FIREMON

Cutting Through The Haze

Three Steps to Gain Control of Cloud Security

Executive Summary

Clouds expand. That's just what they do. Clouds naturally dislike signs saying, "Off Limits." Clouds encircle the globe, they become dense, they thin out. Clouds are amorphous, clouds move unpredictably.

Cloud computing is one of the most aptly named technologies enterprises have. Cloud computing has many of the same characteristics as the natural phenomena in our atmosphere. The cloud is swift, appearing out of nowhere. The cloud is shifty, moving around at a whim. It can be dense. It can be lightly stratified. Cloud computing is not concrete, not homogenous and not stoppable.

Migrating to the cloud offers several advantages. Cloud technology gives enterprises faster application deployment, instant storage, workload versatility and pricing models that decrease initial capital investment. The downside of this expansion in the cloud is in trying to secure something that does not take kindly to control. There are two principle concerns for security in an enterprise cloud: visibility and speed.

VISIBILITY

Clouds are, well...cloudy. It can be difficult to see what's what in the haze. With each new application, cloud instance or Amazon Simple Storage Service (Amazon S3) bucket, enterprises incrementally decrease line-of-sight. Without a firm grasp of where you are, it is impossible to see which direction to go. Visibility in the cloud is inherently limited because of the nature of clouds. The built-in partitions and multi-tenants of clouds prevent us from seeing into the global cloud infrastructure. Security teams must go to each separate cloud instance to discover what's there, and in an enterprise with thousands of infrastructure partitions, that simply cannot scale.

This should sound familiar to enterprises who faced these same challenges as the number of firewall rules skyrocketed in the past decade. As networks became increasingly segmented (DMZ, WAN, virtualization, software-defined networking), we saw an explosion in network policies and rules. Rules reached unimaginable numbers and visualizing them all took months to pull together.

The biggest challenge in securing the public cloud environment is "lack of visibility.*"

*FireMon, LLC. "State of Hybrid Cloud Security: 2019." February 2019.

Executive Summary Cont.

SPEED

The second hurdle for cloud security is speed. Even when you get total visibility into what's happening in your cloud, you still have to keep pace with the rapid growth. Cloud instances are spun up as quickly as they are shut down. Users self-provision, business groups demand best-of-breed cloud apps, and DevOps deploys workloads across multiple clouds to deliver new capabilities at scale, reduce costs, streamline resources, and avoid cloud vendor lock-in. Businesses can move more quickly, applications bring more value to customers, and digital transformation becomes a reality. However, when the cloud adoption rate is measured in nanoseconds, security misconfigurations are bound to happen.

In this eBook, we will examine the steps you can take to thrive in the cloud. Security teams do not need to be the "department of no" or sacrifice security as their enterprise migrates to the cloud. They simply need to manage it all in a coherent and centralized way. The three steps we will cover include:

Step 1 **Cloud Visibility**
Step 2 **Creating Cloud Controls**
Step 3 **Cloud Orchestration**

Each of these steps will fortify your enterprise and help you move to the cloud with confidence. Security doesn't have to be the afterthought. Security can lead, command and fuel the ship that's taking you to cloudy worlds.

36% say inaccuracies, misconfigurations or issues account for 10%-24% of changes that require rework.*

*FireMon, LLC. "2019 State of the Firewall." November 2019.

Step 1

Cloud Visibility

Anyone who has strolled through a dense fog can get an idea of what it's like to be inside a cloud. Now, picture yourself moving through a cloud at 600 miles per hour. This is what it's like to pilot an aircraft through a cloud. With this image in mind, you know what it's like to be a security professional in an enterprise expanding their cloud infrastructure.

You move quickly, never really noticing what's passing by. You can't tell if you're in the beginning, the middle or the end of the journey. You don't know where you are in space. Are you at the center, the edges, somewhere in between? It can be difficult to answer these sort of questions.

Flying blind in the cloud can be exhausting. Not just on an intellectual level, but deep in our emotions. Human beings have a consistent tendency to feel anxious when we are disoriented. When we don't know where we are or what is happening around us, we are prone to paralysis. This all may sound philosophic, but the point is practical. Without a firm grasp of what's happening, we freeze. And the one thing enterprises can never do is stop moving.

Security teams are tasked with keeping the enterprise secure and removing risk. They need visibility into what is in and what is happening in their cloud. Clouds can be public, private or a hybrid of the two. However, the visibility challenge is a defining characteristic of the cloud. Visibility is something that everyone craves, but they don't always know how to satisfy.

To get cloud visibility, leading enterprise security teams are taking steps to put everything in front of their eyes. It comes when you put all your controls in inventory, normalize those controls and customize you views. Let's examine each of the visibility enhancing measures.

34% of respondents noted they have less than 50% percent of real-time visibility into network security risks and compliance.*

*FireMon, LLC. "2019 State of the Firewall." November 2019.

Step 1

Cloud Visibility

INVENTORY CONTROLS

Before we can know which controls could be helping or hurting security, we need to know which controls exist. This starts by gathering security controls from across the global cloud infrastructure. Because these clouds are masters of movement, we'll need to the inventory to update in real-time, at all times, from every corner of the cloud environment.

Having real-time visibility of all controls gives us an inventory. As with any exercise in inventory management, we have to know what's there so we can determine its value.

NORMALIZE CONTROLS

Now that we've gathered all the security controls from the cloud infrastructure, we need to normalize these rules. Every application, IaaS and micro-service contains security controls and settings that lend themselves to normalized structures. By focusing on the essentials (users, permissions, protocols, etc.), we can get a standard that applies to all cloud security controls. For example, we can see that Control A for AWS and Control B for a private cloud have the same parts, even if they need to be rearranged for review.

By normalizing security controls, we get a more accurate lineup of our cloud security and can reach decisions faster. This is like converting between metric and standard measurements when weighing a giraffe. The giraffe is still the same, we just talk about it differently. Your security controls are still there, we're merely translating the way we visualize their components.

COORDINATE CONTROLS

Finally, we need to relate security controls to the corresponding cloud infrastructure. Not all cloud security controls are applicable or a best practice for certain cloud environments or applications or storage. Having the correct security controls will allow to see what's out of bounds and take action to improve security.

Simply having the controls in inventory and normalizing their contents is a great start, but we really get to solid visibility when we are able to see their relationships in context. Clouds do not take care of themselves. They require security controls tailored to the business needs and security intent of the enterprise.

With these factors in place, we have a clear view of our cloud in its current state. All assets and controls are accounted for (inventory), they are all represented the same way (normalization), and they all relate to the intended goal or target (coordination).

Now that we have a good understanding of what's happening in the cloud, we are ready to take the next step to amplify security. And that begins with making sure all cloud security controls are aligned with security intent.

Step 2

Create Cloud Controls

One of the more consistent myths about cloud security is that it is fundamentally different from traditional on-premise security. This myth comes from a thought that goes, “If the setting is different, the security needs are different too, right?” Wrong.

Policy (security intent) is the bedrock of all security programs because it distills the most essential statements about security: this is allowed, that is not. When you consider the requirements to refine your cloud security, it will always come down to policies that prescribe exactly what is permitted.

Once security controls are inventoried, normalized and correspond to the right cloud resource, we can begin creating the security controls that align with security policy. Again, not fundamentally different from on-premise security policy. Policies only need to be translated for your cloud.

Step 2

Create Cloud Controls

TRANSLATION

To begin, we must first acknowledge what makes up our desired state. This can include: compliance standards, security best practices, industry regulations, government requirements and so on. Then, we can model the ways we want our cloud environments to behave. We set the rules for the game.

Next, we have to appreciate the full array of players in the cloud game. We need to acknowledge these players of tendencies if we're going to have resilience in our cloud. Users tend to want access. Applications tend to share information. Infrastructure-as-a-Service (IaaS) tends to group, parse and support the users and apps.

FireMon takes your security intent (your one constant) and translates that intent to the right cloud controls for all environment types: private, public and hybrid. Rather than having an assorted blend of security controls, you have consistent policy that calibrates the right rule for the right context to ensure your intent flows to any cloud.

AUTOMATION

Translation turns your security intent into specific cloud controls, and automation checks the design against all possible contingencies, scores the risk and if all is cleared, pushes rules to the cloud. Change management for the cloud is like the Wild West: lawless with the nearest sheriff 90 miles away. But when automating security intent and orchestrating translated controls, there's no need to worry. Controls are instantly applied based on the global security intent.

One of the key security challenges of cloud security is the speed at which cloud technology is adopted. FireMon keeps pace with this growth with instant translation of your policy with automatic implementation to protect data with each change to your cloud infrastructure.

The change agent needed to address the security skills gap is automation, which eliminates guesswork and errors stemming from manual tasks, yet 65% of respondents are not using automation to manage their environment.*

*FireMon, LLC. "2019 State of the Firewall." November 2019.

STEP 3

Cloud Orchestration

Finally, we come to the key to continuous security for the cloud: orchestration. With a hodge-podge of buzzwords in the security industry, orchestration stands out with its imagery of a single conductor directing all the moving (and different) parts of the band brought together to play the symphony.

In the context of the cloud, orchestration continuously discovers our weak spots, simulates attacks, simulates patches, checks for compliance and makes changes to the cloud environment with zero human touch. These critical areas of orchestration enable your organization to command security of the cloud.

VULNERABILITY MANAGEMENT

Just as the cloud can be fuzzy, so are the lines of responsibility. We read stories that snatch headlines where a misconfigured cloud instance or storage was invaded by cybercriminals: who's responsible? Is it the cloud service provider or the enterprise? The confusion comes from the sensation we get when thinking about infrastructure-as-a-service (IaaS). We think, "Well, this is a service. The service provider is responsible." However, it is important to acknowledge the first word in the IaaS moniker: Infrastructure.

Although this resource comes from a cloud service provider (CSP), the enterprise is still the primary responsible party for data protection. It is the enterprise's infrastructure. With that in mind, it is important for organizations to manage vulnerabilities for their cloud (private, public and hybrid). There are two helpful techniques for vulnerability management that lend themselves to orchestration: 1) attack simulation and 2) patch simulation.

Attack simulation combines vulnerabilities with your security controls and policies. By seeing what's allowed and how a vulnerability could be reached, you know how an exposure could become exploited. FireMon's orchestration happens through a single pane of glass, wrangling all these data points to put you in the shoes of an attacker, scoring your risks and giving prioritized direction to improve security.

Consider this an active, ongoing, continuous pen-test. By orchestrating all the data, no vulnerability remains hidden or misunderstood.

Patch simulation is the photographic negative of attack simulation. Using orchestration, FireMon customers can prioritize their patching because they can 'play' with options to see which patches will deliver the best results. Often, it can be difficult to chase each vulnerability in a growing cloud environment. So, we end up patching at random.

Without orchestration, we would be patching in one place in our cloud infrastructure, only to be flanked by a cybercriminal somewhere else. Patch simulation is orchestration at its best. Orchestration brings all the data together to make sure you know which changes have the greatest impact.

STEP 3

Cloud Orchestration

COMPLIANCE

Much is said about compliance in the cloud. Compliance isn't limited to regulatory compliance.To be compliant, we must also adhere to the security intent and goals of the enterprise, which are often more critical than a point-in-time audit.

A critical feature of any enterprise security program is continuous compliance, which can only be realized through automation and orchestration. Compliance controls sit here, cloud controls sit there. Users and applications don't sit still. To make sure we're always compliant – with both internal and regulatory requirements – we need a single place to establish the controls, leverage all the sources just mentioned and examine the benchmarks continuously in real-time.

Orchestration is up to the challenge. Using FireMon's orchestration, enterprises have ongoing, active, real-time compliance checks across 350+ customizable controls. Let's put this magnitude in perspective.

Imagine you have, say, twenty assessments. With FireMon's library of controls, that gives you up to 437 sexdecillion (that's 437 followed by 51 zeros) possible combinations of security controls.

This is impossible to check without orchestration. But with FireMon, this compliance evaluation is completed in less than 0.2 seconds. FireMon's sub-second analysis of security controls is made possible through our unique architecture and Elastic search backend that scales to any size without performance degradation.

Almost one-fourth (24%) of respondents aren't sure or wouldn't admit if they failed a compliance audit in the last 12 months.*

*FireMon, LLC. "2019 State of the Firewall." November 2019.

STEP 3

Cloud Orchestration

MAKING CHANGES TO CLOUD CONTROLS

Now that we've simulated attacks, surveyed our patch options and checked compliance (all within seconds), we are ready to make changes to the cloud infrastructure. Again, control changes also lend themselves to orchestration.

If we know the cloud controls we have in inventory and can assess them in light of prevailing vulnerabilities and can translate policy (security intent) into cloud security controls, we can make changes that persist in our cloud infrastructure.

FireMon is the only solution with orchestration for cloud infrastructure. Other solutions require your cloud to play host to a traditional firewall camping out in your cloud infrastructure (Amazon Web Services (AWS), Micrsoft Azure, Google Cloud Platform (GCP), etc.) the same as on-premise.

But that assumes you have all the security controls in place and that you merely need to control traffic to the cloud's front door. Wrong.

We need to make changes that go directly to the cloud security controls. AWS, for example, uses Amazon Security Groups to hold all our cloud security controls. To truly orchestrate security, in the AWS example, we must command security rules directly into the security groups. If one single unused or overly permissive rule in a firewall is sitting in front of the cloud, all hell breaks loose when that firewall allows unauthorized access. FireMon orchestration avoids this mishap with direct integrations to the infrastructure. Only FireMon can do this.

We now see how orchestration puts a bow on our cloud security program. Orchestration pulls together disparate security solutions, simulates attacks, models patching options, performs sub-second compliance checks and commands changes to fortify your enterprise's cloud infrastructure.

Security no longer has to be compromised when moving to the cloud.

Conclusion

We have seen that clouds don't have to run amuck; they can be understood and commanded with absolute precision. By taking an inventory of what's there, assessing cloud security in the light of existing security policies and intent, translating that intent to top-notch security controls and orchestrating the whole process, we have a program for cloud security and with it, continuous security and compliance for the cloud.

We began this eBook by saying, "Clouds expand. That's just what they do," and went on to explain the similarities of natural clouds with our computing resources of the same name. There's no stopping the cloud. There's no way to force it into shapes and sizes that are agreeable to human minds that demand malleability with everything we touch.

But as your cloud expansion unfolds, you can fly into it with the tools you need to keep things secure. It only takes a method of honest assessment of where you are, the confidence to push controls that meet your security intent and tools to orchestrate and keep pace with the cloud.

About FireMon

FireMon is the #1 security automation solution for hybrid cloud enterprises. FireMon delivers persistent network security for multi-cloud environments through a powerful fusion of real-time asset visibility, compliance and automation. Since creating the first-ever network security policy management solution, FireMon has delivered command and control over complex network security infrastructures for more than 1,700 customers located in nearly 70 countries around the world.

Learn how FireMon can help you acheive real-time visibility and control of your hybrid cloud.

REQUEST A DEMO

+1 913.948.9570 | info@firemon.com | firemon.com | REV 1222019RGB

FIREMON