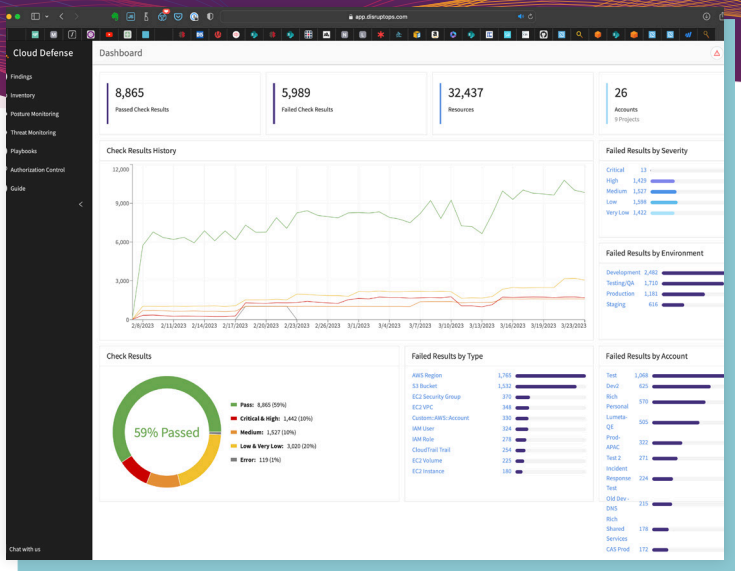
DATASHEET

Cloud Defense

Real-time cloud security, compliance, maturity, inventory, misconfiguration, and threat detection. Now with proactive IAM defense.



A More Powerful CPSM

Simple doesn't scale. As organizations continue to adopt cloud services, security complexity increases exponentially. Improving security, managing compliance, maintaining inventory, improving maturity, tracking changes, reducing misconfigurations, all while handling threats and users, is a massive challenge. Organizations need tools that support cloud security operations across decentralized cloud teams and operations.

FireMon Cloud Defense

Understand More: FireMon Cloud Defense is designed to get you the prioritized information you need to understand your security and compliance risks, without flooding you with noise.

Communicate Better: Our deep ChatOps integration is built to meet the needs of decentralized cloud operations. Issues are routed directly to the teams who can respond to them while keeping security in the loop.

Remediate Faster: Our event-driven automation engine can fix issues automatically or use our ChatOps integration to embed guidance and 1-click actions for a human decision.

Cloud Defense Features

Real-time Cloud Posture, Inventory, and Change Tracking

FireMon Cloud Defense oversees API activity within your cloud deployments, constantly refreshing inventory, and conducting real-time security and compliance evaluations to safeguard against any oversights. Cloud Defense provides a searchable repository of cloud assets, complete with comprehensive change history, attributing changes to specific IAM entities. Its adaptable security assessments swiftly detect misconfigurations, tailored to specific environment's classification. Continuous compliance monitoring and reporting, along with environment filtering and compensating controls, ensure adherence to standards. Additionally, Cloud Defense's integrated intelligent issues feed guides you to prioritize critical problems and vital resources, streamlining your cloud management process.

Cloud Native Threat Detection and Response

Cloud Defense instantly detects potential hostile activity and generates enriched alerts to help discern external attacks, malicious insiders, or innocent mistakes. FireMon Cloud Defense automatically enriches alerts with vital context, including resource and posture details, expediting analysis and investigation. Additionally, it's advanced filtering capabilities empower you to fine-tune issues and alert management across various projects, deployments, and environments, reducing false positives and alert fatigue. Cloud Defense enhances your cloud provider's native security alerts by seamlessly integrating enrichment, filtering, and routing functionalities.

Automated Cloud Security Maturity Model Assessments to Improve Your Security Program

Automatically assess individual deployments or your entire cloud footprint using the latest Cloud Security Maturity Model 2.0 released by the Cloud Security Alliance, IANS, and Securosis. FIreMon Cloud Defense evaluates your environments using the Key Performance Indicators from the CSMM to provide a holistic view of your program in the 3 Domains and 12 Categories of the model. Learn your strengths, weaknesses, and opportunities for improvement in areas like network security, IAM, and incident response. The automated CSMM features and visualizations keep you focused on the big picture while tracking and guiding security program improvements over time.

Identity Defense to Protect IAM Exposures

Eliminate static credentials and long-term permissions by implementing just-in-time approvals, out-of-band visibility, and session restrictions with FireMon Cloud Defense. With seamless integration into your existing identity provider, Cloud Defense ensures the security of identities and credentials. Users can request authorization through ChatOps or a web console, enjoying a frictionless approval process with advanced options for single or multipurpose approvers and self or automatic approvals. Cloud Defense supports multiple policies, source IP restrictions, variable session lengths, and other variables, effectively reducing IAM risks. All activities are meticulously logged and integrated into ChatOps for heightened visibility and accountability.

Deep ChatOps Integration to Bridge Silos

FireMon Cloud Defense bridges the communication gap between decentralized cloud operations teams, ensuring effective security across teams for rapid assessment, response, and remediation of misconfigurations and attacks. Cloud Defense offers comprehensive support for Slack and Teams, facilitating notifications and actions. Advanced routing ensures that teams exclusively receive issues relevant to their deployments, while still allowing security to oversee all aspects. Notifications are enriched with detailed information, and one-click remediation options are provided directly within the channel. FireMon Cloud Defense allows security teams to seamlessly collaborate with their cloud teams through ChatOps, expediting investigations and responses.

Event-Driven Automation and Assisted Remediation

Cloud Defense offers advanced, event-driven, serverless architecture that sends notifications and takes action at the speed of your cloud platform. Alerts are swiftly routed, appearing in under 30 seconds on AWS or GCP and within 2 minutes on Azure. FireMon Cloud Defense offers support for fully automated remediations, specifically targeting designated deployments. Moreover, all ChatOps notifications can incorporate predefined or recommended one-click remediation options, simplifying administrator decision making. Seamless integration with third-party systems enables ticket creation and external workflow triggering for enhanced flexibility and efficiency.

Feature	Benefit
Real-time Cloud posture, inventory, and change tracking	Natively monitors API activity in your cloud deployments, updates inventory, and runs security and compliance assessments in real-time.
Cloud native threat detection and response	Instantly detects potential malicious activity and generates enriched alerts to help discern external attacks, malicious insiders, or innocent mistakes.
Automated Cloud Security model assessments to improve your security program	Discover and quickly assess your cloud security readiness and identify steps to strengthen your security fortifications using Key Performance Indicators.
Identity defense to protect IAM exposures	Eliminates the need for static credentials or long-term permissions with just-in-time approvals, out-of-band visibility, and session restrictions.
Deep ChatOps integration to bridge silos	Bridges the communication gap between decentralized cloud operations teams, ensuring effective security across teams for rapid assessment, response, and remediation of misconfigurations and attacks.
Event-driven automation and assisted remediation	Advanced, event-driven, serverless architecture that sends notifications and takes action at the speed of your cloud platform.

Start using Cloud Defense Free for 30 Days Now!

FIREMON

FireMon is the only real-time security policy management solution built for multi-vendor hybrid enterprise environments. FireMon provides policy automation for the latest network security technologies helping organizations achieve continuous compliance while minimizing firewall policy-related risk. Only FireMon delivers complete visibility and control across an organization's entire IT landscape. Firemon.com

DS0249-EN-20231011-02