tufin The Security Policy Company.

Tufin Cloud Security Guide

Addressing Enterprise Cloud Security Challenges Head-on

Executive Summary

Powered by new cloud technologies and processes, the modern enterprise is more responsive to customer needs and competitive pressures than ever before. However, traditional security tools and processes used by IT were designed for a slower, less-dynamic landscape; leading many organizations to trade security for agility. To protect the enterprise, IT leaders need a deeper understanding of the roots of cloud security challenges and how to address them via increased visibility, automation and control. By adopting cloud-native and DevOps practices, IT security can help the enterprise restore the balance between agility and security.

The Enterprise Moves to the Cloud; Security Concerns Follow

There's no disputing a tectonic shift is occurring as enterprises move to the cloud. In fact,more than 50% of organizations moved their workloads to the cloud in 2020 according to the 2021 Flexera State of the Cloud report.

According to 451 Research, however, 46% of those surveyed for the Voice of the Enterprise report suggest that security and compliance is their most significant concern when adopting cloud-native technologies. Many security, network and cloud operations teams are now faced with balancing the requirements of security and agility in a multi-cloud, hybrid world.

The level of concern security professionals feel is reasonable, given the prediction from Gartner is that through 2025, at least 99% of cloud security failures will be due to misconfigurations.

This whitepaper will help enterprises better understand the roots of cloud security challenges and how to effectively handle them via increased visibility and more effective security controls. Let's take a deeper look.

Why Enterprises Struggle with Cloud Security

In a survey conducted with ESG Research, the resulting report, "Network Security Operations Transformation: Embracing Automation, Cloud Computing and DevOps," offers a 360-degree perspective of where cloud security challenges are cropping up for enterprises today. More than half of the security professionals say that network security operations are more challenging today than two years ago.

Why? It comes down to a few factors:

- More connected devices
- Rising cloud adoption
- More frequent and severe cyberattacks
- More vulnerabilities

Further complicating the picture, the report, along with other recent industry research, indicates that hybrid cloud computing and agile development are both on the rise, alongside the usage of containers and microservices in the enterprise. Working within a public cloud environment is considerably different from the traditional network. An IT team used to on-prem environments often lack familiarity with cloud best practices and misunderstandings around cloud security controls can lead to end user errors that increase risk for the business. For example, teams may accidentally configure access to cloud resources too broadly, creating openings for direct attacks or a lateral move from a breached service. Differences between traditional and cloud computing environments make operating a hybrid IT program challenging and add to the security concerns that arise.

Additionally, as we will explore more in-depth, agile development requires DevOps and IT teams to find ways to work security checks into the development pipeline early and often. Done right, this results in faster and more secure code releases; but it is a challenge to get there.

What will it take to successfully surmount the obstacles that enterprises face? As the ESG report puts it, "CISOs must address these additional challenges by consolidating network security operations to gain visibility into cloud workloads, manage security policy, and automate security processes."

Sounds simple enough, right?

"Companies Don't Know What They Don't Know"

Here's the rub: Most organizations simply do not have sufficient visibility into what is going on in their cloud infrastructure. Another research report from Enterprise Management Associates (EMA) found some troubling statistics that indicate deep misunderstandings in what constitutes visibility.

For example, 98% of organizations who were using manual inspection processes for security believed that they had moderate to high visibility into how applications communicate within their infrastructure. Another 97% said they had high to moderate visibility into how requested changes might negatively impact running applications. So far so good…

Yet 58% of those using manual policy inspection tactics admitted that their inability to maintain standardized security policies was a significant or very significant factor in security or ops incidents that had taken place. Of those, 34% said security device misconfigurations were the primary cause of outages. We saw similar patterns around application testing as well.

The take-away? Companies don't know what they don't know. They may believe that they have sufficient visibility when doing manual inspections, but this is likely because they don't recognize what full infrastructure visibility \ looks like. Nearly half of the respondents even admitted that, when migrating business-critical apps to the cloud, they found out the hard way that they did not fully understand application communication flows—indicating that their visibility was insufficient.

Addressing Enterprise Cloud Security Challenges Head-On

If you're an enterprise operating today, odds are the picture we've painted above looks pretty familiar to you. But you might be asking yourself, how can I gain visibility into my cloud environment in order to ensure security?

In a nutshell, organizations must integrate security into the entire estate—including on-premises, private cloud, public cloud, and microservices—as well as into the development team's everyday processes for the continuous integration and deployment (CI/CD) pipeline. Moreover, the only way to cover the estate effectively is through a laser focus on security policy.

As the EMA report puts it, "Security should not restrict business; it should facilitate it… In the race to continue forward, many organizations seem to forget that security policies are not tied but must be driven by business processes."

Let's explore what this means.

Adoption Driven by Agility: The State of Enterprise Cloud Today

Enterprises are, increasingly moving to the cloud. Here's what motivates this move and how it impacts business priorities.

The Need for Speed and the Reality of Hybrid Cloud

Digital transformation and business agility are imperative for an enterprise to remain relevant and compete today and an executive priority at all forward-looking enterprises. This focus is driving cloud adoption and new development practices.

While legacy applications are still very essential and have not gone away, large organizations are increasingly shifting to public cloud infrastructure to meet the agility demands of the modern business world. And with massive investments in legacy infrastructure, it's not a simple rip-and-replace. The resulting hybrid and multi-cloud environments are an inherent part of the new computing reality. A consequence is that you have complex, fragmented environments that are difficult to manage. When making strategic decisions—including those that involve security, you must consider how to manage the hybrid landscape.

Optimizing DevOps

DevOps is often thought of as a job title, but it is, more accurately, an approach to development within organizations. DevOps encompasses the practice of automating software development, testing, and deployment processes, ultimately empowering businesses to release software faster without sacrificing reliability or quality.

Because DevOps requires teams to think in terms of iteration and constant improvement (vs. one-and-done releases), DevOps cannot succeed without automation. Automation is the backbone that makes workflows across development and operations teams more efficient than ever before. These agile teams are able to rapidly spin up and iterate new applications and services that drive major business value, making DevOps increasingly popular with enterprises today.

The challenge this poses is that DevOps teams often want to move faster than IT or security teams can handle with traditional processes. For example, developers can't wait weeks to have infrastructure provisioned and update firewall rules, but that is the current reality at most companies This often puts NetOps, SecOps and DevOps at odds when it comes to deployment and this must be reconciled to balance the goals of speed/agility and security. All teams must learn to work in close alignment and build processes that enables the rapid release of secure code.

"Mode 2" IT

The combination of DevOps and modern software architectures (microservices) enables organizations to gain agility not possible with traditional IT paradigms (what Gartner calls "Mode 1 IT"). Taking the place of monolithic architectures and waterfall development models is Mode 2 IT. Gartner describes Mode 2 IT in this way: "Mode 2 is exploratory, experimenting to solve new problems and optimized for areas of uncertainty. These initiatives often begin with a hypothesis that is tested and adapted during a process involving short iterations, potentially adopting a minimum viable product (MVP) approach."

While it can be hard to get rid of Mode 1 altogether, enterprises are increasingly employing bimodal IT practices. As with DevOps, Mode 2 IT enables agility but, transitioning to the cloud securely is the key to long-term success for enterprises.

The Five Major Roadblocks to Enterprise Cloud Security

Of course, this is easier said than done. In our experience, there are five major roadblocks to moving to the cloud securely if you are an enterprise. The roadblocks can be surmounted with the right approach, but it's key to understand them fully in order to build a comprehensive security strategy.

Visibility

Organic cloud adoption can make it challenging to obtain and maintain visibility, since instances spring up all around the enterprise and naturally come and go. Traditional security practices are often circumvented or engaged too late in the deployment cycle. Additionally, legacy practices tend to require manual intervention, or, even worse, lack support for cloud and cloud-native security controls altogether. Therefore, IT cannot reliably measure risk.

Compliance

Meeting compliance is difficult on-premises and the cloud adds an additional layer of complexity. Existing tools and practices can make it difficult to exert control over the cloud, without slowing everything down. For example, businesses who are beholden to HIPAA compliance must understand at all times where any PHI data is being stored, moved, or accessed. Fortunately, there are well known best practices for enforcing compliance in traditional environments. However, implementing similar protections in the cloud requires different tactics using cloud-native controls that can, for example, very effectively meet HIPAA requirements. Nevertheless, you must understand how the cloud works to properly implement these controls.

Automation

Within the enterprise, security teams have a persistent fear that automation is synonymous with "loss of control," so it may be seen as a roadblock to cloud security. In reality, automation enables proactive detection and correction of security issues before they get into production. Automation of security policy changes provides the pathway for consistent application of security rules and measured compliance. Done properly, automation can free up security professionals from mundane tasks so they can focus on higher value (and often more interesting) challenges.

Conflict Between Development and Security Priorities

DevOps teams often want to move as fast as possible, while the security team is focused on ensuring that nothing goes out that has not been reviewed to ensure it adheres to policy. Individually, each team strives to address their responsibilities and meet goals that provide business value. However, their well-worn processes tend to keep each operating in near isolation rather than collaborating, early and often, to insecure code being released. These dual requirements has also led to the increased establishment of DevSecOps to ensure the enterprise can balance the needs of security and development.

Hybrid IT

Hybrid or "bimodal" IT (as we previously described) is the reality at many enterprises today, but it can add complexity, especially due to the need for different security practices. While existing security tools and practices in the enterprise may be sufficient for Mode 1 (predictable, well-understood, legacy IT infrastructure and applications), they do not apply for Mode 2 projects. With a bimodal IT program, the key is to understand and accept that security practices which work well for Mode 1 projects will rarely carry over to Mode 2.

For example, in traditional networks, we assign IP addresses to physical and virtual machines. The workloads running on those machines tend to stick around for a long time—months or even years—so you wouldn't swap out IP addresses very often, making these markers a simple way to keep track of what's going on from a security perspective.

By contrast, cloud-native workloads are highly dynamic and can be deployed at much larger scale than traditional apps. Moreover, cloud-native workloads are built from a set of services, each of which is deployed separately. As a security parameter, a static set of IPs is too rigid for such a fluid environment.

This is just one example of where traditional security practices fail to measure up in the world of cloud infrastructure.

Additionally, even enterprises who are ready to embrace a cloud-first approach often find themselves saddled with on-premises applications and resources, and these can linger for years or even decades. Organizations will have cloud-native applications that require access to on-premises resources, which means they need to embrace security policies that work across hybrid infrastructure.

The Path Forward

If you have read to this point you have identified with the challenges of the cloud so what does the path forward look like?

At a high level, we believe that security must be integrated into the overall IT landscape for your best measure of success, no matter if you are deploying your applications on-premises, in the private or public cloud, and/or microservices. Security cannot be an afterthought or an add-on; it needs to be tightly bound up with everyday processes and efforts.

To make this a reality, there are four key steps we believe every enterprise should take.

Empower a Security Advocate

It's true in all areas of life. If no one is specifically responsible for a given task, it doesn't get done. Applying this principle to security, we recommend assigning an internal advocate. This should be the person whose goal is to foster collaboration throughout the organization, from NetOps and SecOps to DevOps and DevSecOps. The security advocate's mission is to help their teams resolve and avoid security issues in service of enabling the entire organization to succeed.

The security advocate can be your CISO, a security practitioner, or even a member of the DevOps team with a strong grasp of security. The person you assign to this role should be passionate about proactive security and understand at a deep level why security is so key to the success of your business.

This person should be the face of security at your organization. You can have them lead brown bag lunches on relevant security topics periodically to ensure that everyone at the company knows who they can turn to with questions or concerns that relate to security.

A caveat: The security advocate should not be the be-all end-all for security at your organization. Success depends on having all team members accept the responsibility of security, so this person's job is more to educate and model the value of security and to facilitate cross-departmental collaboration, so that everyone can get on board with security best practices.

When it comes to DevOps and security, you will want to ensure there is a bidirectional exchange. The security champion can't reasonably advocate for specific security measures without a deep understanding of DevOps practices and, to some extent, the tools they use. A security champion doesn't just teach DevOps about security best practices; they collaborate on developing an approach to security that works seamlessly with DevOps practices.

Adopt Guardrails: A Laser Focus on Security Policy

Traditional security policies tend to be quite broad, but in the cloud—with its proliferation of apps and services—you must be very specific. For this reason, the challenge of applying legacy security models to the cloud is that security policies can quickly become too complex and difficult to use.

Instead, we recommend using what we refer to as guardrails; a set of policy rules that can be broadly applied to multiple applications and resources. For example, the security team may define guardrails that limit public access to data storage, or guardrails that restrict dev/test environments from access and production resources. Your security team defines the guardrails, and these will be used to protect the data and applications deployed in the cloud. Primarily, you want to build guardrails that automatically enforce which services can talk to which, which is also known as segmentation policy. For greater control, you can define microsegmentation rules that extend guardrails to very granular levels.

We also recommend that your guardrails be application-focused (as opposed to infrastructure-focused). This will allow you to look at business applications and see security policy errors or risk within the appropriate context and will empower business owners to quickly view and understand what is going on from a security perspective.

The simpler your guardrails are to implement, the more likely they will be applied appropriately across your entire environment. A laser focus on security policy, implemented via consistent guardrails, will enable your team to remain focused on their value-add work and not become derailed by the intricacies of security policy.

Consider New Tools

What are the steps you need to take for successful enterprise cloud security? Part of the answer is adopting the right technology.

To date, organizations have tested out a variety of technological approaches to cloud security, and some have fallen short including:

- custom, in-house tools and scripts (difficult to maintain and implement)
- technological solutions that focus on security operations (ineffective and difficult to scale)
- firewalls (fall short when the network perimeter evaporates)
- cloud-only security tools (can't protect hybrid environments and result in additional security islands)

To avoid false starts in your cloud security, we recommend you seek out solutions that are both well-versed in the cloud and applicable to hybrid environments. To be more specific, there are five key attributes that you should look for in a strong cloud security solution that will apply to the whole enterprise.

- **Cloud-Native:** This might seem like a no-brainer, but you want to choose tools that are built in the cloud and for the cloud. You should start by using the security tools that are built into the cloud platforms you are using, including security groups, IAaM policies, and role-based access controls. Beyond these basic controls, look for cloud-native security tools that will give you the level of visibility and insight you need for your unique business.
- **Application-Focused:** It's very difficult to manage cloud security at the infrastructure level because of the overwhelming volume of information that exists. Instead, we recommend choosing solutions that look at the application level. This viewpoint allows you to see policy errors or risks within context and have a meaningful conversation with those who involved in deploying the app. It makes it much easier to do security right within a complex organization.
- **Multi-Cloud & Hybrid:** Most enterprises today have a multi-cloud environment, meaning workloads distributed across various cloud instances and providers. They also typically have some legacy on-premises infrastructure in place, and as we have discussed, this isn't likely to go away overnight. So make sure you choose security tools that are able to work across your entire hybrid and multi-cloud infrastructure.
- **Integrated into the CI/CD Pipeline:** Continuous development and continuous integration are so key to enterprise success today, as we have discussed in this paper. To make sure that you don't slow down these processes, look for security tools that are easily integrated right into the delivery pipeline.
- **Easy to Deploy:** If a particular tool requires a long deployment, extensive fine-tuning, and significant team resources to manage, odds are it won't be used to its full potential and you will find yourself with security gaps.

When you are evaluating cloud security tools, ask yourself whether they check these five boxes and whether they achieve the end-goal of securing all aspects of your infrastructure.

Measure Success

Once you have nominated a security advocate, put guardrails in place, and chosen new security tools, you will want to develop a program to measure your success and make improvements over time. Here are some of the key metrics that we recommend you pay attention to:

Metric	Before	After
Time spent on security checks		
Number of incidents		
Number of security checks in DevOps pipeline		
Number of security exceptions		

We recommend that you track these KPIs because they allow you to demonstrate that your approach is working. This can be useful from a compliance perspective, and it can help you to secure an ongoing security budget to support your program.

Conclusion: Fear Not the Cloud

Your enterprise need not fear the transition to the cloud. While the cloud may bring additional complexities on the security front, the benefits in terms of speed and agility, time and money saved, and up leveling of output are inarguable.

As more and more large organizations move to the cloud, it's time to rethink how we approach security and find a path forward that embodies the principles of agility and speed. We believe security must be integrated into the entire estate—from on-premises to cloud to microservices—as well as into the application development and deployment pipeline. The best way to achieve this is to understand the differences between your traditional and cloud security requirements and to implement best practices via a robust yet simple to execute security policy.

Using this guide, you can embrace the benefits of the cloud while maintaining agility and security across your access and connections, no matter how unique or complex.