Intelligent Security Management
Helping Enterprise Security Teams Improve Resource Efficiency & Reduce Overall Risk Exposure
TABLE OF CONTENTS

01 EXECUTIVE SUMMARY
02 THE CHALLENGE OF ADDRESSING COMPLEXITY IN SECURITY MANAGEMENT
03 CREATING OPEX EFFICIENCIES
04 QUANTIFYING THE VALUE OF OPEX & RISK REDUCTION
05 WHAT NEXT-GEN SECURITY LOOKS LIKE - INTELLIGENT SECURITY MANAGEMENT
06 CONCLUSION
Network data breaches are at their highest level\(^1\) with the average total cost of a breach sitting at $4 million (up 29% over the past three years\(^2\)). To address this rising trend, organizations, and specifically Chief Information Security Officers (CISOs), are significantly increasing their annual spend in security technology and personnel.

By some estimates, global information security spend will exceed $170 billion by 2020\(^3\). However, if past trends are any indication, the increased investment will do nothing to quell the number of breaches. In fact, it will increase complexity within the security infrastructure – creating more access rules and security data than existing resources can manage.

The answer, it would seem, is to hire additional personnel. However, complexity is growing at a rate that far outpaces the ability to staff, leading to a “complexity gap.” According to an Aberdeen Group Report\(^4\), overly complex enterprise network firewall infrastructure leads to the time-consuming and error-prone manual management of policies, rules and configurations, which increases operational costs and security-related risk. And even when the staff is in place, an IBM cybersecurity intelligence study\(^5\) found that 95% of all security incidents involve some sort of human error.

Security breaches are not the result of an investment, technology or staffing problem. With hundreds of thousands of network events per hour, daily firewall rule changes, on-going upgrades, increasing device and policy complexity, tens of thousands of policy rules, ineffective policy and risk assessment, compliance fire drills and limited resourcing, how can a CISO properly address the scale of these security issues without adversely affecting the business? Is there a way to make quantifiable improvements relevant to risk, complexity and events/incidents that also reduces costs and resource effort?

Solving these challenges requires an intelligent solution that utilizes simulation, benchmarking and analysis to more effectively manage policies and remediate inefficiencies, security gaps and discovered incidents. Intelligent Security Management from
FireMon consolidates all of these functions into one scalable, cost-effective platform for seamless prevention, detection and response that addresses the complexity gap and helps CISOs deliver on their mandates.

This white paper reviews the challenges, mandates and focus areas of typical enterprise security teams and introduces an intelligent framework for security management; specifically, one that enables a security organization to address network scale, efficiency and process change as it relates to their security operations and incident response processes.
The Challenge of Addressing Complexity in Security Management

When we talk about Security Operations, the big focus today is around addressing scale and complexity. The network infrastructure and its associated processes must continuously manage an increase in the volume of data that is moving in and out of a network surrounded by a complex maze of multi-vendor firewall devices and associated applications. To address this complexity, what are the quantifiable improvements a CISO can make to help them optimize how they manage daily firewall rule changes, on-going upgrades, increasing device and policy complexity, ineffective policy and risk assessment, compliance fire drills and event/incident triage all with limited and often under-skilled personnel?

Compliance Audits

Without any form of management technology, change documentation, risk assessments and rule review for compliance audits must be done manually. In fact, it is not uncommon for these events to result in key security, engineering and finance personnel to spend an average of 16 hours per network device plus an average of 3 hours per report for a PCI/ISO/SOX compliance audit. If you are a large organization with 100-200 firewalls, you could have 10-20 people spending many hours per year just on this one task.

AVOID: ~36 hrs. migrating & validating each FIREWALL UPGRADE

STOP: The manual assessment of Network ACL & Firewall policies at an ~16 hours p/device plus ~3 hours p/report for PCI/ISO/SOX COMPLIANCE AUDIT

SAVE: ~2.4 hours collating logs & data, remediating overly permissive rules for PERIMETER REVIEWS

REDUCE: ~8 hours spent identifying disruptive changes that cause DOWNTIME & EXPOSURE

GAIN: Data loss awareness with network visualization & detection of security exposure & define broad response & remediation strategies
Optimization

The organization may not have experienced a breach, but how prepared is it to examine the data if a breach occurs or a risk assessment/audit determines that their device policy rules are too permissive (allowing too much network access) or too restrictive (creating network bottlenecks)? Collating logs and other data for this effort without the correct set of tools could take several hours of tedious work.

Next-Generation Upgrades & Migrations

As CISOs upgrade their firewalls to enable new technology and functionality, they face two challenges: 1) how much time it will take their organization to upgrade the firewalls and 2) what do they do with all the policies and rules that are in place on the old firewalls and how do they optimally bring the “good” rules over to the next-generation device from the old device? Migrating and validating these policies can take up to 36 hours per firewall. If you have 200 firewalls, this process could take months to complete without the proper technology tools.

Assessing the Impact of a Breach

Once a breach has occurred, how does a CISO stop that type of behavior in their network? What additional visibility is needed to prevent additional loss through looking at network vulnerability and risk exposure that may contribute to a potential Denial-of-Service downtime or unauthorized retrieval of sensitive data in a hacking event? Without the proper technology, an organization could spend hours per incident identifying disruptive changes that need to be made to their network policy to eliminate this downtime and exposure. You need technology that maps policy to the way you look at vulnerability in the network so that you can optimize the way you look at data, including the way it flows through your network, monitoring your traffic, looking at the access path to that data and plugging the hole in that security policy that contributes to that vulnerability.

If a CISO of an organization that has 200 firewalls, that enterprise could be managing over 5,000 policy changes a year encompassing over $100,000 in annual resource expense. What if a CISO could save 80% of this OPEX through proper tools and process improvement?
The Change Management Process should be an optimization exercise in an organization. Implementing point-specific automated changes in a quick way without a structured and consistent form of review and analysis can result in unintended consequences, primarily increased network complexity and risk. A prudent CISO needs to look at what personnel needs to do to implement the right changes in an organization and look at how to use technology automation to implement the right solution around the right process that creates the desired efficiencies wanted without the unintended consequences, increased complexity and risk. This top-down view of policy change management that properly links security and network operations is called Intelligent Policy Automation and is only available from FireMon.

Intelligent Policy Automation (IPA) captures the policy change request and documents it forever so security personnel can review how they changed it and how they designed that flow (particularly in hybrid environments where there are multiple firewall vendors and multiple pathways of network traffic).

INTELLIGENT POLICY AUTOMATION
1. Capture Request details
2. Identify rules for Design
3. Review for compliance/risk
4. Skip-review for low-risk changes for fast deployment
5. Implement rules with customizable workflows
6. Automatically verify planned changes were made
7. Post-implementation Monitoring & ongoing review

- Model the RIGHT change to reduce complexity
- Review & automate the LEAST RISK Change as part of an integrated workflow without customization

Exclusive to FireMon
The change is also reviewed before it is implemented to make sure that policy change won’t cause downtime once implemented (for example, you don’t want to implement a policy change in the middle of day against the 5 most active firewall environments). Automation needs to be carefully timed and executed in unison with the network infrastructure. Once the policy change is implemented in a single flow, it is done with consistency and can subsequently be monitored and reviewed to verify that the desired positive security posture outcomes and efficiencies have been achieved.

The importance of review, verification and monitoring as part of an overall Intelligent Policy Automation implementation process cannot be overstated or de-emphasized. How can you assess or measure improvement if you don’t review what you are going to do before you do it, verify that what you intended to do actually happened and proactively monitor the associated productivity impact that change had on your operation? Without these critical steps, a security organization is just saving someone time in network operations and not looking at that impact of that change on the entire enterprise. When automation is integrated into this process, IPA makes sure that the automation occurs as part of an overall framework for implementing change not just for satisfying a need to save a Network Operation Engineering a few hours of labor.
Quantifying the Value of Reducing OPEX & Risk

When a CISO looks at process and improvement, what outcomes do they want to look at to quantify that value?

- **Operational Management OPEX Reduction** – Good process change leads to better use of staff and technology resources associated with managing rules, audit, upgrade, complexity and analytics.

- **Downtime Reduction** – Early vulnerability detection leads to improvements in uptime and support rates by reducing outages and business interruption.

- **Data Breach Impact** – The type and rate of change together with the effect on network complexity directly correlate to risk of breach. By qualifying the impact of security policy change and relating that to the events and alerts associated with network segments, we can show measurable reduction in incident rates, and in turn, a data breach, that would negatively impact an organization’s productivity and brand.

When this process improvement is monetized (through an ROI calculation), the CISO can determine how much time and money they are saving by resource and by the reduction in tasks associated with actual activities in the organization.
The CISO Needs Timely KPIs & Analytics

A high priority of a CISO is to monitor productivity of an organization, typically done through Key Performance Indicators (KPIs) and reporting those KPIs back to company executive management or to a Board of Directors. These KPIs help articulate the enterprise’s security posture, incident response and breach analytics and quantify improvement in these areas. To do that, KPIs need to assess risk. Risk comes from controls, and control frameworks are derived from the organization’s infrastructure so that they have effective and qualitative reporting throughout the entire process - not just for a particular point in time, but over a timeline, so that accurate trend analysis and risk improvement can be derived. In addition, that improvement can be mapped to the reduction in complexity, a key bottleneck in determining vulnerability created through bad implementation of blindly pushing policy rules through as quickly as possible without considering consequence.

This type of measurement moves the CISO from a reactive security posture of "break-fix" to one of proactively looking for incidents very quickly - a fundamental shift in thought process and investment cycle thinking around security.

Key Performance Indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Inventory</td>
<td>11</td>
</tr>
<tr>
<td>Devices Revised (last 7 days)</td>
<td>27.27%</td>
</tr>
<tr>
<td>Unused Rules (last 90 days)</td>
<td>44.13%</td>
</tr>
<tr>
<td>Average Security Concern Index</td>
<td>7.01</td>
</tr>
</tbody>
</table>

Failed Rules by Control Tag (Top 10)

Rule Usage by Cumulative Severity
How Do You Measure the Impact of a Breach – Do You Really Know?

Once a CISO thinks in this paradigm, moving from protection to detection, what would happen if a breach occurred? What would the impact be to the organization? How quickly can the organization respond and minimize the breach’s impact?

Today, CISOs have many ways to analyze breaches, including collecting a massive amount of data through the use of a Security Information and Event Management (SIEM) tool. The collection of large volumes of data is only one piece of the analytics puzzle; the data still needs to be interpreted. SIEMs collect data in the context by which their queries have been defined. If you want to analyze other data points from different devices, such as behavioral antics of activity, the organization needs to have the data enriched so they can make decisions quickly. This may involve the need for a CISO to hire expensive Data Scientists to spend 1-2 days per week creating complex datasets for their own interpretation.
What needs to happen is to analyze the event at the time the event is occurring in a view of information that directs organizational behavior. Personnel need to triage data events and alerts to the point where they can quickly sift through 98% of the “noise” that’s involved in the analysis and focus on the small percentage of data collected that is involved in the breach alert/event. Then they direct the behavior of the cyber team or event triage team to automatically plug holes in the security policy that would immediately improve their overall security posture protection.

To do so requires the proper technology to do the triage, which involves incorporating a natural language analysis technology that can enrich that data at the point of acquisition, direct the behavior of the SIEM team to have outcome workflow and integrate with the security organization to understand what is needed to better protect the perimeter of the network going forward. This combination of technology, workflow and integration is important to document when an organization is applying for incident response cyber insurance.

This industry-unique integration of real-time event monitoring integrated with the security policy management process is only available on the Intelligent Security Management platform from FireMon.
Visibility into Complexity

The speed of business is accelerating, the complexity of infrastructure is multiplying and the severity of threats is increasing. Only Intelligent Security Management from FireMon uses an infrastructure-independent, single-pane view to monitor the current situation and analyze the best course of action – disrupting complexity and simplifying what was previously unmanageable.

Next-Level Proactivity

The best way to deal with a breach is to prevent it from happening in the first place. The Intelligent Security Management platform uses non-service affecting change simulation to improve an organization’s ability to manage the infrastructure it already has, allowing it to take a more proactive posture with regard to risk assessment and mitigation.
Accelerated Business Agility

Intelligent Security Management uses automated, context-aware change management workflows to improve response rates, deployment times, labor efficiency and infrastructure performance as well as overall security posture. Agility creates competitive advantage, and FireMon enables security to move at the speed of business.

Quantifiable Impact

FireMon’s team of security professionals have decades of experience helping clients solve security challenges. But we recognize that no matter how fast the process, or how strong the partnership, outcomes can only be measured by the impact they have. FireMon Intelligent Security Management provides a CISO the ability to quantify risk/resource impact by providing security intelligence data that can be easily communicated and shared across the enterprise.

Mapping the Value of the Right Technology to Key CISO Mandates

This integration maps well in addressing several CISO mandates, from regulatory security audit and policy refresh/enforcement to an M&A asset addition, data center consolidation, improvement and upgrade impact assessment. The bottom line, whether related to OPEX reduction, risk mitigation or process improvement, Intelligent Security Management provides seven clear areas of measurable benefit to IT, security, network and cyber operations as follows:

1. Security OPEX Management – Use technology to manage increased data volume, increased network complexity and reduced personnel resources as well as to quantify savings.
2. Network Operations OPEX – Use technology to improve the way you look at vulnerability via access path analysis, traffic flow analysis and vulnerability assessments.
3. Risk & Trend Analysis – Use technology to score security policy data over time and monitor how your scores relate not only to your improvement but also to others in your industry.
4. Firewall Perimeter & Stability Review – Use technology to visualize how the network is configured, and you can examine current and newly created vulnerability points that are mapped to a formalized risk assessment model that is attached to your security management policy.
5. Real-Time Event Triage – Use technology to connect protection to events so that you look at the consequence of improvement from a policy and efficiency perspective and how that contributes to overall risk reduction and breach.

6. Proactive Incident Response – Manage the alert fatigue associated with SIEM and cyber operations by enriching data sources in real-time to effectively search, learn and navigate the true meaning of breach events for improved insight and workflow relative to incident response.

7. Cyber Forensics – Quickly and efficiently analyze a range of data sources for improved insight and direction in mitigating the exposure associated with cyber breach.
The CISO is responsible for aligning corporate IT security to company mandates, owns security programs that achieve mandates and creates security projects to cover gaps in programs. These programs include:

- Compliance Management to support adherence to industry standards, regulations and contractual obligations within the company
- Incident Response that identifies, contains and eradicates threats and attacks
- Risk/Audit Management that identifies risks to company and provides assurance on investments related to risk mitigation
- Business Continuity that ensures IT and other business functions have plans in the event of business disruption
- Security Operations that maintain cyber technologies and staff chartered in supporting the above programs

These programs are designed to prevent breaches and loss of sensitive company and company client information.

Adding additional technology to the existing security infrastructure or adding personnel will not be sufficient in successfully addressing the growing number of breaches and attacks. Organizations must adopt next-generation security management solutions to support Policy and Standards Development, PCI DSS, ISO and SOX Compliance Projects, Policy Enforcement, Annual Audits, Firewall and Perimeter Stability Review projects as well as provide SOC Improvements and Security Analytics projects required for real-time insight into response and forensics.

Addressing the complexity gap, which results when the scale and complexity of firewall policies outpaces the addition of skilled personnel required to effectively manage them, requires implementing an Intelligent Security Management platform. This platform, available only from FireMon, provides a CISO with a cohesive, cost-effective, decision-making tool for security prevention, detection and response that addresses the complexity gap, provides key metrics of security posture and threats and prepares the organization for technology change.

Conclusion

The CISO is responsible for aligning corporate IT security to company mandates, owns security programs that achieve mandates and creates security projects to cover gaps in programs. These programs include:

- Compliance Management to support adherence to industry standards, regulations and contractual obligations within the company
- Incident Response that identifies, contains and eradicates threats and attacks
- Risk/Audit Management that identifies risks to company and provides assurance on investments related to risk mitigation
- Business Continuity that ensures IT and other business functions have plans in the event of business disruption
- Security Operations that maintain cyber technologies and staff chartered in supporting the above programs

These programs are designed to prevent breaches and loss of sensitive company and company client information.

Adding additional technology to the existing security infrastructure or adding personnel will not be sufficient in successfully addressing the growing number of breaches and attacks. Organizations must adopt next-generation security management solutions to support Policy and Standards Development, PCI DSS, ISO and SOX Compliance Projects, Policy Enforcement, Annual Audits, Firewall and Perimeter Stability Review projects as well as provide SOC Improvements and Security Analytics projects required for real-time insight into response and forensics.

Addressing the complexity gap, which results when the scale and complexity of firewall policies outpaces the addition of skilled personnel required to effectively manage them, requires implementing an Intelligent Security Management platform. This platform, available only from FireMon, provides a CISO with a cohesive, cost-effective, decision-making tool for security prevention, detection and response that addresses the complexity gap, provides key metrics of security posture and threats and prepares the organization for technology change.
References

2. 2016 Cost of Data Breach Study: Global Analysis published by Ponemon Institute, June 2016
3. MarketsandMarkets
4. Quantifying the Value of Firewall Management, Aberdeen Group, written by Derek E. Brink, CISSP, Vice President and Research Fellow, Information Security and IT GRC, October 2016
5. Forrester: Zero Trust Network Threat Mitigation Technologies, Q4 2016