TOP 10 CLOUD SECURITY BEST PRACTICES

GLOBALSCAPE

"More companies are selecting cloud providers because they will

IMPROVE SECURTY."

–Ponemon, 2017 Global Cloud Data Security Study

The cloud buzz has yet to wear out its welcome, and rightly so. The ever-practical cloud means high utilization and a smooth ride for both the peaks and valleys in operational workloads. The cloud is a powerful tool in the business arsenal, and can easily help reduce overhead costs, enhance agility, and enable rapid deployments—within minutes for simple projects and within weeks for the more complex projects. Yet, with all of the obvious cloud benefits, there are still concerns circling around security and compliance support. However, those concerns have yet to slow the pace of cloud adoption.

These days, cloud security concerns influence **how** a business will transition to the cloud, not if. In this guide, we discuss how to approach security during your transition to a cloud platform.

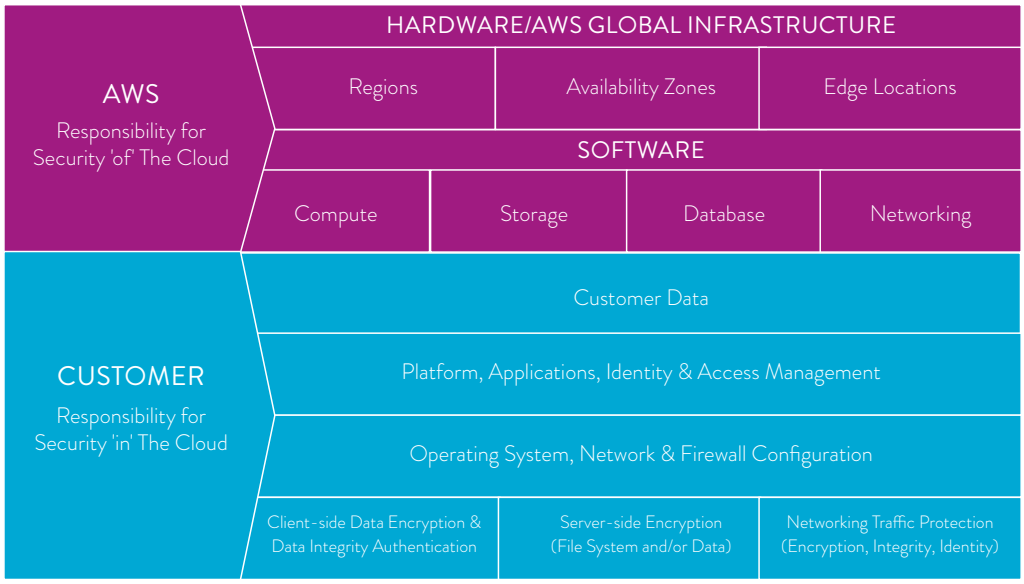
BEST PRACTICES

1. UNDERSTANDING THE SHARED RESPONSIBILITY MODEL

When it comes to determining who is responsible for what, there are different service-level agreements for every cloud service model and provider. There is not any one standard that covers the "shared responsibility model." It ultimately depends upon the cloud service and provider. AWS and Azure both have their own shared responsibility model, which determines what they are and are not responsible for in terms of security and compliance. Many cloud providers follow suit with AWS and Azure's definition of the shared responsibility model. (TechTarget)

In general, the enterprise is responsible for security management in a private cloud environment. There are some parts of the security and compliance requirements that the cloud provider owns in a public cloud offering. However, the customer owns the management of their overall security profile and hygiene.

AWS AND THE SHARED RESPONSIBILITY MODEL



(Source: Amazon)

SECURITY OF THE CLOUD

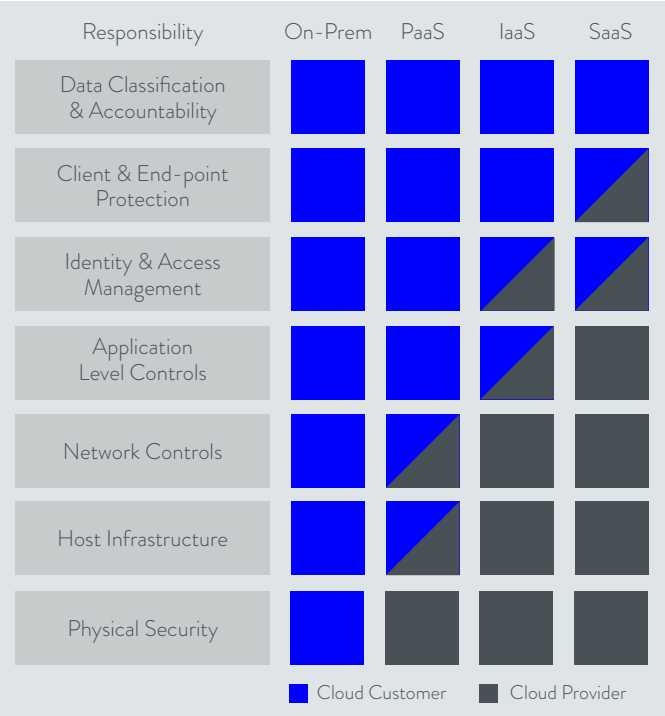
AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

SECURITY IN THE CLOUD

Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, services such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Virtual Private Cloud (Amazon VPC), and Amazon S3 are categorized as Infrastructure as a Service (IaaS) and, as such, require the customer to perform all of the necessary security configuration and management tasks. If a customer deploys an Amazon EC2 instance, they are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

(Source: Amazon)

AZURE AND THE SHARED RESPONSIBILITY MODEL



(Source: Microsoft)

This graphic describes which responsibilities belong to the cloud customer, and which belongs to the cloud provider, as described below:

- **For on-premises solutions,** the customer is both accountable and responsible for all aspects of security and operations.
- **For IaaS solutions**, the elements such as buildings, servers, networking hardware, and the hypervisor should be managed by the platform vendor. The customer is responsible or has a shared responsibility for securing and managing the operating system, network configuration, applications, identity, clients, and data.
- **PaaS solutions build on IaaS deployments**, and the provider is additionally responsible to manage and secure the network controls. The customer is still responsible or has a shared responsibility for securing and managing applications, identity, clients, and data.
- **For SaaS solutions**, a vendor provides the application, and abstracts customers from the underlying components. Nonetheless, the customer continues to be accountable; they must ensure that data is classified correctly, and they share a responsibility to manage their users and end-point devices.

(Source: Microsoft)

2. VETTING THE CLOUD PROVIDER

You have to ensure that you get a good understanding of your cloud provider. This includes the provider's:

- financial stability
- security hygiene
- methods and procedures
- certifications
- customer preferences
- service agreements

When using either AWS or Azure, it is also crucial that you to understand the shared responsibility model. This will help determine what they are responsible for and what you are responsible for when it boils down to security and compliance requirements.

3. IDENTITY AND ACCESS MANAGEMENT

Identity and access management are key components of your long and short-term security management strategy. They will help you govern and control application and data access. You can also better maintain a secure environment when your applications support multi-authentication, which will help you reduce unauthorized access, while also reducing the threat of username and password theft.

4. DEVELOP SECURITY POLICIES AND TRAINING (CLOUD-SPECIFIC AND BEYOND)

Your staff needs training on your internal security policies AND they need training on security best practices. They should be able to understand how to spot dangerous emails, how to create strong passwords, and how to avoid shadow IT. Establish guidelines on who can use cloud services and how to use it securely, without compromising the security of your IT infrastructure.

5. ENDPOINT SECURITY

The modern cybersecurity landscape has shifted with the growing rate of cloud adoption. If you want to have a strong system of defense against growing security risks, it is critical that your network has a robust level of network security, including firewalls, anti-malware, intrusion detection, access control, and more. Reducing your internal threats, like shadow IT, also helps to better secure potentially vulnerable endpoints.

You must have a clear view of your environment to better govern and control all activity within your purview. A managed file transfer (MFT) platform can help mitigate potential endpoint vulnerabilities by providing you with a centralized platform for easier access and operational visibility. In turn, you can identify security vulnerabilities before they become a bigger challenge.

If you want to have a strong system of defense against growing security risks, it is critical that your network has a robust level of network security, including firewalls, anti-malware, intrusion detection, access control, and more.

As a whole, securing data at rest or in transit takes a proactive and robust strategy.

6. DATA ENCRYPTION, AT REST AND IN TRANSIT

Data in transit refers to data being in motion. Whereas data at rest refers to data that is stored on a device or network, and is not actively moving from one location to another. The risk factor for either data at rest or in transit largely depends on the security measures in place for either state. Encryption and key management services are important aspects to consider when evaluating cloud providers. If they offer encryption, you need to ensure that it will work seamlessly with your existing processes, in turn eliminate your need to require end users to comply with encryption policies by taking on additional actions.

When securing data in transit, many organizations will encrypt sensitive data before allowing it to move from one location to another. In many cases, they will use various encrypted connections such as HTTPS, SSL, TLS, FTPS, or SFTP, to ensure the security of data in transit. While data is at rest, many organizations encrypt their data prior to storage or they encrypt their storage drive.

As a whole, securing data at rest or in transit takes a proactive and robust strategy. For many, that includes the security supporting controls of an MFT platform, security policies and training, data protection solutions that categorize and classify data wherever it resides (systematically triggering the appropriate protections), and much more.

7. INTRUSION DETECTION AND PREVENTION

On premises or in the cloud, a multi-layered approach to security will provide the most reassurance and protection. Consider looking for solutions that support both environments and help to identify when an attack has happened and how to stop an attack in progress. If your environment is disparate or siloed, if you lack a centralized platform to manage your environment, and if you lack the appropriate tools and strategy, it will be difficult to detect and prevent an intrusion.

Cloud platforms like AWS and Azure often have their own security services that customers can add to a cloud platform product. These include intrusion detection and prevention systems, most of which can be preconfigured to their virtual devices and appliances. In the case of a public cloud platform and customer-owned environment, where more control is needed, SSH or HTTPS can be used within a system of management like an MFT platform.

8. COMPLIANCE REQUIREMENTS

Reviewing your cloud provider's solution and compliance requirements will be critical to determining whether or not the platform will help meet your data security needs or get in the way. This means following all of the listed security best practices, from the shared responsibility model and beyond. At the same time, you also need to be clear about what data you're storing and where it will be stored to ensure that everything is managed within your security and compliance requirements. The following are also critical requirements:

- High encryption standards at rest and in transit
- Data and cloud access controls set to deter attacks, with patches and fixes quickly installed
- Compliance monitoring including audits, an accurate record of log retention
- Firewall compliance rules and standards

9. CONDUCT AUDIT AND PENETRATION TESTING

How secure is your existing environment? Is it enough to protect your data and applications? A data audit and penetration test will help you identify vulnerabilities within your environment. The testing evaluates various areas of security, from the physical technologies and personnel, to the network. Regular audits are crucial to ensuring your current security profile. Conducting an audit will help you evaluate a cloud vendor's capabilities. Penetration testing is considered "ethical hacking," and helps security personnel identify different levels or risk and vulnerabilities.

After you have completed your data audit and penetration testing, you should be able to identify where your potential security vulnerabilities may be within your own environment and within a potential cloud vendor.

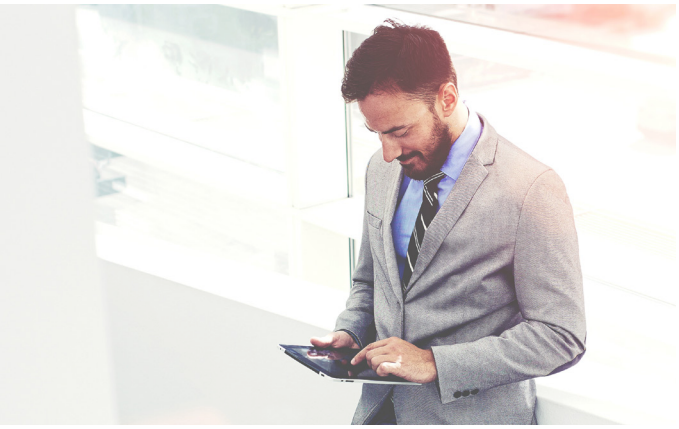
10. UNDERSTAND THE CLOUD PLATFORM

Moving your applications to the cloud requires you to learn new technologies and best practices. The technologies and techniques you have used to manage and secure your on-premises deployments will certainly change when moving to the cloud. While cloud technologies are similar from the various cloud vendors, each one has its own idiosyncrasies that require a certain level of expertise. It is important to train your existing personnel or hire cloud expertise to achieve the business goals your company has set forth.

HOW MFT MAKES YOUR MOVE TO THE CLOUD MORE SECURE

A managed file transfer (MFT) solution provides a centralized and efficient platform to help you maintain the control and security you need to manage your environment from within and beyond the cloud. Here are a few practices that MFT help an MFT platform manage a secure and efficient cloud environment:

- Complex workflows are more efficient and protected
- Compliance requirements are easier to meet
- Segments users into groups in order to reduce shadow IT practices
- Provides an audit and report environment with advanced features
- Limits inefficient manual processes with automation
- Protects data in transit and at rest



EFT ARCUS: YOUR CLOUD STRATEGY'S SECRET WEAPON

EFT Arcus is a SaaS MFT platform developed with the multi-layered security standards of an on-premises platform, combined with the cost-savings and flexibility of the cloud. Whether you are moving all or part of your IT infrastructure to the cloud, EFT Arcus provides a proactive way to support your data security and workflow requirements. A variety of safeguards is available with our SaaS MFT platform, including:

- Encryption
- Secure protocols
- Password policies
- Strong ciphers
- Integration with virus scanners
- Integration with data loss prevention (DLP) tools

The cloud infrastructure required to properly secure data is absolutely critical and should be very carefully vetted by any company before putting data in the cloud. That is why Globalscape uses AWS and Azure as they have gone through extensive design and vetting to ensure the highest levels of security and compliance – levels that the typical enterprise cannot afford to do themselves. Once the right cloud infrastructure is chosen, companies benefit from substantially greater security, reliability, and resiliency, giving it a substantial competitive edge. In addition to security, they also enjoy operational cost reductions, because they no longer have to maintain complex networking environments. For most companies, provided they do their vetting to allay their fears, it is a win-win.

Don't take our word for it. **Try EFT Arcus Today!**

MAKE BUSINESS FLOW BRILLIANTLY

Globalscape, Inc. (NYSE MKT: GSB) is a pioneer in securing and automating the movement and integration of data seamlessly in, around and outside your business, between applications, people and places, in and out of the cloud. Whether you are a line-of-business stakeholder struggling to connect multiple cloud applications or an IT professional tasked with integrating partner data into homegrown or legacy systems, Globalscape provides cloud services that automate your work, secure your data and integrate your applications – while giving visibility to those who need it. Globalscape makes business flow brilliantly. For more information, visit **www.globalscape.com** or follow the blog and Twitter updates.

GlobalSCAPE, Inc. (GSB)
Corporate Headquarters
4500 Lockhill-Selma Rd, Suite 150
San Antonio, TX 78249, USA
Sales: 210-308-8267 / Toll Free: 800-290-5054
Technical Support: 210-366-3993
Web Support: www.globalscape.com/support

GLOBALSCAPE