FIREMON

Debunking

4 Common Myths

of Security Policy Compliance

Improve your security posture, reduce risk, and find threats in real-time… without sacrificing agility

EXECUTIVE SUMMARY

In today's world, it's impossible to get away from overflowing regulations, ever-changing compliance standards, and the looming threat of a data breach. System glitches cause 25 percent of data breaches in 2019, and human error is the root cause of 24 percent of breaches. While much attention in the security world is placed on malicious attacks, it's worth noting that breaches caused by system glitches and human error can have consequences that are just as serious.[1] To make matters worse, 53 percent of organizations reported a problematic shortage of cybersecurity skills—and there's no end in sight.[2]

Organizations are constantly searching for a solution to these converging issues—all while keeping pace with business and regulatory compliance. Many have become cynical and apathetic from the continuous failure of investments meant to prevent these unfortunate events. As digital transformation initiatives are fundamentally changing how you operate and deliver value to customers, partners, and employees. In turn, your approach to network security policy and firewall management must also change. There is no silver bullet, and waving a white flag is just as problematic.

The fact is, no one knows what could happen next. We can adopt methods of reason, evidence and proactive measures to maintain compliance in a changing world. Dethroning the concept of passive compliance is an important step to achieve security agility, reduce risk, and find threats in real-time across all your network devices and cloud instances.

This paper highlights the suggested steps to improve your security posture, achieve continuous compliance, and gain real-time visibility and control to protect your hybrid environment.

[1] Ponemon, Larry. "What's New in the 2019 Cost of a Data Breach Report." Security Intelligence. Jul. 23, 201

[2] Oltsik, Jon. "The cybersecurity skills shortage is getting worse." CSO Online. Jan. 10, 2019.

Who And What Is At Risk?

Many organizations have adopted a passive compliance playbook, potentially leaving anyone and everyone exposed to threats. With little to no visibility into their network, they fail to discover hidden threats that could lead to the next data breach or uncover compliance failures.

A passive approach to compliance includes:

- Collecting a lot of data
- Putting the data in a database with modeled triggers
- Waiting for any alerts

This approach doesn't make your organization any safer. Depending on your specific sector, you may have industry and regulatory standards like PCI-DSS, HIPAA, SOX, or NERC-CIP on your plate. The levels of manual effort by security teams involved in reducing risk and completing compliance audits are compounded by the lack of real-time visibility of what is truly going on in their networks.

Take the first step by recognizing the four myths of policy compliance.

MYTH #1: Compliance Is All About Rules And Access Control

Compliance and network security is not just about creating rules and access control for an improved posture. You need ongoing, real-time assessment of what is happening in your hybrid environment. Hiding behind rules and policies is no excuse for compliance and security failures.

Organizations overcome this myth with direct and real-time log analysis of what is happening in their hybrid environments at any moment. Security and compliance come from establishing policies for access control across your network and ongoing analysis of actual network activity to validate your organization's security and compliance measures.

FireMon customers have seen a **4x reduction** in the number of days per year spent on Audit & Compliance

LOG ANALYSIS WITH FIREMON

• Real-time advanced threat detection	• Powered by Elasticsearch, real-time scalable search
• Anomalous user and machine behavior	• Automated data assembly and association analysis
• Digital forensics and investigations	• Accurate remediation recommendations

MYTH #2: Compliance Is Only Urgent When There Is An Audit

The evolution of hybrid environments remains the most critical challenge to maintaining security and compliance. Unfortunately, that evolution does not politely stand by while compliance and security personnel try to catch up.

Standards for compliance are also changing within the context of these evolving hybrid environments. For example, GDPR & CCPA both ask where consumer data is stored. In the cloud? This adds new dimensions to ongoing compliance mandates beyond those that are top of mind during an impending audit.

Next-generation firewalls and logging technologies take advantage of the data streaming out of your network, but compliance is achieved when you have a process and the tools to analyze all of the data. By looking at the data in real-time your compliance and network security teams can quickly make adjustments and reduce risks.

Tightened network controls and access gives auditors the assurance that your organization is taking proactive steps to orchestrate network traffic. But what does your actual network tell you? Without constant log analysis, there is no way to verify compliance has been achieved. This continuous analysis must happen independent of an upcoming or recently completed audit.

Typical FireMon customer see a **>300% reduction** in the time it takes to produce audit reports

The lesson to learn from this myth is that compliance must be concurrent with your network's evolution and standard changes. Compliance can no longer be a point-in-time assessment—it must be a continuous validation process with real-time, continuous monitoring.

REAL-TIME, CONTINUOUS MONITORING WITH FIREMON

• Out-of-the-box (e.g. PCI-DSS, NERC-CIP, etc.) and customizable assessments to ensure compliance	• Ongoing backup for device configurations
• Continuous change detection based on syslog, not polling	• Automated assessments for any change relevant to compliance standards
• Change attribution and user behavior analysis	• Traffic flow analysis traces the source and destination of every rule in every firewall policy to understand network traffic behavior
• Distributed architecture for high throughput and data retrieval	

MYTH #3: It's Better To Block Than To Permit Access

One of the oldest security practices is to "just say no." The trouble with just saying no is that it bypasses defining business requirements before establishing an optimized security posture. Security and compliance teams may default to block or limit access, but this can impact a business's speed to market.

You do need security and access controls to protect your organization, but reducing or eliminating access is just as damaging. Those implementing "block" as a default are waving a white flag, stating that compliance and access control is too difficult or time-consuming to give thoughtful consideration to the reasons and outcomes of granting the appropriate access.

A balance can be found—we do not need to withhold access to vital assets and information in our hybrid networks, nor do we need to open the floodgates to any and all who demand it. Instead, your network policies adapt to the needs of your business; policies that are asset and entity-centric. Policies that follow the user, service, host and information can conform to your compliance standards. With ongoing analysis, you can discover compliance slips, quickly course-correct, and take action to regain compliance.

The lesson from this myth is that the alleged silver bullet of blocking has the potential to backfire. However, with careful and consistent data-driven analysis, compliance and security personnel can spot any failure and quickly remediate in real-time.

Average customers have seen **62% faster SLA** by automating pre-change modeling and risk optimization.

DATA-DRIVEN ANALYSIS WITH FIREMON

• Visualize usage of existing rules and policies, including threats denied by access policy	• Automated assessments for any change relevant to compliance standards
• Trace the source and destination of every rule in every firewall policy to understand network traffic behavior with traffic flow analysis	• Automated rule and policy design
• Eliminate overly permissive or redundant rules	

MYTH #4: Real-Time Visibility Is Impossible

With legislative and regulatory changes coming so rapidly, network security and compliance teams need real-time visibility and access to data across their entire networks.

Because data comes in multiple formats and structures, compliance reporting becomes an exercise in 'data stitching' in order to validate that network activity conforms to rules and policies. Security and compliance staff must become de facto data scientists to get answers from the ocean of data.

How do you know if a given rule or policy is going to have the desired effect (conform to compliance)? Like most organizations, you do not have the personnel or time to assess network activity in the context of compliance standards. By the time a new compliance standard is due, the data stitching process is not complete, leaving you unsure if compliance has been achieved. No matter how fast you stitch data, you'll never be done.

Of course, the other side of this dilemma is that these standards genuinely do prevent data compromises. But while a good chunk of your resources is tasked with testing and rolling out standards, another part of the team is implementing even more permutations in your network.

FireMon customers typically detect **40% more** rogue or shadow devices that they can bring under management.

It is natural to assume, "Well, I guess it just can't be done." With automated processes, you can shorten the time to assess compliance standards and the outcomes policies and rules produce.

The lesson learned from this myth is that real-time, global visibility is possible. Real-time, continuous visibility across your entire network reduces your attack surface, eliminates data leaks, and ensures continuous compliance.

REAL-TIME VISIBILITY WITH FIREMON

• Real-time situational awareness across the hybrid enterprise eliminates blind spots	• Full data retention
• Single console for enterprise-wide search and reporting	• Search across your entire enterprise using SiQL
• Powered by Elasticsearch, real-time scalable search	• Automatic live stream from all network devices, enterprise-wide
• Distributed architecture for high throughput and data retrieval	

CONCLUSION

Establishing and maintaining security and compliance across your hybrid network is an essential effort. Often, unforeseen circumstances can interfere with our best efforts to accomplish compliance objectives and security mandates. Understanding how to succeed in the wake of constant changes can give you a pathway forward to improve network security and compliance.

A comprehensive security and compliance strategy consists of people, process and technology, none of which can function without the other. It is a three-legged stool, with each playing a significant role to hold up security and compliance.

The best outcome is achieved by removing the false pretense of these compliance myths. Compliance is more than just rules and access control. It's relevant all the time. You can enable your business with sound security policies that work for your organization. And you can have real-time visibility into your ***entire*** network.

Falling out of compliance will happen and chances are it is happening as you read this. But by cutting down the time to discovery, assessing the appropriateness of policies and continuously inspecting your data you can regain compliance.

LEARN MORE ABOUT FIREMON COMPLIANCE.

SCHEDULE DEMO

ABOUT FIREMON

FireMon is the only agile network security policy platform for firewalls and cloud security groups.

FireMon is the fastest way to streamline network security policy management, which is one of the biggest impediments to IT and enterprise agility. Only FireMon offers Continuous Policy Automation, including the full range of capabilities to dynamically secure firewall and cloud security group policies—and increase enterprise agility. Since creating the first-ever network security policy management solution, FireMon has delivered command and control over complex network security infrastructures for more than 1,700 customers located in nearly 70 countries around the world.

For more information, visit www.firemon.com