STATE OF CLOUD SECURITY 2018

CLOUD SECURITY ALLIANCE
GLOBAL ENTERPRISE ADVISORY BOARD
© 2018 Cloud Security Alliance – All Rights Reserved

All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at https://cloudsecurityalliance.org/download/state-of-cloud-report/ subject to the following: (a) the draft may be used solely for your personal, informational, non-commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.
The Cloud Security Alliance Global Enterprise Advisory Board, founded in 2016, is a collection of leading experts from large multinational companies representing over 10 unique industries. This board has been constituted to represent the point of view of large IT end users, and to articul the perspective of the consumers of cloud computing related to the topic of information security. The goal of the Global Enterprise Advisory Board is to increase enterprise collaboration on cloud technologies that enable businesses by adopting secure practices and techniques. These efforts intend to encourage cloud service providers to meet the security and privacy expectations of the end user and encourage regulators to keep up with new technologies and features that help meet and evolve regulatory compliance. The report issued by this board is among a number of activities designed to raise awareness of cloud computing security and the importance of enterprise end user collaboration.

The quality of IT systems and their inherent security capabilities are related to the demands of the sophisticated consumers from large enterprises and the agenda they set for the industry. We hope your primary takeaway from this report is that the state of cloud security is a work in progress and that it is incumbent upon the cloud user community to collaborate and speak with an amplified voice to ensure that their key security issues are heard and addressed. We welcome your feedback to this report and encourage you to follow our activities as we outline what needs to happen to speed up the secure cloud adoption process between the enterprises, cloud service providers, and regulators.

Web https://cloudsecurityalliance.org/geab
Email geab@cloudsecurityalliance.org
Twitter @csageab

Vinay Patel Citi Infrastructure, Chair
Niall Casey Johnson & Johnson
Pete Chronis Turner
Gurdeep Kaur Horizon Blue
Vjay LaRosa ADP
Michael Panico Disney
Marisa Ruffalo Chevron
Joe Zacharias Caterpillar
Table of Contents

Foreword
Table of Contents
Introduction
Adoption of Cloud and Related Technologies
What Are Providers Doing About Security?
What Are Enterprises Doing About Security?
The Threat Landscape Is Changing
Working With Regulators
Industry Skills Gap
Summary
About the Cloud Security Alliance (CSA)
Introduction

Innovators and early adopters have been using cloud for years taking advantage of the quicker deployment, greater scalability, and cost saving of services. The growth of cloud computing continues to accelerate offering more solutions with added features and benefits, including security. In the age of information digitalization and innovation, enterprise users must keep pace with consumer demand and new technology solutions ensuring they can meet both baseline capabilities and security requirements.

This paper provides insights into some of the latest cloud practices and technologies enterprise information security practitioners must be aware of as IT and sensitive data extends beyond the traditional corporate perimeter. Providers, regulators, and the enterprise must cooperate to establish baseline security requirements across these services. Understanding the use of cloud and related technologies along with the roles and responsibilities of data security and ownership up front will improve the procurement and long-term management of these services.

Adoption of Cloud and Related Technologies

Enterprises are often overwhelmed with the breadth, scope, and availability of cloud services available today. The Infrastructure-as-a-Service (IaaS) landscape is dominated by the three major providers and their services often overlap with Platform-as-a-Service (PaaS) offerings. New capabilities further decouple hardware and software capabilities. “Serverless” and “Function-as-a-Service” offerings allow users to build their applications and rely on the providers to completely manage and provision the allocation of server compute resources. Additionally, the Software-as-a-Service (SaaS) market has expanded offering new products to help address data, security, network, and identity challenges. Furthermore, services such as Cloud Access Security Broker (CASB), Software Defined Perimeter (SDP), and Managed Security Service Provider (MSSP) create new operational complexities as they attempt to manage beyond the traditional corporate perimeter.
As IT budgets in security have increased over the past two years and project continued increases in the next five years, these services needed to be researched and shared among enterprise users to understand their functions and how to implement them securely. Many cloud services contain native security controls that help companies improve their security posture by adding security controls not met in traditional environments and eliminating redundant controls and overlap in traditional security services. Planning ahead to research, test, roll out and train users on these these native security controls is absolutely necessary to maximize security gains.

The use of cloud services is being leveraged in many innovative ways. Both consumers and enterprises are taking advantage of new emerging technologies that leverage cloud capabilities. Internet of Things (IoT) devices extend the edge of computing allowing the collection and analytics of data in the field. Artificial Intelligence (AI) offers greater analytics and application of machine-learned functions to data. Blockchain technology applies transparent and secure messaging and ownership of transactions. Application containers and microservices introduce architectures that leverage secure, agile development and communication in engineering operations. Cloud has opened the door to these and other related technologies. Exploring case studies and potential use cases will be important to keep pace with market adoption and creating secure industry best practices.

Establishing small projects for emerging technologies ensures familiarity with new technologies and how they integrate with existing IT infrastructure and tools. Sharing successes and challenges with industry partners allows adopters to build patterns of functionality and security into each project that can scale into larger workloads and across the industry. Collaboration within industry partners and providers will ensure that baseline security requirements are met by all partners in the cloud supply chain.

1. https://www.gartner.com/newsroom/id/3836563
What Are Providers Doing About Security?

Increased adoption in cloud services has followed consumer confidence with the security of cloud providers. As providers invest in the security of their platforms, a McAfee survey showed complete trust in public cloud offerings increased 76 percent in 2017. But trust should also be evidence-based. Providers are addressing security in the cloud with self assessment and third-party tools like the CSA STAR program, ISO 27000-series certifications, and the FedRAMP authorization program. These platforms leverage security controls and countermeasures to cloud specific risks. Reviewing common sets of controls allows providers to be assessed over common criteria for consistent evaluation.

Security for cloud providers also falls into their ability to quickly detect, contain, and mitigate an attack. Cloud providers prioritize their ability to respond to threats by participating in cyber information sharing programs. These threat intelligence exchanges allow ease of sharing between the smallest and largest providers. Threat actors shared from the smallest providers can prevent breaches in large providers. These practices are being standardized and open to larger communities including enterprises. As adversaries collaborate quickly to evolve their attacks, the information security community needs to respond as swiftly with collaboration in threat intelligence exchanges across industries and with both providers and enterprise send users. This helps everyone maintain standard security solutions.

As the threat landscape evolves, providers continue to add new features into their platforms to address the latest concerns. Security and configuration features are introduced at a rapid pace but should be well communicated with the end user. Trainings videos and manuals may not be enough as enterprises are using multiple cloud services and can't keep up. To help enterprises battle against the technology sprawl of features, the aim needs to be towards safe and secure default configurations and ensuring the proper use of new features. Any breach of a service, even due to user error, can negatively impact customer trust and reliability of a product. User interface and behavior should be just as important as the features themselves.

2. Building Trust in a Cloudy Sky: The state of cloud adoption and security
3. https://cloudsecurityalliance.org/star
5. https://www.fedramp.gov/
What Are Enterprises Doing About Security?

Cloud adoption and migration present separate challenges for security. Adopting cloud services still requires enterprises to meet compliance requirements with their new cloud service providers. The shared responsibility model delineates which security controls are owned by the cloud provider and/or enterprise. Meeting these security requirements help demonstrate compliance requirements for the enterprise. This type of shared security model is encouraging enterprises to move more business critical workloads, such as Enterprise Resource Planning or ERP, to the cloud.

Many enterprises are moving to the cloud for its robust capabilities, including security. To maximize security benefits, there is still a need to adjust and evolve workloads to fully take advantage of the cloud platform. Enterprises already maintain security postures for on-premises workflows but these approaches cannot simply be applied to the cloud. Migrating workload involves understanding how to properly re-architect to cloud services and is key to building security and taking advantage of cloud native tools. Development and deployment lifecycles using Dev(Sec)Ops approaches with microservices, application containers, and immutable architectures emphasize the characteristics and nature of the cloud. The use of automation increases our ability to build projects and add security into the development process. These tools are centralized on the cloud management plane and can help the enterprise limit exposure to attacks by securing the APIs and leveraging the security of cloud platforms. While new applications can be easier to build in the cloud and leverage cloud native tools, migrating legacy workloads and applications can be much more complex, leading to breaking down workloads into smaller parts and using multiple cloud services for proper security and reliability.

Threat intelligence sharing should not be restricted to service providers. Enterprise traffic is exposed to both blanket and targeted attacks. These common threat actors and indicators of compromise can be shared within enterprises and the provider ecosystem to discover the source of the attack and mitigation techniques. It will be important to have a collaborative effort and standardized approach on what to share, how to share, and who to share with in order to effectively correlate and mitigate threats. Information sharing works best if there is collaboration between sharing incidents, understanding procedures, and deploying tactics between targeted parties.
The enterprise needs to understand and evaluate all the risk factors involved with migration, provisioning, and adopting cloud services. A staged approach on migrating sensitive data and critical applications is recommended. If done properly, cloud can enable data categorization to add visibility, scale, and automation to a previously manual process. Proper training and education on cloud services being used allows enterprises to architect properly and take advantage of cloud native tools and security. At the end of the day, critical data in the cloud should be protected with the implementation of security controls by both the cloud provider and the enterprise.

The Threat Landscape is Changing

Cyber attacks and breaches are making headlines everyday. The enterprise is expected to stay up to date and protect against the latest threats, risks, and vulnerabilities. Ransomware attacks like WannaCry affected over 250,000 computers in 2017. Additionally, Bad Rabbit, Petya, and Not Petya also stormed the industry in 2017. Distributed-Denial-of-Service (DDOS) attacks like the one on Dyn DNS affected over 70 major online services. Other malware like the Mirai botnet in 2016 was responsible for multiple DDOS attacks on credible sites due to unsanitary security practices. Misconfigured cloud services such as the S3 bucket leaks by Alteryx\(^7\) that exposed information on 123 million Americans and one at Verizon\(^8\) impacting 6 million individuals. Meltdown and Spectre vulnerabilities exploited almost every modern processor to leaky data and passwords.

The enterprise needs to train employees on basic security practices. Avoiding phishing attacks and proper password management practices can prevent many of the malware attacks such as ransomware and DDOS. Faster response and implementation of security patch and Common Vulnerability and Exposure (CVE) response mechanisms should be refined to protect against these types of malware. Cloud providers also need to have transparency with their patching mechanism response time and coordinated disclosure with enterprise customers.

With these latest threats, enterprises need to have awareness, know how they impact business, and have mitigation plans and techniques ready. Sharing intelligence across the industry is one way but also having references and security best practices examples like the CSA Top Threats Report, Verizon Data Breach Investigations Report, and the OWASP Top Ten Reports help enterprises build preventative, detective, and corrective mitigation.


Working With Regulators

When meeting regulatory compliance, it is important for enterprises to practice strong security fundamentals to demonstrate compliance rather than use compliance to drive security requirements. Security controls need to be malleable to include new technologies and practices while still meeting regulatory security requirements.

Awareness and preparation for privacy is also on the rise. Any organization holding customer data must consider enhancing their privacy policies, in particular towards EU citizen data according to the new European General Data Protection Regulation or GDPR. Every partner in the supply chain controlling or processing this data will need to comply with GDPR privacy requirements. Architectures, technology solutions, and practices for privacy will need to be implemented to ensure that all parties in the supply chain meet these expectations. Regulators and those enforcing these new principals need to provide clear understanding and direction so that those responsible can properly use and protect customer data.

Education and training of new technologies and provider capabilities should be a partnership between the enterprises, regulators, and providers. Regulations can then evolve together with the secure use of technologies, such as cloud, to provide better security and privacy practices for all. Industry organizations can support education to regulators on cloud solutions and technologies that drive security and meet compliance requirements.
Industry Skills Gap

Several studies estimate there are at least one million unfilled cybersecurity jobs. According to the Cybersecurity Ventures 2017 Cybercrime Report,⁹ this number is predicted to triple by 2021. A lack of qualified applicants is the primary reason for this gap. Information security professionals who are employed face tremendous challenges in keeping their skills current in the face of the accelerating pace of change catalyzed by cloud that is altering the security industry around them. The proper use of new technologies and existing solutions can aid today's security practitioners. Our security education ecosystem needs to be greatly expanded, which will enhance the opportunities for today's security industry professionals.

We need to focus on generating more qualified professionals in the information security field and improving the skillsets of the existing professionals in particular around cloud technologies.


Summary

Technology is moving faster than the business' set of skills to adopt them. As organizations react to this demand to stay competitive, secure adoption of these technologies becomes an even greater challenge. With cloud and new IT technologies, the supply chain ecosystem needs to collaborate so that large enterprises and regulators can understand how to securely adopt new technologies and new features on existing provider technologies. Each party must play a role in securing customer data and sharing best practices for secure operations.

Education and awareness still needs to improve around provider services and new technologies for the enterprise. Small-scale adoption projects need to be shared so that security challenges and patterns can be adopted to scale with the business and across industry verticals. This skills gap, particularly around cloud and newer IT technologies, needs to be met by the industry through partnership and collaboration between all parties of the cyber ecosystem.
About the Cloud Security Alliance (CSA)

The CSA is the world’s leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA’s activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.