Clouds Are Secure: Are You Using Them Securely?

Refreshed 7 October 2019, Published 31 January 2018 - ID G00350439 - 16 min read

FOUNDATIONAL This research is reviewed periodically for accuracy.

By Analysts Jay Heiser

Initiatives:Cloud Computing

CIOs need to ensure their security teams are not holding back cloud initiatives with unsubstantiated cloud security worries. Instead, they should encourage their teams to apply imagination and energy to develop new approaches to securely and reliably leverage the benefits of SaaS, PaaS and IaaS.

Overview

Key Challenges

- Many organizations are paying an opportunity cost by allowing unwarranted fears about security to inhibit their use of public cloud services.
- Disproportionate attention to the cloud service providers' (CSPs') security posture has negatively impacted security by distracting attention away from the establishment of cloud control, visibility and auditing processes.
- Organizations that haven't taken a strategic and carefully governed approach to the use of cloud computing can easily use it in a manner that is less secure than traditional computing, resulting in unnecessary compliance incidents and data leakage.

Recommendations

CIOs responsible for cloud computing:

- Develop an enterprise cloud strategy, including guidance on what data can be placed into which clouds and under what circumstances.
- Implement and enforce policies on cloud ownership, responsibility and risk acceptance by outlining expectations for form, significance and control of public cloud use.
- Follow a life cycle approach to cloud governance that emphasizes the operational control of your virtual enterprise of SaaS-, PaaS- and IaaS-based services.
- Develop organizational expertise in the implementation and control of each of the cloud models you will be using.

- Implement central management and monitoring planes to overcome the inherent complexity of multicloud use.

Strategic Planning Assumption

Through 2022, at least 95% of cloud security failures will be the customer's fault.

Introduction

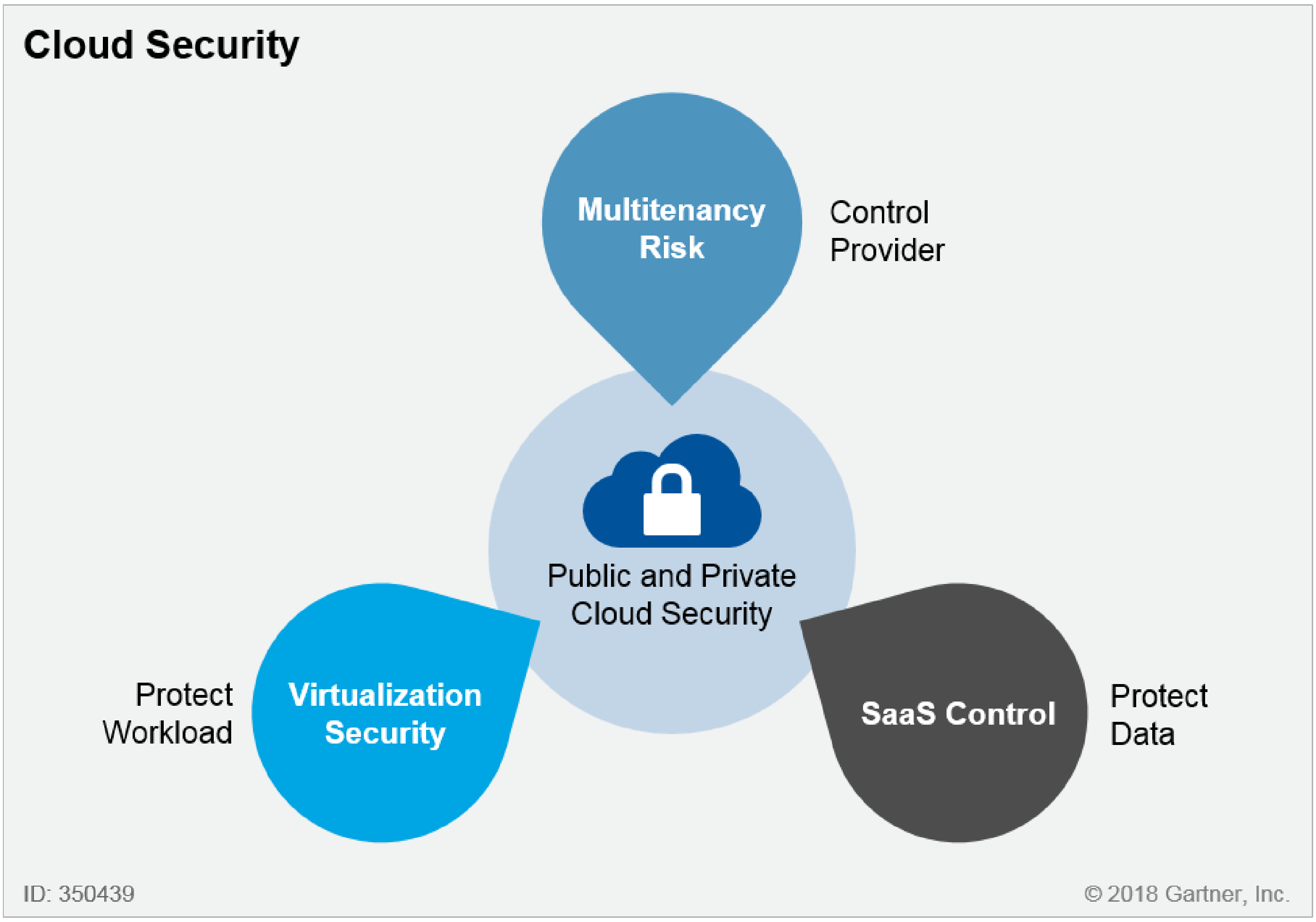
Multiple news stories have demonstrated that information can leak out of clouds. [1] However, these examples demonstrate that it is almost always users, not the cloud provider, who fails to manage their controls to protect their data. Clouds are secure, but organizations are often not using them securely. Unfortunately, it can also be the case that exaggerated fear about the security of clouds can result in lost opportunity and inappropriate spending.

The recent history of public clouds has demonstrated that brand-name, multitenant public cloud services are highly resistant to attack, providing a more secure starting point than most traditional in-house implementations. [2] The cloud business model and the realities of internet visibility provide huge market incentives for service providers to put a higher priority on security than is typical of end-user organizations. This includes physical security, their technical and process approach, and their undertaking of formal third-party security evaluations, such as International Organization for Standardization (ISO) 27001, Service Organization Control (SOC) 2 and Federal Risk Authorization and Management Program (FedRAMP). The top cloud services use purpose-built technology enabling them to avoid many of the security vulnerabilities typical of in-house services and applications. They leverage experienced system and vulnerability managers, and their economies of scale make it practical to provide around-the-clock security monitoring and response. It isn't just end-user organizations that find security benefits in the public cloud. Most SaaS offerings are based on some other cloud provider's infrastructure as a service (IaaS) or platform as a service (PaaS). This allows the SaaS provider to concentrate on the features and security of their applications, without having to worry about the security of the data center OS or database.

Unfortunately, much of the IT world continues to operate under a counterproductive misconception about the relative security posture of public clouds — namely that shared cloud infrastructure is inherently risky. Such flawed assumptions unnecessarily reduce the ability to take full advantage of the cost savings and agility of commercial cloud services. Ironically, avoidance of cloud services may even lead to unnecessary security risks, as organizations continue to rely on poorly managed in-house systems that often have more security vulnerabilities than their public cloud equivalents.

The parts of the stack under customer control can make public cloud computing a highly efficient way for inexperienced users to implement poor practices, which can easily result in security or compliance failures (see "Staying Secure in the Cloud Is a Shared Responsibility"). The most commonly reported forms of cloud security incidents involve open shares, in which someone deliberately makes sensitive data available to outsiders, a mechanism that is ubiquitous in both IaaS and SaaS. The safe use of all forms of public cloud requires new organizational policies, skills and activities. No technologies — on-premises or in the public cloud — can ever be considered 100% secure or reliable — especially when users and IT staff are provided a new capability with no guidance on its use or management. The Gartner clients that are having the most success in rising to the cloud control challenge have explicitly organized themselves around the unique considerations of IaaS workload security, SaaS control, cloud configuration management and cloud service provider (CSP) management, developing new skills in each of these areas (see Figure 1).

Figure 1. Cloud Security Overview



Source: Gartner (January 2018)

Analysis

Develop an Enterprise Cloud Strategy

Organizations without a strategic approach to the use of public cloud services unnecessarily constrain themselves, resulting in tactical approaches to security and governance that inadequately address cloud risks. The most significant step an organization can take to ensure appropriate levels of cloud security is for the corporate leadership to agree that cloud computing has become indispensable, and that it should be governed through planning and policy (see "Your Cloud Strategy Needs to Be Bimodal"). The Gartner clients that have made explicit executive decisions on their cloud strategy are providing far more guidance to the business — and IT —

including better requirement analysis, more sophisticated architectural planning and flexible risk acceptance processes. A structure can and should be put in place to ensure the safe and legal ongoing use of public cloud services, especially given the growing significance of General Data Protection Regulation (GDPR) and other regulations. Gartner clients are exploring cloud contingency planning earlier and more often (see "Designing a Public Cloud Exit Strategy").

Because cloud strategies usually lag behind cloud use, most organizations have a large amount of unsanctioned, and even unrecognized, public cloud usage. Especially when sensitive or regulated data is involved, unapproved clouds represent an unnecessary risk exposure. When unapproved external services support mission-critical processes, it means an undesirable exposure to continuity and vendor risks. Corporate data may be trapped inside an inflexible service that cannot meet future needs or, worse, be held by a relatively small provider teetering on the edge of bankruptcy (see "A Public Cloud Risk Model: Accepting Cloud Risk Is OK, Ignoring Cloud Risk Is Tragic"). It is equally counterproductive to set cloud supplier standards so high that few, if any, CSPs are able to meet them.

Without an enterprise strategy outlining the organizational expectations for the form, significance and control of public cloud use, chief information security officers (CISOs) and other IT leaders feel that they lack the mandate to influence, let alone constrain, the use of public clouds on the part of business units. Fortunately, a growing number of Gartner clients are undertaking top-down strategic approaches. Driven by the CIO, chief technology officer (CTO) or chief digital officer, and led by IT strategy, architecture or business solution functions, a cloud strategy provides guidance on how upcoming purchases should be conducted and what should be done about the security and control of current and future public cloud services (see "Developing Your SaaS Governance Framework").

Implement and Enforce Policies on Cloud Ownership, Responsibility and Risk Acceptance

No organizational process can be reliably undertaken, and no enterprise asset will be reliably used, unless responsibility is explicit and enforced. The foundational policy underlying the controlled use of public cloud services is ownership. If somebody wants to undertake the use of a public cloud service that is not supported by corporate IT, then their business unit manager must explicitly accept the ownership of that service. That includes responsibility for demanding compliance with the relevant policies, personal acceptance of the associated risks, and, if necessary, additional budget for security and compliance controls. It should be no surprise when IT leaders recommend against the use of cloud computing if they expect that management will avoid taking responsibility for compliance. It is unreasonable to expect the CIO or CISO to accept the full implications for the use of services that they did not choose and have no ability to control, especially when their traditional security and management tools lack visibility.

Efficient and noncontentious decisions about the risk acceptability of new public cloud services and use cases are best-accomplished through some structure, including a defined security requirement process. A risk-based acceptance process that starts with a concept of data sensitivity or use-case criticality enables cloud security specialists to concentrate their time and energy on the most critical and business-useful situations (see "How to Evaluate Cloud Service Provider Security"). Requests for cloud use that are neither sensitive nor critical should require little or no risk assessment effort. Just saying "no" as the routine response for requests to approve cloud use is counterproductive and no longer acceptable in most organizations.

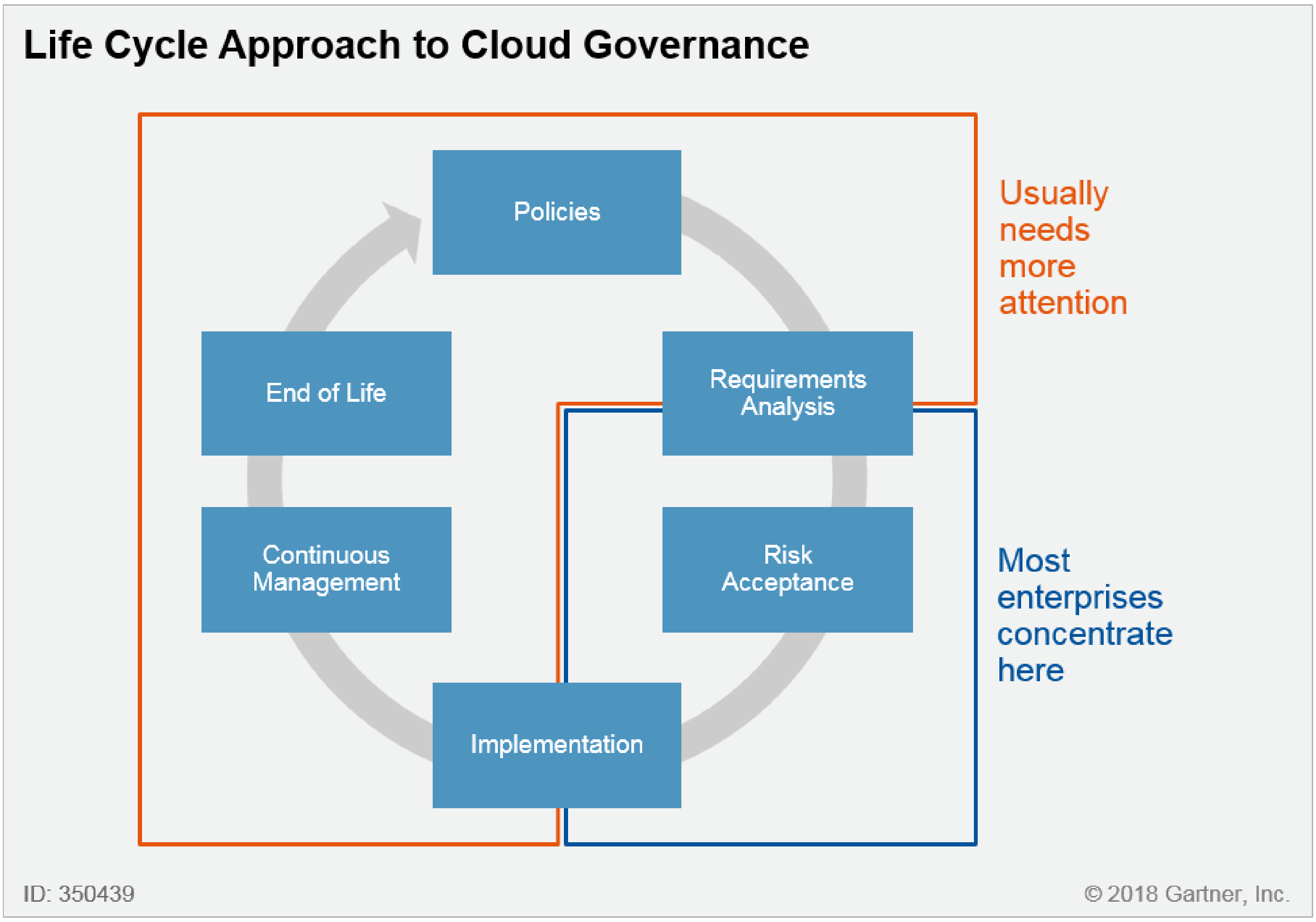
Organizations can make the CSP assessment process more effective by demanding higher levels of transparency from cloud service providers. At a minimum, Gartner recommends asking providers to demonstrate successful completion of a formal third-party security evaluation, such as ISO/IEC 27001, SOC 2 or FedRAMP. Lengthy and complex approval processes are counterproductive, sending the message that clouds are not desired, and encouraging the line of business to find its own applications without asking IT for assistance in selection or governance. The IT department and security practitioners should be proactive in anticipating organizational needs, and promulgate the use of a set of preapproved and supported cloud services.

In practice, every organization should maintain an inventory of public cloud services in use, tracking the ownership and associated responsible people. If your organization lacks a comprehensive list of public cloud services currently in use, Gartner recommends conducting a cloud application discovery.

Follow a Life Cycle Approach to Cloud Governance

The failure to establish processes for the oversight and support of public cloud leads to the inappropriate sharing of sensitive data and the use of unsanctioned cloud services. It leaves the organization unable to explain to auditors, regulators, customers, citizens and the board why regulated and proprietary data was placed into uncontrolled services without first establishing policies and guidelines over appropriate use. At a minimum, public cloud use requires regular attention to the status and performance of those CSPs that are being used for levels of processing that are deemed critical (see Figure 2).

Figure 2. Life Cycle Approach to Cloud Governance



Source: Gartner (January 2018)

The governance of IaaS-based services follows patterns that parallel traditional in-house computing. Although the control technologies and some of the techniques may be unique to virtualized public cloud environments (see "Understanding and Implementing Security in Microsoft Azure"), successful use of IaaS requires attention to cloud-specific (and usually automation-driven) architecture, coding practices, testing, change management and vulnerability management. Be aware that any IaaS and PaaS asset — including data and applications — can be openly exposed to the internet by someone with the necessary privilege, a cloud feature that too often becomes an unnecessary security hole.

Organizations that have not fully explored the implications of SaaS use often make the mistaken assumption that the provider bears full responsibility for security. The service provider maintains the operating environment and application; however, what is actually done within that environment — especially involving identity and access management (IAM) and data security — is under the control of the customer. Most SaaS applications make it quite easy for individuals to inappropriately share data internally, and many applications also give individuals the ability to share large amounts of data externally, with little or no authentication required for access. Unfortunately, several of the most popular SaaS applications default to allowing all users to share all data with anyone in the world.

Effective control over the use of cloud computing is not about saying "no"; it's about having the ability to know what is being done within the public cloud. It also includes being able to provide affirmative answers to questions from managers, board members, auditors, regulators and partner organizations that cloud computing is being used effectively and appropriately, utilizing the innate advantages of the product model to reduce the potential for security incidents (see "Developing Your SaaS Governance Framework").

Develop Organizational Expertise in the Security Implementation and Management of Each of the Cloud Models You Will Be Using

Gartner clients are struggling to obtain adequate security knowledge to fully address the use of a single IaaS provider — a knowledge gap that is exacerbated by the use of multiple IaaS services, each with its own user interface and vendor-specific characteristics. While the amount of security attention needed for SaaS is relatively lower than for IaaS, every service has different implications, unique features, and its own administrative interface, which creates a significant knowledge challenge for operations and security staff. To ensure effective levels of visibility and control over various forms of externally provisioned services, the organizational strategy for the use of public cloud must explicitly address the reality that different cloud models have different risk and control ramifications. A successful approach must explicitly allocate resources to the development of adequate skills to ensure that all strategically important cloud use cases are used securely and compliantly.

The basic deployment and operational framework of IaaS use is broadly the same as the processes and skills used in traditional IT. Yet, the professionals completing these tasks will need to learn and develop virtualization and CSP-specific knowledge, especially regarding DevOps-style automation of virtual infrastructure, IAM, workload protection, network security and encryption. Organizations that want to use IaaS for sensitive use cases will need staff with a sophisticated understanding of cloud-specific security technologies and how to leverage the programmatic infrastructure of IaaS providers for security automation (see "How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center").

In contrast, the entire SaaS technology stack is under the direct control of the service provider, which means that enterprises that want to govern their usage of SaaS must focus on IAM permissions management and the protection of sensitive data. This is accomplished by relying on whatever mechanisms each SaaS provider makes available or by use of some third-party product such as a cloud access security broker (CASB). SaaS security and governance involve the organizational tasks of setting policy and encouraging compliance with those technologies. The controls that can be applied — typically, creating or linking accounts, password maintenance, data access policies, and activity monitoring — are almost exclusively performed through web-based dashboards and consoles, so SaaS oversight processes are less demanding of technical expertise. The employees managing SaaS processes may be in IT operations, IT security, or even the compliance or privacy function, but they are generally not the same people who are interested in system internals or network protocols. In some cases, business units may choose to manage SaaS themselves — and therefore undertake managing the security of SaaS as well.

Over time, as SaaS providers continue to expand their APIs, and as the user base becomes more demanding of control, customization and integration, the effective utilization of SaaS will require more architectural and coding expertise. As demonstrated by Salesforce and ServiceNow, cloud-based applications of record, which are often some of the most strategically significant applications, typically have programmatic platform capabilities. The greater the degree of customization demanded by the enterprise, the greater the need for individuals who understand the visibility and control ramifications and interfaces of SaaS platforms. And, of course, as PaaS becomes more common, and as it is increasingly used as an integration mechanism for SaaS, it will require technology experts who are familiar with the specific APIs and conventions of each service being used.

The growing use of public cloud also requires new knowledge on the part of sourcing and procurement professionals, and is significantly expanding the need for a continuous vendor risk management function. Contractual representations can sometimes help manage risk by delineating the respective security responsibilities of the service provider and the customer.

Implement Security Management and Monitoring Planes

The control of cloud computing primarily relies on the cloud provider's native mechanisms, and the need for third-party security technologies remains an open question. However, one of the downsides of the use of a public cloud service is that it is innately diffuse, leading to console proliferation and management inefficiency. IaaS becomes complex because the number of workloads can expand indefinitely. SaaS is complex because of the number of providers, with virtually every organization regularly using at least a few dozen externally provisioned applications and the largest of enterprises accessing over a thousand. Enterprises can partially compensate for their cloud skills gap, and greatly improve operational and security efficiency, with the use of dashboards, or "control planes." Such third-party tools are becoming more popular as orchestration mechanisms, especially for the majority or organizations with a multicloud approach. Multifunction control consoles providing an integrated view across multiple public and hybrid clouds will become increasingly desirable as mechanisms to facilitate the full benefit of public clouds, while also ensuring that they are meeting regulatory compliance requirements and security expectations (see "Hype Cycle for Cloud Security, 2017").

The foundation for the well-managed use of external clouds of all types is identity governance and administration. It starts with the integration, or federation, of external clouds with the organizational directory service. Increasingly organizations are taking advantage of identity and access management as a service (IDaaS), with authentication as the most important function. Identity governance ensures that only the appropriate people are using organizational accounts, and that only authorized users have permission to access sensitive data (see "Magic Quadrant for Access Management, Worldwide"). Control over privileged users is especially important, and should ideally be protected through multifactor authentication and activity logging.

Evolving new IaaS security orchestration products, such as cloud workload protection platforms (CWPP; see "Market Guide for Cloud Workload Protection Platforms") and cloud infrastructure security posture assessment (CISPA), provide convenient single points of control over the workloads, networking and storage of thousands of IaaS-based assets.

As the use of encryption grows, centralized cloud key management will become increasingly desirable, and even necessary (see "Prioritize Enterprisewide Encryption for Critical Datasets").

Arguably, SaaS is harder to control than IaaS. Each application comes from a different vendor (with a different set of features, weak spots, control capabilities and administration consoles), and where an enterprise may only have one or two IaaS providers, they may have hundreds of SaaS providers. Orchestration products such as CASBs (see "Magic Quadrant for Cloud Access Security Brokers") are demonstrating the possibility of implementing single points of control over policy and activity across hundreds of SaaS applications.

Evidence

[1] Reports of security failures on the part of cloud-using organizations are prominent. Examples include:

- "Cloud Security Failure: Millions of Wrestling Fans' Personal Data Exposed," eSecurity Planet.
- "Massive Leak exposes Data on 123 Million US Households," CNET.
- "Cloud Storage Error Exposes Over Two Million Dow Jones Customer Records," Forbes.

[2] Reports of cloud security failure continue to be conspicuous by their absence from conversations with Gartner clients and news reports. Virtually no mention of cloud service provider failures appears in prominent studies, such as the annual Verizon Data Breach Investigations Report. In January 2018, a ransomware attack resulted in a one-week service outage for 1,500 customers of Allscripts' SaaS offering (see "Allscript Still Recovering From SamSam Ransomware Attack," SC Media).

Document Revision History

Clouds Are Secure: Are You Using Them Securely? - 21 July 2016

Recommended by the Author

Security of the Cloud Primer for 2019

The Cloud Strategy Cookbook, 2019

How to Evaluate Cloud Service Provider Security

Inform Your Cloud Service Choice With Provider Maturity

Staying Secure in the Cloud Is a Shared Responsibility

CISO Playbook: How to Retain the Right Kinds of Control in the Cloud

A Public Cloud Risk Model: Accepting Cloud Risk Is OK, Ignoring Cloud Risk Is Tragic

Developing Your SaaS Governance Framework

What to Include in Your SaaS Security Policy

Recommended For You

Cool Vendors in Cloud Computing

Cloud Computing Primer for 2020

‘Distributed Cloud’ Fixes What ‘Hybrid Cloud’ Breaks

Cloud Architects: What They Do and Why You Need One

The Cloud Strategy Cookbook, 2019