

Table of contents

- Introduction 3
- Convenience at a cost? 3
- Build cloud-native applications from the AppSec perspective 5
 - Understand shared responsibility and infrastructure security in the cloud 5
 - Address software vulnerabilities: Application security testing 6
 - Secure your system design: Infrastructure as code 7
- Maintain your software security initiative in the cloud..... 7
- How Black Duck helps 8
 - Plan your deployment 8
 - Prepare your applications 9
 - Train your staff in cloud security 9



Introduction

Moving to the cloud once meant taking a leap of faith into unknown territory. That's no longer the case, as an increasing number of companies are using cloud services as the foundation for their infrastructure and/or application stacks to accomplish these goals:

- **Reduce capital expenditure.** Organizations don't need to create their own networks, purchase their own servers, or build their own data centers to house them.
- **Achieve scalability.** Organizations that need an elastic model for allocating and consuming resources can quickly provision, scale, and release those resources.
- **Control operating costs.** IT teams don't have to worry about infrastructure maintenance and could potentially reduce or reallocate headcount.

However, of the companies invested in the cloud, an overwhelming majority (91%) are concerned about cloud security.¹ The tension between security concerns and the financial benefits of the cloud is putting pressure on security teams to keep pace with cloud adoption and growth. This presents a challenge for IT because cloud deployment and cloud-native software development require a fundamental change in approaches to security.

For organizations considering a move to the cloud, this means deliberately planning and implementing new organizational policies, skills, and activities. For those that have developed a DevOps culture and the corresponding toolchain to support their workflows, it means integrating security into that toolchain to further establish and reinforce its efficiencies within the cloud.

In this eBook, we'll discuss how organizations can proactively address risk management within the cloud. We'll uncover the unexpected security challenges many organizations face when shifting their applications and workloads to the cloud, and we'll discuss the security implications of building cloud-native applications. Read on to ensure you're prepared.

Convenience at a cost?

The advantages of the cloud are well-documented, yet concerns about security remain the biggest reason more organizations aren't completely adopting it. In the 2018 Cloud Security Spotlight Report, organizations mentioned general security risks (39%) and data security, loss, and leakage risks (38%) as two of the top barriers to cloud adoption.² The top spot went to lack of staff resources or expertise (42%).



Barriers to cloud adoption

38%
Data security, loss,
and leakage risks

39%
General security risks

42%
Lack of staff
resources or expertise

No amount of monitoring, patching, or firewall protection can keep your applications safe if a hacker is determined to exploit them. In fact, because cloud service providers (CSPs) focus on doing everything they can to bolster the security of the hosting environments they provide, the point of greatest security weakness is the application itself.

Even if you host only a portion of your sensitive data and applications in the cloud, your entire portfolio may be at risk if your cloud applications have security defects or you're using your cloud provider's security controls unsecurely. It's likely that your cloud applications interface with your on-premises applications via database connection points. If threat agents find a path into an unsecure application, they can pivot—penetrating more applications and higher-value assets in your own network.

Consider some of the most common security concerns about public clouds today:

Table 1. Biggest security concerns in public clouds

Threat	Solution
Assessment and management of security and compliance risks*	Create internal teams that can: <ul style="list-style-type: none">• Provide a top-level view of all cloud-related risks• Communicate their needs to CSPs so visibility and control mechanisms are in place• Perform adequate risk assessment on a per-cloud basis*
Misconfiguration of the cloud platform / wrong setup†	Use cloud-based automation to significantly reduce security vulnerabilities that result from misconfiguration, mismanagement, missing patches, and mistakes.*
Unauthorized access†	Require mandatory granular identities and permissions management.*
Unsecure interfaces/APIs†	Require an API gateway and/or event broker to be used for serverless functions when possible.*

Sources: * Neil MacDonald, [Security Considerations and Best Practices for Securing Serverless PaaS](#), Gartner, Sept. 4, 2018. † Crowd Research Partners, [2018 Cloud Security Spotlight Report](#), 2017.

Cloud service providers offer customers a front end to access the management plane for the hosting environment. They use a variety of APIs to provide management features (provisioning, modifying settings or lists, etc.) and continually release new and updated services that are accessible via APIs. The way these APIs are glued together and the design flows used to manage credentials and authorization affect the security of your applications.

So then, how should development teams approach application security in the cloud?

Build cloud-native applications from the AppSec perspective











At the end of the day, application development in the cloud is effectively the same as it is on-premises, but the application security approach with regard to infrastructure is new. In other words, to have a cloud-first security posture, organizations must extend testing for security vulnerabilities beyond the applications themselves to the underlying infrastructure stack. The first step in this process is understanding the relationship between you and your cloud service provider.

Understand shared responsibility and infrastructure security in the cloud

While there are many advantages of migrating workloads to a cloud environment, CSPs are increasingly delineating where their responsibility for security and compliance ends and the customer's begins. This division of security labor is called shared responsibility, and it's important to understand what you're responsible for. Gartner notes that in the near future, at least 95% of cloud security failures will be the customer's fault.³

In IaaS models, for example, your cloud provider provides the infrastructure (servers, virtualization, storage, and networking), and you run virtual machines on that infrastructure. Your cloud provider may give you access to security features, such as database configuration, firewall controls, clustering, and group settings. How you put these building blocks together is up to you. If you don't set them up and customize them correctly, you could compromise your security posture.

Table 2. A comparison of cloud service models

		Infrastructure-as-a-service (IaaS)	Platform-as-a-service (PaaS)	Software-as-a-service (SaaS)
People		You	You	You
Data		You	You	You
Applications		You	You	CSP
Runtime		You	CSP	CSP
Middleware		You	CSP	CSP
Operating system		You	CSP	CSP
Virtual networks		You	CSP	CSP
Hypervisors		CSP	CSP	CSP
Servers and storage		CSP	CSP	CSP
Physical networks		CSP	CSP	CSP

In the near future, at least 95% of cloud security failures will be the customer's fault.



An example of this is the highly publicized, and completely avoidable, Amazon Simple Storage Service (S3) bucket breaches. According to reports published last year, up to 7% of S3 servers can be accessed by the public without authentication, and as many as 35% are unencrypted.⁴

These statistics highlight the importance of addressing security controls in your application architecture and implementing them correctly in your cloud environment. Organizations moving to the cloud must think differently about entitlements and authorization to account for new types of connections between services, databases, and multiple applications. Otherwise, they risk opening themselves up to these types of breaches.

At the very least, you should follow these best practices for ensuring cloud architecture security:

- 1. Keep IT up-to-date with current cloud security practices.** Expertly trained cloud security professionals know how to identify and respond to potential threats. They remain one of the best ways to help protect your organization in the shared responsibility model.
- 2. Use your software security tools and the security features of your CSP.** It's important to use both the security features already built into your cloud solution and third-party software to ensure you have implemented proper cloud security controls.
- 3. Implement security in containerized / virtual machine (VM) environments.** Many cloud providers use open source software components or container technology to develop and deploy applications, which can introduce unforeseen security weaknesses.

Address software vulnerabilities: Application security testing

Finding and fixing software vulnerabilities in the cloud requires all the same activities as it does on-premises. As a first step, you should use application security testing tools to help identify security weaknesses in code. The types of tools you should use vary based on a host of factors, but here are some techniques to consider:

- **Static application security testing (SAST)** analyzes source code to identify vulnerabilities during development.
- **Software composition analysis (SCA)** detects third-party open source components in source code and binaries. It's useful for building containers and application images.

- **Interactive application security testing (IAST)** performs runtime code analysis through instrumentation during testing.
- **Dynamic application security testing (DAST)** allows you to conduct penetration testing in running applications.

Secure your system design: Infrastructure as code

Application security testing is a crucial step in preparing your applications for cloud migration, but it won't solve all the problems that could affect your cloud deployment. Many problems that occur in cloud deployments result not from flaws in code but from misconfigurations, design flaws, and architectural weaknesses.

- A skilled testing expert can perform **threat modeling** to model real-life scenarios with manual business logic testing. Threat modeling exposes vulnerabilities and can help you address them.
- An architect with an understanding of security controls and frameworks can perform an **architecture risk analysis**. An ARA can help you design an architecture that lowers your risk of a security breach.

Maintain your software security initiative in the cloud

Automation and containerization help organizations build fast and deliver continuously, but they can make managing security a challenge. Using cloud security controls securely and building security into the continuous integration (CI) pipeline in your cloud development environment gives you the visibility, agility, and speed you need for fast, continuous delivery. As you continue to use the cloud, you must focus on developing a mature software security initiative there. That initiative should include these six security capabilities:

1. Identity and access management (IAM). IAM forms the backbone of cloud security deployment. You must be able to establish an account and have the appropriate level of privileges to provision or orchestrate resources. At the very least, you should:

- Conduct audits for sources of authentication and authorization.
- Establish policies and procedures for appropriate user groups.
- Determine roles and responsibilities for minimal human access to production systems.

2. Data protection. Safeguarding important data is a critical piece of building and operating information systems in the cloud. You must:

- Evaluate your inventory and classification of data assets.
- Establish policies and procedures for safeguarding data in transit and at rest.
- Evaluate compliance requirements based on business needs and risk tolerance.
- Identify opportunities for encryption and responsible retention of data.

3. Infrastructure security. The foundational infrastructure for your cloud must be inherently secure, whether it is public, private, or hybrid. When you assess this capability, review the network topology for segmentation and multitenancy concerns. Also look for:

- Network, computing, and storage requirements
- Access control requirements
- Provisioning needs for automation and orchestration opportunities

4. Logging and monitoring. Logging and monitoring is key to providing greater visibility into occurrences within a cloud environment in real time, or near real time. Recommended activities:

- Obtain inventory lists of logging assets to identify aggregation, correlation, and analysis opportunities.
- Establish policies and procedures for alerting and notifications.
- Determine appropriate thresholds for critical business functions.
- Identify an appropriate set of tools for logging and monitoring activities.

5. Incident response. You need a solid incident response plan to contain an event and return to a known good state. To assess your incident response plan:

- Conduct an audit to categorize critical business functions and assign risk profiles.
- Review policies and procedures for incident response, alerts, and notifications.
- Establish metrics to determine the severity of incidents and assign an appropriate response.

6. Vulnerability and configuration analysis. Using an automated security mechanism for both configuration management and vulnerability assessments can be a cost-effective approach for cloud environments.

How Black Duck helps

No matter where you are in your cloud migration, the Black Duck portfolio of [products and services](#) will help you make effective, and externally defensible, risk acceptance decisions about the use of public clouds.

Plan your deployment

We can advise you on how to take full advantage of the security controls and capabilities of your cloud provider. Our services help developers and security professionals decrease their time to market without sacrificing security.

- **Create a [Maturity Action Plan \(MAP\)](#).** Provide a plan and roadmap to enhance your software security as a part of your cloud migration strategy with our Cloud Security MAP.
- **Implement cloud security policies.** You probably have a security policy in place, but we can ensure that it's updated to cover cloud concepts and help you establish platform security baselines.
- **Complete a [Cloud Configuration Review](#).** Unlike traditional pen testing, a configuration review provides insight into how effective your cloud applications are at using your cloud provider's security controls to protect workloads.
- **Review your Cloud Security Blueprints.** These blueprints are infrastructure-as-code solutions that provide baseline security controls to help guide development teams and systems integrators building or deploying cloud applications.
- **Perform a [Cloud Architectural Risk Analysis \(ARA\)](#).** A cloud ARA focuses on the design of cloud applications and on cloud infrastructure support of application and security controls. Our experts will evaluate your applications for cloud preparedness across several domains, including container and VM security, deployment model, and authentication, authorization, and data residency.

Prepare your applications

Before you migrate your applications to the cloud, we can identify and prioritize the security risks affecting them.

- **SDLC integration.** Integrate Black Duck SCA scans using AWS Code Services or supported development tools, such as CodeBuild, CodePipeline, Visual Studio, Eclipse, Jenkins, and Artifactory.
- **Ongoing monitoring.**
 - Coverity® Static Analysis is a powerful SAST solution that helps you find and fix common software vulnerabilities in your source code.
 - Black Duck is a comprehensive SCA solution for managing risk from open source and third-party software. Our industry-leading scanning algorithms and KnowledgeBase ensure complete open source identification coverage originating from over 13,000 sources and over 80 programming languages.
 - Seeker® Interactive Analysis correlates code and dataflow at runtime to ensure every identified vulnerability is real and exploitable and uncover complex vulnerabilities and logic flaws other tools can't.
- **CI pipeline integration.** Integrate SAST and open source scans into your CI pipelines to increase speed and agility while ensuring security and compliance.
- **Secure containers.** Ensure the security and compliance of your containers using Black Duck for Elastic Container Registry or the Elastic Kubernetes Service.

Train your staff in cloud security

Our cloud instructor-led training (ILT) and assessments teach your team to identify and resolve missing or weak security controls affecting your product. Your team will also learn security best practices for your cloud service provider and become better equipped to mitigate security flaws affecting your applications, reducing your risk.

References

1. Crowd Research Partners, [2018 Cloud Security Spotlight](#), 2017.
2. Ibid.
3. Christy Pettey, [Why Cloud Security Is Everyone's Business](#), Gartner, Aug. 19, 2016.
4. Catalin Cimpanu, [7% of All Amazon S3 Servers Are Exposed, Explaining Recent Surge of Data Leaks](#), BleepingComputer, Sept. 25, 2017.



Black Duck can help you secure your apps in the cloud.

[Learn more](#)

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.

©2024 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. September 2024