IDC ANALYZE THE FUTURE

IDC WORKBOOK

Sponsored by: ExtraHop

While the need for cloud security is better understood, CISOs now require guidance to grasp the security requirements for which they are responsible as well as practical recommendations for how to handle them.

Cloud Security Road Map: Identifying Limitations to the Shared Responsibility Model as well as Requirements and Best Practices

August 2019

Written by: Christopher Rodriguez, Chris Kissel, Frank Dickson

AT A GLANCE

WHAT'S IMPORTANT

The massive amounts of data processed or stored in the cloud have attracted the attention of threat actors, which means enterprises must now figure out how to extend their IT systems to the cloud without introducing new vulnerabilities or increasing exposure to cyber-risk.

Introduction

The race to cloud adoption has reached its zenith, as public cloud adoption continues to increase at a rapid pace, with 58% of organizations worldwide now using the public cloud to support their production workloads and services. This is up from 49% in 2017, representing a 18% increase year over year, according to IDC's May 2018 *CloudView Survey*. Furthermore, IDC expects that by 2022, the top 4 cloud "megaplatforms" will host 80% of infrastructure-as-a-service (IaaS)/platform-as-a-service (PaaS) deployments, and by 2024, 90% of G1000 organizations will mitigate lock-in through multicloud and hybrid cloud technologies and tools. The massive amounts of data processed or stored in the cloud have attracted the attention of threat actors, which means enterprises must now figure out how to extend their IT systems to the cloud without introducing new vulnerabilities or increasing exposure to cyber-risk.

Cloud Security Lessons Learned

Cloud is an umbrella term that includes private cloud systems built and operated by a private organization, public cloud systems hosted by a third party and accessed via the internet for general consumption, and private clouds that are operated offsite by a third party and accessed via the internet for a specific organization (private hosted). Public cloud systems are further categorized based on the level of control that customers have over the computing environments. The primary categories are IaaS, PaaS, and software as a service (SaaS), each with varying levels of control and customizability of underlying technologies. These options allow organizations to control how "hands-on" their cloud deployments are.

The benefits of cloud are numerous and well documented — cloud computing enables more efficient use of resources, turning computing into a utility with variable consumption-based pricing in place of stiff up-front costs. The cloud model enables massive scalability. Cloud services require little or no capital investment while delivering benefits of IT agility and flexibility.

But recent media coverage of cloud-related data breaches has stimulated concerns about the security of cloud services. In IDC's January 2018 *Cloud and AI Adoption Survey,* respondents were asked, "Has your organization migrated any applications or data that were primarily part of a public cloud environment to a private cloud or on-premises environment?" 80% indicated they had, with "level of security" as the leading reason. Cloud vendors deeply understand the importance of securing customer data and have invested heavily to secure their cloud infrastructure.

However, customers also bear some of the responsibility. Several security solutions have emerged to secure this migration to the cloud: cloud security gateways, cloud workload protection, microsegmentation, and virtualized versions of security devices. There is also an expectation that customers will be able to combine security information and event management (SIEM), endpoint detection and response (EDR), and network detection and response (NDR) tools to cover both on-premises and cloud environments. This combination is critical because it enables security operations centers (SOCs) to leverage data sources such as logs, network traffic, and activity on endpoint devices to gain the holistic visibility required to defend against elusive and sophisticated threats.

Additionally, despite high and growing adoption rates of cloud, IT organizations are recognizing that certain applications or data types are not ready for cloud deployment. According to IDC research, 80% of organizations have reported repatriation activities, with security concerns as the leading reason (cost, control, and performance were also cited as challenges).

Overall, the cloud adoption hype cycle is entering an era of maturity that includes security awareness. While the need for cloud security is better understood, buyers now require guidance to grasp the security requirements for which they are responsible as well as practical recommendations for how to handle them.

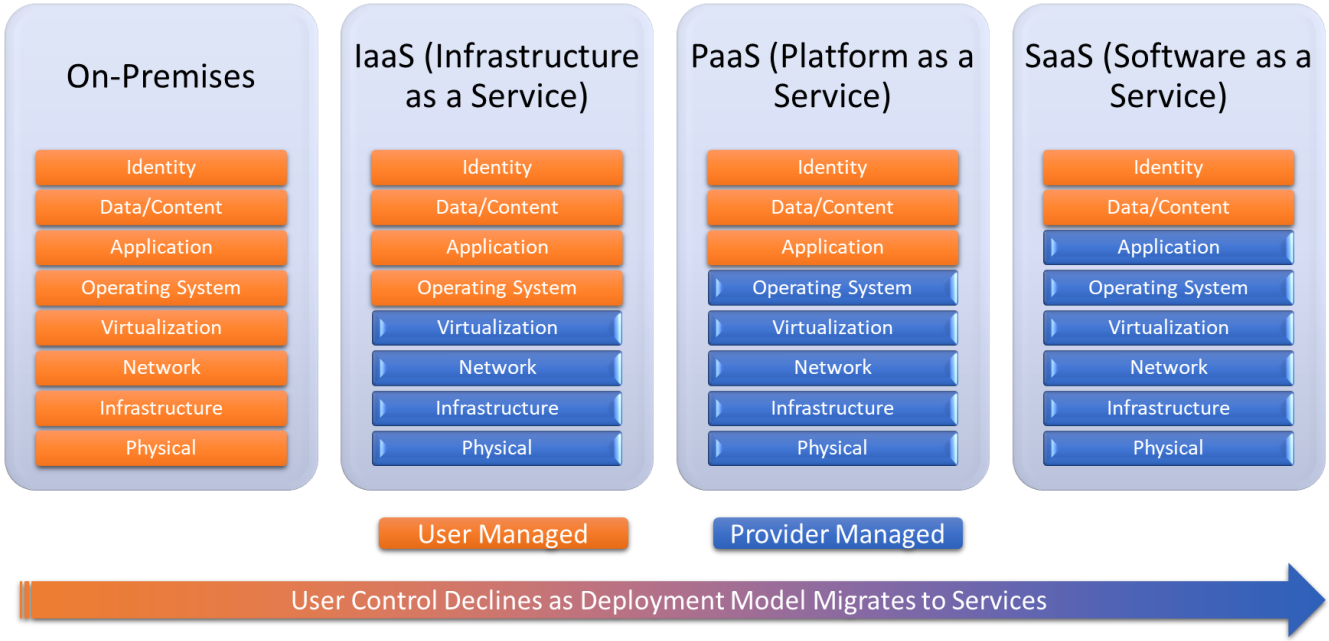
Cloud Security Optimization: The Shared Responsibility Model

The shared responsibility model is an emerging approach to cloud security to ensure that the risks associated with cloud adoption do not outweigh its many benefits. The concept of shared responsibility is gaining more visibility as a road map to aid companies in determining their jurisdiction and subsequent requirements for security practices.

Although cloud relieves users of securing infrastructure, it does not absolve them from handling other security responsibilities. As shown in Figure 1, shared responsibility promotes the concept that customers are expected to take greater ownership of their own cloud environments depending on how much or how little control the service provider offers. For example, IaaS environments provide customers with control over everything "above" the hypervisor, including operating systems (OSs), middleware, applications, and data. This control provides customizability while maintaining the enormous benefits of cloud scalability and efficiency. Under the shared responsibility model, businesses are also responsible for securing everything "above" the hypervisor.

For illustrative purposes, consider that an IaaS customer would be responsible for patching the operating system of workloads as well as any guest operating systems and applications. However, a PaaS customer would be responsible only for the applications and data. In both cases, the cloud provider handles security for the physical systems, infrastructure, and hypervisor. While this base level of security offers tremendous value for many customers, it still is only a component of the security solution.

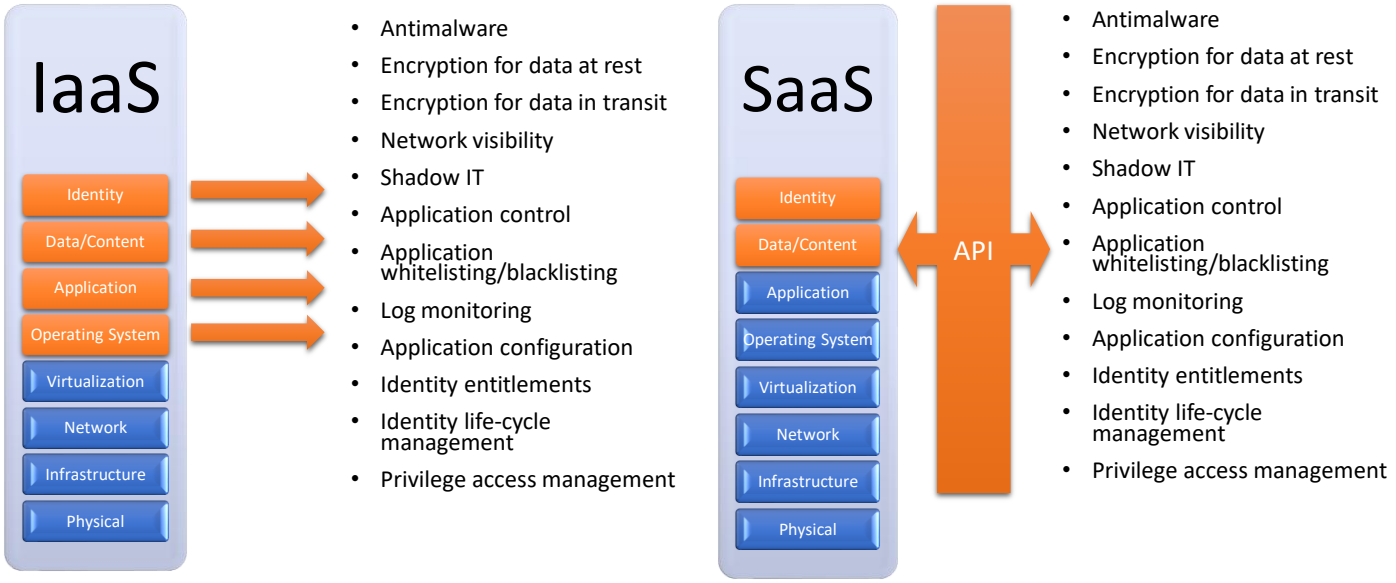
FIGURE 1: ***Shared Responsibility Model***



Source: IDC, 2019

Figure 2 overlays the shared responsibility model with common security duties. Ultimately, the model's overarching theme is enforcing tasks such as antimalware, encryption, network visibility, shadow IT, and application control. These practices are still owned by the user. In the case of IaaS, a variety of flexible options exist to enforce security policies. The built-in workload security capabilities of the workload OS or IaaS provider might be used along with third-party security functionality that can be built using host-based OS agent software, sidecar container services, agentless security wrappers, and APIs. However, the creation and implementation of security policies still belong to the user. Note that security responsibilities cannot be avoided by simply using SaaS. SaaS environments provide the least control and customizability for customers, who may not realize that they remain responsible for a number of security practices.

FIGURE 2: ***Security Requirements Under the Shared Responsibility Model***



Source: IDC, 2019

Table 1 provides suggested security practices for various forms of cloud environments based on the shared responsibility model. Some security practices, such as auditing, identity management, and data loss prevention (DLP), are universal, though they may vary in implementation. Other practices are unique to the type of cloud environment. For example, IaaS customers may be responsible for securing the networking of cloud instances. Customers may utilize the built-in tools offered by the cloud provider (such as AWS Security Groups rules) or may extend virtual versions of firewalls from third-party specialists to secure these connections.

Customers may be surprised to realize that these responsibilities do not always align neatly under either "customer responsibility" or "provider responsibility." For example, cloud vendors may offer patching and maintenance of the host OS, but customers will still be responsible for patching and maintenance of any guest OS and applications layered on top of the host OS.

TABLE 1: ***Cloud Shared Responsibility Model: Suggested Security Practices for Customers***

	IaaS	PaaS	SaaS
Security Hygiene/Vulnerability Management			
OS updates	x	x	
Patching	x	x	
Vulnerability management	x		
Policy Enforcement			
Security groups	x		
Application whitelisting/blacklisting	x	x	
Access control lists	x	x	x
Identity life-cycle management	x	x	x
Privilege access management	x	x	x
Visibility			
Network flow visibility	x		
Network packet visibility	x		
Asset discovery and categorization	x	x	
Application visibility	x	x	x
Application dependencies	x	x	x
Log management	x	x	x
Threat Detection/Investigation			
Antimalware	x		
Network security	x		
Threat/anomaly detection	x	x	x
Response/remediation	x	x	x
Configurations/Compliance			
Network configurations	x		
Application control	x	x	
Application configurations	x	x	x
Identity entitlements	x	x	x
Compliance, corporate policies	x	x	x
Compliance, industry-specific policies	x	x	x
Auditing	x	x	x
Data			
Encryption for data at rest	x	x	
Encryption for data in transit	x	x	
Content discovery	x	x	x
Shadow IT			x
DLP	x	x	x

Usage			
Onboarding/offboarding across the user life cycle, including permissions/privileges	x	x	x
User activity monitoring	x	x	x
Identification/removal of inactive accounts	x	x	x
Detection/alerting of excessive usage	x	x	x
Application usage	x	x	x

Source: IDC, 2019

Checklist: Recommendations for Cloud Security Best Practices and Technology Solutions

Table 2 offers a set of critical, important, and recommended best practices for cloud security. They are mapped to specific customer cloud security concerns such as privacy, compliance, configuration, and hygiene. These recommendations include advanced capabilities such as real-time detection and threat investigation, which will become increasingly important for enterprise IT and security organizations. In IDC's *Worldwide Security Information and Event Management Forecast, 2019–2023* study, advanced technologies that facilitate real-time detection and threat investigation such as machine learning (ML) were rated as "important" by midsize companies (1,000–2,499 employees) and large companies (2,500–9,999 employees) and "very important" by enterprise organizations (10,000+ employees). ML becomes central to reducing alerts to a single version of truth, creating and implementing playbooks, and helping on the back end to generate tickets or facilitate workflow.

TABLE 2: ***Cloud Security Best Practices and Recommendations***

	Critical	Important	Recommended
Privacy/compliance (e.g., GDPR)	Have a comprehensive understanding of local data handling laws. Public cloud use is often heavily restricted in certain national/local jurisdictions.	Establish what entities have responsibility for data handling/encryption, key distribution, and microsegmentation across SaaS, PaaS, and IaaS.	Have the ability to generate reports based upon industry compliance standards to satisfy regulators and simplify audits.
Automation	Have a central dashboard to process information from SaaS, public cloud, private cloud, on-premises, and virtual environments.	Have a platform that can harmonize, index, and correlate multiple sources of data such as external threat intelligence, cloud data, network traffic, flows, logs, and endpoint activity.	Have a centralized analytical platform to prioritize alerts and automate action.
Real-time detection	Integrate real-time network performance criteria such as packet entropy, abnormal port activity, and session data as indicators of compromise (IOCs).	Leverage user behavioral analytics (UBA) to create an individual version of truth for each entity on the network.	Implement change management to identify events that would not be detected by manual human investigation.
Hybrid visibility (unified view of on-premises and cloud environments)	Have a mechanism to create and interpret network traffic/packets from public cloud sources.	Generate real-time inventory of all assets and users as well as their network topography and what applications they have access to.	Use a cloud-based platform to manage and distribute the same policy across multiple environments, security devices, and user groups.
Configurations/ security hygiene	A platform/appliance keeps a historical record of internal devices such as routers, switches, and servers so the administrator can reset the network after power outages.	Automatically identify assets that require configuration improvements and provide actionable suggestions.	Benchmark certain classes of devices and compare groups to look for bottleneck issues on a network.
Threat detection/ investigation	A combination of machine learning and algorithms creates contextual awareness, reducing numerous signals into a unified and comprehensive case view.	Leverage machine learning to correlate wire data and logs to eliminate similar alerts from multiple point products.	Implement change management to track items such as privilege escalation and other events that support investigation.

Source: IDC, 2019

The journey to cloud security will require numerous technologies and practices, though the burden can be managed by technology solutions that offer capabilities such as comprehensive and centralized network visibility as well as real-time threat detection and response. The checklist in Table 3 is designed to guide buyers in identifying and prioritizing key capabilities of a cloud security solution. IDC recommends that vendors be short-listed by their ability to address high-priority issues before moving to proof-of-concept testing.

TABLE 3: ***Cloud Security Solution Checklist***

	Critical		Important		Less Important	
Questions for Cloud Security Technology Solution Vendor	Yes	No	Yes	No	Yes	No
1. What visibility is provided into cloud environments?						
Workloads Applications and dependencies Anomalous behaviors Layers 2–7 visibility Line rate visibility of encrypted traffic via decryption Line rate visibility of encrypted traffic via analytics Network flow visibility Network packet visibility						
2. What data sources are offered?						
Endpoint Wire data SIEM/logs Data correlation Support for multiple sources of data including external threat intelligence Packet capture Native audit of Kerberos Native audit of Active Directory Device identification/profiling/configuration Benchmarking device performance/monitoring						

3. What type of detection is provided?						
Sub-5-minute detection Sub-1-minute detection Real-time detection Use of network performance data (packet entropy, session data) as IOCs UBA/UEBA Rule-based detection Behavior-based detection Threat hunting Change management tracking Machine learning/advanced analytics Threat risk scoring Attack chain visualization						
4. What management and reporting options are provided?						
Cloud-based management interface Centralized management of SaaS, public cloud, private cloud, on-premises, and virtual environments Integration with orchestration tools Report templates for industry-specific standards Automation to reduce repetitive or low-priority alerts Time comparison views Alignment with security frameworks						

Source: IDC, 2019

About the Analysts

Christopher Rodriguez, *Research Manager, Cybersecurity Products*

Chris Rodriguez is a Research Manager in IDC's Cybersecurity Products research group focused on the products designed to secure today's complex enterprise networks. IDC's cybersecurity research offerings to which he contributes include Endpoint Security; Network Security Products and Strategies; Security Analytics, Intelligence, Response, and Orchestration (Security AIRO); and Identity and Access Management research programs.

Chris Kissel, *Research Director, Security Products*

Chris Kissel is a Research Director in IDC's Security Products group, responsible for cybersecurity technology analysis, emerging trends, and market share reporting. Mr. Kissel's primary research areas are identity and access management (IAM) and security and vulnerability management (SVM) platforms. Cybersecurity extends beyond premises-based solutions, and the emphasis of Mr. Kissel's research will be on the establishment of identity across heterogeneous networks (including cloud environment) and the role of analytics pertaining to SVM.

Frank Dickson, *Program Vice President, Cybersecurity Products*

Frank Dickson is a Program Vice President within IDC's Cybersecurity Products research practice.
In this role, he leads the team that delivers compelling research in the areas of Network Security; Endpoint Security; Cybersecurity Analytics, Intelligence, Response, and Orchestration (AIRO); Identity and Digital Trust; Legal, Risk and Compliance; Data Security; IoT Security; and Cloud Security.

MESSAGE FROM THE SPONSOR

The cloud may be a force multiplier for business and IT, but for security teams already struggling to manage a sprawling attack surface and a shortage of skilled analysts, public cloud platforms create friction and vulnerabilities. It's time to move past the legacy tools and processes that keep security teams one step behind. The best way to embrace the speed and elasticity of the cloud is to build your security the way you build your enterprise: cloud-first, and give SecOps the same agile, scalable approach as the development and application teams they support.

ExtraHop Reveal(x) Cloud is a SaaS-based solution that helps organizations adopt a cloud-native approach to protecting their hybrid attack surface. With inside-the-perimeter threat detection, investigation, and response across Virtual Private Clouds (VPC) and workloads security teams can secure their applications and confidently scale their hybrid business.

Read more about ExtraHop Reveal(x) Cloud at ***www.extrahop.com/cloud***

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com