EBOOK

FIREMON

Proven Ways to Boost Your Hybrid Cloud Security

Executive Summary

Cloud computing is one of the most aptly named technologies enterprises have. Cloud computing has many of the same characteristics as the natural phenomenon. The cloud is shifty, moving around at a whim. It can be dense. It can even be stratified.

Embracing the cloud offers numerous advantages. Cloud technology allows enterprises faster application deployment, instant storage, workload versatility, and pricing models that lower initial capital investment. And hybrid cloud environments allow enterprises to reap the benefits of extending the life of their on-premises investments and the migration to cloud-based resources.

The downside of this meteorological fusion is that the security measures that work well for traditional datacenters do not work as well for clouds or hybrid clouds. There are significant differences between the processes and technologies—all well-established—that secure traditional networks, and those that aim to secure hybrid networks, especially those that incorporate one or more public or private clouds. These differences are all but insurmountable using traditional network security solutions alone.

Hybrid Cloud Security Challenges

Let's start by looking at some of the key difficulties that arise when trying to secure a hybrid environment.

Limited Visibility

Visibility into hybrid clouds is often limited. With each new deployment of an application, workload or cloud instance, enterprises incrementally decrease line-of-sight. Moreover, the built-in partitions and the multi-tenant nature of some clouds prevent us from seeing the cloud infrastructure in its entirety.

Security teams must go to each separate cloud instance to discover what's in there, and in an enterprise with thousands of infrastructure partitions, this could be hugely challenging. This problem will be familiar to enterprises who saw the number of their firewall rules skyrocket in the past decade. As networks became increasingly segmented, such as by DMZ, WAN, virtualization, and software-defined networking, we saw an explosion in network policies and rules. As the number of rules increased, gaining real-time visibility into all the changes happening across the network was impossible.

Since it is much harder to protect something that you don't know even exists, the ability to see absolutely everything in your network—no matter what and where it is—is foundational.

Need for Agility

Another key hurdle to hybrid cloud security is the need to deliver agility to your business. Even if you do achieve visibility into what's happening in the cloud, you still must keep pace with the rate of digital transformation demanded by your business. 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.

When leveraging the cloud, businesses can move more quickly, applications bring greater value to customers, and digital transformation becomes a reality and a true game-changer. But when the time it takes to spin up a new cloud is measured in seconds, security misconfigurations, a.k.a. human errors, are bound to happen.

In this eBook, we will examine the proven strategies you can implement to boost your hybrid cloud security. Security teams do not need to choose between being either the "Department of No" or sacrificing security, as their enterprise migrates to the cloud. They simply need to manage it all in a coherent and centralized way.

Here are the three methods to achieve this:

- Use Automation to Reduce Misconfigurations
- Mitigate Risk through Cyber Situational Awareness
- Eliminate Audit "Fire Drills" through Continuous Compliance

FireMon believes that you don't have to choose between enabling the enterprise with agility and ensuring robust security. You can have both.

Method 1

Use Automation to Reduce Misconfigurations

The more humans are involved in a process, the more opportunity there is for error.

With that in mind, consider that about one in five enterprise applications have transitioned to public cloud environments. But securing those applications and clouds—in fact, network security in general—remains a largely manual process for many enterprises. Enterprises are still relying on manual processes as they try to secure complex, multi-vendor and multi-cloud hybrid network environments.

The heavy use of manual processes in a complex and rapidly changing network environment is a formula for human errors and misconfigurations. To cite just one headline-making example, the Capital One breach in 2019 was attributable in large part to a firewall misconfiguration at the application layer. To make the issue as clear as possible, one leading analyst firm stated bluntly that “Through 2025, 99% of cloud security failures will be the customer’s fault.”

The goal is to replace manual intervention with automation in as many aspects of your cloud security processes as possible. This does not, of course, need to be an all or nothing project.

Every time you replace a single manual step in a security workflow, you minimize human error. The bonus? The more you automate, the more your security processes can move with velocity, and the easier it becomes to securely deliver the cloud-driven agility that businesses need.

Method 2

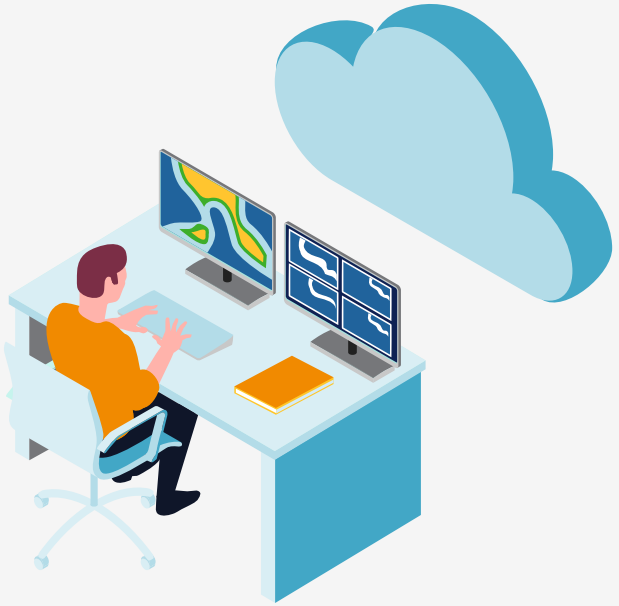
Mitigate Risk through Cyber Situational Awareness

Just as the cloud can be fuzzy, so are the lines of responsibility for security.

We read stories 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 just intensifies when this relates to infrastructure-as-a-service (IaaS). We think, "Well, this is a service. Security is the service provider's responsibility." However, it is important to acknowledge the first word in the IaaS acronym: Infrastructure.

Although this resource is hosted by the cloud service provider (CSP), their customers are still primarily responsible 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) and doing so requires a set of capabilities.

First, you must gain visibility across 100% of your enterprise. You can't afford to have resources that you are unaware of in your network, and with the resources you are aware of, you can't afford to have inadequate configurations.



Second, you must have visibility across all activity in your hybrid network. That means identifying all paths through your network, to the cloud, and the Internet.

Third, both of the above must happen in real-time. You must receive real-time alerts about any changes in your network and potential vulnerabilities or exposures as they arise.

Method 3

Avoid Audit “Fire Drills” with Continuous Compliance

Few activities take up as much time for security teams as tasks related to audits.

This is in part because 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.

Users and applications are in a constant state of flux. Cloud instances spin up and spin down according to the demands of the business.

Rather than taking a reactive approach to compliance—that is, rather than performing the routine fire drills of data gathering for an impending audit—the goal is to be continuously compliant with both internal and regulatory requirements. You must achieve a state where preparation for any audit requires nothing more than a few clicks to generate the necessary reports.

40% rank "Compliance (Industry/Regulatory/Internal)" as one of the biggest roadblocks and challenges that keep organizations from moving workloads to the public cloud.

*FireMon, LLC. "2020 State of Hybrid Cloud Security." February 2020.

Conclusion

The amorphous nature of the cloud creates challenges when it comes to security, and those challenges are even greater for hybrid environments that can be a mixture of on-premises and cloud resources, whether public, private, or both. We looked at the three methods that can help you boost your hybrid cloud security and here is how FireMon can help you achieve this.

Use automation to reduce misconfigurations. FireMon Automation puts you in control, with the most robust API in the market and flexibility to apply security policy automation in alignment with your changing requirements across your increasingly complex, dynamic hybrid environments. FireMon enables Continuous Adaptive Enforcement™ so that you can deliver business agility with immediate and dynamic security compliance. The second method is to mitigate risk through cyber situational awareness. FireMon gives visibility and analysis to understand, in real-time, what is changing with your attack surface and what actions you need to take to protect it. With this, you can immediately eliminate blind spots, leak paths, and points of exposure in your hybrid environment. FireMon gives you the actionable, prioritized insights and recommendations you need to reduce your organization's attack surface.

The third method is to eliminate audit "fire drills" through continuous compliance. FireMon's compliance engine uses a combination of intelligence and logic that continuously and proactively checks every policy, and all changes to policy, against regulatory standards and internal requirements. This means you have continuous compliance...no matter what!

Tackle your hybrid cloud challenges with FireMon. GET STARTED

FireMon is the #1 network 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. For more information, visit www.firemon.com.