Secureworks®

WHITE PAPER

# Cloud Security: A Shared Responsibility Model

## Security Again Tops the List of CISO Concerns, With 83% Saying Enterprise Challenges Have Declined With Maturity – Except for Security

Security concerns are most pronounced amongst cloud intermediates (85%) but remain substantive amongst beginners (86%) as well as advanced users (77%). Businesses of all types have moved workloads to the cloud. But that usage does not indicate trust, even with those most familiar with the technology.[1]

Security is achievable in the cloud. This paper provides clear recommendations for securing applications and data in the cloud. This paper also focuses on security in third-party cloud Infrastructure-as-a-Service (IaaS) environments, the different stages of organizations' deployments, and how security is shared between the Cloud Service Provider (CSP) and customer.

**96%**

**of IT professionals reported using at least one public cloud.[2]**

## The Cloud (Third Party) is a Shared Security Responsibility Model

**Public Versus Private? Consider Third Party Versus In-House Instead**
From a security perspective we do not see much value in distinguishing "private" and "public" clouds. Rather, security should be framed in terms of "third-party" cloud environments and "in-house" cloud deployments. Regardless of type of cloud environment in use or under consideration, using third parties introduces vendor-related risk requiring you to consider how security is architected and managed. For example, one assumption is a private cloud implementation is more secure than a public cloud implementation. However, let's say your organization has a private cloud infrastructure. If your organization relies on a service provider to host that private cloud infrastructure, then you still are introducing risk from the vendor. With any third party, organizations need to consider exactly how the security of their applications and data is addressed, and by whom.

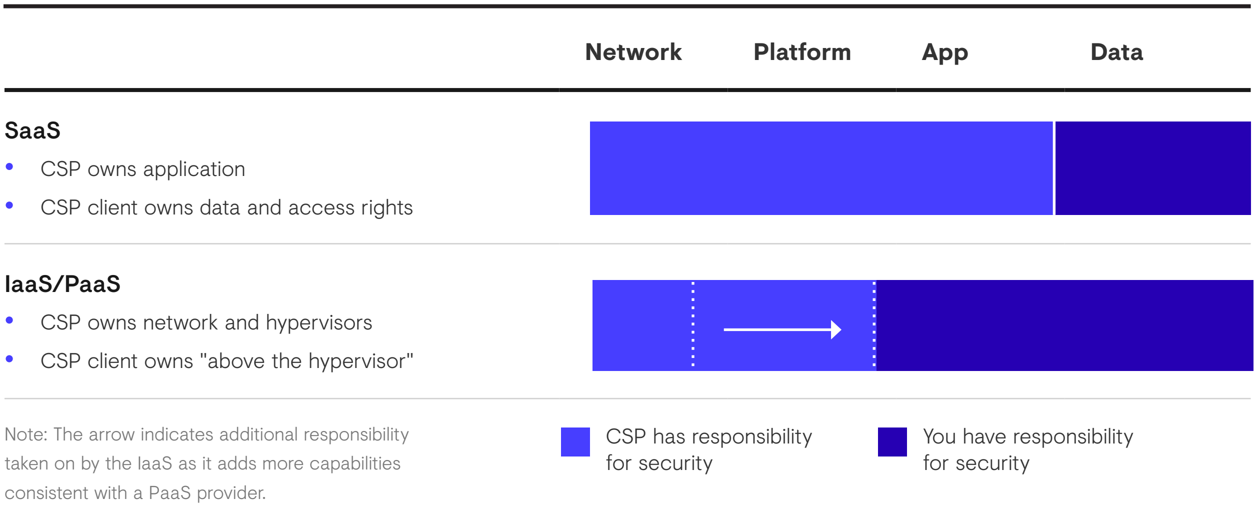
## It All Comes Down to IaaS and SaaS

Many have heard about three outsourced or third-party cloud platforms: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). However, we make the case there really are only two types– IaaS and SaaS. IaaS cloud providers have steadily rolled out new service options to such a degree, the traditional distinction between IaaS and PaaS no longer makes sense.

> **"Because you're building systems on top of the AWS cloud infrastructure, the security responsibilities will be shared: AWS manages the underlying infrastructure, and you secure anything you put on the infrastructure or connect to the infrastructure."**
>
> **Amazon Web Services**
> "Sharing the Security Services"

[1] Flexera (formerly RightScale*), State of the Cloud Report — Feb 2020
[2] Flexera (formerly RightScale*), State of the Cloud Report — Feb 2020
*RightScale acquired by Flexera

### Expanded Offerings by IaaS Vendors Are Blurring the Lines Between IaaS and PaaS



**SaaS**

- CSP owns application
- CSP client owns data and access rights

**IaaS/PaaS**

- CSP owns network and hypervisors
- CSP client owns "above the hypervisor"

Note: The arrow indicates additional responsibility taken on by the IaaS as it adds more capabilities consistent with a PaaS provider.

🟦 CSP has responsibility for security

🟪 You have responsibility for security

### The Shared Security Responsibility Model Explained

The diagram above explains the division of security responsibilities between the Cloud Service Provider and its customer. CSPs very clearly call this out.

### Challenges Deploying to the Cloud

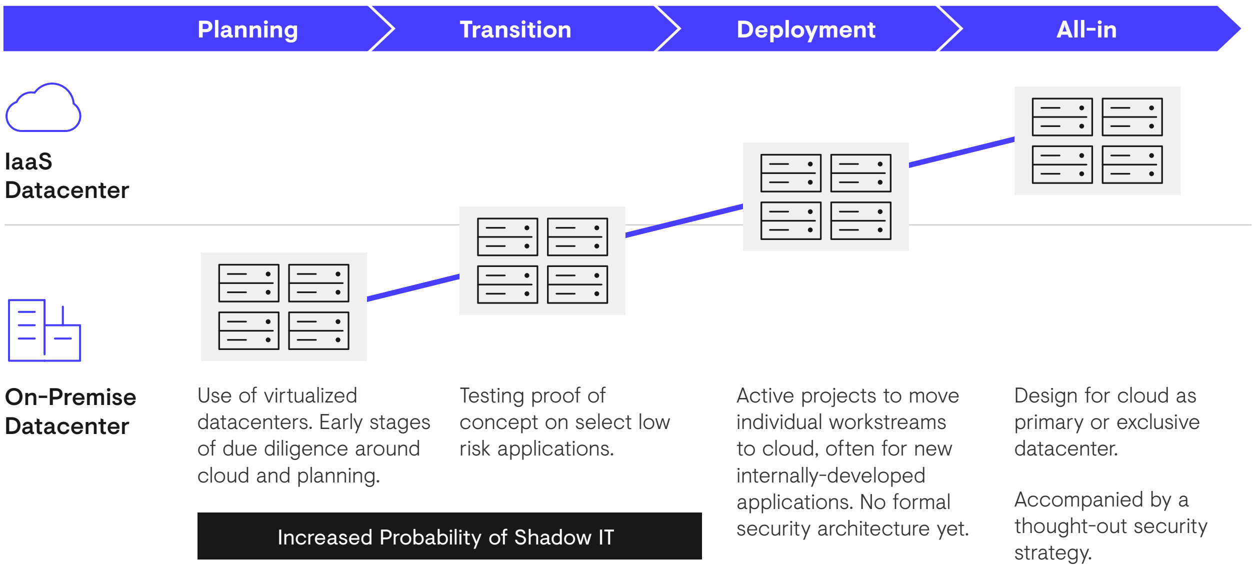
Concerns over cloud security has resulted in four distinct manifestations of behavior in organizations:

- **Shadow IT** - One behavior we see is “Shadow IT.” Unfortunately, while IT and IT Security teams grapple with the question of securing applications and data in the cloud, their own business units have been using the cloud’s flexibility to ramp up operations at will. This introduces risk into the organization and increases pressure on providing flexibility to business units, while ensuring the integrity of deployed applications and data.
- **Wrongly Assume** - Unfortunately, many still don’t understand or wrongly assume their applications running in the cloud are under the protective umbrella of the security protections the IaaS provider has to protect its underlying infrastructure. As a result, organizations’ applications and data are vulnerable to exploit by threat actors.
- **Overly Cautious** - Concerns for meeting various compliance mandates is another area for concern and is keeping some companies from fully utilizing third party cloud infrastructure.
- **Limited Deployment** - Another behavior is limited deployment of nonsensitive and tertiary applications to the cloud. This hesitant approach does not allow organizations to fully capitalize on the cloud’s faster provisioning and quicker go-to-market capabilities, leading to lost opportunities.

### Stages of Deployment to the Cloud

We see a pattern develop for how organizations consider, plan and migrate operations to the cloud, through the course of many conversations with IT and IT Security. This pattern is illustrated in the following Cloud Adoption and Maturity Model (CAMM):

### The Cloud Adoption and Maturity Model (CAMM)



Planning — Transition — Deployment — All-in

IaaS Datacenter

On-Premise Datacenter

Use of virtualized datacenters. Early stages of due diligence around cloud and planning.

Testing proof of concept on select low risk applications.

Active projects to move individual workstreams to cloud, often for new internally-developed applications. No formal security architecture yet.

Design for cloud as primary or exclusive datacenter.

Accompanied by a thought-out security strategy.

Increased Probability of Shadow IT

This model is useful in categorizing where an organization resides regarding cloud deployment. Regardless of phase, security should be addressed at every step.

Keep in mind not all organizations will progress to the final “All-In” stage. For many organizations, third-party cloud adoption will be done in more of a blended or hybrid model for some time to come.

A select few organizations (not reflected in the CAMM here), may find their operations in the cloud so great that scale advantages no longer apply. In these instances, these organizations may find bringing back their infrastructure in-house yields a stronger ROI.

**93%**

**of enterprises have a multi-cloud strategy.**[3]

**87%**

**of enterprises have a hybrid cloud strategy.**[4]

[3] Flexera (formerly RightScale*), State of the Cloud Report — Feb 2020

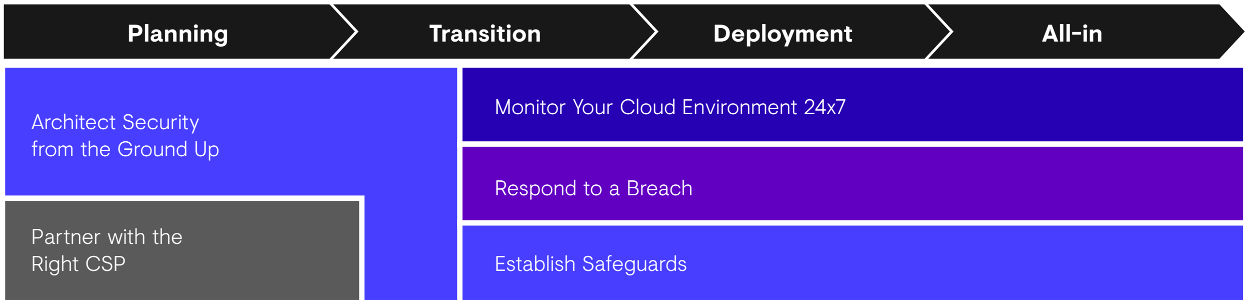
[4] Flexera (formerly RightScale*), State of the Cloud Report — Feb 2020

*RightScale acquired by Flexera

## Recommendations for Security in the Cloud

**Security - Break it down**

The Cloud Adoption and Maturity Model (CAMM) is also useful for compartmentalizing how security must be addressed in the cloud.



Planning

Transition

Deployment

All-in

Architect Security from the Ground Up

Partner with the Right CSP

Monitor Your Cloud Environment 24x7

Respond to a Breach

Establish Safeguards

## Partner with the Right CSP

**Vet the Provider**

Understand where your provider's responsibilities end and yours begin. This varies depending on the type of cloud service. Be sure to understand the CSP's full security capabilities and exactly what the provider covers.

**Don't Go It Alone**

Engage a partner who understands your legacy environment, the target cloud environment, your business goals and your security needs.

**Utilize IAM**

Make sure your identity and access management solution is robust and cloud-aware. Tie it into your existing systems for increased user adoption and lower management costs.

**Establish Right to Audit**

Make sure you have the right to audit your environment. Just like the rest of your environment, you need the ability to capture key log and other information. This is especially important if you suspect a breach may have occurred.

## Architect Security From the Ground Up

### Utilize Available Tools

Plug into the CSP's infrastructure to take advantage of capabilities the cloud provider may offer. CSPs offer a plethora of tools and services; it can be hard to keep up. Because misconfiguration is the most common threat vector, take advantage of Cloud Security Posture Management tools to ensure configurations are not open. Use CASB to identify shadow IT.

### Establish Defense-in-Depth

Just like your on-premise environment, establish Defense-in-Depth in the cloud. Address cloud security in terms of access controls, network, application and host level security.

### Avoid Lock-In

Make sure your data and applications are mobile and not locked into a proprietary format.

### Establish Retrieval/Removal Processes

Make sure you have a method for locking down access to your application(s) data.

## Monitor Your Cloud Environment 24x7

### Monitor Everything

Monitor your entire cloud environment. This includes "server" activity, user activity, device activity and data in motion. Other examples include telemetry from CloudTrail, Azure Monitor, S3/storage access, load balancers, WAFs, firewalls, and endpoint agents. Additionally, you should use tools like Secureworks TDR, AWS GuardDuty, and Azure Security Center to alert you on anomalous or malicious activity in your Cloud environment.

### Scan Your Applications

Perform continuous vulnerability and web application scanning, and patch applications as quickly as possible based on risk.

## Respond to a Breach

### Be Ready to Conduct Incident Response Involving the Cloud

Discuss and run through scenarios with your team for how they would respond to an incident. These scenarios should cover practical aspects of response, such as how logs are captured and how forensic analysis is conducted in the cloud.

### Forcing IT's Hand

With the increasing pace of acquisitions, large acquiring organizations are having to address cloud security much more seriously than they've been comfortable with as the smaller organizations they are acquiring are often "all-in" in the cloud.

## Establish Safeguards

### Back It All Up

Back up your images, applications and data to a location that is not managed by your CSP, but is readily accessible from your cloud environment.

### Encrypt Everything

Encrypt your data in transit, and especially at rest. Make sure you manage your keys effectively and make sure your Cloud Service Provider does not have direct access to your encryption keys (otherwise, encryption is a pointless expense).

### Use Two-Factor Authentication

Add a secondary security mechanism that reconfirms an identity is legitimate by using two factor authentication.

### Use Root Access Only When Absolutely Necessary

Use cloud-provider role-based access for most operations, instead of using root access. Always use two-factor authentication in conjunction with root access whenever it's absolutely necessary to use the root account.

## Conclusion

Despite long-standing concerns captured in a myriad of surveys, security in the cloud has progressed to a more practical and achievable level.

The cloud represents a shared security responsibility model whereby that responsibility is split between the Cloud Service Provider and the cloud customer. For organizations moving some or all of their applications and data to the cloud, acceptance of this model clears the way to more thoughtful consideration for how security can and should be architected – from the ground up. As a result, IT and IT Security leaders now have a much clearer trajectory to support their business operations in the cloud in a secure manner.

Secureworks®

## Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

### Corporate Headquarters

**United States**
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

### Europe & Middle East

**France**
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

**Germany**
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

**United Kingdom**
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

**United Arab Emirates**
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

### Asia Pacific

**Australia**
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

**Japan**
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp

Availability varies by region.