The growth of the public cloud has been exponential in the past few years – be it Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or Software as a Service (SaaS). Large IaaS providers such as Microsoft Azure, Amazon Web Services (AWS), and Google Cloud deliver platform capabilities that allow applications to be built and deployed quickly. In parallel with the rapid sprawl of cloud technologies, enterprises are contending with a number of daunting challenges, especially in terms of shrinking security personnel, some loss of control over their enterprise assets in the cloud and ensuring security and trust. According to FireMon’s 2020 State of Hybrid Cloud Security report, 69.5 percent of respondents have a security team of 10 people or less.

Another important development is the deployment of multiple cloud platforms, be it private, public, hybrid, distributed, and edge, emphasizing the need for versatile tools that can work across this blended infrastructure to ensure seamless visibility, security, and compliance.

What if you could see every access path, every device, every network connectivity and protect each one of these through policy-driven security? That is the power of FireMon’s integration with public cloud platforms such as Azure and AWS.

One Platform, Multiple Infrastructure

FireMon’s security-first approach is designed to address the needs of the most diverse customer groups, whether you have a mature cloud migration strategy or are in early-stage migration of your private data centers to the public cloud. FireMon’s security-first model focuses on continuous monitoring and management of cloud security risks and threats, leveraging security tools and automation for:

- Monitoring security threats through real-time discovery
- Attributing context to security threats through data
- Remediating threats through automated policies, processes, and controls
- Validating your organization’s security posture against internal and external compliance mandates with robust and real-time reporting

FireMon understands the native networking components of multiple public cloud accounts, and, more importantly, we can normalize and unify security policies into a single pane of glass – removing your struggles with separate solutions for cloud and data center environments. Customers migrating from on-premises infrastructure to the public cloud can now work with a platform they are already familiar with, which means less training, and minimal change.

FireMon can manage and ensure continuous compliance of native public cloud security policies across accounts, subscriptions, virtual machines, and security groups in Azure Virtual Network and AWS Virtual Private Cloud.

Broad and Deep Integrations

FireMon’s extensive library of APIs allows customers to integrate with a variety of security platforms,
ranging from firewalls, switches, routers and unified threat management (UTM) to security information and event management (SIEM) and security, orchestration, automation, and response (SOAR) platforms. A combination of rich APIs and automation through pre-built security workflows helps customers orchestrate security management across your entire network, irrespective of the network fabric.

With the FireMon platform, customers have the ability to manage any firewall policy deployed in the cloud. This means integrating next-generation firewall policies from vendors like Check Point, Palo Alto Networks, Cisco, Fortinet, and Juniper Networks into AWS and Azure environments. Whether the firewall is located in a physical or virtual environment, you can monitor its security policies with as much visibility as with a physical firewall.

Cloud Security @ the Speed of Business
FireMon’s global policies, combined with automation, allows you to consolidate global security workflows and generate reports for these, making audits quick, automated, and continuous. As enterprises embrace hybrid cloud environments, involving a mix of on-premises, cloud, and edge data centers, FireMon ensures detection, risk mitigation, and security policy management using a common set of tools and APIs. Your business will continue to be in a continuous state of security and compliance because our tools instantly and automatically adapt to network changes. Our compute engine allows for the detection of network configuration changes across your heterogeneous, hybrid environment and delivers Continuous Adaptive Enforcement that transparently adapts and recalibrates your global security policy.

FireMon Public Cloud Support
- A single platform for on-premises, private, public, and edge deployments. Cut down the cost and complexity of managing multiple security policy management tools for different infrastructure types
- Leverage existing investments in FireMon tools/platforms and skills to secure workloads when they move from the data center to the public cloud
- Enable data center extension to the public cloud for policy-driven security management, control, orchestration, and compliance
- Extend the security and control that you enjoy for your on-premises network, devices, and applications to the data center and the public cloud without retooling
- Build a secure and compliant infrastructure by leveraging the broad range of support we offer, right from discovery and monitoring to security management, guardrails, compliance, and reporting

Unify, simplify, secure, and manage your disparate network infrastructure in one place. FireMon is the number one security automation solution for your hybrid environment with unmatched flexibility and visibility across on premises, and public/private clouds.

Contact FireMon today to learn more about how we can help you integrate your security infrastructure across the extended enterprise and remove the challenges of visibility and complexity from your daily network management by visiting www.firemon.com.