Make the Most of your IT and Security Investments with FireMon Integrations

One of the biggest pain points of security teams, development teams, and CISOs is the sprawl of multiple security devices in their network. What is even more challenging is that many vendors do not offer a consistent application programming interface (API) framework to maximize the opportunities for enterprises to integrate their devices across their security stack.

Good APIs are hard to come by and inefficient coding has far reaching implications. DevOps teams working to spin up and integrate newer applications will find it difficult to understand and interact with poorly written APIs, and they might need to write additional, more complex code in order to use them. Programming complexity could also result in longer lead times to test these codes as they tend to be buggy. Independent analyst firms have stressed the importance of delivering robust and flexible APIs, with some noting that the global cloud API market is expected to grow at USD 763 million by 2022, at 20% of CAGR between 2018 and 2022.1

The ability to easily exchange information between disparate security solutions via well-defined API structures can serve a number of benefits:

- Increase the total value and overall efficiency of an enterprise's combined security solutions
- Leverage solutions with robust API integrations so that enterprises can optimize their security posture across all of their environments
- Realize a better return on enterprise security investments
- Securely forge new avenues for business innovation and growth

FireMon RESTful Open APIs

FireMon RESTful APIs adopt the standardized Open API or Swagger toolset to deliver flexible, high-octane connectivity between different third-party enterprise network security tools. By enabling two-way data sharing between different security platforms, FireMon enables enterprises to extract critical data and deliver it instantly where it is needed the most. There are THREE key attributes to the FireMon integrations – these are extensible, flexible, and innovative. FireMon targets several critical KPIs to measure the success of our integrations:

- Enhance user experience; encourage greater interaction with the intuitive user interface
- Help DevOps quickly understand the API to spin up applications with ease
- Prompt DevOps teams to find novel, innovative uses for our APIs
- Easily trial FireMon platform in test environments for specific use cases

Extensibility of Integrations

FireMon believes that its integrations are not just another feature. The value of FireMon's integrations is in fostering the extension of our network security policy management into tools and platforms that provide powerful adjacencies in enhancing the enterprise's overall security posture. Here are some FireMon integrations serving specific use cases:

Use Cases	FireMon Platform Extensibility	Use Cases
Identify security vulnerabilities that put enterprises at risk	Native visibility features of FireMon integrated with vulnerability scanners to obtain real-time scan, correlating these with network topology and security configuration data from FireMon Security Manager.	A risk-centric approach to operations that reliably delivers better security and compliance with less effort and expense.
Support changing enterprise network environments	Integrate FireMon's security management platform with a variety of security devices on-premises and in the cloud.	Evolve network infrastructure, migrate to new device platforms and incorporate evolving security capabilities, including firewalls and cloud services without risking enterprise security posture
Accelerate change management	FireMon offers out-of-the-box, fast-track integration option with ITSM tools to accelerate the speed of change.	Control the lifecycle of security policy-related changes with minimum disruption to IT services
Support enterprise automation to reduce manual processes	Automation not limited to policy management but extends to supporting discovery, risk mitigation and cloud/network configuration and management through native functionality as well as integration with third-party tools	Monitor application/network connectivity and configuration changes and ensure security policy-based controls through continuous adaptive enforcement
Streamline and speed up incident response	Integration with security orchestration, automation, and response (SOAR) tools to combine threat alerts from SOAR with FireMon's rule recommendation and automation	Instantaneous alerts to SOC teams on misconfigurations, compliance violations, or breach avenue with accompanying policy recommendations for remediation

Flexibility of FireMon API

With support for the market's leading security devices and platforms, along with the ability to incorporate additional systems without requiring product updates, FireMon Security Manager enables all-inclusive network security assessment. FireMon offers broad and advanced integration options:

- Quick and easy integration across your environment Support for partial customization through highly flexible APIs – developer teams can quickly understand and interact with our API stack to make the necessary modifications and additions
- Complete customization available with FireMon Professional Services
- Broad and deep integrations offered across multiple platforms, including but not limited to SOAR, ITSM, and CI/CD; allows DevOps to use their own toolchain for all integrations instead of multiple proprietary vendor SDKs

Support for New Use Cases

Many of our customers have extended the application of our API to novel and innovative use cases. The FireMon API is designed to support the fine-grain functionalities of the applications it is exposed to, which allows enterprises to address additional use cases, over and above those it is intended for. A number of FireMon integrations with large enterprises have evolved with use as they can quickly create mock-ups of the services that they wish to add on. This helps DevOps and security teams to:

- Address new business requirements as they emerge, especially enterprise migration to the cloud
- Use the FireMon API abstraction layer so that other tools in your enterprise security stack can interact with it to create newer functionality
- Meet the fast-changing demands of the cloud in terms of cloud visibility and control, compliance, and security orchestration

FIREMON

"No API, Look Elsewhere: Any vendor or technology worth their salt will have advanced API integration available for your team to use for development purposes as well as to integrate other security solutions into your Zero Trust ecosystem. If your selected technology doesn't have solid APIs to use, find another vendor that does."—Forrester Research

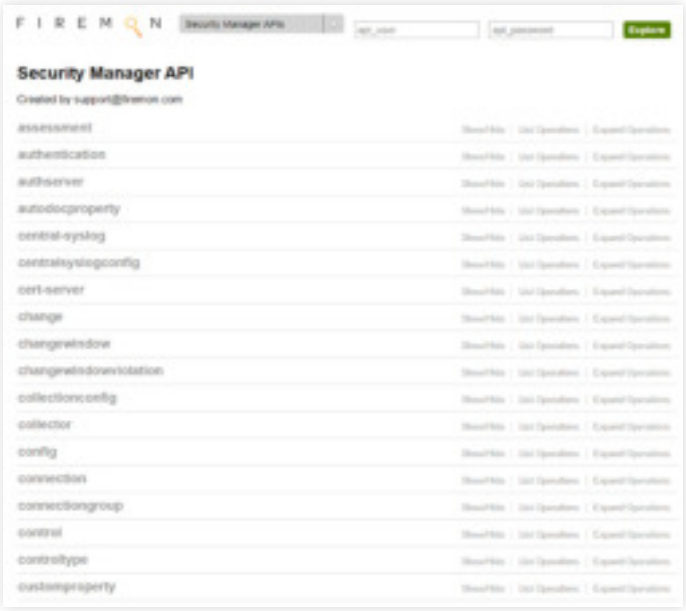


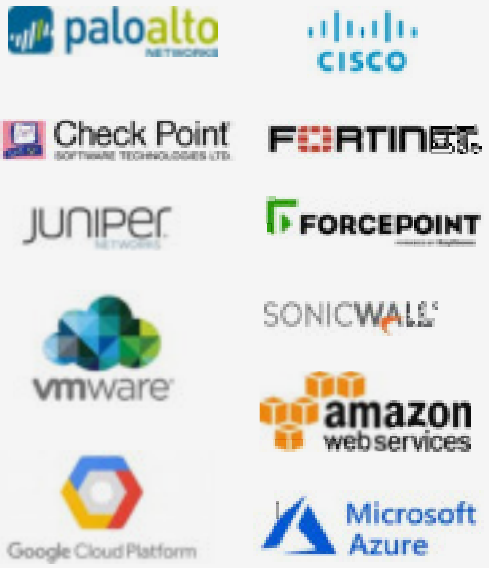
Figure 1. FireMon API using Swagger

Figure 2. Example List of API Operations

FireMon Integration Benefits

- ☑ Extend FireMon Compliance, Automation and Risk Mitigation into third party architectures
- ☑ Flexible integrations for multi-vendor security stacks
- ☑ Support two-way data sharing between major security devices, platforms, and applications
- ☑ Strong technology partnerships to continuously build FireMon APIs
- ☑ RESTful APIs with Swagger provides flexible, dynamic connectivity between different third-party enterprise network security tools
- ☑ Monetize enterprise digital assets; maximize security investments

Hybrid Platforms



Other Integrations

1 Market Research Future. “Cloud API Market Research Report – Forecast to 2022.” February 2020.
2 Cunningham, Chase, et. al. “The Zero Trust eXtended (ZTX) Ecosystem.” Forrester Research, Inc. January 18, 2018.