3 Tips to Secure & Automate Your Public Cloud Architecture

WHITEPAPER

It's key to have a public cloud

environment that is both robustly secured and able to evolve swiftly and often, especially given the frequently-changing threat landscape of modern business. According to Cybersecurity Insiders' **2018 Cloud Security Report,** "The top three cloud security challenges include protecting against data loss and leakage (67 percent), threats to data privacy (61 percent), and breaches of confidentiality (53 percent)."

Many in IT have now embraced cloud as a standard for modern business demands. But this doesn't mean that concerns and headaches surrounding security don't still abound. Cybersecurity Insiders' **survey report** claims, "As more workloads move to the cloud, cybersecurity professionals are increasingly realizing the complications to protect these workloads. The top three security control challenges SOCs are struggling with are visibility into infrastructure security (43 percent), compliance (38 percent), and setting consistent security policies across cloud and on-premises environments (35 percent)."

While organizations have grown accustomed over the years to on-premise environments that harness a certain speed of service, this puts cybersecurity teams in a bind when going to the cloud. A cybersecurity team's duty is to protect against rising threats that contribute to data exposure, extended downtime, and reputational damage – having confidence in cloud security while maintaining a similar deployment speed can be tricky. But that's not to say you can't gain both security and speed in the cloud – in fact, it's more than possible to balance these two areas when you've designed and implemented an environment that emphasizes both qualities.

This white paper shares how to ensure your data and applications are secured within a cloud environment by leveraging best practices and automation to keep pace with business demands.

1 BUILD SECURITY AND AUTOMATION AS YOUR FOUNDATION

Building security into the very foundation of your cloud environment takes strategy and planning upfront, engaging with stakeholders and consulting with experts. As with any technology adoption, it's important to have widespread buy-in. Getting multiple perspectives and having a clear understanding of your company's long term roadmap saves a lot of legwork and headache down the road.

Several cloud types exist for businesses to harness the benefits of cloud in a setup that's right for their goals. From a private cloud setup to a public one, to a hybrid between an on-premises and fully-virtualized environment, it's up to stakeholders to make the ultimate decision of where to put your data and workloads. The majority of those who choose the public cloud have been leaning toward either Microsoft Azure or Amazon Web Services (AWS) of late — AWS with a larger adoption rate. According to **Statista**, 88% of organizations are planning a move to, experimenting with, or running applications in AWS.

Once you've identified the type of cloud that's right for your business, the design process begins for how to get your IT systems there. This is where security is paramount.

AWS lays out in their white paper, "Security by Design," the approach they prefer for cloud security:

1. Understand your requirements
2. Build a secure environment that fits your requirements and implementation
3. Enforce the use of templates
4. Perform validation activities

However, your organization's IT team is responsible no matter what AWS or another public cloud provider does. This is because, while security in the cloud environment is handled by the public cloud company, their security practice doesn't extend across the full stack and to the application level. For this reason, teams must secure areas of security gaps, which can be a daunting task. Taking a foundational approach towards security builds in a focus on security, and the rest of the business operates within that structure.

One key way businesses can ensure efficiency and security in the cloud is using automation from the beginning. Too often companies decide after having migrated to the cloud that they'd like to experiment with automation. If you plan for this usage from the start, you'll be able to address security concerns upfront and as they arise—and be able to address these concerns from an implementation perspective in tangent with your entire environment's build.

THE PATH AUTOMATION

Rich set of APIs = Ability to Automate

Teams can use tools like automated scanning to determine changes to their cloud environment. The faster a business can identify unwarranted changes, the better their compliance team will be able to secure and react to the situation. Here, using automation can speed up detection methods, thereby reducing the time window to detect and react—which could not only save a business from becoming non-compliant, but also allow for quick action to save revenue and reputation.

Taking a foundational approach towards security builds in a focus on security, and the rest of the business operates within that structure.

2 USE AUTOMATION TO ENFORCE COMPLIANCE STANDARDS

Increasing compliance in most every industry is driving the need for more oversight and awareness. From compliance frameworks to client audit requests, to standards of internal governance, having predefined policies for addressing security aspects as they arise are key to overall threat mitigation. To ensure ongoing security for compliance standards, clearly understand the security requirements that apply to your organization before making the journey to the cloud. Once you're in the cloud, this established process will aid in confirming that those requirements are continuously in place.

From compliance frameworks to client audit requests, to standards of internal governance, having predefined policies for addressing security aspects as they arise are key to overall threat mitigation.

Compliance requirements have historically been an area where security practices can slow down a business in quickly meeting market demands. Policy-making can be reactive in nature. By the time a regulatory standard is introduced, the industry has usually seen repeated incidents that have culminated in its need. This can be at odds with cybersecurity, which by its nature strives to be proactive in order to prevent breaches.

Policy-making can be reactive in nature. By the time a regulatory standard is introduced, the industry has usually seen repeated incidents that have culminated in its need. This can be at odds with cybersecurity, which by its nature strives to be proactive in order to prevent breaches.

In a public cloud setting, personnel have the ability to create a whole new cloud environment overnight, potentially without security or compliance oversight. Since this could easily make a business vulnerable to a breach, the security team must devise proper enforcement in this area, getting control of DevOps creations of cloud one-offs before a compromise. When you apply automation to compliance challenges such as this one, teams are able to diminish some of the more cumbersome aspects of regulatory obligations and ensure continuous oversight. Using automation for identity access management, encryption assurance, blueprinting of architecture/design, templating of systems and components, software defined networking, and compartmentalized storage can increase the speed of deployment, assist in policy crosschecking to ensure continuous compliance, and aid in the validation of reference architectures.

"DevOps has changed the pace of innovation in business. To keep up with demands, security operations professionals (SecOps) must balance the protection of data, applications and reputation through the codification and automation of controls, which enable the pace of change without increasing risks often associated with rapid development."

Kevin Van Mondfrans
Senior Director of Product Management at InterVision

If the written policy changes, how does everything get changed and people know to change it? Policy as code (codification of policy), while still in the emerging stages of technology innovation, includes taking lengthy policy statements and translating those statements into an intermediary language that bridges the gap between governance and compliance requirements with the technical implementation and deployment specifications for developers. It essentially tells developers what they need to bake into their code, unit tests, and pipelines when developing and deploying new solutions. Since DevOps teams can't be expected to be lawyers in order to shore up IT systems for compliance, it's incumbent on policy writers or their intermediaries to make their verbiage appropriate for proper implementation. Policy as code is just one step in that direction, even though it's equal parts a process as a full set of software, scanning, and enforcement technologies.

USE GOVERNANCE TO DELINEATE SHARED RESPONSIBILITIES

When it comes to security in the cloud, it's important not to neglect aspects that fall outside of a cloud environment that can have impacts on it, whether it be the physical components of hybrid infrastructure upon which the cloud rests, data going into the cloud, or user mistakes that could permeate into the cloud. This includes maintenance and testing activities that serve to keep the cloud environment running smoothly. Since there could be several touchpoints occurring and if maintenance activities aren't performed, the health of your cloud assets could be at risk; it's important to consider every responsibility that goes into a healthy cloud environment for your business.

Consider whether these responsibilities should be shared among team members or offloaded to an expert third party. Some aspects will inevitably be offloaded already—such as the public cloud itself, which is managed by the public cloud provider. For those responsibilities that do fall onto your IT team's shoulders, what areas could artificial intelligence or machine learning assist in?

For example, the testing process can be cumbersome and time-consuming—nevertheless, it's essential to do it on a regular basis. Machine learning can act as a predicter for how healthy a cloud environment is, translating how often you've made changes to the environment and time between your last test into digestible information about recoverability. This helps with efficiency and exposes areas for iterative improvements to overall security posture.

> ***Governance can help translate people, tools and policy into process by guiding the construction, maintenance, and testing of every IT environment, cloud and not.***

Governance can help translate people, tools and policy into process by guiding the construction, maintenance, and testing of every IT environment, cloud and not. Here, companies should note who in the business will own determining, revising, and policing governance protocols and how to integrate security into software development/software release processes – not make it an afterthought. Governance can help IT teams orient their design thinking from the start, so that post-release scrambles to shore up security and compliance become a thing of the past.

Indeed, a successful use of public cloud involves thinking in terms of people, process, and tools. What security experts do you need? How do you integrate security into your processes, and what tools can you use so you are not building everything from scratch? If you intend to have the expertise for security in house, then how do you go about creating security experts on your team? This also applies to both standards/requirements and security infrastructure.

Helping to delineate the responsibilities that each group is tasked with is essential to the ongoing security of an environment. Governance can help DevOps know what they're supposed to do prior to launching new applications.

> ***Helping to delineate the responsibilities that each group is tasked with is essential to the ongoing security of an environment.***

A DevOps team wants automation to have a baseline method for blueprints and templates, so they can go fast without the need to rearchitect after deployments or handling numerous unique configurations ad hoc. Comparatively, a security team wants monitoring and alerting, resiliency scalability, code validation, and logging baked into the development process, so that they can get the necessary data they need to automate analysis and event management. Applying automation wherever possible to internal standards of governance can solve for the needs of both groups.

Azure offers Automation as a Service. As they say, when you find yourself doing something twice, automate it. A fair amount of automation is also already ingrained in AWS environments, where Amazon monitors trends that users are doing with and in their cloud to improve client experience, identify threats, and make iterative improvements to the cloud itself. Shared security enhancements from AWS are developed from thousands of environments instead of a single, on-prem environment. As a result, companies in the AWS cloud benefit from what other companies are doing in that cloud, leveraging the power of many.

AREAS THAT NEED DELINEATION OF RESPONSIBILITIES:

- Governance
- Controls
- Testing
- DR and Cybersecurity
- Artificial Intelligence/Machine Learning
- Data and Log Management
- Maintenance and Lifecycle of Tools

Another area that governance can, by its very nature, address is establishing a holistic perspective for cybersecurity. According to Cisco's **2019 CISO Benchmark Study**, "Today 90% of [security] incidents are still related to malware, or the evolution of malware such as ransomware and similar attacks." These types of incidents demand not only robust detection and mitigation controls to prevent intrusion, but also an equal emphasis on restorative measures like IT disaster recovery to keep data safe from loss and extended downtime.

> "Today **90%** of [security] incidents are still related to malware, or the evolution of malware such as ransomware and similar attacks."
>
> -Cisco's 2019 Benchmark Study

Both BC/DR and cybersecurity teams align under the same goal of IT resiliency.

Organizations must keep in mind that a holistic cybersecurity strategy demands both BC/DR and cybersecurity professionals work in tangent with each other to ensure no gaps exist across the entire spectrum of their data's journey, whether it be in transit, at rest, in multiple locations and not. Indeed, both BC/DR and cybersecurity teams align under the same goal of IT resiliency. Use this common goal to emphasize a two-pronged approach toward protecting the entire business: a balance of preventative and restorative measures, with detection measures as a bridge between the two.

How can a Strategic Service Provider help?

Offloading some of the everyday operational demands of business, like certain aspects of cloud security, DR, etc., allow internal IT teams to focus more on revenue-driving and competitive innovation projects – which also contributes to better IT talent retention overall. Not only can using a third party help IT embrace projects that are more meaningful to them, there's also no need for IT teams to fear for their jobs when they provide this renewed value back to their organizations.

Having too many vendors can also have a downside though. The more vendors businesses invite as touchpoints to their IT systems, the more they invite risk and therefore, put more responsibility on the business to manage that risk. According to Cisco's **2019 CISO Benchmark Study**, "To better manage alerts, one best security practice is to reduce the number of vendors and point solutions. In 2018 there were 54% of respondents with 10 or fewer vendors in their environment, whereas now this number has risen to 63%." This means that vendor consolidation is on the rise, perhaps because more vendors have come to mean more burden on the internal IT team. Not to mention, more hurdles to verify compliance.

This is an area where a strategic service provider (SSP) can be particularly valuable – an SSP will have both a wide array of technology solutions and services to meet any IT demand AND a deep bench of expertise on-hand to deliver on those needs. One vendor to engage. One throat to choke.

It takes a lot of pre-planning when going to the cloud. Even if you're already in the cloud, it takes vigilance to spot ever-evolving security gaps. Even in a public cloud environment with a shared responsibility model, it can take a lot of bandwidth from team members to maintain ongoing cybersecurity. Building comprehensive security into the design and management of your cloud environment can be daunting, especially given such a diverse threat landscape. For this reason, it's important not to forget your company's long-term goals when constructing security in the cloud. Speed without security can result in consequences for the long-term. Security without speed hinders the competitive viability of a business. Teams must collaborate to create a solution that's right for all parties.

An SSP will have both a wide array of technology solutions and services to meet any IT demand AND a deep bench of expertise on-hand to deliver on those needs.

START YOUR CLOUD SECURITY JOURNEY WITH THESE INTERVISION OFFERINGS

NIST Assessment

NetDefend® Threat Assessment Consultation

NetDefend® Vulnerability Assessment

To learn more about InterVision's unique approach as a strategic service provider, contact us at www.InterVision.com or call 844.622.5710.