FIREMON

WHITEPAPER

PROACTIVE SECURITY INTELLIGENCE RETURN ON INVESTMENT

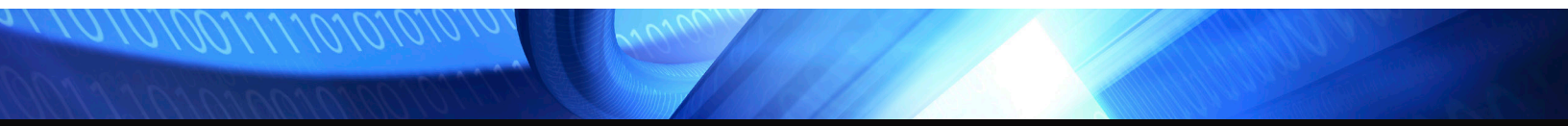
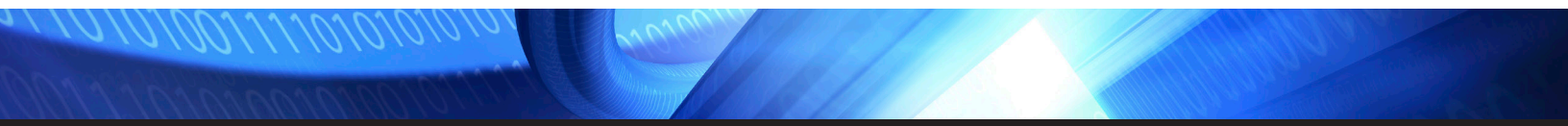


Table of Contents



Introduction: Proactive Security Intelligence: Is it Worth the Investment?

While it may seem obvious that more proactive, intelligence-based management of network firewalls and other security device infrastructure — including access routers, load balancers and the like — provides numerous opportunities to improve defense and prevent related compromise, documenting the financial and process-oriented benefits of this approach lends significant weight to its overall impact.

Traditionally, when IT professionals and security management officials consider the ROI and overall value proposition of solutions investment, discussions primarily emphasize direct financial benefits realized when adopting the involved solution(s). However, when reviewing the intrinsic strengths of embracing a Proactive Security Intelligence approach to management of network security device infrastructure, it is worthwhile to detail how this methodology also facilitates the evolution and improvement of many other related processes.

Based on an independent survey of over 125 FireMon customers conducted by researchers TechValidate:
54 percent of all FireMon customers report 100 percent ROI on their investment in 12 months or less.

The following information and justification highlights the pervasive ROI appreciated via adoption of this Proactive Security Intelligence management paradigm.

Business Case: Proactive Security Intelligence

The continued prevalence of network compromise and related data breach incidents drives home the undeniable reality that organizations continue to encounter myriad challenges in addressing the growing complexity and inherent nature of change central to the management of firewalls and other network security device infrastructure, including adaptation of related policies.

In direct contrast with the widely held perception that both known and undiscovered vulnerabilities reside in these systems remain the most problematic aspect of this troubling conclusion, leading experts have positioned that, in fact, fragmented and inconsistent management of core network defenses remains the most problematic issue.

For example, trusted industry analysts Gartner report that *"through 2018, more than 95 percent of [all related] breaches will be caused by firewall misconfigurations, not firewall flaws."*

In a recent survey of more than 250 security management officials representing financial services, government and business services organizations, among others, a litany of statistics supporting the need for more automated, context-aware oversight of firewalls and other network security device infrastructure emerged, including:

- 73% of all firewall policies are considered "somewhat complex" to "out of control"
- 75% of respondents cite firewall management as a labor intensive, manual process
- 75% of respondents still perform manual firewall/policy audits using internal staff
- 71% of organizations lack staffing to perform analysis needed to better manage firewalls
- 77% of respondents agree firewall audits should be performed continuously/quarterly
- 70% of respondents cite time needed to identify firewall changes as problematic
- 70% of respondents note increasing policy complexity extends analysis timeframes
- 35% of organizations believe themselves capable of analyzing firewalls on a quarterly basis

These statistics strongly reinforce that while organizations understand the need for more frequent, conclusive analysis of firewalls and related policies, there remains a distinct need for automated solutions allowing continuous assessment and providing targeted intelligence for informed response.

By adopting a Proactive Security Intelligence approach to analysis and management of network security device infrastructure, organizations can directly address the shortcomings of traditional firewall assessment and rein-in policy matters creating gaps in defense that enable network compromise.

Real-World ROI: Proactive Security Intelligence

The most effective manner of determining the specific ROI of the FireMon Security Intelligence Platform is gained by reviewing the solution's impact in real-world environments. Using measurements gathered from a sizeable telecommunications provider employing FireMon to automate assessment and improve alignment of network security device infrastructure, as well as optimize related policies, significant benefits are detailed.

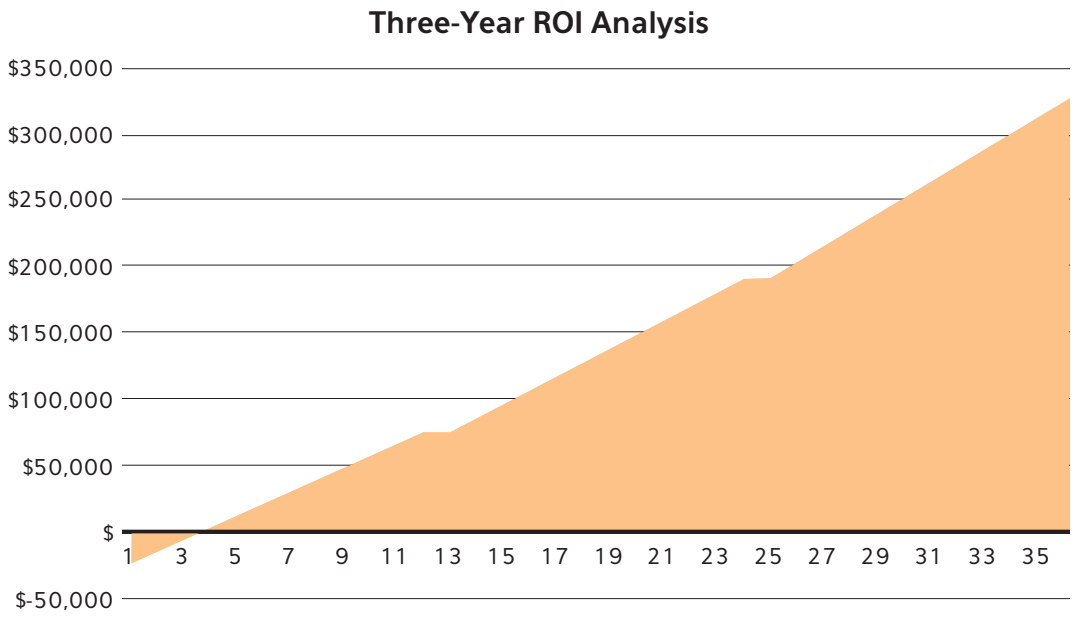
While the FireMon solutions platform empowers a much broader set of benefits across a wide range of network operations, security management, audit/compliance and IT risk management processes, this analysis focuses on actual cost reduction affecting this organization's bottom line. In the reported case study, FireMon directly affects matters of labor efficiency, firewall auditing expenses, and costs resulting from outages of misconfigured firewalls, among others.

It is asserted that within the first 12 months of implementing the core FireMon Security Manager solution, the customer was able to create $122,000 in value (time spent in other areas) using the product to automate firewall rules configuration and lower policy complexity; within 5 months of implementation, the entire investment in FireMon was recovered.

Measured Annual ROI: FireMon Security Manager

YEAR 1

By Month	1	2	3	4	5	6	7	8	9	10	11	12
Investment	$ -46,656	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Savings	$ 10,204	$ 10,204	$ 10,204	$ 10,204	$ 10,204	$ 10,204	$ 10,204	$ 10,204	$ 10,204	$ 10,204	$ 10,204	$ 10,204
ROI	$ -36,453	$ -26,249	$ -16,045	$ -5,842	$ 4,362	$ 14,566	$ 24,769	$ 34,973	$ 45,177	$ 55,380	$ 65,584	$ 75,788



ROI Analysis: Inputs and Measurements

The following firewall review ticketing data was utilized to arrive at reported ROI calculations:

	Year 1	Year 2	Year 3	
OPERATIONAL EFFICIENCY				
Number of change requests (weekly)	50	53	55	Requests
Average loaded cost of IT Professional (by the hour)	55	55	55	$
Average Time Spent per Request:				
By the Requestor	15	15	15	Minutes
By the Network Team	30	30	30	Minutes
By the Security Team	20	20	20	Minutes
Percentage of Re-Opened Change Tickets	25	25	25	%
False Alarm Percentage	5	5	5	%
ADDITIONAL SAVINGS (OPTIONAL)				
Annual Firewall Related Auditing Expenses	0	0	0	$
Annual Number of Outages Due to Misconfigured Firewalls	0	0	0	Outages
Estimated Cost Per Outage	0	0	0	$

The following time calculations regarding the involved customer environment were utilized based on real-world observations and other related experiences regarding use of FireMon in similar environments:

Assumptions	
Time to process a General Request — Requestor	50%
Time to process a General Request — Network Team	30%
Time to process a General Request — Security Team	10%
Reduction in "false alarm" Request Time — Requestor	50%
Reduction in "false alarm" Request Time — Network Team	20%
Reduction in "false alarm" Request Time — Security Team	0%
Reduction in Re-Opened Ticket	0%
Cost-Saving Auditing Expenses	85%
Cost-Saving Outages Expenses	60%
Loaded Cost Per Minute	**$0.92**

ROI Calculations: Observed and Projected Results

Based on the proceeding inputs, measurements and assumed results, the following ROI calculations were produced:

Calculations	First Year	Second Year	Third Year
Number of weekly "already works" requests	3	3	3
Time to process an "already works" request with Security Manager	13.50	13.50	13.50
Number of weekly General requests (Re-Opened Tickets)	35	37	39
Time to process a General request without Security Manager	65.00	65.00	65.00
Time to process a General request with Security Manager	18.50	18.50	18.50
Total Annual Operational Cost without Security Manager	**$154,916.67**	**$162,662.50**	**$170,795.63**
Total Annual Operational Cost with Security Manager	**$32,472.92**	**$34,096.56**	**$35,801.39**
Auditing Expense Savings	$0.00	$0.00	$0.00
Outages Cost Savings	$0.00	$0.00	$0.00
Total Annual Savings	**$122,443.75**	**$128,565.94**	**$134,994.23**

ROI Overview: Direct Benefits

In reviewing the supplied calculations, a number of immediate and substantial financial benefits are made clear, including:

- Over the initial 12 months of the measured timeframe upfront investment ROI of nearly 2x
- Over the initial 36 months of the measured timeframe upfront investment ROI of more than 6x
- Time necessary to process involved firewall review tickets reduced by more than 70%
- Related operational costs associated with firewall review tickets reduced by almost 80%
- Over the initial 36 months of the measured timeframe savings of 70% over upfront investment

Additional unmeasured, yet significant savings are also highlighted, including proposed costs compliance/audit expenses related to the same processes addressed by FireMon Security Manager. Also highlighted are indeterminate costs related to unforeseen service interruptions resulting from inefficiencies or errors introduced by traditional, manual oversight of firewalls, rules and policies.

ROI Overview: Real-World Environment

As an example of FireMon's immediate impact in real-world environments, consider the measurement of time/resource savings when used in one large government organization. After a specific instance of compromise, security analysts were required to conduct an audit of all network assets:

- Using FireMon Security Manager Platform, analysts were able to audit five complete network enclaves (connected environments under the control of a single authority) in approximately 1.5 hours (1 analyst/1.5 work hours/90 minutes), for an average of 18 minutes per enclave.
- Without FireMon, a similar audit of 40 enclaves required 2 months to complete (140 analysts/320 work hours/19,200 minutes), for an average of 8 hours per enclave.

ROI Overview: Non-Financial Benefits

Among the most significant and lasting benefits supplied by FireMon Security Manager are inherent improvements that directly result in more effective assessment and oversight of firewalls, network security device policies and related processes including:

- Prevention of network compromise and resulting data breaches related to poor access management
- Increased ability to tie network security management directly to business requirements
- Improved performance of overall network infrastructure driven by reduction in complexity
- Closed-loop, integrated policy management workflow, including what-if change analysis
- Rapid, informed response and defense reconfiguration related to changing conditions
- Continuous audit, validation and recertification of mandated policy compliance
- Prioritized (real-world exposure-based) mitigation of vulnerabilities and underlying IT risks

Conclusion: Clear ROI of Proactive Security Intelligence

When reviewing the current scenario of largely inefficient, highly fragmented and ultimately reactive processes used to address analysis and management of network security device infrastructure, related policies and underlying IT risks, it is clear that there is significant need for a more effective approach and supporting solutions.

Whether in consideration of specific expense items or numerous undocumented costs related to inefficiencies addressed comprehensively by FireMon Proactive Security Intelligence — and most importantly within the larger context of improving network defenses to prevent compromise and resulting outcomes — investment in the FireMon Security Manager Platform has immediate and undeniable benefits.

By utilizing FireMon Security Manager and its supporting modules to empower existing staff to address the persistent reality of spiraling complexity and ongoing change in network security device infrastructure, it is possible for organizations to greatly advance process and program maturity — enabling continuous assessment and monitoring, evolving overall management strategy, and, just as critically, freeing up substantial resources for application in other adjacent domains.

Addendum: Applicability in Real-World Breach Incidents

It is worth noting that in addition to the significant ROI benefits outlined in the proceeding document, use of FireMon Security Manager can prevent many common network compromise and data breach scenarios, including some of the largest incidents recently reported.

For example:

- Using FireMon Security Manager to understand overly permissive access and underlying attack paths, retailer Target would have been able to understand inappropriate routes open to its HVAC contractor which led to compromise of its point-of-sale network, exposing millions of consumers and incurring huge losses.
- Using FireMon Security Manager, industrial giant Monsanto could have seen gaps in its defenses that resulted in its reported breach of network security whereby attackers bypassed access servers to steal sensitive information — including customer names, addresses, tax ID numbers, and (in some cases) financial information.
- Using FireMon Security Manager, online marketplace leader eBay could have identified improper network access and used existing controls to prevent exposure of its users' password data, which resulted in significant reputational damage, potential lawsuits and major operational interruptions.

- Using FireMon Security Manager, payroll company Paytime could have visualized and mitigated compromise of vulnerabilities in its Client Service Center systems which led to unauthorized access to customer information, including Social Security numbers, direct deposit bank account information, wage information and other data.
- Using FireMon Security Manager, Sony Computer Entertainment America LLC could have visualized and mitigated improper access and poor network segmentation that led to exposure of personal financial details of its online gaming community members, for which it recently agreed to $15 million in damages.

About FireMon

FireMon is an enterprise security management company headquartered in Overland Park, Kansas. Founded in 2004, we help organizations find, correct, and ultimately avoid gaps in their existing network security infrastructure.

Our proactive, real-time enterprise security management platform gives security decision makers key management and operations data to reduce risk and provide appropriate levels of access. FireMon Security Manager provides a perfect framework for making intelligent, informed decisions to enact security countermeasures in real time, so you can protect your organization's network and keep business operations running smoothly.

CONTACT FIREMON:

8400 W. 110th Street, Suite 400
Overland Park, KS 66210
USA

Phone: +1.913.948.9570
Fax: +1.913.948.9571
Email: info@FireMon.com

FIREMON

Follow us on Twitter @FireMon

Like us on Facebook: www.facebook.com/firemon

8400 W. 110th Street, Suite 400 · Overland Park, KS 66210 USA ·
Phone: 1.913.948.9570 · E-mail: info@firemon.com · www.firemon.com

rev090514