



# THE NEXT GENERATION OF CLOUD SECURITY

The CIOs Guide

# Summary

Microsoft CEO Satya Nadella has famously said, "Every company is now a software company." So, if you are spending on software development, or using a wider range of application technologies than before, then you are like most other companies. Your organization might have a mix of traditional & modern applications. Traditional applications might run on virtual machines, while modern applications might run in containers orchestrated by Kubernetes. Some of your applications might be leveraging microservices that cut across cloud boundaries making your attack surface more complex than ever before. Organizational roles & responsibilities are also changing. More & more DevOps teams are being asked to shoulder the burden of application security. Therefore, they can decide which security tools they want to use. Also, the speed of software delivery is increasing, and the DevOps team wants to deliver new features weekly or even daily. Against this backdrop, you must consider –

- *Has your security approach evolved to take into account new technologies & ways of working?*
- *Are you still using the old security approaches, and if so, are they successful in achieving optimal outcomes?*
- *Is your approach producing the desired results, or is it reflecting that you still need to take steps to modernize?*

CIOs have been asking these questions ever since the term DevSecOps was coined. In simple words, DevSecOps is the seamless integration of security testing & protection throughout the DevOps lifecycle. In this E-Book, we will explore various ways security tools & processes must adapt to address the agility requirements of organizations implementing modern software methodologies. The objective is to help organizations understand how they can align their security approach with the directions they are taking, their risks, and the high level of automation that modern business practice demands.

# Cloud Security Concerns

Even though many organizations have decided to move sensitive data & essential applications to the cloud, concerns about how to protect it abound.

## Data Loss/Leakage

In cloud-based environments, it is easy to share data stored within them. These environments are easily accessible from the public internet & include the ability to share data easily with other parties through direct email invitations or by sharing the public link to the data. While it's easy to share data in the cloud – a key collaboration asset – it creates profound data loss or leakage concerns. And around 70% of organizations point to this as their biggest cloud security concern.

## Data Privacy/Confidentiality

Data privacy & confidentiality is a significant concerns for many organizations. Data protection regulations like GDPR & HIPAA mandate the protection of customer data. Placing such data in the cloud has advantages, but it is a significant security concern for 67% of organizations. Many organizations have adopted cloud computing but need the knowledge to use it securely.

## Legal and Regulatory Compliance

According to the data protection regulations like PCI DSS and HIPAA, organizations must demonstrate that they can limit access to protected data. This means they must create a physically or logically isolated space in their organization's network. And this space should be only accessible to the right employees who have a legitimate need to access this data. When migrating such data (which has been protected by regulations) to the cloud, achieving a demonstrative compliance ability can be more difficult. In cloud deployment, companies only have limited visibility and limited control of cloud infrastructure. Therefore, legal and regulatory compliance can be a significant cloud security issue. And nearly 44% of organizations feel so. And they require specialized cloud compliance solutions for that.



### Accidental Exposure of Credentials

Phishers usually use cloud applications & environments as a pretext for phishing attacks. As the use of cloud-based Emails – G-suite, Microsoft 365, etc. – and document-sharing services grow, employees have become habituated to receiving emails with links that might ask them to confirm their account credentials before gaining access to their data. In this way, cybercriminals can quickly learn employees' credentials for cloud services. Therefore, accidental exposure of cloud credentials is a primary concern for 44% of organizations as it compromises the privacy & security of their cloud-based data.

### Data Sovereignty/Residence/Control

Most cloud providers have data centers that are geographically distributed. This contributes to improving the accessibility of cloud-based resources. And also ensures that CSPs can maintain service level agreements in the event of business disruption due to natural disasters, power outages, etc. Businesses opting for cloud services often have no idea where their data is stored in the CSP's data centers. As a result, many organizations are concerned about data sovereignty, residence, and control. There are regulations like GDPR, which limit where the EU citizens' data can be stored & sent. Opting for CSPs with data centers outside the approved areas means the businesses will be in a state of non-compliance with the regulations. Apart from this, different jurisdictions have different laws concerning accessing data for law enforcement and national security; this can impact a business's data privacy and security.

## Incident Response

Many organizations have strategies for responding to cybersecurity incidents. In the traditional model, the organizations own all their network infrastructure. Also, security personnel is based on-site. Hence, the incident can be locked down. Also, this ownership means that the company can identify the incident's scope and take the appropriate remediation actions. In a cloud-based environment, a company only has partial visibility, and they don't have complete ownership of its infrastructure. This makes the traditional processes and security tools ineffective. Around 45% of companies are concerned about whether they can perform incident response effectively in the cloud.

ISmile Technologies helps you to confront cloud security challenges by beginning with end-user protection tools & methods.

When planning enterprise IT policies, we help & provide consultation to keep your cloud services secured.

[Request a Free Consultation](#)



# Four technologies enabling digital transformation acceleration which security personnel need to be aware of

There are several new technologies & methodologies that security personnel must be aware of when designing a security architecture.

## Containers

Containers run in combination with orchestration systems like Kubernetes. They provide a more automated & reliable way to deploy and scale software applications than ever before. They can spin up and down rapidly. Quite interestingly, the average lifespan of some containers could be just minutes. But a word of caution – container speed and effective opacity could be problematic for traditional security tools. In a recent survey, 63% of CISOs said container runtime environments have, in recent times, made it even more challenging to detect and manage vulnerabilities in the software.

## DevOps

DevOps is increasingly used to make software more quickly and high-quality. The traditional functions of software development, QA, and operations siloed earlier are now being merged into a single team to bring more agility efficiency. In DevOps philosophy, developers are responsible for the software quality, and tools are being provided to monitor their applications in runtime. As a result, fast feedback cycles are created, and inefficiencies that arise from scattered information across different teams can be avoided. Today, automation is being used by high-performing teams in everything they are doing. But if you do not automate the security tooling, it will be seen as an inefficient function and will be avoided by developers.

## Open-source software

You will see that several open-source software is used to accelerate the development of custom applications. An average application today consists of nearly 70% of open-source components. And this percentage has almost doubled in the last five years. There is no doubt that this reusable bundle of codes is beneficial in speeding up application development, but it can leave security vulnerabilities in the application.

## Hybrid Multicloud Environments

While it might not be a new technology, it's undoubtedly a dominant operating environment for most businesses. Today, modern applications, especially those that leverage microservices, span across more than one cloud boundary; these applications are said to be present in the "hybrid cloud" environment. In a recent survey, nearly 75% of organizations said they currently use multicloud or hybrid cloud environments for their applications. Unfortunately, unlike today's applications, traditional security software does not operate in multi-cloud environments – they are siloed.

### At ISmile Technologies we see DevOps as CI/CD driven software delivery approach

Which believes that a single integrated delivery function from requirements to development to production will provide high business value to the customers.

[Request a Free Consultation](#)



# Traditional Security Approaches are inappropriate in today's high-speed environment.

Traditional approaches to cloud security are struggling. The following are some common failure points.

## **Slow Speed**

One thing about traditional security products is that they were not designed for today's high-speed environments. It may take some time for them to produce results. It may take days to coordinate between the development team that developed the code and the security team that looks after the security of the products and prepares the reports. Another area where the slow speed of operation is a problem is environmental scanning. Recent research by the IDC shows that nearly 50% of organizations scan their production environment for vulnerabilities once a month. This is why the organizations implementing DevSecOps say their top priority is increasing the frequency of development environment scanning. They know that the speed of the containers significantly outpaces the speed of their traditional security tools.

## **Lack of Automation**

Traditional security products have to be configured separately to ensure the security of applications. This is a lack of automation and is not what DevOps teams live in. And because of this reason, many application developers say they intentionally don't use security tools. They also say they avoid working with security teams for this reason. Security staff is also concerned by the lack of automation. Because of the manual setup, they can only be sure that some applications are monitored correctly. Security teams must do a lot of manual work to answer security questions. And, given the shortage of security staff, this extra work is indeed burdensome.



### **Siloed and Limited Viewpoint**

Most security products cannot look at the vulnerabilities across platforms – they have a siloed view of it and thus cannot have an integrated view of risk. For that, you will have to use multiple products for multiple environments and then take a holistic view of things. And the problem is getting worse, not because security products lack merit, but because operating environments are becoming more complex, and applications are getting distributed. Both of which are only making the problem of silos even more complicated. A security product sold by a particular CSP is an example of a siloed security product. Suppose your application is made of microservices that transfer information across cloud boundaries. In that case, a siloed security product will not be able to monitor your entire application or understand what it connects to.



A siloed or limited-scope security product is can't examine inside containers to see which libraries the application uses. The result is that the scanner is incapable of producing any meaningful information and may generate many false positives. Even the latest generation of "cloud workload protection platforms" are plagued with the same problem. Though they have been designed with containers in mind, they can only scan container images at rest in registries or look at the Docker file manifest. The cloud workload protection platforms must know that the application uses which libraries in run time to accurately differentiate between a potential vulnerability and a real danger.

## ISmile Technologies helps you reimagine cloud security by building it into the foundation of your company,

so that it can meet your businesses' evolving needs cost-effectively as a fully managed, consumption-based, as-a-service model ensuring business continuity, seamless compliance, and advanced security.

[Request a Free Consultation](#)



## Modern Technologies & Challenges

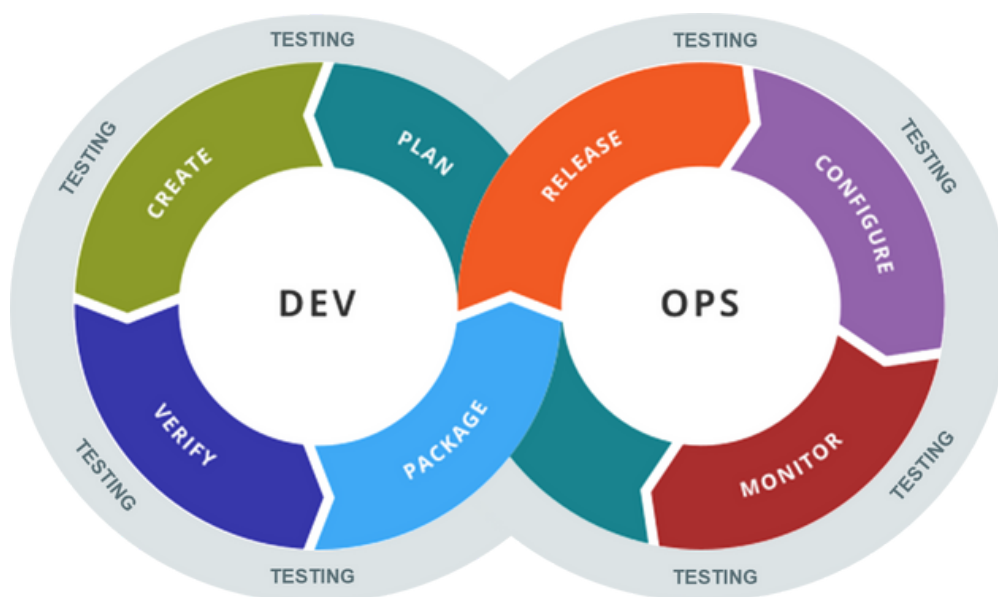
When you compare the characteristics of the modern development environment with the commonly available security tools, there are several areas of incompatibility that are apparent –

MODERN TECHNOLOGY	CHALLENGES
Containers	Containers have a shorter life span and that makes it hard for the traditional security tools to monitor them in the production environment. This leads to visibility gaps. Containers are therefore opaque to many traditional security tools that can see inside the applications in the runtime. In that case security analysts rely on just the Docker file which leads to many false positives.
Open Source Software	Statics application scanning tools have problems in identifying which part of the open source software package is being used by the application, and how are they being used. This leads to many false positives vulnerability detections.
Rapid Software Development	With slow security tools, developers have to wait for the results. This leads to delay in the release. Sometimes, security tests are intentionally skipped to keep things on schedule. False positives leads to wastage of time & frustrate developers.
Hybrid Multicloud	For many security tools it's not possible to see beyond cloud boundaries, and therefor they are incapable of giving a complete picture of your application. The result is you cannot enforce security policies consistently across boundaries.

## Adopting DevSecOps – shift-left & shift-right

For the past decade, the chief approach to improving security for high-velocity DevOps teams has shifted the security left. This implies doing security assessments early in the software development lifecycle. The following realizations lead to the urge to shift security left:

- Since the containers are increasingly temporary, there was no time left for traditional vulnerability scanners to find vulnerabilities in the production environment.
- As the containers are immutable, the developers must do the patching, not the IT operations staff.
- It is far easier & cost-effective for a developer to fix a vulnerability if they find it sooner than later.



This was all fine, but now, enterprises realize it needed to be better to abandon the production environment completely. There have been many successful attacks against the Kubernetes environment – from the malicious images into the Docker hub to the attacks against Azure & Tesla, all originating from 'cryptojacking'. Nearly 45% of the organizations are planning to adopt new runtime security controls over the next 1-2 years.

The new emphasis on monitoring the production environment is called shift-right security & is essential because of the given reasons.

## Production is Vulnerable

Most attacks happen here. Therefore, it becomes essential to find new ways to monitor your running containers which are not visible by traditional security tools.

## Scanning an Image is Insufficient

Scanning an image either in the repository or in the development environment can't give the insights you can get by observing the application in the runtime in production. For example, you won't be able to see what libraries are called, how they are used, whether any process is being exposed to the internet, or whether a process is interacting with sensitive corporate data.

## Most organizations don't have a perfect set of Homogeneous CI/CD Pipelines

Some applications might go through the prescribed testing pipeline during preproduction, but others may go past it without adequate testing. For example, maybe there was too little time left for security testing because of a deadline, Or maybe an application was an off-the-shelf application that did not go through the hands of the developers. This application appears in production without going through the prescribed testing procedure and creates an attack surface that must be assessed.

## New Vulnerabilities are discovered after an App has been deployed into Production

New vulnerabilities lurk out there, exposing you to risks. No doubt, shift-left security is excellent. But it would be a unwise to think that only the development end of the software development lifecycle needs to be monitored. Just as the DevOps loop spans the entire SDLC, a suitable security apparatus must also span the entire SDLC. Today, you must focus on something other than your application and leave the rest on the firewall. A threat could come from a service that is connected to another service, which is connected to.

## Built with Robust security, ISmile Technologies' DevSecOps managed service has been designed

To enable your DevOps team to redefine your operation & security to work in cohesion to build a secure delivery workflow from the ground up without compromising on the time-to-market velocity.

[Request a Free Consultation](#)



## Cloud Security Checklist

We see rapid changes in the technology & process workflow, so what should be the ideal characteristics of an enterprise cloud security program? Here's a checklist –

### Automation in Deployment

There should be no manual steps involved in the running of the tool. There should be no configurations, no custom scripts, etc. It should provide information even to those application developers who avoid using security tools for the fear that it would slow them down and to the IT teams running COTS applications that your developers never touched. Only with 100% automated deployment everywhere can you truly feel confident in the information your system is giving you.

## It should have Broad Scope

The security tool should function across all compute environments, such as containers, Kubernetes, serverless, PaaS, and traditional VMs.

## All Environments

The security tool should be able to assess the applications in different types of environments – both hybrid cloud & multicloud environments. By seeing across boundaries, the security tool will be able to properly understand the transitive dependencies & the chain of risks present in modern microservice-based applications.

## Developers should be Onboarded

All the things related to the security program, which also includes the products & the processes, must be accepted by the developers who will be tasked with remediating the issues that are found.

## Low Impact & High Stability

The security tools should not place a lot of demands on the workload. Also, it should not disrupt the stability of the application.

## Complete Lifecycle

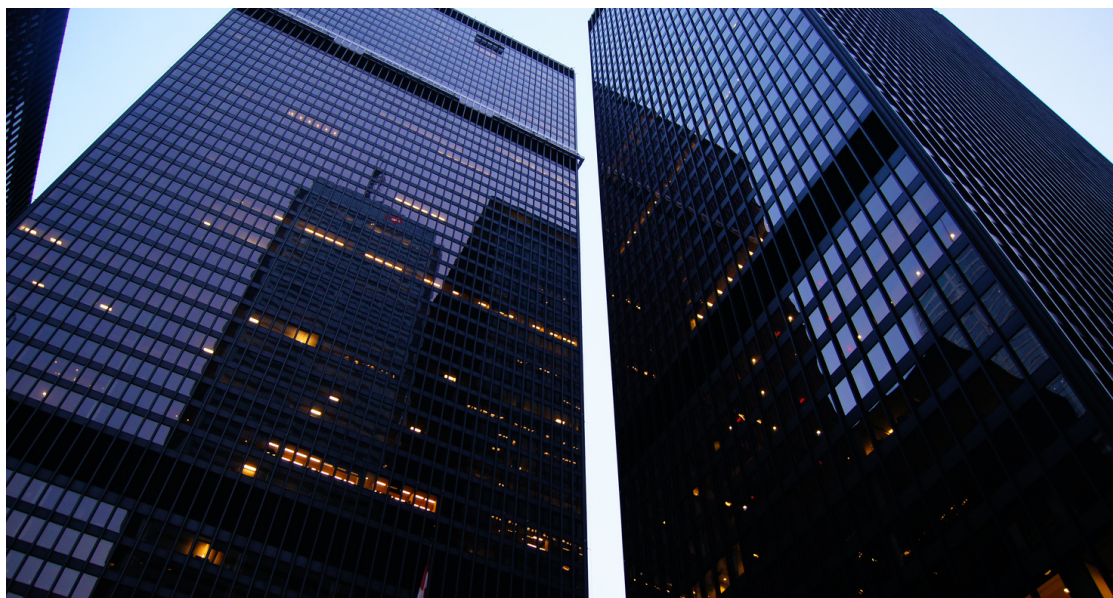
Static image scanning is insufficient, and there should be complete runtime visibility. The security tools should be able to run across the entire software development lifecycle, including both the preproduction & production environment.

## Observability & Contextual Awareness

The security product should be able to see inside each workload to comprehend how each library is used to distinguish a theoretical vulnerability from a real one. Also, it must be able to see outside each workload to understand if the vulnerability has been exposed to an attacker. Finally, it requires some way to understand the importance of each asset so that it can measure the potential impact on the organization if the vulnerability is attacked & compromised.


**About**

# ISmile Technologies



**ISmile Technologies is a proud automation-enabled intelligent cloud solution and managed IT services provider, and it is your multi-cloud technology advisor & key implementation partner.**

We operate globally and leverage disruptive technologies alongside deep expertise to deliver business-specific cloud solutions. We maximize impact at an unparalleled value and securely accelerate business agility while infusing competitive excellence.

 [+1 \(844\) 845-9236](tel:+18448459236)

 <https://www.ismiletechnologies.com>

 [service@ISmileTechnologies.com](mailto:service@ISmileTechnologies.com)

 [501 S Weber Rd Unit 108, Bolingbrook, IL 60490](#)