SOLUTION BRIEF

FireMon Cloud Solutions

Consolidated security posture management for cloud and hybrid environments.

Introduction

As organizations continue to expand their adoption of public cloud services, it's harder than ever to answer the question, "am I secure?" The evolution from traditional on-premises data centers to the cloud drives exponential complexity in all aspects of infrastructure management and security due to increased decentralization, higher volatility, increased Internet exposure, and fundamental technical differences. New resources, services, applications, software defined networks, and multi-cloud deployments make it nearly impossible to manage with traditional tools and manual processes.

This new landscape comes with its own problems such as misconfigurations that are often instantly exposed to the Internet, attacks that attempt to compromise powerful cloud credentials, and vulnerabilities that open the door to threats that can leverage the cloud to breach the data center, or the data center to breach the cloud.

FireMon's cloud solutions are your allies in navigating the complex terrain of cloud and network security, arming you with powerful management tools to tackle daily challenges head-on. Whether it's supervising security policies across cloud and hybrid networks, revealing unidentified applications, services, and devices, assessing potential risks, or spotting threats throughout the entire ecosystem, FireMon has you covered. With a comprehensive suite of services, innovative features, and unparalleled industry expertise, FireMon puts you in the driver's seat to confidently answer the pivotal question – "Am I secure?

Manage Network Policies Across the Hybrid Cloud

Most organizations have a complicated mix of public cloud, private cloud, and on-premises networks. Each of these has its own set of devices, services, and applications with access that is controlled by an intricate set of policies and rules. Managing these on one network alone is tough, but it grows vastly more complex when you span across a hybrid deployment that includes one or more public cloud services.

FireMon provides a complete centralized inventory of every network device, resource, rule, and policy across the environment no matter where it is or which vendor it's from. Rules are imported into a common normalized rulebase, providing a comprehensive view that automates compliance reporting, speeds making policy changes, and reduces policy-related risk for cloud and hybrid environments.

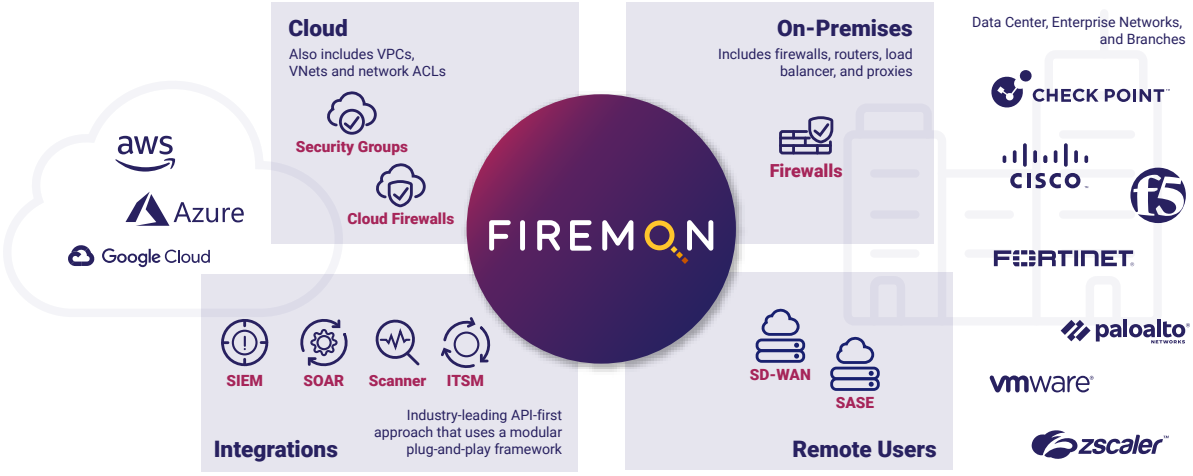

Figure A. FireMon unifies security policy manage across the entire environment from the cloud to the data center.

Automate compliance

Highly customizable reports deliver a one-click overview of compliance throughout the entire environment tailored to precise business needs. Automatic scans identify and remove rules that violate internal and external compliance standards including PCI-DSS, HIIPA, and GDPR. Real-time detection identifies then notifies administrators of existing policy violations and scans for any new ones before changes are deployed.

Speed policy and rule changes

The second you're done cleaning and fine tuning your cloud security groups and firewall rule base, new requests come along that can easily undo everything you worked so hard to achieve. Worse yet, unauthorized changes can undo everything, without you ever knowing about it. FireMon solves both of these problems with real-time change detection and alerts, and easy-to-use workflows that streamline the process to create, change, and deploy rules and policies. No matter how many cloud security groups, firewalls (cloud, virtual, and traditional), VPCs, VNets, network ACLs, and other policy-control devices you have on your network, FireMon knows every detail of every device and intelligently designs rule changes that are optimized for your environment and can even automatically deploy them.

Reduce policy-related risk

FireMon's unified risk dashboard gives a full view of risk across the entire environment using the proprietary Security Concern Index. Risk analysis and modeling provides insight into network topography along with attack scenarios and mitigation recommendations. Integration with leading vulnerability scanners provides deep insight into policy-related risk. Consolidated assessments allow organizations to get up and running quickly with fully customizable risk and compliance reports.

Easily migrate to the cloud

Whether it's simply moving a single firewall or a migration of the entire environment to the cloud, FireMon can streamline and simplify the process. Only bring over what is needed and known to be safe by finding and removing unused, overly permissive, and other high-risk rules, then cleaning them up before they're transferred to the new environment. Once ready, FireMon can speed the process and ensure accuracy by automating the rule deployment process and can validate that the new policy deployment is working as designed.

See Everything Across the Hybrid Environment

With the expansion to the cloud comes the challenge of monitoring and managing assets across the entire hybrid-cloud landscape. FireMon provides a comprehensive approach to discover and identify assets, resources, devices, services, and networks seamlessly, ensuring that enterprises stay a step ahead in their compliance, change tracking, and risk identification efforts.

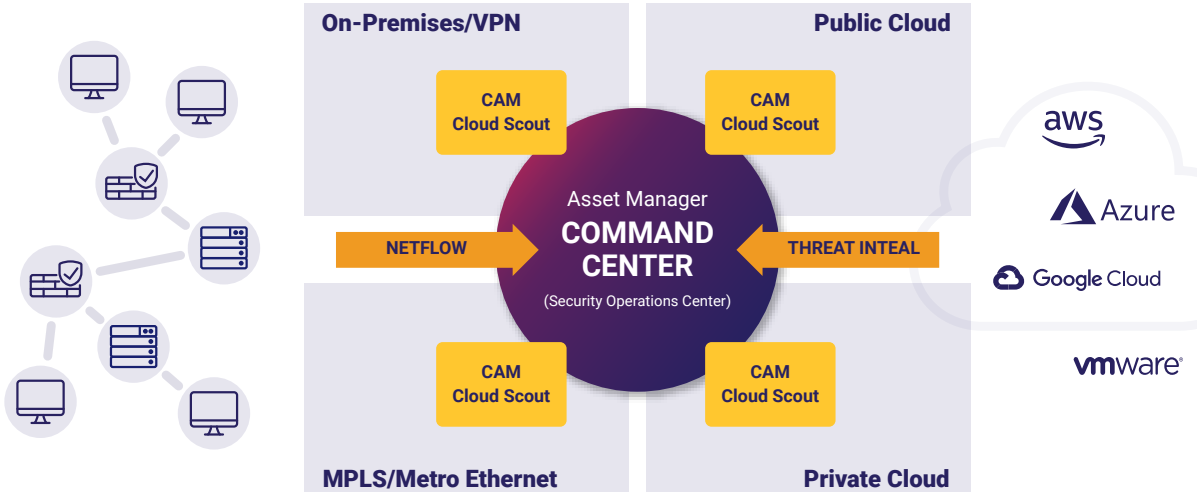

Figure B. FireMon discovers, identifies, and consolidates all assets into a single pane of glass.

Consolidated view of assets, devices, services, applications, and networks

At the heart of our asset management solution is the capability to offer a panoramic view of all assets across diverse environments. Using a variety of IP- and API-based methods, FireMon offers a complete view of everything from on-premises devices to servers, services, and applications based in the cloud. This no-stone-left-unturned approach ensures that organizations remain compliant with evolving regulations, but also empowers them to monitor changes efficiently and spot potential risks before they escalate.

Unified console with real-time reporting and alerts

Simplifying the management process, FireMon provides a single console that displays assets, devices, and resources from on-premises, private, and public cloud environments. This consolidation provides a single view that closes the gaps and enables comprehensive real-time dashboards, reports, and alerting that speeds incident response and threat detection.

Complete Cloud Asset Inventory with Change History

Dive deep into your cloud assets with our extensive inventory tool that not only provides a snapshot of the current state, but also maintains a comprehensive change history, with identity attribution. This historical data is invaluable in tracking asset evolution, ensuring accountability, and making informed decisions.

Detect and Mitigate Risk in the Cloud

Simple doesn't scale. That's especially true as organizations embrace the expanding world of cloud services. The security landscape becomes more intricate with every new cloud deployment, and managing compliance, maintaining an inventory, tracking changes, minimizing misconfigurations, and tackling threats and users can seem like a Herculean task. Organizations require tools that bolster their cloud security operations, even across decentralized teams and operations.

FireMon's Cloud Security Posture Management (CSPM) solution is a comprehensive and innovative service designed to ensure robust security across cloud environments.

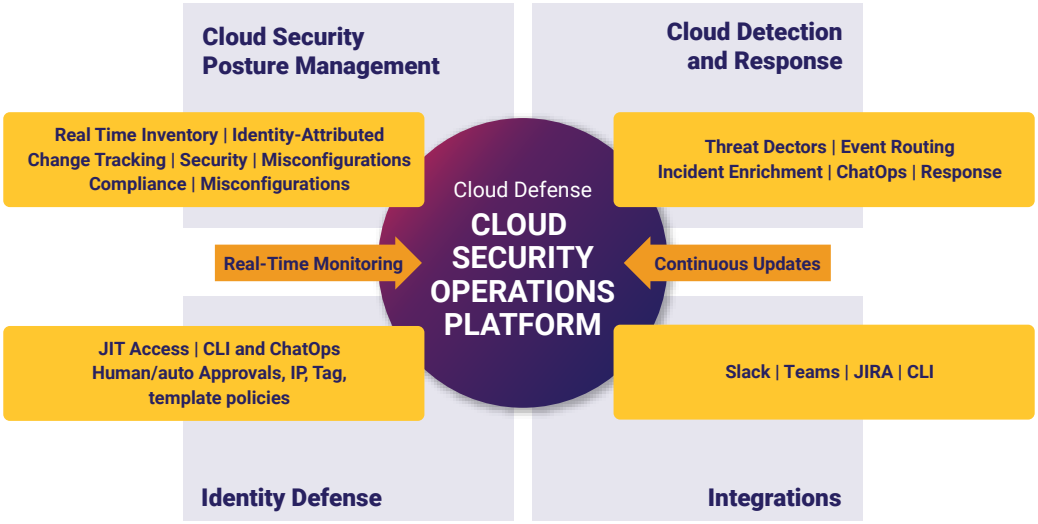

Figure C. FireMon Cloud Defense consolidates cloud security into a single platform.

Identifying vulnerabilities and threats in real time

As one of the only real-time cloud security tools in the market, once integrated into your cloud environment, FireMon continuously monitors all cloud assets, configurations, networks, and data, scanning for any anomalies or deviations from established security policies. If a risk is detected, it's automatically prioritized for remediation powered by integrated ChatOps workflows using Slack or Microsoft Teams. Teams get detailed recommendations on how to rectify the identified issues, whether they be misconfigurations, non-compliance with industry standards, or exposed data.

FireMon offers comprehensive and highly customizable reporting capabilities and security assessments that are based on the classification of the environment. Comprehensive reports provide insights into the security posture of the entire cloud landscape, helping organizations understand their risk exposure and make informed decisions to enhance their security strategies. Our key performance indicator tracking helps security leadership assess, monitor, and communicate the overall maturity of their program over time and identify program-level strengths and weaknesses.

FireMon's integrated cloud detection and response (CDR) capabilities go beyond CSPM to provide real-time threat identification and intelligent alert routing. FireMon also integrates with the cloud provider's native threat alerts to add filtering, enrichment, investigative support; enhancing the usefulness of the powerful, but difficult to manage, threat tools from cloud providers. When threats are detected and communicated, FireMon then provides powerful investigative support with our historical change tracking, resource configurations, and identity attribution to dramatically reduce the time needed for analysis and investigation.

Intelligent issue prioritization and resolution

FireMon sifts through the noise to provide security teams the information they need to understand security and compliance risks. Every event is scrutinized and enriched with posture information then scored for severity to allow teams to filter results and easily see the problems they need to address from false positives and low-level nuisance alerts. Findings are easily organized and filtered based on characteristics like environment (development vs. production) or deployment owner to reduce alert fatigue and better prioritize keeping teams focused on what matters most.

Enhanced just-In-time authorization protection for cloud administrators

The most critical attack vector of cloud environments is identity and access management. Most users are assigned identities with privileges that are seldom, if ever changed, leaving critical infrastructure and resources at an elevated risk of abuse and vulnerable to attack. FireMon reduces these elevated permanent privileges with just-in-time session access that eliminates permanent, over-privileged accounts by providing the right access at the right time.

Summary

FireMon's cloud solutions provide consolidated security posture management for cloud and hybrid environments. They offer effective policy management, automates compliance, and reduces policy-related risks across diverse networks. FireMon provides a comprehensive view of all assets across the environment, complete with real-time dashboards and alerts, ensuring effective risk identification and compliance. Its Cloud Security Posture Management (CSPM) identifies vulnerabilities and threats in real-time, prioritizes issues for resolution, and enhances authorization protection for cloud administrators. With FireMon, organizations can confidently answer the question, "Am I secure?" while navigating the complexities of cloud and network security.

FIREMON

© 2023 FireMon, LLC.
All rights reserved. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

SB0309-EN-20231019-01