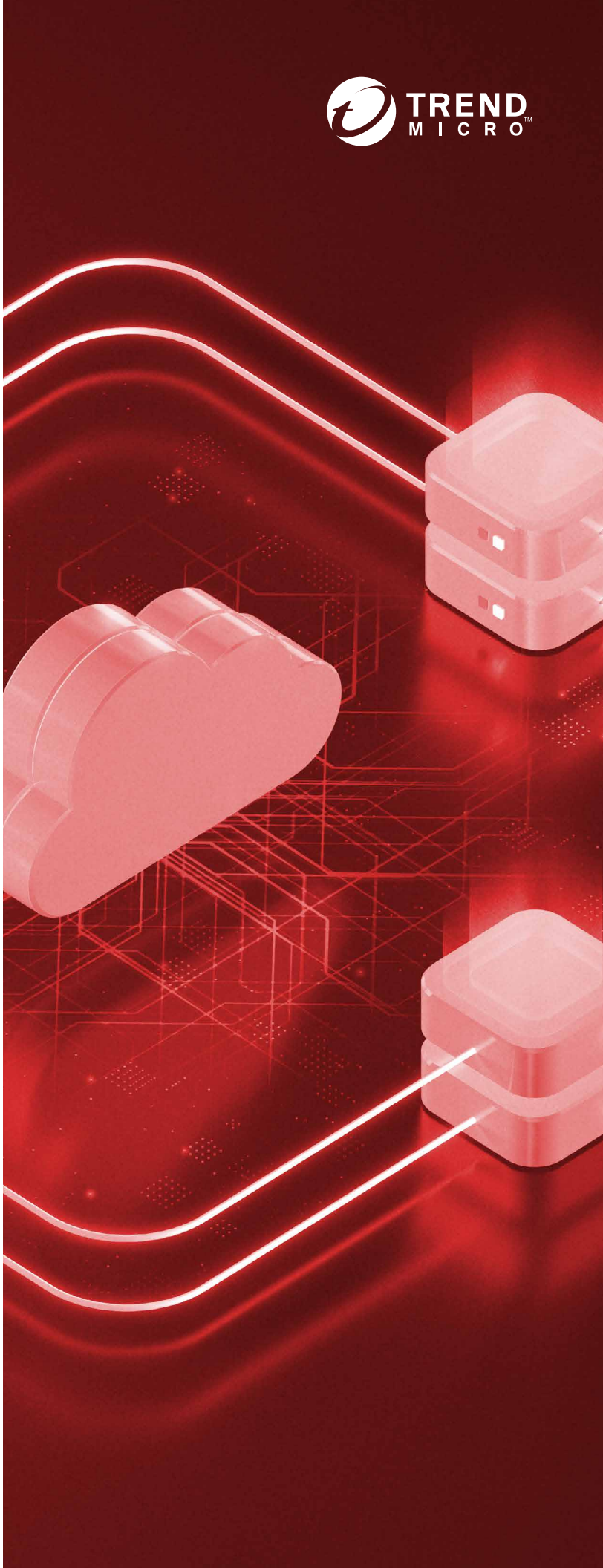
Cloud Security Simplified

With an exploding set of cloud infrastructure services and an increasing number of stakeholders involved in infrastructure and security decisions, the cloud has formed the perfect storm for security. Business requirements and DevOps processes demand faster application delivery, however, if you increase the speed of delivery, everything else must follow suit.

In order to gain the benefits of the cloud and meet business objectives, cloud security needs to match that set of cloud infrastructure services and the speed of application delivery. Through three use cases, cloud operational excellence, cloud migration, and cloud-native application development, we will help you calm the storm and shine some light on how to simplify your cloud security. Already have some of these covered? Navigate to the sections that best apply to your cloud security needs by clicking below.

- **Cloud operational excellence**
- **Cloud migration**
- **Cloud-native application development**



Cloud Operational Excellence
Guardrails to avoid cloud misconfigurations

Building the Foundation of Great Architecture

There is no shortage of benefits when it comes to the cloud, and your teams are taking notice. Capitalizing on the advantages of the cloud, your organization is racing to make the shift, however, you need to take a step back to ensure operational excellence is a priority.

When it comes to cloud operational excellence, some jump to the assumption that it doesn't require the same attention as traditional on-premises environments. But the truth is, there are many aspects that need to be considered to achieve this type of excellence. If anything, the stakes and opportunities are higher than ever to ensure that strong operational excellence strategies are implemented. This is especially true when it comes to partnering with cloud service providers (CSP) and ensuring you are holding up your end of the bargain as part of your CSP's Shared Responsibility Model.

A Framework for Simplicity

The first step in the journey to operational excellence is ensuring cloud builders are following best practice architectures, like the Amazon Web Services (AWS) Well-Architected Framework and Microsoft® Azure™ Well-Architected Framework. These frameworks were developed to help cloud architects and developers build secure, high-performing, resilient, and efficient infrastructure for their applications.

Operational excellence is a key theme in both frameworks to keep a system running in production and provide a consistent approach to evaluate architectures and implement designs that will scale over time.[1] It's important to ensure your architecture and workloads are aligned with engineering best practices and standards to ensure they are truly operationally excellent.[1] These frameworks provide a foundation for businesses to build in the cloud more effectively and deliver greater business value. Let's dive into some of the ways operational excellence can help to build architecture that enables business success.

Rest Easy with Operational Guardrails

When it is time for your company to organize Cloud Centers of Excellence and implement shared services across your cloud environments, you will want to ensure best practices are consistently enforced. These operational guardrails move organization towards operational excellence, ensuring standard functions occur predictably and consistently across the organization. With these controls in place, you will have confidence that:

- Critical data stored in the cloud is protected by automatic enforcement
- Network access policies and security groups are always properly configured to minimize unrestricted access
- Identity and access management permissions are defined for controlled access

Automatic operational controls ensure rules for these shared services are enforced at scale and are following best practices, external regulatory compliance, and your organization's internal governance. Now, take a deep breath and rest easy knowing your organization won't be in tomorrow's headline for the latest security breach.

Did Someone say Automation?

To leverage the agility of the cloud or experience the cost savings typically associated with cloud adoption, automation will reign supreme. Even the most skilled, dedicated, and experienced developer makes errors, it's just human nature.

Treating your operations as code, such as scripting your runbook and playbook activities, reduces the risk of human error, but introduces different risks to operational excellence. Developers often find themselves in high-pressured scenarios, forced to meet deadlines and deliver something that works—even if they know that they are not following coding best practices. As an example, in a rush to meet a deliverable, your IT team may decide not to configure granular IAM permissions for a virtual server. Granular permissions using IAM roles provide an additional level of protection by ensuring that your infrastructure is aware of its users, so it enforces coarse-grain permissions on what they can do. Now, without the proper configuration, the organization could easily suffer a devastating security breach. The bottom line is, it's important to ensure best practices are followed across the development process, even on the tightest of timelines.

Automation can ensure you get the most out of your cloud infrastructure by utilizing things like auto-scaling, self-healing, deployment scripts, customized reporting, and more. Operations as code allow architects and DevOps engineers to version the application infrastructure as much as the developers are versioning the code. Building and operating architecture that maximizes efficiency and is highly responsive will free your teams to build applications to support business goals.

Infrastructure as Code = Fast Innovation

As discussed, the increasing preference for automation, alongside the accelerated adoption of cloud computing and CI/CD practices, means infrastructure is now designed, deployed, and configured in an entirely new way. Needless to say, the cloud is your oyster and you can achieve almost anything you wish.

In the cloud, you can:

- **Apply the same engineering discipline that you use for application code to your entire cloud environment**
- **Define your entire workload as code and update it with code**
- **Script your operations' procedures and automate their execution by triggering them in response to events**

Terraform

AWS CloudFormation

Another way to increase your usage of automation is with Infrastructure as Code (IaC). This entails the provisioning and management of cloud resources and infrastructure through formatted, machine-readable files. **The management of virtualization through automation** and using automation tools, like AWS CloudFormation or Terraform templates, is a great way to do this. CloudFormation can be used to create and provision cloud infrastructure resources, such as Amazon Elastic Compute Cloud (Amazon EC2) instances, with a simple text file. This text file describes a collection or stack of AWS resources to be deployed and configured together.

The business benefit of using IaC is its consistency, speed, and the lower costs for projects to be created and deployed. This advanced and efficient infrastructure deployment method means critical changes on your cloud environments can be completed quicker than ever. So, what's the catch?

Unfortunately, security, compliance, and performance implications can also be introduced just as easily. To instill more confidence in using IaC, there are solutions that test your CloudFormation scripts before deployment, so only the cleanest and most secure templates make it to your environments. Thus, potentially damaging changes can be easily inspected or rolled back. For example, if an Amazon Simple Storage Service (Amazon S3) bucket is created without server access logging enabled, an AWS Lambda function could be triggered to automatically implement the best practice. Checks for improvements and the quality of your CloudFormation collection without the need to execute the code first is extremely valuable for cloud builders.

A Giant Step to the Left

DevOps has brought a methodology of "fail fast, fail often" to the masses, which has helped teams innovate and move faster than ever. While this may seem great, a lack of quality can be hard to explain when a critical failure is discovered, such as an unencrypted Amazon S3 bucket, resulting in a data leak.

Ideally, you would have guardrails as far left as possible in the CI/CD pipeline—right into the developers' hands. Leading cloud builders are using these automated, preventative measures before code is deployed to ensure security and compliance. Here are some examples of common and easily missed misconfigurations:

- **Allowing public access to Amazon S3 buckets that are storing sensitive data**
- **Opening too many TCP ports within Amazon EC2 security groups**
- **Allowing unrestricted access through Azure Network Security Groups (NSG)**
- **Permitting malicious behavior in Azure SQL Database**
- **Granting permissions to wrong IAM users and roles**

To enable full confidence that security vulnerabilities, cloud resource leaks, and performance and reliability issues won't make it into production, you need a solution that can:

- **Predict if an incident will happen and then provide remediation early in development—resolving multiple concerns before they even occur**
- **Check your workloads against rules before deploying them live to your cloud infrastructure. Each resource should be checked against hundreds of industry best practices, including the AWS Well-Architected Framework, CIS Microsoft Azure Foundations Security Benchmark, ISO 27001, HIPPA, PCI DSS, and GDPR**

Shifting operational excellence, security, governance, and compliance checking to the earliest phase of the CI/CD pipeline enables automated, proactive prevention of misconfigurations. What's more, these same checks and self-healing can also be performed in live cloud environments. Regardless of when you scan your code to check for alignment to best practices, give your organization peace of mind that they are building great architecture.

Too Many Cooks in the Kitchen

One of the biggest challenges in modern software development is that every deployment is dependent on multiple teams. Developers, operations, infrastructure engineers, and business units all have a role to play in ensuring that an application is delivered successfully. Getting alignment from all of these different teams can be tough. Regardless of your team's structure, working towards operational excellence will help overcome the challenge.

Rather than being a burden, operational excellence can serve as a cultural goal that is shared by all teams and team members during the software development and deployment process. By transforming operational excellence into a culture, your teams can have an overarching goal to strive towards, which is important when working with cross-functional teams. A culture of operational excellence helps to set a standard of best practices, continuous improvement, and collective pride in what the team is building and deploying, ultimately contributing to the success of the business.[2]

Times are Changing…Are You?

Cloud service providers are constantly coming out with new services and best practices. Even if your accounts were completely optimized, reliable, efficient, and secure a few weeks ago, there's no guarantee they are today or tomorrow.

How valuable would it be to have comprehensive visibility of your infrastructure and automatically adhere to best practices, security, and compliance? With this information, you can continue to evolve your cloud infrastructure, while continually building great architecture. Ultimately, helping to foster innovation and the foundations for business success in your organization.

Operational excellence is a combination of processes and continuous improvement to ensure your infrastructure remains secure, reliable, efficient, and cost effective. Every operational event and failure should be treated as an opportunity to improve your architecture. For developers and IT teams, this can seem like a daunting task, but with a culture of operational excellence, you may find teams are up for the challenge.

Now What?

Enabling cloud operational excellence to support your business's innovation goals relies on finding a solution that has:

- Multi-cloud visibility for a real-time view of security, compliance, and governance within your cloud infrastructure
- Hundreds of automated checks with self-healing based on CSP's well-architected framework, the latest best practices, and industry compliance requirements—eliminating risks
- Reporting features that can run reports on an endless combination of filters to exhaustively audit your infrastructure
- Seamless integration into your CI/CD pipeline and existing workflows through APIs, enabling the ability to have deep and intuitive integration into your live public cloud environments
- Template scanners that are used during the coding process to ensure your teams are building well-architecture for automated, proactive prevention of vulnerabilities

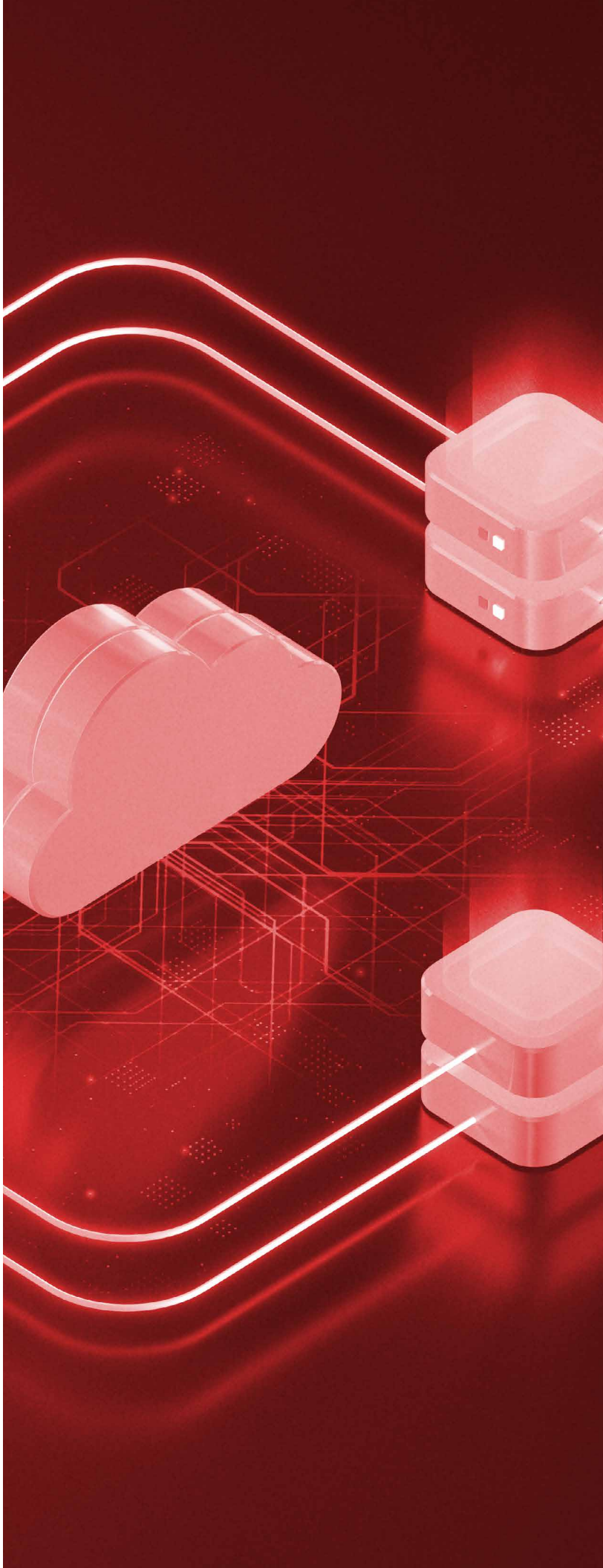
Whether you are in the cloud, making the transition, or just about to jump in, having a culture of cloud optional excellence will provide the foundation needed for proper configuration, compliance, and overall success. Keep all of these tips and tactics in mind as you continue into the next section, where we review four security considerations for cloud migration.

Cloud Migration: Achieve More Together with Four Security Considerations

The Cloud is Here

The conversation around making the transition to the cloud has shifted from a discussion of ***if*** to ***when*** and ***how***. The days of only using in-house servers has become increasingly rare.

A hybrid or multi-cloud strategy is becoming more and more popular. The combination of on-demand reliability, high availability, cost-effectiveness, and enhanced flexibility makes a hybrid cloud strategy especially valuable to an organization—the best of both worlds. However, while a lot of good can come from adopting cloud computing, there are risks.



“At this point, cloud adoption is mainstream.”[3]

SID NAG, RESEARCH VP AT GARTNER

Cloud Computing: The Good, the Bad, and the Ugly

There’s no silver bullet when it comes to cloud migration. However, the likelihood of a successful migration is boosted when organizations are aware of best practices. This starts with taking the time to research and create a strategic plan that anticipates predicted challenges and includes the early integration of security.

The migration process and cloud itself, open an organization to a whole new world of security risks, including web application exploitation, cloud malware injection, and more. With that said, if you plan and take a proactive approach, you will help to limit the risks and complete your journey more or less unscathed. But the work doesn’t stop once the migration is deemed “complete”. In order to achieve an on-going strong security posture, you must maintain continuous security throughout your cloud.

Now that your organization has this shiny new platform to work on, teams are eager to explore the new possibilities they can take advantage of. While all have good intentions, this can transform the cloud from a valuable tool to a security nightmare. Without proper processes and controls, your organization is going to find itself with cloud sprawl—multiple teams starting new cloud projects in multiple clouds and operating systems.

“A report by International Data Services (IDC) said public cloud spending will grow from $229 billion in 2019 to nearly $500 billion by 2023, which is good news for telecommunications companies and hyperscale cloud providers. The compound annual growth rate (CAGR) for public cloud spending is projected to be 23%.”[4]

Creating a consistent security posture across a hybrid cloud environment requires a balance of careful preparation and a roll-up-your-sleeve-and-jump-in mentality.

Here are four security considerations to help ensure that you are prepared and empowered to properly secure your cloud migration and future cloud projects—without slowing down the process.

1

The Right Place at the Right Time

Security can quickly become complex when adopting a hybrid cloud strategy that consists of workloads running in multiple environments, with different tools and teams. Having data sprawl like this forces security to become much more intelligent. Having workloads in multiple private and public cloud infrastructures, as well as in on-premises servers, introduces new vectors for breaches. And whether you're running bare-metal workloads, virtual machines, containers, or serverless functions, each workload requires its own unique set of security capabilities to protect against known and unknown threats.

Simply placing a firewall at the perimeter of the cloud infrastructure will not cut it. You need integrated security that can protect your cloud migration simply, seamlessly, and securely—anywhere.

To do this, you must make sure that you're equipped with the capabilities needed to secure each type of workload, but not adopt too many point solutions that will end up increasing costs and creating a lack of consistent visibility. Security should be viewed holistically, taking inventory of the type of workloads, environments, platforms, and operating systems that will be leveraged during the cloud migration. This will assist in creating a security strategy that is streamlined, automated, and provides the capabilities needed—without slowing down development or creating siloed security.

2

GDPR, HIPPA, PCI, FISMA, Oh My!

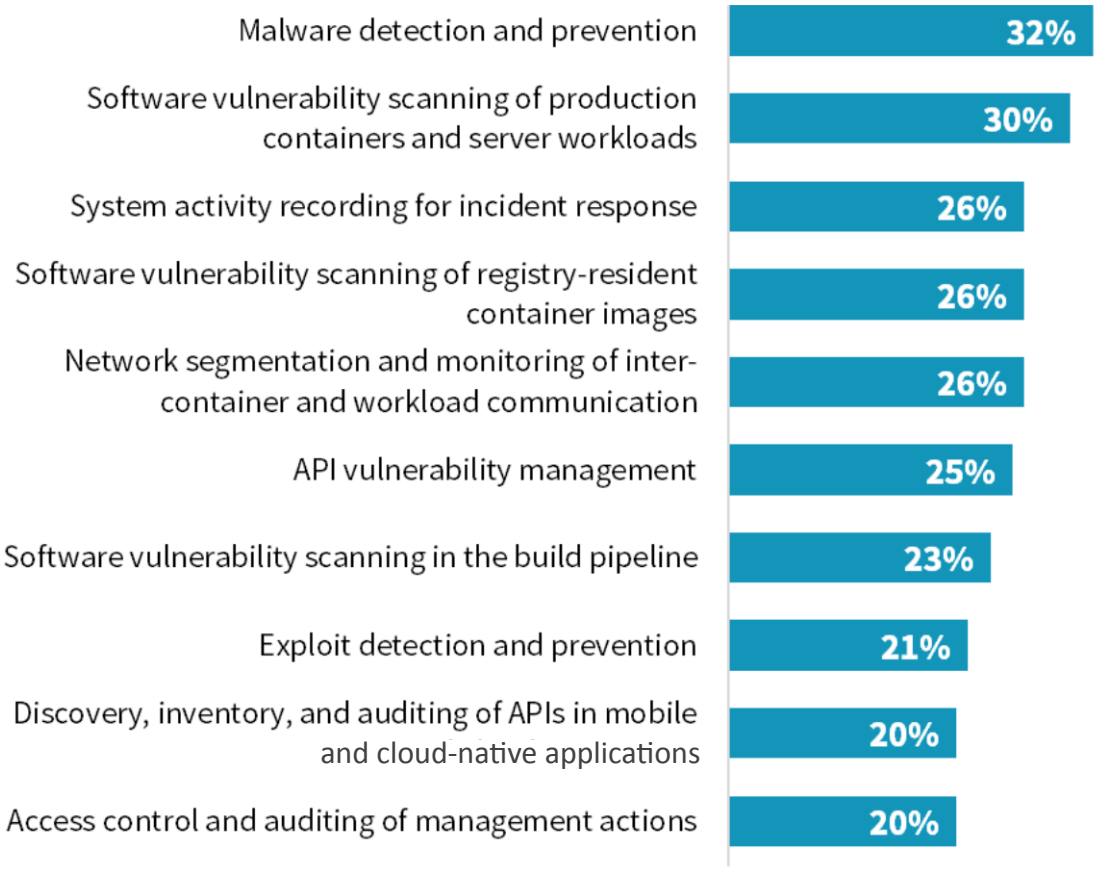
Achieving and maintaining compliance in the cloud can be a daunting task. The phrase "look before you leap" is especially fitting here. Not only are there more servers and instances than before, but they are ephemeral and can last as briefly as a few hours. With the mounting number of compliance standards, such as GDPR, HIPPA, and PCI, understanding your organization's compliance standards before starting on your cloud migration is essential. In doing this, you will help prevent future roadblocks, such as reconfiguration, staffing rearrangements, and budget reallocation.

Having a strong knowledge of the shared responsibility model will provide clarity into what your CSP is responsible for securing, versus what is your organization's domain. A rule of thumb when working with public clouds, such as AWS, Microsoft® Azure™, or Google Cloud Platform™, is that your CSP is responsible for the security of the cloud: Protecting the hardware and infrastructure. Whereas, your organization is responsible for security in the cloud: Securing the data and applications you put into the cloud. Being aware of compliance standards in the early stages of your cloud migration can help ensure your business remains compliant, as well as avoids regulatory fines, unplanned development interruptions, and possible reputation damage.

The most important security controls span stages

Runtime malware prevention, auditing, access controls, along with pre-deployment vulnerability mitigation, take the top 7 out of 18 spots.

Question text: Which of the following types of cloud-native application security controls are most important? (Percent of respondants, N=371, five responses accepted)



Leveraging DevSecOps to Secure Cloud Native Applications, Doug Cahill, Senior Analyst and Group Practice Director; Bill Lundell, Director of Research; Jenn Gahm, Senior Project Manager, The Enterprise Strategy Group, Inc, July 2019.

3

Jack of All Trades, Master of All

Similar to ensuring the technological infrastructure is prepared, you also need to do all you can to ensure your human infrastructure is prepared. Properly equipping your staff with the skill set needed to work on and manage a cloud migration is essential for success. This will help avoid cloud misconfigurations and other human errors.

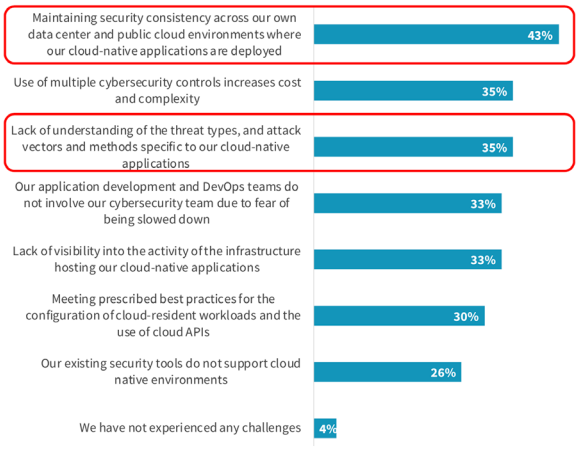
Managing and securing a hybrid cloud computing environment is totally unique, compared to those found in local data centers and routine virtualized resources. Being a jack of all trades is becoming an increasingly common requirement for IT and DevOps, wearing so many hats that the closet becomes full and security is lost in the mess.

On the job training is the new reality. Encouraging employees to be willing to learn, experiment, innovate, and adopt agile processes along the way, while not being afraid of failure, will be the mentality that bolsters excitement, instead of fear.

The top concerns for managing a hybrid cloud environment: Ensuring consistency across data center and public cloud environments, as well as a lack of understanding of the cloud threat types and vectors.[5]

Environmental Differences Require Retooling and Creates Complexity

Technical differences in cloud-native applications require a retooling of all aspects of a cybersecurity program, resulting in the use of too many specialized controls.

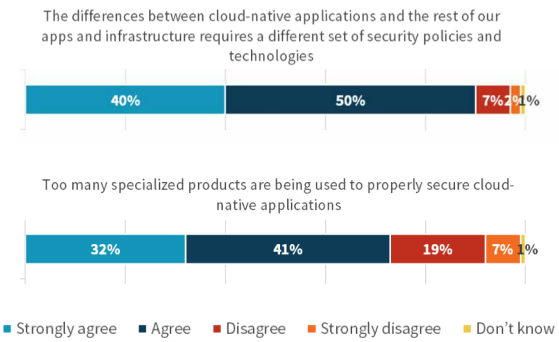


Consistency Across Hybrid Clouds is the Top Challenge

The perceived need for specialized controls by environment creates concerns around consistency, cost, and complexity. Respondents also understand they need to update their threat model.

Question text: Which of the following represents the biggest cloud-native application security challenges for your organization?

(Percent of respondents, N-371, three responses accepted)



Leveraging DevSecOps to Secure Cloud Native Applications, Doug Cahill, Senior Analyst and Group Practice Director; Bill Lundell, Director of Research; Jenn Gahm, Senior Project Manager, The Enterprise Strategy Group, Inc, July 2019.

4

To the Left, to the Left

It's no secret that moving workloads to the cloud can result in cost, scale, and geographic benefits. But there is also value to be gained from the cloud migration process itself. This journey can provide your company with the opportunity to shift its culture. Developers will be working closely with management during this transition, and this cross-functional collaboration can result in the adoption of more agile and DevOps-focused processes, such as incorporating CI/CD pipelines to encourage faster release cycles.

Security can benefit from this transformation by injecting security earlier in the pipeline—before workloads are pushed to production. With this shift to the left, security solutions can detect vulnerabilities and malware earlier and more efficiently. Now, security can empower developers to continue to iterate fast and ship often, instead of slowing it down.

Achieve more together

Cloud migration is an all hands-on-deck process. There needs to be support and collaboration from almost every team in the organization, but most importantly IT Security and DevOps. With a cross-functional and collaborative effort, you can achieve your top-level cloud migration objectives, while meeting the needs of the teams involved.

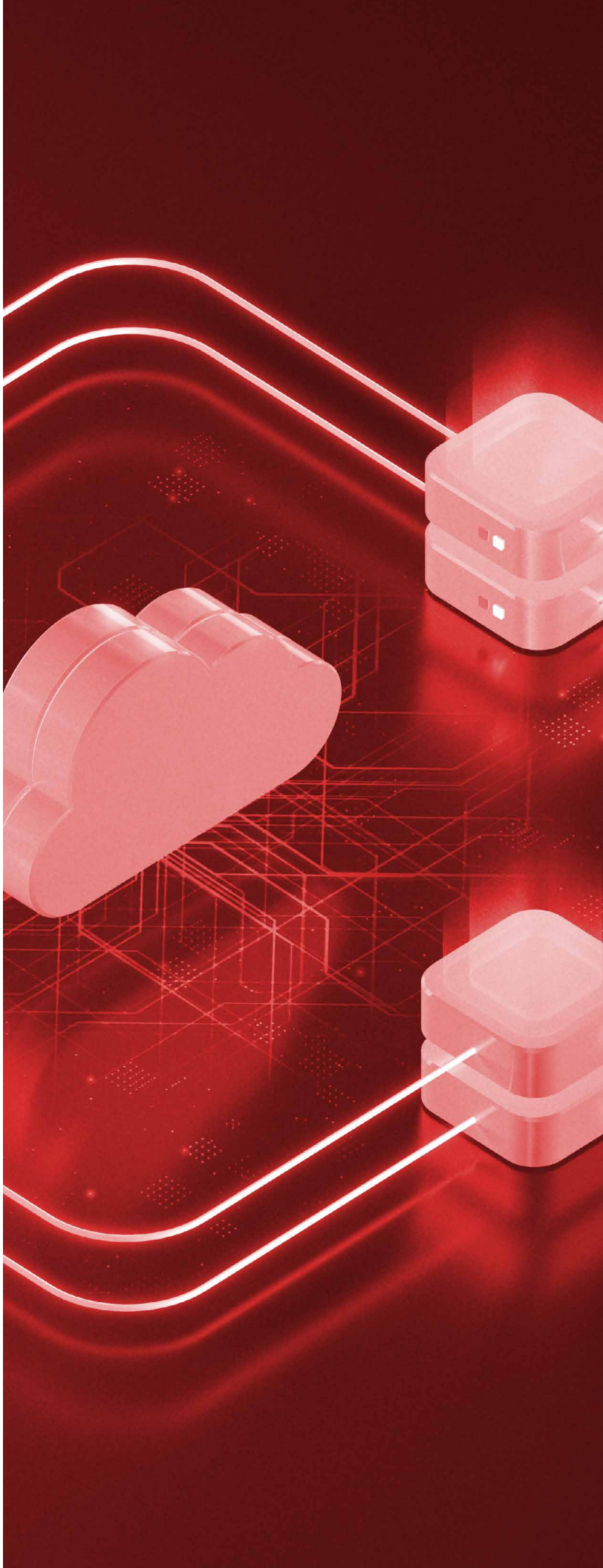
Now that we know how to make a strong foundation and transition to the cloud; it is time to take things to the next level and make your life a little easier. In this next section, we are going to look at four ways to get cloud-native smart and secure, looking at the power of automating security early in your build pipeline and across your cloud environment for complete visibility and protection against threats. Sounds intriguing, right? Let's continue.

Four Ways to Get Cloud-Native Smart and Secure

The Transcendence of Cloud-Native Application Development

Cloud-native application development has transcended legacy infrastructure and opened doors to advanced container architecture and service platforms.

With rapid integration and deployment for development teams and increased automation and visibility for operations teams, application development has given rise to microservices-based architectures leveraging agile DevOps processes. And with immutable infrastructures, organizations have focused on cloud-specific strategies and innovations to compete and deliver better business outcomes and success.



According to an Enterprise Strategy Group (ESG) study, 74 percent of companies who cite an extensive use of DevOps are also employing agile software development practices.[6]

While this all sounds amazing, we are forgetting something…security. Traditionally, security teams have been tasked with securing the network perimeter, data center, and monolithic applications. But this is all changing, as DevOps teams are moving at a faster pace than traditional security can keep up with. Organizations are recognizing the need to shift mainstream security techniques to focus on the development processes, services, and packages that make up cloud-native applications. Whether its cloud migration, container development, or serverless computing, IT security teams are challenged with how best to protect and manage agile cloud development ecosystems and deployment and runtime platforms, without slowing down DevOps. So, how can security become more agile and protect this new world?

Spoiler: Security doesn't go away; it just takes on different forms.

Cloud Native at its Core

Depending on who you ask, the term cloud native can mean different things to different people. Although a common misconception is that the term describes where an application is built, but in actuality, cloud native is all about how an application is built and deployed.

At its core, cloud-native application development is a method for developers to create and deploy scalable and dynamic applications. Designed for agility and flexibility, cloud-native applications enable developers to run new features quickly, as they aren't chained to a monolithic software codebase. Making them even more alluring, cloud-native applications are typically created using DevOps processes and developer-friendly architectural technologies, commonly referred to as microservices. So, to make a long story short, what is cloud native? It's a DevOps dream.

Cue Microservices

There has been a steady rise of microservices adoption over the traditional monolithic application. Microservices use an architectural style that enables an application to be divided into a number of smaller, individual, and independent services, like containers and serverless functions. Each microservice can be created from a different language on a different platform—amazing, right? Developers sure think so, and why wouldn't they? Microservices enable fast deployment, scalability, flexibility, and service isolation, which is everything DevOps embodies. However, as with any new technology, we are faced with new risks.

From Monolithic to Cloud Native—All for One and One for All

Mitigating and overcoming cloud-native application security challenges can only be done when developer, operations, and security teams step out of their silos and work together. This isn't as easy as just knocking a wall down, it takes a whole different approach to cloud infrastructure. Organizations must manage cloud instances and workloads in a different manner than before.

For example, cloud instances and workloads can be used for development and production requirements as well as storage, but are run by CSPs. While security agents can deploy security on these configurable cloud servers, other instances, such as serverless platforms and compute, can require security to be included when the application is being built and instantiated. This delivers the ability to identify threats at runtime with deep instrumentation and visibility into the code stack, including the line number and vulnerabilities. As cloud providers remove access to container environments, these restricted scenarios require new ways of securing the instances and data hosted within. This shared responsibility model prevails and safeguards organizations from unforeseen risks and relaxed security practices.

For developer, operations, and security teams, embracing a common security objective helps create a stronger cloud application strategy and compliance posture without impacting all the layers of abstraction and speed associated with cloud adoption.

A New Approach to Security

Legacy data center and on-premises security techniques aren't built for this new modular and agile environment. Holding onto old security habits can expose your applications to new vulnerabilities and threats. Adapting your security to a cloud-native world may appear to be a setback, but it also opens the door to exciting opportunities to implement and leverage security in a whole new way.

As you know, microservices architectures allow for multiple operating systems (OS) and programming languages. But did you know that this creates many more threat vectors that may be vulnerable? With so many cloud application migrations and new development projects taking place across multiple business units, an organization must think differently about their security strategy.

Containers can be built and managed using multiple tools, on multiple platforms. If development teams are just beginning their cloud-native transition, there could be discrepancies in how containers are designed and deployed—a lack of standards or direction can result in unknown security gaps and lack of visibility. Today's cloud-native application security parameters are much different than protecting monolithic applications. They take into account greater risks associated with open-source dependencies, build pipeline vulnerabilities, and lack of runtime defenses.

Here are four ways to rethink and apply security in this new frontier of microservices and cloud-native application development.

1

Protect the Messenger!

APIs are everywhere and are essential to the development and deployment of applications. They act as an intermediary or digital gateway to allow apps to communicate and share data in a fast and easy way. As integration and interconnectivity between microservices are becoming increasingly important, so are APIs. However, APIs provide a new attack vector for threats, and recent events have shown that broken, exposed, or hacked APIs are the cause of major data breaches—we need to protect them.

The three most common problems that lead to security issues are:

- Exposing sensitive data
- Intercepted communications
- Launching denial-of-service (DoS) attacks against back-end servers

But not all hope is lost. You can improve API security by leveraging encryption, quotas, tokens, API gateways, and throttling. When selecting a security vendor, look for features like automated deployment, seamless integration, and real-time support to make everyone's life a little easier. For instance, Trend Micro offers an **Automation Center** built by developers for developers. In there, you'll find automation guides/cookbooks, API references, including parameter descriptions, request and response schemas, and language-specific SDK examples. It also offers direct engagement and support from our team members on Stack Overflow, integrated with our internal automation support Slack channel.

2

Integrate, Deploy, Integrate, Deploy, Integrate, Deploy…You Get it

The CI/CD methodology is the backbone of the modern DevOps environment and is the new standard for how modern developers build great products. The demand for faster delivery cycles is pressuring teams to update their monolithic development models for more agile, streamlined processes. The CI/CD pipeline allows teams to release a constant flow of updates into production, weekly, daily, or even multiple times a day.

The challenge with pipeline security is twofold:

- Securing CI/CD workloads
- Securing the pipeline itself

Traditional and manual security, that rely on human interaction, can't scale to meet the needs of the continuous build and release structure. What is needed is a more agile and automated approach to security, with greater visibility and control to account for the faster and more dynamic delivery cycles. The key is shifting earlier in the build pipeline to enable continuous scanning for malware, vulnerabilities, secrets, and keys before the image is pushed to runtime. This ensures that the workload is better protected without slowing down the delivery time.

Security teams don't want to restrict the high-volume release cycles of cloud-based applications and impact business and customer goals; they want to minimize the risk of a breach that would slow you down. With todays increased attention on cyber threats, cloud vulnerabilities provide an opportunistic climate for novice and expert actors alike, as a result of:

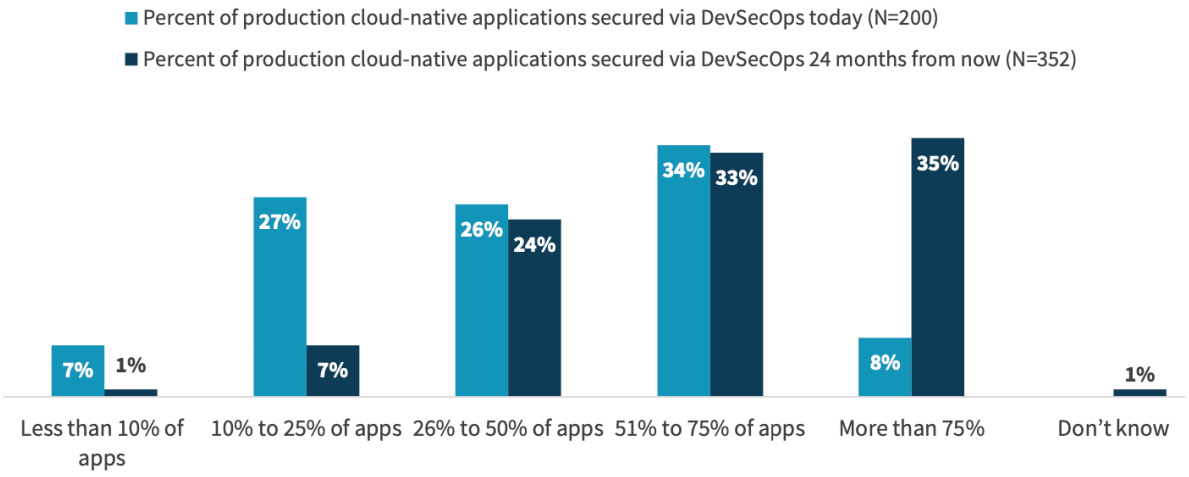
- Slow-paced adoption of hybrid and cloud-native protection practices at the expense of people, processes, and technology
- Rapidly growing dependencies on modern application development tools and practices outside of IT
- Increased challenges and business uncertainty that lead to costly endeavors in both time and skills

Security teams can't possibly administer security policies across all cloud instances and workloads or check that those instances have met security requirements. Companies need to adopt container-specific security solutions that can scale across the requirements of the CI/CD pipeline and minimize potential compromise.

This is accomplished by using an integrated, automated solution at pre-deployment and runtime. The seamless integration allows developer and operations teams to continue to deploy at speed and gives your IT security team the ability to adhere to compliance requirements. Automation at scale is necessary for security and visibility in today's microservice architectures and runtime environments.

Apps Secured via DevSecOps will Grow Over Time

As DevOps teams establish repeatable and scalable DevSecOps integrations, more applications will be secured via such use cases.



"DevOps teams too often view security as impeding innovation and slowing down projects. As such, the first step in implementing a secure DevOps program is to gain organizational alignment."[6]

DOUG CAHILL, ESG

3

The Key to Success

Containers solve a critical issue in the DevOps world—they allow applications to run correctly across various computing environments. With developers turning to multi-cloud, multi-language infrastructures, this flexibility has become the key to success; as containers provide infrastructure flexibility without having to rewrite apps or perform major configuration changes. Containers also require minimal overhead, offer fast deployment cycles, and allow for smooth scaling.

There are a lot of moving pieces of the container environment: Code repos, pipeline images and registries, container runtime platforms and hosts, and orchestrators. These all need to be considered when implementing a secure cloud environment. Each layer provides unique opportunities for bad actors to engage in a growing threat landscape.

To learn more about securing your containers, **read our report** on 6 steps to comprehensive container security.

4

With performance demands and application release cycles becoming more and more ambitious, many organizations are turning to serverless compute architectures. Enabling developers to run containers without having to manage the host, run infrastructure as code (IaC) without having to provision, or manage the physical and virtual servers has changed the way applications are consumed, deployed, and built.

This hassle-free methodology allows developers to focus on what they do best—code. A key benefit for product development and cloud teams is that organizations only have to pay for the compute resources they use, ensuring no idle capacity is wasted.

While serverless introduces new attack vectors, there is an upside. With a serverless architecture, organizations don't have to worry about network, host, or infrastructure security. This relieves a lot of the security burden, but there are other vectors that should be top of mind, such as event injection, broken authentication, insecure deployment settings, and DOS attacks.

There may not be a silver bullet to protect against all types of serverless risks, but you can take steps to protect these platforms, such as:

- Sourcing and writing clean code
- Performing input validation
- Protecting secrets and keys
- Error handling

Utilizing all of these practices will help ensure that your serverless deployments stay secure.

You Can Have It All—Satisfy Security and Development Objectives

The benefits of cloud-native application development are endless, but there can be major security risks. Modern development practices and technologies, like CI/CD, containers, and serverless, require application security that provides earlier detection, immediate protection, and assurance that your cloud services meet security best practices—all while maintaining the speed and flexibility that DevOps teams require. This can be a lot to consider, but if you rethink security and apply it in a new way, it can enable you to continue to move quickly and securely.

Meet your cloud security needs.

There will always be different drivers behind your constantly evolving cloud security priorities. Whether you are looking to adopt a cloud center of excellence model, transition to the cloud, or take advantage of cloud-native applications, you need a powerful security solution that allows you leverage all of the benefits and efficiencies the cloud offers your business—securely.

It takes continuous work to secure your complex and fast paced multi-cloud environment—so let's simplify it. Trend Micro Cloud One™, a security services platform for organizations building in the cloud, delivers the broadest and deepest cloud security offering in one solution, enabling you to secure your cloud infrastructure with clarity and simplicity.

- Automated deployment and discovery lead to operational efficiencies and accelerated, streamlined compliance.
- Flexible to choose the cloud, the platforms, and the tools, and we leverage our turn-key integrations and broad APIs, freeing you to procure the way you want and deploy the way you need.
- All–in-one solution that has the breadth, depth, and innovation required to meet and manage your cloud security needs today and in the future. Cloud-native security delivers new functionalities weekly with no impact on access or experience. Seamlessly complements and integrates with existing AWS, Azure, VMware®, and Google Cloud™ toolsets.

Learn more today: https://www.trendmicro.com/en_ca/business/products/hybrid-cloud.html

Sources:

1. Fitzsimons, P., B. C., Steele, J., & King, R. (2018). Amazon Web Services – Operational Excellence AWS Well-Architected Framework. Retrieved from https://d0.awsstatic.com/whitepapers/architecture/AWS-Operational-Excellence-Pillar.pdf?ref=wellarchitected-wp
2. Tozzi, C. (2019, November 19). Operational Excellence and the Success of Software Deployments. Retrieved from https://devops.com/operational-excellence-and-the-success-of-software-deployments/
3. Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020. (2019, November 13). Retrieved from https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020
4. Robuck, M. (2019, July 03). Public cloud spending will near $500B by 2023: Report. Retrieved from https://www.fiercetelecom.com/telecom/spending-public-cloud-will-more-than-double-by-2023-report
5. Leveraging DevSecOps to Secure Cloud Native Applications, Doug Cahill, Senior Analyst and Group Practice Director; Bill Lundell, Director of Research; Jenn Gahm, Senior Project Manager, The Enterprise Strategy Group, Inc, July 2019.
6. The Secure DevOps Imperative: Three Best Practices for Securing Cloud-native Applications, Doug Cahill, Senior Analyst and Group Practice Director, The Enterprise Strategy Group, Inc, November 2019.

TREND MICRO™ | Securing Your Connected World

[eBook01_Cloud_One_Full_200827US]