FIREMON

Be Curious. Ask Questions. Improve Security.

FireMon and Elasticsearch: Warp Speed Security

THE **CHALLENGE:** Reduce network risk with data. Loads of data.

Security devices are pummeled with network traffic. Each packet, transmission and rule-hit comes with data to reveal how the network is behaving and where to find security risks. This flood of data needs analysis, it needs storage, it needs speed.

Hidden in all that data is the signal that will show just how vulnerabilities can be exploited, how network rules are opening access and how policies impact network security and risk. Handling it all can be overwhelming, and sitting by waiting for reports to finish doesn't help anyone stay secure.

Specific challenges include:

- Data format and rule syntax are inconsistent
- Reports take too long, decisions stall
- Risk increases with unknowns hiding in the security data
- Exploits slip through the cracks when waiting for reports to load

WHY **FIREMON?**

Speed
Leveraging Elastic's inverted index for high-throughput, instant data mapping and full-text query, FireMon delivers full data retention and lightning fast search results across petabytes of data.

Scale
FireMon pulls data from every corner of the network for global, comprehensive details for every rule, every object, every device, every time.

Flexible

Distributed architecture means distributed data ingest, all backed by RESTful APIs that integrate with network systems to pull in the ocean of data streaming from enterprise network devices.

Real-Time Monitoring

FireMon is the only network policy platform with real-time monitoring. Elasticsearch and FireMon's unique architecture put an end to polling and other ancient methods for data retrieval and give you a live-stream for instant security.

THE **SOLUTION:** Sub-Second Security Search and Reporting

FireMon is the only network security policy solution with the power of Elasticsearch. FireMon lets you perform and combine any search – structured, unstructured, geo, metric – to find it all, in less than one second.

FireMon uses Elasticsearch to have unrivaled data ingest, scaling out to the global enterprise and indexing petabytes of device data in the blink of an eye. When others give you status bars and wait times, FireMon gives you answers. Truckloads of answers.