Carnegie Mellon University
Software Engineering Institute

Cloud Security Best Practices Derived from Mission Thread Analysis

Timothy Morrow
Vincent LaPiana
Don Faatz
Angel Hueca
Nathaniel Richmond

July 2019 (Updated September 2021)

TECHNICAL REPORT
CMU/SEI-2019-TR-003
DOI: 10.1184/R1/12363563.V1

CERT Division

[Distribution Statement A] Approved for public release and unlimited distribution.

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM21-0611

Change Log

September 2021

- Added two risk examples to Section 2
- Added information about compliance with industry and government standards or regulations to Section 4
- Updated cloud service provider (CSP) tools and capabilities, where appropriate, in Section 4
- Added a discussion of positives and negatives of multi-CSP strategies to Section 4

Table of Contents

List of Figures

Abstract

This report presents four important security practices that are practical and effective for improving the cybersecurity posture of cloud-deployed information technology (IT) systems. These practices help to address the risks, threats, and vulnerabilities that organizations face in deploying or moving applications and systems to a cloud service provider (CSP).

The practices address cloud security issues that consumers are experiencing, illustrated by several recent cloud security incidents. The report demonstrates the practices through examples using cloud services available from Amazon Web Service (AWS), Microsoft, and Google.

The presented practices are geared toward small and medium-sized organizations; however, all organizations, independent of size, can use these practices to improve the security of their cloud usage. The focus here is on hybrid deployments where some IT applications deploy or move to a CSP while other IT applications remain in the organization’s data center. Small and medium-sized organizations likely have limited resources; where possible, these practices describe implementation approaches that may be effective in limited-resource situations.

1 Introduction

This report presents a collection of security practices that are practical and effective for improving the cybersecurity posture of cloud-deployed IT systems. Researchers at the Software Engineering Institute's CERT Division developed these practices by identifying the risks, threats, and vulnerabilities faced in deploying or moving applications and systems to a cloud service provider (CSP) [Morrow 2019]. They defined five mission threads[1] and used them to study the effect of these risks, threats, and vulnerabilities on cloud-based application and system security.[2] Analysis of these mission threads identified a collection of four practices organizations should follow to manage cybersecurity risk when deploying applications and systems to the cloud.

The four practices presented here are not the complete collection of actions needed to securely use cloud computing. These four practices address the specific risks created by the specific threats analyzed in the mission threads. These four practices should be complemented with practices provided by CSPs, general cybersecurity practices, regulatory compliance requirements, and practices defined by cloud trade associations, such as the Cloud Security Alliance [CSA 2018].

These practices are geared toward small and medium-sized organizations; however, all organizations, independent of size, can use these practices to improve the security of their cloud usage. The focus here is on hybrid deployments where some information technology (IT) applications deploy or move to a CSP while other IT applications remain in the organization's data center. This hybrid deployment model is likely to be the norm for quite some time.

Small and medium-sized organizations likely have limited resources; where possible, these practices describe implementation approaches that may be effective in limited-resource situations.

Prior to describing the practices, the report presents a few risk examples. These examples describe actual cybersecurity incidents. For each example, there are pointers to one or more practices that, if applied, could have reduced the risk of the incident.

The four important practices are

- **Perform Due Diligence**—Due diligence requires that cloud consumers fully understand the security implications of deploying or moving applications and systems to a CSP. Consumers must understand how CSP services should be used to support business activities while protecting information.

[1] "A mission thread is an end-to-end set of steps that illustrate the technology and people resources needed to deliver expected behavior under a set of conditions and provide a basis for identifying and analyzing potential problems that could represent risks. For each mission step, the expected actions, outcomes, and assets are assembled. Confirmation that the components appropriately respond to expected operational use increases confidence that the system will function as intended even in the event of an attack." https://www.acsac.org/2013/program/wips/Woody.pdf

[2] The five mission threads were (1) account compromise threat, (2) multi-tenancy with side channel threat, (3) management API vulnerability, (4) self-provision resources and services, and (5) data deletion.

- **Manage Access**—Managing access involves identifying the different categories of users in a cloud-based IT environment, determining the responsibilities of each user category, and ensuring access to resources is controlled in ways that allow users to carry out their responsibilities while protecting resources from inappropriate or unauthorized use.
- **Protect Data**—Protecting data addresses two consumer challenges: (1) preventing the accidental or unauthorized disclosure of data and (2) ensuring continued access to critical data in the event of errors, failures, or compromise.
- **Monitor and Defend**—Monitoring and defending requires the CSP and cloud consumer to work together to monitor cloud-based systems and applications to detect unauthorized access to data or unauthorized use of resources.

To illustrate the practicality of these practices, examples are presented that use cloud services available from one or more of the “big three” cloud service providers—Amazon Web Service (AWS), Microsoft, and Google [AWS 2019a, Microsoft 2019a, Google 2019a]. These are examples only and are not an endorsement of these cloud service providers or their service offerings. Other CSPs offer capabilities similar to those described in these examples.

The examples span the range of cloud service models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Not every practice has examples for all service offerings. However, across all of the practices, there is at least one example for each service model.

2 Risk Examples

The practices presented here address cloud security issues that consumers typically experience. This section presents examples of notable cloud security incidents. Each example includes references to the practices that mitigate the risk of that incident type.

2.1 Unsecured AWS Storage Services

Several instances of unauthorized exposure of data to the Internet have been linked to improperly configuring AWS Simple Storage Service (S3), thus leaving data accessible.

On September 5, 2017, *The Register* reported, "Records of roughly four million Time Warner Cable customers were exposed to the public Internet after a contractor failed to properly secure an Amazon cloud database" [Nichols 2017]. The access policy on an AWS S3 bucket was improperly configured, allowing public access to data in the bucket. Press reports surrounding this incident suggested that misconfiguration of AWS resources by consumers is a common problem. (Practices that would mitigate this risk include Perform Due Diligence, Manage Access, Protect Data, and Monitor and Defend.)

On June 1, 2017, a security researcher found sensitive files openly available on the Internet. The files were stored in plain text in an Amazon S3 bucket with no password protection. Zohar Alon, co-founder and CEO of cloud infrastructure security company Dome9, said, "Yet security of S3 buckets to prevent accidental data exposure is often poorly understood and badly implemented by their users, even someone as technically savvy as an engineer with one of the world's leading defense contractors" [Barth 2017]. (Practices that would mitigate this risk include Perform Due Diligence, Manage Access, and Monitor and Defend.)

2.2 Deloitte Email Compromise

On September 25, 2017, *The Guardian* reported the global consulting firm Deloitte[3] was "… the victim of a cybersecurity attack that went unnoticed for months" [Hopkins 2017]. The attack used a compromised system administrator credential to access the firm's email system hosted in Microsoft Azure. The administrator account used only a password for authentication. (Practices that would mitigate this risk include Manage Access and Monitor and Defend.)

2.3 Accidental Data Loss

On April 21, 2011, 0.07 percent of data stored in Amazon Elastic Block Storage (EBS) volumes in a US-EAST region availability zone were irretrievably lost [Blodget 2011]. An error in a maintenance procedure caused a significant drop in network bandwidth within an EBS cluster [AWS 2011]. This loss of bandwidth ultimately resulted in a race condition causing EBS cluster

[3] For information on Deloitte LLP, go to https://www2.deloitte.com/us/en.html.

nodes to fail. After repairing the EBS cluster, Amazon was able to recover most customer data. However, a small amount of customer data was permanently lost. (Practices that would mitigate this risk include Protect Data.)

2.4 Code Spaces Data and Systems Destroyed

Code Spaces was a CSP that provided SaaS source code management tools such as Git and Apache Subversion to software developers. Code Spaces built its SaaS offering using AWS. In 2014, a Code Spaces privileged user AWS credential was compromised. Within 12 hours of the compromise, most of Code Spaces' data and all of its virtual machines were permanently deleted. Code Spaces lost its customers' data and, as a result, ceased operations [Goodin 2014]. (Practices that would mitigate this risk include Perform Due Diligence, Manage Access, and Protect Data.)

2.5 OneLogin Data Breach

OneLogin is a CSP that provides SaaS Identity and Access Management (IdAM) services to business [OneLogin 2019]. OneLogin's products use AWS. In May 2017, the company reported a hacker obtained access to a set of AWS keys through a third-party vendor. With these keys, the hacker was able to access and compromise all of OneLogin's records at its U.S. data center [Whittaker 2017]. (Practices that would mitigate this risk include Manage Access, Protect Data, and Monitor and Defend.)

2.6 Ransomware Leverages the Cloud

Although there seem to be few confirmed incidents to date, reports indicate that ransomware providers are actively using cloud backups to exfiltrate data that can then be ransomed instead of only encrypting victims' data where it resides. Cloud-based backup software was reportedly targeted and/or used by Doppelware and Maze ransomware operators to steal or destroy backups as a normal tactic during attacks [Abrams 2020]. (Practices that would mitigate this risk include Perform Due Diligence, Manage Access, Protect Data, and Monitor and Defend.)

2.7 SolarWinds "Solorigate" Supply Chain Attack

SolarWinds is a business software provider of network, system, and information technology management products. On December 13, 2020 FireEye [FireEye 2020a] published threat research about an intrusion campaign where advanced threat actors compromised the SolarWinds software supply chain to access global private and government networks. Attackers then used on-premises access to gain unauthorized access into victim Microsoft 365 cloud environments [FireEye 2020b]. Had zero trust explicit verification controls been implemented, least privilege access would have been enforced and the unauthorized access might not have happened [Weinert 2021]. (Practices that would mitigate this risk include Perform Due Diligence, Manage Access, Protect Data, and Monitor and Defend).

3 Shared Responsibility Model in Cloud Computing

CSPs use a shared-responsibility model for security. The CSP accepts responsibility for some aspects of security; other aspects are shared between the CSP and the consumer. Finally, some aspects of security remain the sole responsibility of the consumer. This shared-responsibility model is an example of the three security control types (i.e., CSP responsibility, consumer responsibility, and shared responsibility) defined by the U.S. National Institute of Standards and Technology (NIST) in Special Publication 800-53r4 [NIST 2021].

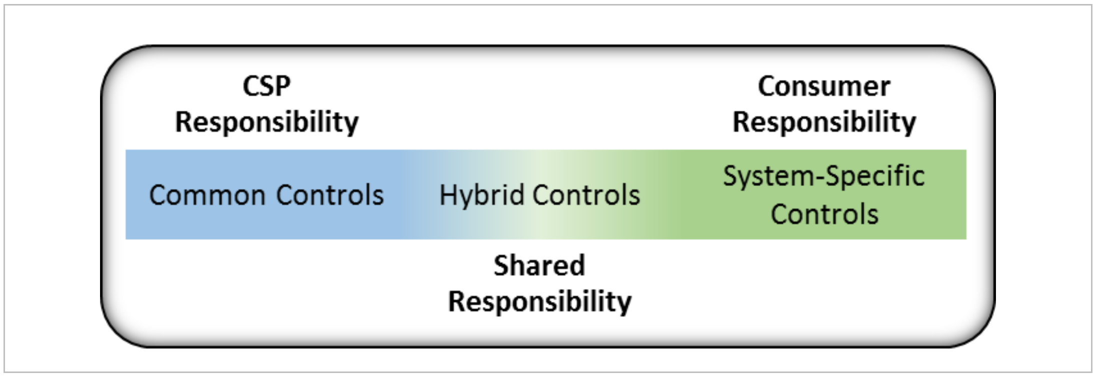

Figure 1: Shared Responsibility for Cloud Security

NIST defines common controls, hybrid controls, and system-specific controls. In cloud computing, *common controls* are the security controls that are fully implemented by the CSP. These controls are inherited by all consumers. Physical security[4] for the computing infrastructures used to deliver cloud services is an example of a common or CSP-provided security control.

In cloud computing, *hybrid controls* are security controls that are partially implemented by the CSP and partially implemented by the consumer. Controlling access to CSP services by consumer personnel[5] is an example of a hybrid or shared security control. The CSP provides mechanisms to define and enforce access control policies. The consumer must use these mechanisms to specify which personnel are permitted to access cloud services. The consumer's policies, enforced by CSP mechanisms, implement access control.

[4] NIST SP800-53r4 security control PE-3 is an example of a security control provided by the CSP.

[5] NIST SP800-53r4 security control AC-3 is an example of a security control that, when applied to consumer personnel accessing CSP services, must be partially implemented by the CSP and the consumer.

In cloud computing, *system-specific controls* are security controls that must be implemented by the consumer. In IaaS and PaaS, collecting auditable events from consumer-implemented applications is an example of a system-specific control.[6] In SaaS, system-specific controls are likely to be procedural, such as reviewing audit trails and taking corrective action.[7]

Effective cloud security depends on consumers knowing and meeting all their security responsibilities. Consumers who fail to understand or meet their security responsibilities are a leading cause of security incidents in cloud-based systems.

The risk example of unsecured AWS storage services in Section 2.1 illustrates a situation where cloud consumers failed to meet their responsibilities, resulting in security incidents. In the September 26, 2017 *SANS Newsbites* [SANS 2017], Alan Paler noted,

> *Ian Massingham, a technical evangelist at Amazon Web Services (AWS) explained how, for 'infrastructure as a service,' AWS takes no responsibility for secure configuration of the operating system or security monitoring, for application security configuration or monitoring, for account management, for access control lists, for identity management and more [Massingham 2015]. Amazon provides great tools for implementing security controls, but as you'll see in the Amazon video, you must be very skilled to deploy them broadly and effectively [Franz 2016]. One of the least fun jobs at (all of the) cloud service providers is nicknamed 'CAO' for Chief Apology Officer, having to go to clients and explain to them that whatever they heard about cloud security being better, all the responsibility for making that happen rests on the user.*

[6] NIST SP800-53r4 security control AU-2 is an example of a security control that must be implemented by the consumer as part of applications the consumer develops in IaaS or PaaS.

[7] NIST SP800-53r4 security control AU-6 is an example of a system-specific procedural security control in SaaS.

4 Important Practices

The practices presented in this section describe key cloud consumer responsibilities in ensuring the security of cloud-based systems and applications.

4.1 Perform Due Diligence

It's crucial to perform due diligence across the lifecycle of applications and systems being deployed to the cloud. This includes activities in four phases: planning, development and deployment, operations, and decommissioning.

4.1.1 Planning

The first step in a successful cloud deployment is selecting an appropriate system or application to move to, build in, or buy from a CSP. Getting this step right is challenging for a first-time cloud deployment. You benefit from the experience of others and should use a cloud adoption framework to efficiently use cloud services. A cloud adoption framework provides a process for identifying applications, selecting cloud providers, and managing the ongoing operational tasks associated with public cloud services. Cloud adoption frameworks may be CSP specific or CSP agnostic. A risk taxonomy is also useful to identify the major risk factors associated with cloud adoption and try to reduce or mitigate those risks. The most effective way to reduce the risks is to properly catalog them during the planning phase then address them as early in the adoption process as possible. The Software Engineering Institute (SEI) expects to publish a paper identifying and describing these cloud adoption risk factors.[8]

AWS provides a cloud adoption framework that addresses six perspectives: business, people, governance, platform, security, and operations [AWS 2019h]. While this framework is CSP specific, much of the information and advice applies to any cloud adoption, not just AWS. All the notable CSPs (e.g., Google Cloud and Microsoft Azure) have their own adoption frameworks.

The U.S. government offers several adoption guides and services, including the General Services Administration's (GSA's) Cloud Adoption Playbook and services offered by the Cloud Adoption Center of Excellence. These guides and services are available to other U.S. Government organizations and include solutions architectures, DevSecOps support, cybersecurity solutions, governance, migration planning, and business application consulting [GSA 2021].

Using a framework helps an organization understand the impact of cloud use. For example, using SaaS can provide value to small or medium-sized organizations with limited IT staff. As another example, providing Outlook email and SharePoint Online using Microsoft Office 365 frees IT staff from installing, operating, and maintaining these services locally. However, the existing business workflows, such as provisioning and deprovisioning users or providing technical

[8] forthcoming white paper by Christopher Alberts: "A Prototype Set of Cloud Adoption Risk Factors"

support, must change to support the use of Office 365. Additionally, the current fixed costs of providing email and SharePoint become a combination of fixed and variable costs.

After using a cloud adoption framework to identify both a target system or application for cloud deployment and a CSP, all staff involved in the deployment must be educated on the basics of the selected CSP, the CSP's architecture, the services offered, and the tools available to assist in deployment. Staff members must understand the CSP's shared responsibility model and its impact on their role in the cloud deployment. Having all team members well versed in the basics of the chosen CSP, with emphasis on the other three practice areas, helps to ensure clear communication.

For example, the AWS architecture is a collection of regions with multiple availability zones (AZs) in each region. Services operate and data is stored within regions and AZs. Workloads can be balanced across AZs within a region but not across regions. Team members must understand these concepts to discuss designs and ensure shared and consumer-specific security responsibilities are met.

The availability of applications can be ensured by placing application instances in multiple AZs. Team members must understand these concepts to design and implement applications that meet business availability requirements. Business analysts must be familiar with these concepts to understand how their availability requirements are being satisfied.

For organizations that must comply with industry or government regulations, CSPs may provide guidance on meeting these requirements using their services. For example, AWS provides a "Quick Start" guide for United States Federal Government agencies that must comply with the Federal Information Security Management Act (FISMA) requirements in FIPS-199 [NIST 2004] and NIST SP800-53 [AWS 2019f]. AWS also provides services compliant with the Federal Risk and Authorization Management Program (FedRAMP), a program for standardizing assessment, authorization, and continuous monitoring [AWS 2020a]. AWS provides products and services in scope of various other compliance and certification programs, including Service Organization Controls (SOCs), Payment Card Industry (PCI), International Standards Organization (ISO), Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG), Health Insurance Portability and Accountability Act (HIPAA), and more [AWS 2020b].

Microsoft provides "Azure Security and Compliance Blueprint – PCI-DSS-compliant Payment Processing environments" that provides guidance for meeting Payment Card Industry (PCI) – Data Security Standards (DSS) requirements in an Azure PaaS deployment [Simorjay 2018]. Like other major vendors, Microsoft also provide compliance information for Azure services with FedRAMP, DoD CC SRG, ISO certifications, HIPAA compliance, and more [Microsoft 2020a].

AWS and Microsoft are merely well-known examples of FedRAMP-Authorized providers. The FedRAMP marketplace lists hundreds of additional authorized providers, most with multiple authorized services, for all three service models (IaaS, PaaS, and SaaS). In addition to industry, government organizations also provide authorized cloud services, including 18F Cloud.gov, Workplace.gov, and the USDA Digital Infrastructure Center [FedRAMP 2020].

Finally, though not covered in detail in this report, containers are a common feature of both onsite and cloud platforms. There are a number of existing resources for container security best practices; Thomas Scanlon and Richard Laughlin discuss some of them in the SEI blog post, 7 Quick Steps to Using Containers Securely [Scanlon 2020]. These resources include NIST's *Application Container Security Guide*, the *Docker Security Guide*, and *Docker Reference Architecture: Securing Docker Enterprise and Security Best Practices*.

There are many container security tools available, including OpenSCAP, that provide information about policies, standards, and tooling. Using open source tools is a good place to start before continuing with commercial offerings that may offer more capabilities or simplified usage. Scanlon and Laughlin's blog post includes the following steps for using containers securely:

1. Use available security resources.
2. Rebuild regularly.
3. Secure the image supply chain.
4. Protect the container hosts.
5. Distribute secrets securely.
6. Configure resource limits.
7. Use persistent logging.

4.1.2 Development and Deployment

Training development and deployment teams in the proper use of CSP services is essential. CSPs provide guidance and documentation on best practices for using their services. If you are developing a new application or system, follow the CSP's guidance in designing the system or application.

If you are migrating an existing application or system, review its architecture and implementation relative to the CSP's guidance to determine what changes are needed to deploy the application appropriately. It may be necessary to discuss the deployment with the CSP's technical support staff to understand the changes you require.

CSPs provide tools to ensure resilience in the case of failure. Make sure the team knows how to use these tools correctly; however, there are clear examples showing no amount of customer expertise is enough to avoid outages that are the responsibility of the CSP. One example is a five-hour AWS Kinesis outage in US-EAST-1 that impacted customers and the CSP itself by temporarily interrupting updates to its Service Health Dashboard [AWS 2020c]. Another example is an Azure Active Directory authentication outage caused by an authentication key that is normally removed on an automated schedule but that was marked to "retain" as part of a complex migration, exposing a bug where the "retain" state was not honored [Microsoft 2021a].

CSP services often require specific configurations to provide security. Make sure the team understands these configurations and fully implements them. The incidents of unsecured AWS storage services, described in Section 2.1, were the result of consumers failing to (1) configure the access policy for the storage service correctly and (2) encrypt the stored data. This event reinforces the need for staff to be well trained on the use of CSP resources. To help reduce these errors, AWS recently changed S3 to encrypt data by default [Barr 2017, Coles 2019].

Review the organization's security policies and current security control implementation approaches. Check the CSP's guidance before implementing the on-premises security approach in the cloud. First, verify that, if implemented in the cloud, the on-premises approach would be effective. Then, see if CSP services provide a better implementation approach that still meets security policy goals.

Moving to a cloud environment may present risks that were not present in the on-premises deployment of applications and systems. Check for new risks and identify new security controls that will be necessary to mitigate these risks. Again, consider how CSP-provided control implementations can help.

For example, cloud infrastructure is shared by multiple CSP customers and accessible by CSP administrators. This sharing may increase the risk of unauthorized data exposure and require encrypting data at rest. The CSPs provide tools that can be used to encrypt data. In IaaS and PaaS deployments, the applications that process this data may require modification to properly access and use encrypted data.

Connecting your on-premises IT with cloud-deployed systems and applications changes the risk exposure of those on-premises resources. Review the security controls in place in your on-premises IT environment and ensure those controls adequately address risks once connected to a CSP.

If the CSP provides tools to check for proper and secure configuration of services, use them. AWS provides Quick Start guides that help deploy popular solutions on AWS, based on AWS best practices for security and high availability [AWS 2019c]. Microsoft provides Cloud Infrastructure and Management Practice Accelerators to support development using Azure [Microsoft 2019c].

If using contract resources to migrate an existing application or build a new application using cloud services, the organization's staff must provide effective oversight of the contractor. To provide oversight, staff need both an understanding of the CSP's basic architecture as described in Section 4.1.1 of this report, Planning, as well as a working knowledge of the CSP services being used in the application.

4.1.3 Operations

Once developed and deployed, applications and systems must be operated securely. O'Reilly Media, in describing its book *AWS System Administration* [Ryan 2014], says,

> *Building and deploying infrastructure with Amazon Web Services is simply not the same as dealing with static servers. With tools that let you automatically replace instances and scale up and down in response to demand, it's actually more like programming than traditional system administration.*

Unlike physical servers, disks, and networking devices, cloud virtual infrastructure is defined by software. As such, the infrastructure can be treated as source code. Manage the software that defines the cloud virtual infrastructure using a source code control system. Source code control systems have proven effective in managing software development. These same practices can be adapted to manage cloud infrastructure, support the automation of compliance artifacts, and strive for continuous authority-to-operate (C-ATO). An ATO is an official approval to use a system operationally, and traditional government models of ATO have a reputation for unnecessarily slowing pushes to production, testing, prototyping, and more when compared to using a DevOps approach. C-ATO ideally reinvents ATOs by facilitating pushes to production multiple times per day, rapid prototyping, and defining metrics for test coverage, security, and documentation [Chaillan 2019]. Use the source code control system to enforce change control procedures. Changes to production resources should require independent approval prior to implementation.

System administrators must learn to use the CSP's tools to operate systems and applications. Developing new procedures is necessary to address the combination of operational practices for on-premises and cloud-based applications and systems.

The AWS CloudFormation service is an example of infrastructure defined by software. CloudFormation uses templates that describe cloud infrastructure, such as virtual machines and virtual disks that compose a virtual data center. Since these templates are just text files, they can and should be managed and configuration controlled just like other software. System administrators, however, must learn to use the template language effectively and configure resources securely. Additionally, they need clear procedures for when and how to check templates out of/into a source code control system.

Another example is Microsoft Office 365, which provides Admin Center, a web portal accessible to people with admin user accounts. The portal provides access to all configuration, billing, and operation information related to an organization's Office 365 subscription. Links are provided to service-specific admin centers such as Exchange Online, SharePoint Online, and Skype.

Office 365 administrators must understand the options available to them through the various admin centers, the impact of those options on the operation and security of Office 365 services, and their effect on integrating Office 365 with on-premises applications and systems.

In cases of notable risks like Solorigate, CSPs often provide supplemental material to help customers understand risk, reduce risk, and detect compromise. For example, Microsoft offers an Azure Active Directory workbook to help customers assess Solorigate risk. The workbook provides information about common attack patterns associated with Solorigate so customers can identify modified application and service principal credentials or authentication methods, modified federation settings, new permissions granted to service principals, and directory role and group membership updates [Weinert 2020].

4.1.4 Decommissioning

There are many reasons why a cloud-deployed application or system may need to be decommissioned. The CSP could go out of business. The CSP could discontinue key services used by the application. The CSP's prices could increase, making the current deployment too expensive. Whatever the reason, planning for decommissioning a cloud application or system should be done before deployment. Cloud services are currently unique to each CSP. Therefore, moving an application or system from one CSP to another is likely to be a major effort.

One method to address this risk is by developing a multiple-CSP strategy, though there are concrete arguments against this method discussed later in this section. A CIO.com article provides perspectives on the need for a multi-CSP strategy from several chief information officers (CIOs) [Boulton 2017]. They recommend analyzing how the selected application could be deployed to more than one CSP when making the initial CSP selection. For example, examine how the application or system could be deployed to AWS and to Microsoft Azure. Both AWS and Microsoft Azure have significant overlap in the types of services offered, although details of each offering differ.

Mappings among CSPs, readily available on the Internet, can help identify how an application architected for one CSP might be moved to another [Comparecloud.in 2018]. While the application or system may be deployed to only one of these CSPs, it makes sense to track aspects of the deployment that are unique to the chosen CSP and would require redesign if moved.

Even if you are not deploying to multiple CSPs, consider what would be involved in leaving a CSP. The most important part of any application or system is the data stored and processed within. Therefore, it is critical to understand how the data can be extracted from one CSP and moved to another. This extraction can be difficult with many cloud service models. Even for those—like IaaS, where the consumer has substantial control over how and where the data is stored and has the ability to develop software that can extract the stored data—cost may be a major issue. CSPs typically charge for transfers of data into and out of their services. To incentivize use of CSP services, these charges may be asymmetric—lower for transfer into the CSP and higher for transfers out of the CSP. CSPs have some tools for migrating to their platforms; for example, Google's Migrate for Compute Engine helps with VM migration [Google 2021a], but extracting anything more than the simplest data is likely to continue being a substantial impediment to leaving a CSP.

Additionally, using multiple clouds is not necessarily a realistic strategy when defining multi-cloud as "workloads that can seamlessly run across any cloud provider or your own data centers with equal ease" [Quinn 2020]. Cloud economist Corey Quinn of the Duckbill Group argues that multi-cloud should be avoided by default because it essentially limits the customer's ability to take advantage of anything beyond "baseline primitive offerings" from their CSP. Many advantages of cloud computing evaporate if customers don't leverage CSP-specific products like application load balancers) and instead rely on third-party applications. Quinn points out that technology is not the only way to introduce CSP lock-in—a problem that can happen when customers depend on a single CSP, making it difficult to switch to a different vendor without incurring considerable costs and risking introducing incompatibilities. Quinn also points out that employee expertise on a specific platform can also contribute to CSP lock-in.

SaaS presents a particularly significant challenge since the consumer's data is stored by the CSP where and how the CSP chooses. To move data from one SaaS offering to another, the consumer is solely dependent on the source CSP providing a data extraction tool that exports data in a format that can be ingested by the destination CSP. It is best to know how to do this before storing years of data in a CSP's SaaS application.

Gartner presents a three-step strategy for addressing SaaS CSP exit planning in a report titled *Plan Your Data Exit Strategy Before You Sign a SaaS Contract* [Dayley 2017]. Gartner advises consumers to ". . . test data movement into and out of the cloud during proof of concept, negotiate cloud contracts to allow for easy data extraction, . . . establish migration skills, and develop an internal competency on data availability.” However, Gartner also points out that “…cloud exits are often complex and costly, and they may take years to achieve [Leong 2021].”

The European Banking Authority (EBA) guidelines “…on outsourcing arrangements require institutions to have a documented exit strategy when outsourcing critical or important functions which are in line with their outsourcing policy and business continuity [EBF 2020].” This has motivated U.S.-based CSPs like Microsoft to publish material on cloud exit planning guidelines that use a risk-based approach with the understanding that no exit plan can reasonably be fully tested [Deprins 2020]. Deprins also points out that the Bank of England and European Securities and Markets Authority (ESMA) recommend risk-based approaches to exit planning.

Business Continuity Planning and Disaster Recovery Planning are related to migration from one CSP to another. With applications and systems hosted at CSPs, these plans must address threats to an organization’s data and services at the CSP. Recovery could potentially involve bringing an application or system back on premises or migrating to another CSP, but it is important to understand that an exit strategy is only a small component of business continuity since the time to sever a third-party business relationship is typically longer than is acceptable for a critical activity to be down [EBF 2020].

4.1.5 Key Considerations

Below are the key considerations for performing due diligence:

- Use a cloud adoption framework to identify cloud-appropriate applications and select a CSP.
- Thoroughly train staff in the architecture, use, and operation of CSP services.
- Use a source code control system and change control procedures to manage cloud resource configuration, compliance support, and a C-ATO mindset.
- Adopt a zero trust security model early in the planning step.
- Plan for extracting data and moving applications from the chosen CSP to another CSP or back on premises before deployment.

4.2 Manage Access

As described in Section 3, security in cloud computing is a responsibility shared by the CSP and the cloud consumer. Figure 2, derived from work by The MITRE Corporation, illustrates this shared responsibility in managing access to IaaS resources [Faatz 2017]. The CSP is fully responsible for managing access to physical resources such as computers, network storage devices, and the virtualization system that provides service to consumers.

Access to create, manage, and destroy virtual resources such as virtual machines and virtual storage is a shared responsibility. The consumer must define the policy that determines who has access to perform these actions. The CSP must provide mechanisms to enforce the consumer’s policies.

Access to applications and operating systems is solely the responsibility of the consumer, who must both define access policies and put mechanisms in place to enforce those policies. Control of access to resources is not complete without implementing all three parts correctly and completely.

Managing access to resources determines who can access them and what they can do with the resources they can access. Access management generally requires three capabilities: the ability to identify and authenticate users, the ability to assign users access rights, and the ability to create and enforce access control policies for resources.

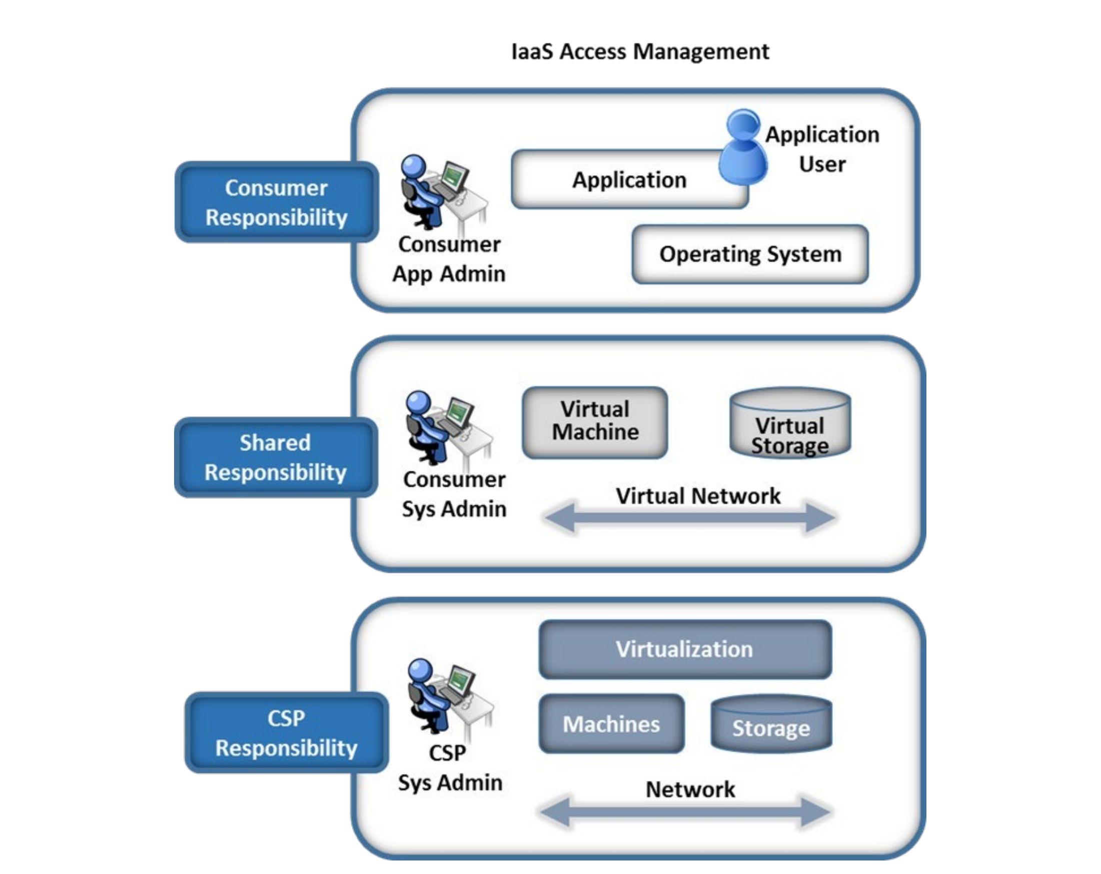

Figure 2: IaaS Access Management and Shared Responsibility
This figure is used and reprinted with permission from The MITRE Corporation. ©2017. All other rights reserved.

4.2.1 Identify and Authenticate Users

The starting point for access management is identifying and authenticating users. Legitimate users are given credentials that bind their identity to an authenticator. The most common credential is a username and password, the password being something only the user knows.

One of the most effective ways of attacking an organization’s information systems is to gain access using legitimate user credentials, especially privileged user credentials. Such credentials can be particularly valuable in accessing cloud services, since management interfaces are accessible from the Internet. While an organization may use a private connection to the CSP, the management interfaces used by customers are also available via the Internet. With stolen privileged user credentials, an attacker can control and configure cloud consumer resources.

The Deloitte email compromise and the OneLogin data breach described in the Risk Examples, Sections 2.2 and 2.5, both demonstrate attacks using compromised credentials. As in the Deloitte case, these breaches often go undetected for months, since all access appears to be performed by legitimate, authorized users. Credentials that depend solely on something the user knows, such as passwords, are particularly susceptible to theft since there is no obvious way for the legitimate user to know the credential has been compromised.

To reduce the risk of credential compromise, use credentials that employ multiple factors to authenticate users (multi-factor authentication or MFA). MFA reduces the likelihood of a credential compromise because it requires an adversary to acquire multiple, independent elements to compromise a credential. In cloud computing, MFA typically combines a password with something the user has, such as a text message sent to a previously registered cell phone. This second factor makes credential compromise more difficult and more likely to be detected quickly. Many cloud providers offer MFA capabilities.

MFA is also an opportunity to introduce the idea of zero trust, which is a type of security model, "…that strives to reduce risk inherent in perimeter-based security architectures" [Sanders 2021]. Zero trust tenets include strict enforcement through explicit authentication and authorization to resources on a per-session basis. In the case of Solorigate, which compromised user and vendor accounts plus vendor software, "…in cases where the actor succeeded, highly privileged vendor accounts lacked protections such as MFA, IP range restrictions, device compliance, or access reviews [Weinert 2021]."

Compromise of privileged user credentials is particularly concerning since these credentials allow the user to manage the IT environment. With the right privileged user credentials, an attacker can more easily achieve persistent access by installing software or creating user accounts. If it is not practical to use multi-factor credentials for all users, start with privileged users.

Microsoft, for example, supports Azure multifactor authentication for Microsoft 365 users. This authentication is easily enabled in the Microsoft 365 admin center [Microsoft 2021b]. Microsoft's security defaults feature requires all users to use MFA with the Microsoft Authenticator app, disabling legacy MFA methods (e.g., text messages and phone calls).

AWS offers several MFA options as well [AWS 2021]. The simplest option is a virtual MFA device using a tablet or smartphone app that supports the open time-based one-time password (TOTP) standard. However, AWS also offers extra-cost options using special hardware tokens.

CSPs typically provide a consumer with an initial privileged credential that can perform all privileged operations. This credential is similar to a "root" credential in Linux or an admin credential in Windows. However, the scope of privilege associated with this credential is much broader than control over one or more machines. This credential is the logical equivalent of granting unfettered access to a physical data center. In IaaS, this credential allows the creation and destruction of virtual machines, virtual disks, virtual networks, and other privileged user accounts.

Compromise of this credential gives an attacker the ability to control a consumer's cloud resources. An attacker could prevent a consumer from accessing his or her cloud resources or delete the consumer's data. Do not routinely use this initial credential to manage virtual resources. Routine use of this credential increases the consumer's exposure to compromise. Use this credential ONLY to define and set up the initial set of users and roles.

Privileged user credential compromise can be devastating. A privileged user credential compromise, as described in the risk example Code Spaces Data and Systems Destroyed, in Section 2.4, caused Code Spaces to go out of business.

4.2.2 Assign User Access Rights

Plan a collection of roles to satisfy both shared and consumer-specific responsibilities. CSPs and others, such as Gartner, provide advice on designing roles [Microsoft 2017, Gartner 2016]. These roles should, to the extent feasible, ensure that no one person can adversely affect the entire virtual data center. In a traditional data center, this separation might take the form of defining separate operating system, storage, and network administrators. However, since all of these resources are virtual in an IaaS cloud and can be managed by writing code, a strategy that separates defining resources from deploying defined resources to production might be more effective.

Individual developers and system managers should not have uncontrolled access to resources. Limiting access can constrain the impact of a credential compromise or a malicious insider. Developers should be constrained to assigned projects. System managers should be constrained to assigned resources. CSPs may provide guidance on appropriate roles and privileges for managing services. When establishing roles, apply the principle of least privilege. Give roles only those privileges explicitly needed to perform their function. Similarly, give services and applications only those privileges needed to operate. Service and application roles should not have elevated privileges.

CSPs offer a variety of ways to implement credential and user access management. One approach defines all users, credentials, and roles in the CSP's system. These are completely disjoint from on-premises users, credentials, and roles. A second approach extends all or part of the on-premises Active Directory (AD) into the cloud environment. A third approach uses the existing on-premises users and credentials, augments them with roles and groups appropriate to the cloud environment, and federates the cloud environment with the on-premises capabilities. Each of these approaches has strengths and weaknesses that warrant consideration in an organization-specific context.

Managing users, credentials, and roles for access to cloud services entirely in the cloud ensures there is no unintended crossover of users from the on-premises environment to the cloud environment. However, it can result in operating two independent identity and access management processes. It can also complicate the user experience, as users have separate credentials for cloud and on-premises access. It can increase the risk of introducing errors, which can impact security. This separation is appropriate for privileged users who create, manage, and destroy virtual resources in the cloud.

Extending all or part of the on-premises AD into the cloud can consolidate identity and access management for both cloud and on-premises users in a single set of processes. This consolidation ensures a single, consistent approach to access management. This approach may be appropriate for application users as it provides the same user experience across on-premises and cloud-deployed applications. However, this approach also potentially exposes the on-premises AD to cloud-based threats. When using this approach, ensure the security controls protecting on-premises AD instances are effective against these additional threats.

To provide further control of privileged user access to operating systems and applications running on virtual machines, use bastion hosts.[9] Using bastion hosts is a best practice for both on-premises and cloud-deployed systems. Bastion hosts are a form of proxy that is interposed between a privileged user and the operating systems and applications they manage. The bastion host determines which systems and applications a privileged user can access and what operations the privileged user can perform on those resources. Additionally, the bastion host maintains a dedicated log of privileged user actions, making it easier to review those actions for indicators of inappropriate privileged access.

The *Best Practice Guide for Department of Defense Cloud Mission Owners* provides guidance on implementing bastion hosts in IaaS cloud deployments [DISA 2015]. AWS provides a Quick Start template that builds a simple Virtual Private Cloud (VPC) architecture incorporating bastion hosts [AWS 2017]. This AWS example can be adapted to other IaaS providers.

Apply configuration management to access permissions for users and roles. This helps prevent accidental or malicious changes to access permissions. Incorporate separation of duties in the configuration management process to prevent any one person from both approving access permission changes and implementing the changes. Periodically review access permissions to ensure users still need their assigned roles and roles still require their configured permissions. Cloud access security broker (CASB) technology is a growing market that could help organizations automate enforcement to prevent incidents, such as the Deloitte email compromise and the OneLogin data breach risk, and simultaneously reduce the burden on IT staff.

4.2.3 Create and Enforce Resource Access Policies

Cloud services may require service-specific access policies. The unsecured AWS storage services risk example in Section 2.1 resulted from improperly configured AWS S3 access policies. It is important to understand access policy configuration requirements associated with cloud services. Additionally, consumers must be aware of updates to cloud services that affect access policy configuration. Upgrades to or maintenance of cloud services can add, remove, or change access policy parameters.

CSPs offer many storage service types such as virtual disks, blob storage, and content delivery services. Each of these has unique access policies that must be configured to protect the data they store.

[9] Information on the use, construction, and hardening of bastion hosts can be found at the SANS website: https://www.sans.org/reading-room/whitepapers/basics/hardening-bastion-hosts-420.

As an example of all the actions a consumer should take to manage access, AWS provides recommendations for AWS identity and access management [AWS 2019d]. While the recommendations are specific to AWS, the underlying actions are applicable to many CSPs. Additional identity and access management recommendations are provided by Microsoft and Google as well [Microsoft 2019b, Google 2019b].

4.2.4 Key Considerations

The key considerations for managing access are below:

- Use multifactor authentication.
- Implement a zero trust real-time policy and explicit verification.
- Implement a collection of roles that provide separation of duties.
- Ensure access policies are properly configured on all storage services.

4.3 Protect Data

To protect data, develop a data protection strategy that addresses both on-premises data and cloud data. Conduct periodic assessments to verify procedures are in place that implement the strategy.

Protecting data involves two separate challenges: (1) preventing unauthorized access and (2) ensuring continued access to critical data in the event of errors and failures.

4.3.1 Prevent Unauthorized Access

As mentioned previously, the unsecured AWS storage services risk example in Section 2.1 resulted from incomplete or missing AWS S3 access policies. This oversight allowed unauthorized access to the data stored in the S3 buckets. However, if the data in the S3 buckets had been encrypted, this unauthorized access would not have disclosed the stored data. Data at rest should be encrypted to protect against disclosure due to unauthorized access; this is generally the default state for data storage options with many CSPs.

AWS provides multiple options to encrypt data stored in S3 and other data storage services. Similarly, other CSPs provide encryption capabilities for their storage services.

Encrypting cloud data at rest may involve encrypting the data in multiple cloud services. Figure 3 shows the architecture of a typical web application deployed to an IaaS CSP. Sensitive data that needs protection spreads throughout the IaaS environment. The data is initially located in the file server, the application server, the object/blob storage, and the database as shown by the blue folders. As the data is accessed, it spreads to the web server and the content delivery network shown by the yellow folders. To protect availability, the data from the file server, application server, and database is copied to the backup service. Backups are eventually rolled off to an archive service. Backups and archives are shown by red folders.

To protect the sensitive data, analyze the cloud deployment thoroughly to understand where sensitive data may have been copied or cached. You must understand and use the encryption capabilities of all the services to which data may have been copied to ensure that, no matter where the data is stored, it is protected.

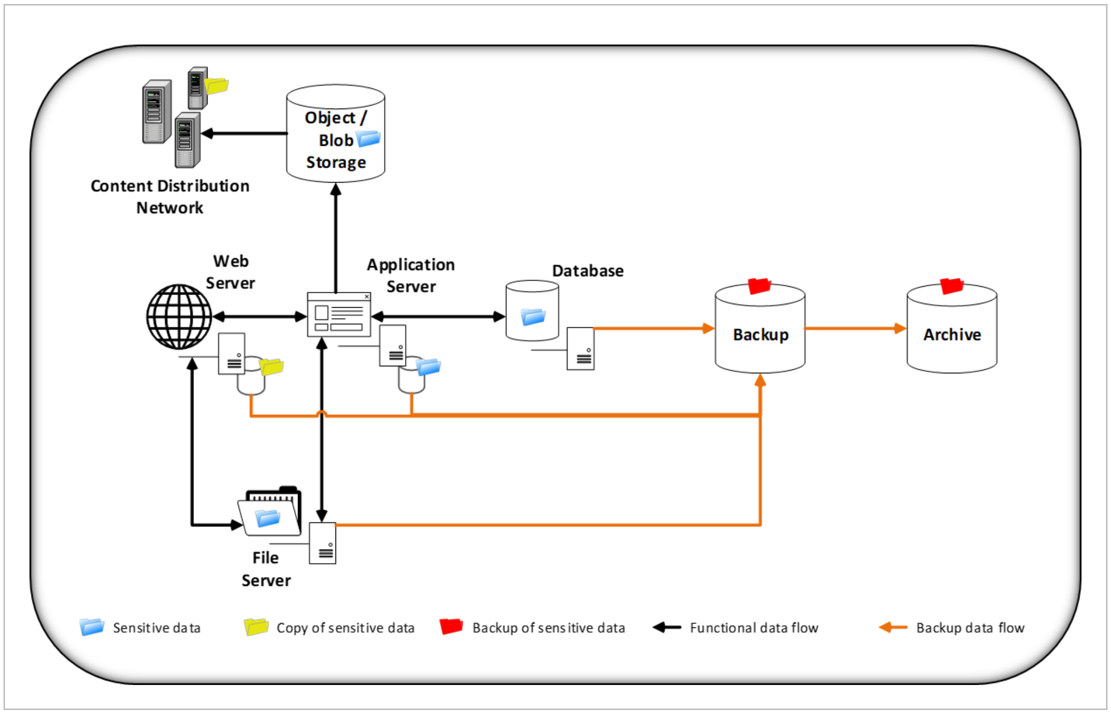

Figure 3: Sensitive Data in a Typical Cloud Web Application

Of course, encryption is only effective if the associated encryption keys are well managed. CSPs offer consumers a choice of CSP-managed or consumer-managed keys. CSP-managed keys are convenient but provide the consumer no control over where or how the keys are stored. Consumer-managed keys place the burden of key management on the consumer but provide better control [Chandramouli 2013, Snedeker 2017]. Consumer-managed encryption keys should not be stored in the cloud with the data they protect. Doing so increases the risk of key compromise and unauthorized access to data. CSPs offer hardware security modules (HSMs) to generate and store encryption keys in the cloud. HSMs target customers who have stringent security requirements or may need to comply with standards like the Federal Information Processing Standard (FIPS) 140-2 or Payment Card Industry (PCI) Data Security Standard (DSS) [Baldwin 2021].

In addition to offering key management systems (KMSs) for key lifecycle management (e.g., AWS Key Management Service, Azure Key Vault, and Google Cloud Key Management), third parties also offer KMSs for use with multiple CSPs. The Cloud Security Alliance identifies four common KMS patterns, including a cloud native key management system, external key origination, a cloud service using external KMS, and multi-cloud KMS (MCKMS) [Egan 2020]. Each pattern can have different strengths and challenges, and the cloud KMS space is rapidly changing; therefore, Egan recommends that "organizations consider the ability to pivot, migrate, or adopt new patterns of cloud KMS" [Egan 2020]. Selecting the correct KMS depends on the context, but the Cloud Security Alliance recommends cloud native KMS as the default since it is the simplest; other patterns should be used only if the consumer has clear reasons to do so.

4.3.2 Ensure Availability of Critical Data

CSPs provide significant guarantees that persistent data will not be lost. However, no system is perfect, and major cloud providers have accidentally lost customer data. For example, the accidental data loss risk example in Section 2.3 describes an incident in which AWS permanently lost consumer data from some Elastic Block Storage (EBS) volumes.

In addition to CSP errors, cloud consumers may also make mistakes that result in data loss. Therefore, it is important to understand CSP data backup and recovery processes to ensure they meet the organization's needs. The organization may need to augment CSP processes with additional backup and recovery actions. CSPs provide services that consumers can configure to perform backup and recovery operations.

In the data loss risk example cited above, Amazon recommended that consumers restore data from their own backups. AWS provides the ability to snapshot EBS volumes to S3 as a means of backing up the EBS volumes. Additionally, S3 data can be migrated to near-line storage in Amazon Glacier[10] to back up the S3 data while reducing storage costs.

As with on-premises backups, cloud consumers must determine the criticality of data and ensure that appropriate backups are performed—by the CSP, jointly by the CSP and consumer, or by the consumer alone.

The Code Spaces Data and Systems Destroyed risk example, described in Section 2.4, illustrates the importance of determining data criticality and ensuring appropriate backups exist to support business continuity. In this case, apparently Code Spaces was entirely dependent on backups maintained in AWS along with its production infrastructure. A single compromise destroyed the data that was critical to its business. Without that data, there was no business, and Code Spaces ceased operation. Given the criticality of the data, a backup strategy using a second CSP or on-premises storage would have been prudent.

Major CSPs now have backup services that can handle multiple data types and workloads (e.g., VMs, block storage, and databases). Microsoft's Azure Backup best practices include considering architecture, vault design, backup policy, security, network, governance, and monitoring and alerting [Microsoft 2020b]. NetApp, Inc., a cloud services and data management company, recommends considering requirements, the type of data or workloads to backup, resourcing and pricing, backup performance, and preparing for recovery with testing and monitoring [Kovacs 2020].

As mentioned in Section 4.1, Perform Due Diligence, ensuring access to consumer data in SaaS deployments is particularly challenging. For example, with a SaaS email system, all of the consumer organization's email is stored in CSP systems. There may not be an effective approach for the consumer to back up this email or extract it from the CSP's system. In SaaS, unless the provider offers a way to export the data, consumers have no means of independently backing up the

[10] "Amazon Glacier is a . . . durable, extremely low-cost cloud storage service for data archiving and long-term backup.https://aws.amazon.com/glacier/

data or migrating it to another application. As discussed previously, it's important to develop plans for extracting data from SaaS applications before adopting the service.

4.3.3 Prevent Disclosure of Deleted Data

While a cliché, the phrase "the Internet never forgets" is relevant to cloud-based storage. Cloud storage services replicate data to ensure persistence. As Figure 3 illustrates, during the course of system operation, sensitive data can find its way into logging and monitoring services, backups, content distribution services, and other places. When sensitive data must be deleted, or resources containing sensitive data are retired, the replication and spread of data through services during normal system operation must be considered.

Analyze the cloud deployment thoroughly to understand where sensitive data may have been copied or cached, and determine what must be done to ensure these copies are deleted. Some services may retain data for defined retention periods following deletion to prevent accidental loss of data. For these services, validate that the data is actually deleted following the retention period.

Data is ultimately stored on media such as magnetic or solid-state disks. These media devices can and do fail regularly and must be replaced. Even though the device itself has failed, consumer data still resides on the device. It is important to understand how the CSP handles storage media removed from production. AWS, for example, destroys all media removed from service. Other providers may choose to sanitize magnetic media using degaussing or other methods.

Encrypting data at rest, as described in Section 4.3.1, ensures that, even if data is not fully deleted or the storage media fails and is not destroyed or sanitized, the residual data is not usable.

4.3.4 Key Considerations

These are the key considerations for protecting data:

- Encrypt data at rest.
- Determine the criticality of data to business operations and ensure appropriate backups are performed.
- When removing data, delete the data from cloud storage services and all other cloud services that have copied or cached the data.

4.4 Monitor and Defend

Figure 4 illustrates the CSP and consumer responsibilities for monitoring when systems and applications are deployed to an IaaS or PaaS CSP.[11] Cloud deployment adds complexity to monitoring. To effectively monitor and defend cloud-deployed systems, consumers must learn to use monitoring information provided by the CSP, augment CSP monitoring information where necessary, analyze both cloud and on-premises monitoring data, and collaborate with CSP security operations staff to resolve incidents.

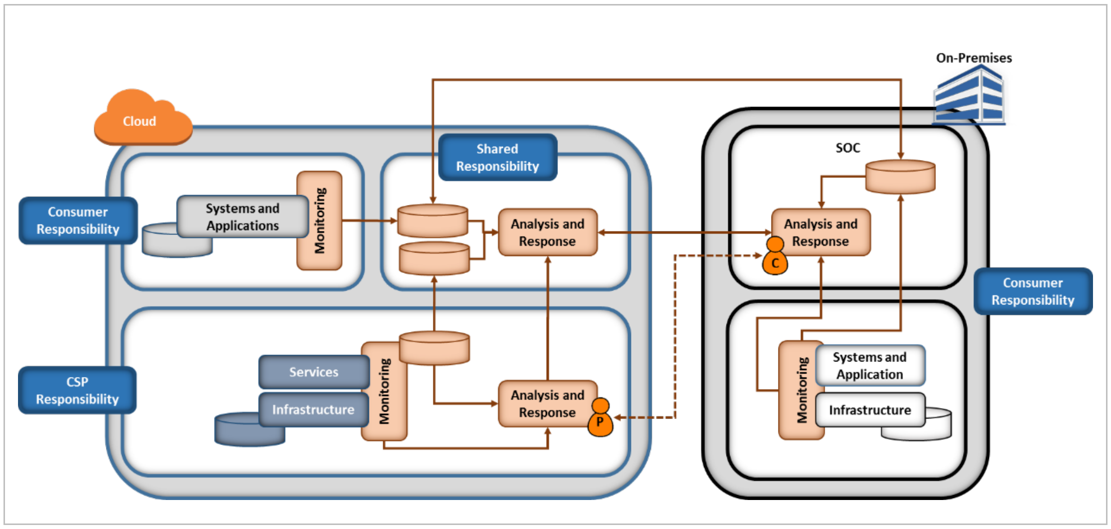

Figure 4: IaaS and PaaS Monitoring Responsibilities

4.4.1 Monitoring Cloud-Deployed Resources

The CSP is responsible for monitoring the infrastructure and services provided to consumers. The consumer is responsible for monitoring the systems and applications created using the provided services. A CSP builds significant instrumentation into its cloud services. A CSP needs this instrumentation to provide metered service, one of the five essential characteristics of cloud computing [Mell 2011], and to defend the infrastructure and services it operates.

From this instrumentation, the CSP provides monitoring information to the consumer that is related to the consumer's use of cloud services. This CSP-provided information is the first line of monitoring to (1) detect inappropriate or unauthorized access to or use of systems and applications, (2) detect unexpected behavior or use of the systems and applications, and (3) identify the users involved. For this monitoring to be effective, the consumer must profile his or her system, services, and data usage. Once a profile of normal operations is established from the CSP monitoring data, the consumer can use the CSP-provided monitoring information to identify unexpected or inappropriate activity.

[11] A SaaS deployment likely does not have consumer monitoring responsibility in the cloud. Instead, the consumer is responsible for analyzing data provided by the CSP and responding to inappropriate or unauthorized use.

Examples of services provided by CSPs to detect inappropriate or unauthorized access, unexpected behavior, and correlate users are below. Note that this is just a sampling of CSP tools available to perform monitoring and response.

Category	AWS Examples	Azure Examples
General Security	• AWS Security Hub • Amazon GuardDuty	• Azure Security Center • Azure Monitor logs
Identity and Access Management	• AWS IAM • AWS SSO • Amazon Cognito	• Azure Active Directory • Azure RBAC
Resource Configuration Monitoring and Evaluation	• AWS Config • AWS Security Hub • AWS CloudWatch	• Azure Advisor • Azure Monitor
User and API Activity Monitoring	• AWS CloudTrail • AWS Security Hub	• Azure Sentinel • Azure Security Center
Incident Response	• Amazon Detective • Cloud Endure Disaster Recovery	• Azure Sentinel • Azure Security Center • Azure Logic Apps • Log Analytics Workspace

AWS, for example, provides the CloudTrail service, which captures information on all AWS API calls within a consumer's AWS resources. CloudTrail records the action requested, who requested the action, and the result of the request. Tools for searching and examining CloudTrail records are also provided. AWS can deliver CloudTrail data to an S3 storage bucket where a consumer can use other tools, customer provided or commercially available, to further analyze the information. Monitoring and analyzing CloudTrail logs must be a routine part of operating AWS-deployed systems and applications.

Microsoft Office 365 provides audit log reports, through Security Center, that contain information on user and administrator activities in Exchange Online, SharePoint Online, OneDrive, and Azure Active Directory. These reports can be queried using tools in the Office 365 Security and Compliance center to look for unusual or suspicious activity related to a consumer's Office 365 services.

CSP-provided monitoring data is obviously different from the data collected in on-premises monitoring. Therefore, consumers must learn how to use the new data to defend their cloud-based assets. This involves understanding what the data means, determining what is normal for the cloud deployment, and learning to use tools provided by the CSP to detect anomalies. The SANS Reading Room contains a variety of short papers that address using CSP-provided data to effectively monitor cloud deployments. For example, a paper titled *Cloud Security Monitoring* explains how to use Splunk to ingest and analyze AWS CloudTrail data [Balakrishnan 2017].

Traditional security product vendors are also developing and selling virtual versions of their products that are already integrated with CSP services. These products can save time and are often already automation-aware. For example, Cisco has extended its on-premises Stealthwatch product to support AWS, Google Cloud Platform, and Microsoft Azure [Cisco 2019]. Stealthwatch uses CSP-provided monitoring data, such as CloudTrail in AWS, to develop models of cloud resources. Stealthwatch then uses these models to monitor resource behavior and detect suspicious activity.

CSPs are also beginning to automate some aspects of monitoring and detection. AWS offers the Macie service, which monitors access to data stored in S3 buckets, develops patterns of expected access, and provides alerts when accesses occur that are inconsistent with historic patterns [AWS 2019b]. Macie automates the determination of normal access patterns and eliminates the need for the consumer to monitor and analyze S3 accesses. Macie may have identified the unauthorized S3 access described in the unsecured AWS storage service risk example in Section 2.1. If Internet access to the S3 buckets were not routine, it would not be included in Macie's access model and could generate an alert when it occurred.

Google developed the Stackdriver service, which can analyze Google Cloud Platform monitoring data as well as AWS monitoring [Google 2019c]. Azure Sentinel uses automation and orchestration for data collection, detection, investigation, and response [Microsoft 2021c].

Consumers should focus on using CSP-provided monitoring tools and data. Consumers can augment CSP-provided monitoring data with monitoring of the systems and applications they operate using cloud services. Be aware, however, that monitoring approaches used on premises may not work in the cloud. For example, virtual routers do not provide virtual span ports that can see all network traffic.

Some on-premises techniques that do work in the cloud still may not be practical. The dynamic nature of cloud services, automatically scaling up and down horizontally, may confuse on-premises monitoring techniques. Consumers often must design and implement cloud application monitoring carefully to ensure it is fully integrated with cloud automation (e.g., autoscaling in IaaS) and can be scaled up or down without manual intervention. The SANS Reading Room offers CSP-specific advice and examples such as *Packet Capture on AWS* [Radichel 2017].

To help make network traffic capture and inspection easier for consumers, AWS and Google Cloud both offer VPC traffic mirroring [AWS 2019e, Google 2021b]. Azure offered a virtual network TAP preview that was put on hold, so consumers need to rely more on Microsoft partners that offer network packet brokers for Azure [Microsoft 2020b].

Although the Solorigate incidents were not detected quickly, once the command and control (C2) infrastructure began to be identified, indicators could be used to identify compromised organizations. However, some amount of the activity likely could have been detected through network traffic analysis and monitoring of crown jewels [Helming 2021].

If bastion hosts are used to manage privileged user access to operating systems and applications as recommended in Section 4.2.2, they can also provide monitoring data that augments CSP provided data. CSP data can show that a user connected to the bastion host. It can also show that the bastion host connected to an operating system instance or an application. It cannot show what the user did over the connection. The bastion host's log information, however, can show the commands that were performed by the user on the operating system or application.

4.4.2 Analyze Both Cloud and On-Premises Monitoring

With a hybrid cloud deployment that moves some resources to a CSP but retains many resources on premises, CSP-provided monitoring information, consumer cloud-based system and application monitoring information, and consumer on-premises monitoring information must be combined to create a complete picture of the organization's cybersecurity posture. Figure 4 shows a cloud-based monitoring and analysis enclave where all three monitoring data sources are combined.

While this enclave could be placed within the cloud or on premises, there may be advantages to a cloud deployment. First, as mentioned in Section 4.1.4, CSPs charge for data transfers into and out of their services. To encourage a continuing and potentially growing use of their services, CSPs often charge more for transfers out of the cloud than they do for transfers into the cloud. Therefore, depending on the volume of data involved, it may be cheaper to move data from on-premises monitoring into the cloud than it is to move cloud-based monitoring data out to an on-premises enclave.

Second, storage for large volumes of data may be cheaper in the cloud, especially storage for archived data that is being preserved but not actively used. Lastly, consumers can benefit from the inherent elasticity of the cloud, rapidly increasing analysis capacity when needed and decreasing capacity to save money when it is not needed.

Again, tools like Cisco Stealthwatch, mentioned previously, and other monitoring tools that can be deployed both on premises and in the cloud, may help analyze combined monitoring data. Other tools like Microsoft's Azure Sentinel, a cloud-native Security Information and Event Manager (SIEM), are designed to collect data from multiple clouds and on-premises sources.

4.4.3 Coordinate with CSP

The CSP is responsible for monitoring the infrastructure used to provide cloud services. That infrastructure could be physical servers, virtualization software, networks, and storage with IaaS, or entire applications with SaaS. Figure 4 shows a dashed line between the CSP's security analyst (P) and the consumer's security analyst (C).

The CSP may detect events that could adversely affect the consumer's applications. If so, the CSP informs the consumer and coordinates a response. Similarly, the consumer may detect adverse events and need CSP assistance to investigate. As with all aspects of cloud computing, responding to security events is a shared responsibility.

Learn to collaborate with the CSP to investigate and respond to security incidents. To collaborate effectively, the consumer must understand what information the CSP can share, how the information is shared, and the limits within which the CSP can provide assistance. The CSP cannot share information about another customer or provide assistance that would affect another consumer's use of services. Update standard operating procedures (SOPs) to include collaboration with the CSP. Monitor the CSP and other communication channels to identify when large incidents might be developing, as recommended on Microsoft's blog on Solorigate and zero trust principals [Weinert 2021], Microsoft's workbook on Solorigate risk [Weinert 2020], and FireEye's blog with links to Solorigate indicators [FireEye 2020a].

Finally, there are monitoring activities conducted on premises that should not be performed in the cloud without first consulting with the CSP. For example, conducting a vulnerability scan of cloud-based resources may look like an attack to a CSP. In response, the CSP may disable connectivity to the consumer’s resources until it contacts the consumer to resolve the issue. Such a situation could create a self-induced denial of service for the consumer. Consumers must understand what activities may look suspicious to the CSP and pre-coordinate these activities to avoid unnecessary response actions by the CSP.

As an example, Amazon’s Acceptable Use Policy prohibits “. . . attempting to probe, scan, or test the vulnerability of a System . . .” [AWS 2016]. However, Amazon also recognizes that organizations should conduct vulnerability scans and penetration testing of their infrastructure as part of a robust cybersecurity program. Therefore, Amazon provides a means for its customers to request permission to conduct this type of testing [AWS 2019g].

4.4.4 Key Considerations

Below are the key considerations for monitoring and defending cloud deployments:

- Use CSP-provided information and services as the primary cloud monitoring mechanism. Augment CSP capabilities only where necessary.
- Combine information from both cloud and on-premises monitoring to provide complete security situational awareness.
- Coordinate with the CSP to investigate and respond to incidents.
- Apply zero trust automation and real-time detection principles to mitigate unauthorized access.

5 Conclusions

Cloud services can provide equivalent or better security than most organizations achieve for their on-premises applications and data stores. To achieve these results, organizations must understand and meet their security responsibilities for using their CSP's services. While potential cloud consumers often worry about the security risk of trusting a CSP to perform some security functions, experience shows that security incidents are more often the result of consumers failing to use the security tools provided.

This report describes four important practices that cloud consumers should follow:

1. Perform Due Diligence
2. Manage Access
3. Protect Data
4. Monitor and Defend

A common theme across these practices is the need for cloud consumers to develop a deep understanding of the services they are buying and to use the security tools provided by the CSP. Incidents like the unsecured AWS storage servers, Deloitte email compromise, and OneLogin data breach would most likely have been avoided if the cloud consumers had used security tools such as zero trust security, correctly configured access control, encryption of data at rest, and multifactor authentication offered by the CSPs.

Cloud computing is a new approach to computing that uses some of the pieces and parts that make up on-premises computing. It is naïve and risky to assume that cloud computing works just like on-premises computing, can be secured using the same solutions used on premises, or is fully secured by the CSP.

Like any new technology or approach, using cloud computing effectively and securely requires knowledge and practice. For small and medium-sized organizations, use of well-established, mature CSPs also helps reduce the risks associated with transitioning applications and data to the cloud.

References/Bibliography

URLs are valid as of the publication date of this document.

[Abrams 2020]
Abrams, Lawrence. Ransomware Attackers Use Your Cloud Backups Against You. *Bleeping Computer.* March 3, 2020. https://www.bleepingcomputer.com/news/security/ransomware-attackers-use-your-cloud-backups-against-you/

[AWS 2011]
Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region. *AWS*. April 29, 2011. https://aws.amazon.com/message/65648/

[AWS 2016]
AWS Acceptable Use Policy. *AWS*. September 16, 2016. https://aws.amazon.com/aup/

[AWS 2017]
Linux Bastion Hosts on the AWS Cloud: Quick Start Reference Deployment. *AWS*. April 2017. https://docs.aws.amazon.com/quickstart/latest/linux-bastion/welcome.html

[AWS 2019a]
Amazon EC2. *AWS*. September 2021 [accessed]. https://aws.amazon.com

[AWS 2019b]
Amazon Macie. *AWS*. February 7, 2019 [accessed]. https://aws.amazon.com/macie/

[AWS 2019c]
AWS Quick Starts. *AWS*. September 2021 [accessed]. https://aws.amazon.com/quickstart/

[AWS 2019d]
IAM Best Practices. *AWS*. September 2021 [accessed]. https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

[AWS 2019e]
New – VPC Traffic Mirroring – Capture & Inspect Network Traffic. *AWS*. June 25, 2019. https://aws.amazon.com/blogs/aws/new-vpc-traffic-mirroring/

[AWS 2019f]
NIST Compliance on AWS. *AWS*. September 2021 [accessed]. https://aws.amazon.com/compliance/nist/

[AWS 2019g]
Simulated Event Testing. *AWS*. September 2021 [accessed]. https://aws.amazon.com/security/penetration-testing/

[AWS 2019h]

The AWS Cloud Adoption Framework. *AWS*. September 2021 [accessed]. https://aws.amazon.com/professional-services/CAF/

[AWS 2020a]

FedRAMP Overview. *AWS*. September 2021 [accessed]. https://aws.amazon.com/compliance/fedramp/

[AWS 2020b]

AWS Services in Scope by Compliance Program. *AWS*. September 2021 [accessed]. https://aws.amazon.com/compliance/services-in-scope/

[AWS 2020c]

Summary of the Amazon Kinesis Event in the Northern Virginia (US-EAST-1) Region. *AWS*. November 25, 2020. https://aws.amazon.com/message/11201/

[AWS 2021]

Multi-Factor Authentication. *AWS*. September 2021 [accessed]. https://aws.amazon.com/iam/features/mfa/

[Balakrishnan 2017]

Balakrishnan, Balaji. *Cloud Security Monitoring.* SANS Institute InfoSec Reading Room. 2017. https://www.sans.org/reading-room/whitepapers/cloud/cloud-security-monitoring-37672

[Baldwin 2021]

Baldwin, M.; Sharkey, K.; Prunella, K.; Mabee, D.; & Neira, B. *What is Azured Dedicated HSM?* Microsoft. March 25, 2021. https://docs.microsoft.com/en-us/azure/dedicated-hsm/overview

[Barr 2017]

Barr, Jeff. New Amazon S3 Encryption & Security Features. *AWS News Blog*. November 6, 2017. https://aws.amazon.com/blogs/aws/new-amazon-s3-encryption-security-features/

[Barth 2017]

Barth, Bradley. Sensitive DoD files found on unsecured Amazon server. *SC Media*. June 21, 2017.

[Blackbaud 2020]

Blackbaud. Security Incident. September 29, 2020. https://www.blackbaud.com/securityincident

[Blodget 2011]

Blodget, Henry. Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data. *Business Insider*. April 28, 2011. http://www.businessinsider.com/amazon-lost-data-2011-4

[Boulton 2017]

Boulton, Chris. Why Your Cloud Strategy Should Include Multiple Vendors. *CIO*. March 21, 2017. https://www.cio.com/article/3183504/cloud-computing/why-your-cloud-strategy-shouldinclude-multiple-vendors.html

[Chandramouli 2013]
Chandramouli, Ramaswamy; Iorga, Michela; & Chokani, Santosh. *Cryptographic Key Management Issues & Challenges in Cloud Services*. NISTIR 7956. NIST. 2013. https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7956.pdf

[Cisco 2019]
Cisco Stealthwatch Enterprise. *Cisco*. September 2021 [accessed]. https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html

[Coles 2019]
Coles, Cameron. "Only 9.4% of Cloud Providers Are Encrypting Data at Rest." *SkyHigh*. September 2021 [accessed]. https://www.skyhighnetworks.com/cloud-security-blog/only-9-4-of-cloudproviders-are-encrypting-data-at-rest/

[Comparecloud.in 2018]
Public Cloud Services Comparison. April 4, 2018. https://ilyas-it83.github.io/CloudComparer/

[Chaillan 2019]
Chaillan, Nicolas. *Continuous ATO.* Defense Acquisition University. August 16, 2019. https://media.dau.edu/media/Continuous+ATO/1_10jrntl6

[CSA 2018]
Cloud Security Alliance. 2018. https://cloudsecurityalliance.org/

[Dayley 2017]
Dayley, Alan; Liversidge, Jo; & Tay, Gavin. Plan Your Exit Strategy Before You Sign a SaaS Contract. *Gartner*. September 1, 2017. https://www.gartner.com/doc/3235417/plan-data-exit-strategy-sign

[Deprins 2020]
Deprins, Tom. *Cloud exit planning guidelines for financial services institutions.* Microsoft. November 23, 2020. https://cloudblogs.microsoft.com/industry-blog/financial-services/2020/11/23/cloud-exit-planning-guidelines-for-financial-services-institutions/

[DISA 2015]
Defense Information Systems Agency. *Best Practices for Department of Defense Cloud Mission Owners*. 2015. https://rmf.org/wp-content/uploads/2018/05/unclass-best_practices_guide_for_dod_cloud_mission_owners_FINAL.pdf

[EBF 2020]
European Banking Forum. *Cloud exit strategy – testing of exit plans.* June 4, 2020. https://www.ebf.eu/wp-content/uploads/2020/06/EBF-Cloud-Banking-Forum_Cloud-exit-strategy-testing-of-exit-plans.pdf

[Egan 2020]
Egan, D.; Kurmi, A.; Rich, P.; Roza, M.; & Schrock, M. *Key Management in Cloud Services.* Cloud Security Alliance. November 9, 2020. https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services/

[Faatz 2017]
Faatz, Don & Spina, Mari. *Cybersecurity in the Cloud: The Federal Landscape for Secure Cloud Services, Systems, and Solutions*. The MITRE Corp. 2017.

[FedRAMP 2020]
FedRAMP PMO. *FedRAMP Marketplace: Authorized Products*. September 2021 [accessed]. https://marketplace.fedramp.gov/#!/products?sort=productName

[FireEye 2020a]
FireEye Threat Research. *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*. December 13, 2020. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[FireEye 2020b]
FireEye (Mandiant). *Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452 (Version 1.0).* FireEye 2020. https://www.fireeye.com/content/dam/collateral/en/wp-m-unc2452.pdf

[Franz 2016]
Franz, Blake & Witoff, Rob. Audit Your AWS Account Against Industry Best Practice: The CIS AWS Benchmarks. *AWS re:Invent*. December 1, 2016. https://www.youtube.com/watch?v=3lkecchwxc4&feature=youtu.be

[Gartner 2016]
Gartner. 2017 Planning Guide for Identity and Access Management. Gartner, Inc. 2016.

[Goodin 2014]
Goodin, Dan. AWS Console Breach Leads to Demise of Service with "Proven" Backup Plan. *Ars Technica*. June 18, 2014. https://arstechnica.com/information-technology/2014/06/aws-consolebreach-leads-to-demise-of-service-with-proven-backup-plan/

[Google 2019a]
Build What's Next. *Google.* September 2021 [accessed]. https://cloud.google.com/

[Google 2019b]
Cloud Identity & Access Management. *Google*. September 2021 [accessed]. https://cloud.google.com/iam/

[Google 2019c]
Google Stackdriver. *Google.* September 2021 [accessed]. https://cloud.google.com/stackdriver/

[Google 2021a]
Migrating VMs with Migrate for Compute Engine: Getting Started. *Google.* April 8, 2021. https://cloud.google.com/solutions/migrating-vms-migrate-for-compute-engine-getting-started

[Google 2021b]
Google Packet Mirroring Overview. *Google.* March 15, 2021. https://cloud.google.com/vpc/docs/packet-mirroring

[GSA 2021]
Cloud Adoption. *GSA.* September 2021 [accessed]. https://coe.gsa.gov/coe/cloud-adoption.html

[Helming 2021]
Helming, Tim. Lessons Learned from SUNBURST for Threat Hunters. *DomainTools*. February 23, 2021. https://www.domaintools.com/resources/blog/lessons-learned-from-sunburst-for-threat-hunters

[Hopkins 2017]
Hopkins, Nick. Deloitte Hit by Cyber-Attack Revealing Clients' Secret Email. *The Guardian*. September 25, 2017. https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyberattack-revealing-clients-secret-emails

[Kovacs 2020]
Kovacs, Gail. Azure Backup: 5 Things to Think About Before You Backup on Azure. *NetApp Blog.* September 21, 2020. https://cloud.netapp.com/blog/5-considerations-before-you-backup-on-azure

[Leong 2021]
Leong, Lydia. *What Is the Risk of Actually Losing Your Cloud Provider?* Gartner, Inc. January 30, 2021. https://www.gartner.com/document/3996169?ref=solrAll&refval=283451208

[Massingham 2015]
Massingham, Ian. Advanced Security Best Practices on AWS. *AWS.* September 22, 2015. https://www.youtube.com/watch?v=zU1x5SfKEzs&t=806

[McGee 2020]
McGee, Marianne. Blackbaud Ransomware Breach Victims, Lawsuits Pile Up. *Information Security Media Group.* September 24, 2020. https://www.bankinfosecurity.com/blackbaud-ransomware-breach-victims-lawsuits-pile-up-a-15053

[Mell 2011]
Mell, Peter & Grance, Timothy. *The NIST Definition of Cloud Computing*. NIST Special Publication 800-145. 2011. https://csrc.nist.gov/publications/detail/sp/800-145/final

[Microsoft 2017]
Azure Active Directory Hybrid Identity Design Considerations. *Microsoft Azure.* July 18, 2017. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-hybrid-identity-designconsiderations-overview

[Microsoft 2019a]
Microsoft Azure Cloud Computing Services. *Microsoft Azure*. September 2021 [accessed]. https://azure.microsoft.com/en-us/?v=18.05

[Microsoft 2019b]
Azure Active Directory Seamless, Secure Identity and Access Management. *Microsoft Azure*. September 2021 [accessed]. https://azure.microsoft.com/en-us/services/active-directory/

[Microsoft 2019c]
Cloud Infrastructure and Management Services. *Microsoft.* February 7, 2019. https://www.microsoft.com/en-us/microsoftservices/Cloud-Infrastructure-and-Management-Services.aspx

[Microsoft 2019d]
Virtual network TAP. *Microsoft Azure.* April 14, 2019. https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-tap-overview

[Microsoft 2020a]
Compliance offerings for Microsoft 365, Azure Cloud Services, and other Microsoft services. *Microsoft*. September 2021 [accessed]. https://docs.microsoft.com/en-us/compliance/regulatory/offering-home

[Microsoft 2020b]
Backup cloud and on-premises workloads to cloud. *Microsoft Azure.* July 22, 2020. https://docs.microsoft.com/en-us/azure/backup/guidance-best-practices

[Microsoft 2021a]
Azure Status History. *Microsoft.* September 2021 [accessed]. https://status.azure.com/status/history/

[Microsoft 2021b]
Set Up Multi-Factor Authentication for Office 365 Users. *Microsoft*. March 24, 2021. https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/multi-factor-authentication-microsoft-365?view=o365-worldwide

[Microsoft 2021c]
Azure Sentinel. *Microsoft*. September 2021 [accessed]. https://azure.microsoft.com/en-us/services/azure-sentinel/

[Morrow 2019]
Morrow, Timothy & Faatz, Donald. *Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud*. CMU/SEI-2019-TR-004. Software Engineering Institute, Carnegie Mellon University. July 2019 (updated October 2020). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=551354

[Nichols 2017]
Nichols, Shaun. Yet Another AWS Config Fumble: Time Warner Cable Exposes 4 Million Subscriber Records. The Register. September 5, 2017. https://www.theregister.co.uk/2017/09/05/twc_loses_4m_customer_records/

[NIST 2004]
National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems*. FIPS PUB 199. 2004. https://nvl-pubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[NIST 2021]
National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication SP 800-53 Rev. 5. 2021. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[OneLogin 2019]
OneLogin Access – Unify Access Management Across All Your Apps. *OneLogin*. July 2021 [accessed]. https://www.onelogin.com/

[Quinn 2020]
Quinn, Corey. Multi-Cloud is the Worst Practice [blog post]. *Last Week in AWS*. August 2020. https://www.lastweekinaws.com/blog/multi-cloud-is-the-worst-practice/

[Radichel 2017]
Radichel, Teri. *Packet Capture on AWS*. SANS Institute InfoSec Reading Room. 2017.

[Ryan 2014]
Ryan, Mike & Lucifredi, Federico. *AWS System Administration Best Practices for Sysadmins in the Amazon Cloud*. O'Reilly Media. 2014. http://shop.oreilly.com/product/0636920027638.do

[Sanders 2021]
Sanders, Geoff. *Zero Trust Adoption: Managing Risk with Cybersecurity Engineering and Adaptive Risk Management*. SEI Blog. March 8, 2021. https://insights.sei.cmu.edu/blog/zero-trust-adoption-managing-risk-with-cybersecurity-engineering-and-adaptive-risk-assessment/

[SANS 2017]
SANS Institute. Cloud (In)Security Surprise. *SANS Newsbites* Volume XIX – Issue #76. 2017.

[Scanlon 2020]
Scanlon, Thomas & Laughlin, Richard. 7 Quick Steps to Using Containers Securely. *SEI Blog*. April 2020. https://insights.sei.cmu.edu/blog/7-quick-steps-to-using-containers-securely/

[Simorjay 2018]
Simorjay, Frank & Baldwin, M. Azure Security and Compliance Blueprint – PCI DSS-compliant Payment Processing Environments. *Microsoft Azure.* 2018. https://docs.microsoft.com/en-us/azure/security/blueprints/payment-processing-blueprintazure/security/blueprints/payment-processing-blueprint

[Snedeker 2017]
Snedeker, Ben. The Pros and Cons of Public and Private Clouds for Small Business. *Infusionsoft*. 2017. https://learn.infusionsoft.com/growth/planning-strategy/the-pros-and-cons-of-public-andprivate-clouds

[Weinert 2020]
Weinert, Alex. *Azure AD workbook to help you assess Solorigate risk.* Microsoft. December 22, 2020. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-workbook-to-help-you-assess-solorigate-risk/ba-p/2010718

[Weinert 2021]
Weinert, Alex. *Using Zero Trust principles to protect against sophisticated attacks like Solorigate*. Microsoft. January 19, 2021. https://www.microsoft.com/security/blog/2021/01/19/using-zero-trust-principles-to-protect-against-sophisticated-attacks-like-solorigate

[Whittaker 2017]
Whittaker, Zack. OneLogin Security Chief Reveals New Details of Data Breach. *ZDNet*. 2017. http://www.zdnet.com/article/onelogin-security-chief-new-details-data-breach/

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. **AGENCY USE ONLY**
(Leave Blank)

2. **REPORT DATE**
July 2019 (Updated September 2021)

3. **REPORT TYPE AND DATES COVERED**
Final

4. **TITLE AND SUBTITLE**
Cloud Security Best Practices Derived from Mission Thread Analysis

5. **FUNDING NUMBERS**
FA8702-15-D-0002

6. **AUTHOR(S)**
Timothy Morrow, Vincent LaPiana, Don Faatz, Angel Hueca, & Nathaniel Richmond

7. **PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. **PERFORMING ORGANIZATION REPORT NUMBER**
CMU/SEI-2019-TR-003

9. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

10. **SPONSORING/MONITORING AGENCY REPORT NUMBER**
n/a

11. **SUPPLEMENTARY NOTES**

12A **DISTRIBUTION/AVAILABILITY STATEMENT**
Unclassified/Unlimited, DTIC, NTIS

12B **DISTRIBUTION CODE**

13. **ABSTRACT (MAXIMUM 200 WORDS)**

This report presents four important security practices that are practical and effective for improving the cybersecurity posture of cloud-deployed information technology (IT) systems. These practices help to address the risks, threats, and vulnerabilities that organizations face in deploying or moving applications and systems to a cloud service provider (CSP).

The practices address cloud security issues that consumers are experiencing, illustrated by several recent cloud security incidents. The report demonstrates the practices through examples using cloud services available from Amazon Web Service (AWS), Microsoft, and Google.

The presented practices are geared toward small and medium-sized organizations; however, all organizations, independent of size, can use these practices to improve the security of their cloud usage. The focus here is on hybrid deployments where some IT applications deploy or move to a CSP while other IT applications remain in the organization's data center. Small and medium-sized organizations likely have limited resources; where possible, these practices describe implementation approaches that may be effective in limited-resource situations.

14. **SUBJECT TERMS**
Cloud-service provider, CSP, Amazon Web services, AWS, Microsoft Azure, Google

15. **NUMBER OF PAGES**
42

16. **PRICE CODE**

17. **SECURITY CLASSIFICATION OF REPORT**
Unclassified

18. **SECURITY CLASSIFICATION OF THIS PAGE**
Unclassified

19. **SECURITY CLASSIFICATION OF ABSTRACT**
Unclassified

20. **LIMITATION OF ABSTRACT**
UL