F I R E M O N

Risk Analyzer

Continuous data protection with attack surface visibility, simulation and risk scoring

THE CHALLENGE: Reduce the attack surface with real-time visualization and analysis.

Vulnerabilities abound. The modern enterprise is teeming with weaknesses that spread across the expanding attack surface. New computing models and platforms create more grooves for attackers to gain a toehold and compromise the network.

Scans, whether passive or active, are not enough. You need to know which exposures are reachable, accessible and under what conditions. Security policy is the missing link.

FireMon's Risk Analyzer brings it all together to change the cyberwar.

THE SOLUTION: Risk Scoring, Attack Simulation and Policy-Based Remediation

FireMon's Risk Analyzer pairs vulnerabilities with network policy to pinpoint exposures before they become exploited. Through recursive mapping and indexing, you are able to see the network in the context of attack paths, quantify precise risks the network faces and the steps to remediate indicators of exposure (IOEs).

Risk Analyzer will simulate your patch options so you have priorities for the greatest impact and halt lateral movement. Finally, orchestrate change in seconds to compress the attack surface and reduce an attacker's opportunity to zero.

Now, risks are isolated, measured and mitigated with absolute precision.

Risk Analyzer **Changes Cyber Warfare**

Attack simulation to uncover hidden paths for exploit

Instantly quantify risks and network exposure

Simulate patch options and prioritize remediation

Fully integrated scanner support to locate network weak spots

A continuous, real-time pen test for better security posture

032118

SOLUTION **FEATURES**

Risk Analyzer's patented risk engine helps IT security teams discover weaknesses in the network, evaluate the impact of a combination of exploits and recommend changes proactively.

REACHABILITY
Calculate how easy it would be for an attacker to reach the network through different network hosts and internet-facing segments and assess the potential damage.

GRAPHICAL ATTACK PATHS
Trace the possible paths an attacker might use across the network layout and identify where you can stop an attack with the least amount of time and effort.

ZERO-DAY ATTACK GRAPHS
Build a zero-day attack graph for each potential vulnerability and prioritize applications according to quantitative risk assessment.

METRICS AND MEASUREMENTS
Score all attack simulations for risk and impact and then re-score once you make improvements to determine the impact of changes.

PROACTIVE "WHAT IF" SCENARIOS
Patch systems virtually, re-run a complete analysis in seconds and compare various patch scenarios to ensure the biggest impact on efforts.

DASHBOARD RISK SCORING
Use an industry-unique, proactive risk score to view your riskiest assets and rules in a dashboard view.

ACCESS PATH ANALYSIS VIA SECURITY MANAGER
Decrease exposure and enable mitigation of risk by tracing all potential traffic paths, identifying problematic routes and implementing recommended adjustments to redirect access. Risk Analyzer performs a topology-aware assessment of critical factors including device rules, access routing and NAT, and prioritizes risks based on ease of reachability, value of underlying assets and known patterns of existing attacks. By adapting device rules to reroute access, risks can be addressed immediately and reduce complexity and time in patch remediation efforts.

WHY **RISK ANALYZER?**

Pair vulnerabilities with network policy to uncover exposures, score network risk and prioritize patches.

- Combine vulnerabilities and network security policy to identify potential exploits.

- See how each asset is exposed and how it is accessible.

- Get a complete score of network risk.

- Run attack and patch simulations.

- Remediate exposures based on greatest impact.

FIREMON