. Using the facilities of a PCI-certified cloud provider is usually not enough to also certify your own infrastructure.

Figure out what threats to look out for and how you'll address them.

New security threats emerge daily. The first step in developing a threat assessment strategy is defining the scope of what your strategy needs to encompass — just the functionalities you've migrated to the cloud? The entire corporate IT infrastructure?

Once you've defined your scope, you'll want to consider the types of threats your system faces:

- Intentional external threats (e.g., malware, DoS attacks, phishing attacks, etc.)
- Accidental threats (e.g., those that result from a computer malfunction or an employee's failure to follow security protocol)
- Threats from natural disasters (e.g., floods, fires, or anything else that could restrict access to your network or bring it down)
- Intentional internal threats (e.g., rogue employees abusing their privileges)

Once you have a strategy for assessing threats to your network, you'll want a plan for minimizing the likelihood of each threat causing harm.

Provide strong encryption protocols and key management for data.

Data must be secured (typically by encryption) in all three of its states:

- **At rest:** Data at rest is the data being stored but not actively being used by network participants. It needs to be protected to ensure that it's not improperly accessed or altered, usually by encrypting it.
- **In use:** Data in use is data that's actively being used by an application or stored in memory or a CPU. If data in use is compromised, it could provide access to other types of data. Make sure your public cloud vendors secure your data in use.
- **In transit:** Data in transit is the data that's traveling through a network at any given moment. It can be protected with encrypted network connections.

Understand that not all data and applications need critical security protection in the cloud.

Security measures affect the speed and performance of a system, so it's best to use them only as needed. Not all data needs top security protection, and not all applications use sensitive data.

It's important to make sure that everything deemed "critical" really is. Classifying your data and applications will give you a sense of where Personally Identifiable Identification (PII) and other sensitive data lives so that you can deploy security tools strategically.

If you are not sure which data or applications fall into the critical tier for security processes, ask your cloud provider. They will have broad experience to share with you and can help you determine the best possible configuration based upon your specific security classifications.

Implement and regularly monitor identity and access controls.

Once you've classified the security levels of all your cloud assets, you'll have to implement tools to limit and control access. These are the areas you'll want to focus on:

- **Authentication:** Connecting your corporate Active Directory to the cloud can simplify verifying (authenticating) the identity of network users. Parameters for authentication might include password creation, password resets, session timeouts, and more. These settings can also be synchronized with your corporate Active Directory. This handy cheat sheet from The OWASP Foundation offers more detail.
- **Authorization:** Authorization protocols may also be required to access PII, such as customer records.
- **Access Control:** Implement role-based access so that network users are grouped to only have the access they need to do their jobs.

Develop a solid backup and recovery plan.

Not all cloud applications or providers offer backup by default, and the ones that do may not give you the backup history you need for compliance. This shouldn't come as a surprise, but your disaster recovery plan has to work. That's why both backup and recovery should be part of the service offering your cloud provider offers. Get a clear idea of the process for restoring backed-up data and how long it takes. Make sure your critical data is backed up in systems that allow rapid restoration (if you need it back online quickly).

A secure cloud relies on everyone.

Growing organizations face many unique security challenges in adopting cloud infrastructure, not least of which is employee turnover and new users entering the system. Educational and awareness-building efforts about the importance of privacy and security in the cloud must be ongoing.

Ensuring a secure cloud means not just verifying that the setup is technically secure, but also that all users are active participants in bolstering security. Achieving this state requires cross-departmental communication and some creativity, but the security gains are well worth the effort.

If you're curious about how we've helped companies migrate securely to cloud solutions in the past, read about our work with Florence Corporation and DePaul University. If you'd like to learn what a secure cloud migration might look like for your business, please get in touch — we'd love to help.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Additional Questions

For more information, visit https://www.deft.com/ or contact us at (312) 829-1111 and sales@deft.com

About Deft

Deft offers managed cloud services, cloud consulting, cloud-native software development, business continuity solutions and managed data center services. We work with companies, large and small, that see IT as their critical success factor.

Deft is a SOC 2 audited company. We are proud to be an 8-time Inc. 5000 Honoree.

Learn more at www.deft.com or call us at (312) 829-1111.