
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

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.