ENTERPRISE RISK MANAGEMENT SPECIAL

CIOReview

The Navigator for Enterprise Solutions

JUNE 23, 2016 CIOREVIEW.COM

IN MY OPINION

Dominic Casserley,
President and Deputy CEO,
Willis Towers Watson

CIO INSIGHTS

Christopher R. Barber,
EVP & CIO, Commonwealth
Business Bank

CXO INSIGHTS

Adrian Brown,
Chief Risk Officer, Seibels

FireMon: The Enterprise Security Management Vanguard

Jody Brazil,
Co-founder &
Chief Product Strategist

$ 15US

SE 37

0 74470 91626 0

CIO REVIEW
44790, S Grimmer Blvd.
#202, Fremont, CA-94538

CIO Review 20 MOST PROMISING ENTERPRISE RISK MANAGEMENT SOLUTION PROVIDERS - 2016

FireMon :

The Enterprise Security Management Vanguard

By Samden Sherpa

The 1990s was a busy decade for networking. It was during one fateful night in this era—post the development of the network firewall—that Jody Brazil, co-founder and Chief Product Strategist of FireMon, received a call from a customer. The issue was quite odd—a firewall was blocking traffic between two parts of the network that should have been permitted. "The issue was urgent and critical," recalls Brazil. "The customer presumed that the firewall was down." On the contrary, the firewall was functioning perfectly—controlling the network traffic flow as designed." An incorrect change in the firewall—made by the customers' administrator—was the culprit. "The firewall was a complex technology, and it was easy to make a mistake, particularly by IT administrators doubling as the organization's IT security staff," says Brazil.

It was a "Eureka" moment for Brazil. The following days saw him thoughtfully designing a simple scripting solution that captured every change made by the administrator and presented a report that brought in transparency and visibility into the network infrastructure. As time passed, new market opportunities erupted, and the metamorphosis of the solution led to the birth of FireMon—an intelligent firewall management software platform. Approaching 20 years of innovation, Brazil's team, based in Overland Park, KS, today builds and sells network security management solutions to help enterprises make the most of their existing security technology. Their flagship product, Security Manager, assists large enterprises in reducing the complexity of managing security and overcoming challenges in firewall management with

the end goal of improving their overall network infrastructure security and reducing risks.

The Intelligent Security Platform

With the expansion of the network security infrastructure, organizations—both old and modern—are becoming highly complex, leading to greater risks. For an organization to stay resilient and optimized, it is mandatory for risk managers to understand and account for all types of risk, from financial to security risks, compliance and operational risks, spanning hidden threats and emerging hazards. FireMon delivers intelligence that allows enterprises to continuously analyze, visualize, and improve their existing network security infrastructure. "We help in identifying the proximity of the risks and the gaps in their tools or infrastructure. We understand where their weakness lies and help them efficiently and effectively secure their enterprise," asserts Brazil.

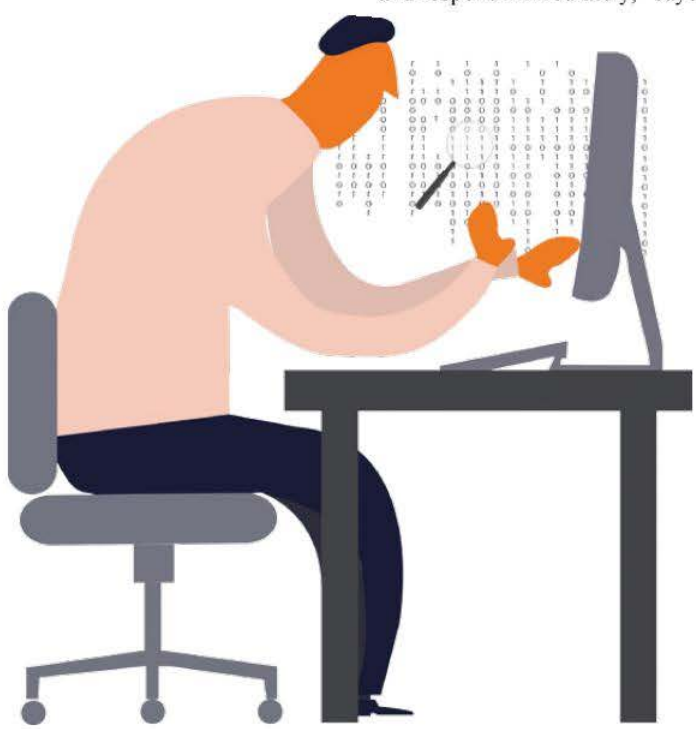
The FireMon platform pulls real-time data such as log files, changes, vulnerabilities and configurations from the customer's existing network devices into one single dashboard to give a complete picture of their network defenses with a security risk score. With a high performance engine and distributed data architecture, the platform provides enterprises with continuous assessments of their security policies. "Our platform offers a set of feature-rich capabilities that enable practitioners to effectively improve the firewall management of policies and changes, ensure network compliance and also assess network risk," affirms Brazil.

A web-based platform, Security Manager increases the visibility into device controls and configurations that allow enterprises to monitor and modify policies to maximize security on the network. Customers can experience more effective security management, lower cost of operations and reduced exposure to risk. "Our platform has helped many enterprise customers and Federal agencies—that often spend millions of dollars in security infrastructure—to effectively manage their network infrastructure while optimizing resources and reducing costs," states Brazil. "The platform's dynamic and flexible application programming interface (API), allows it to smoothly integrate into today's diverse enterprise environments for comprehensive, centralized management of network security infrastructure," says Brazil.

> "Every decision that we make—the features to build, the products to bring to market next—always starts with the customers' needs

The More the Better

FireMon's security platform is complemented with the presence of four modules—Risk Analyzer, Policy Optimizer, Policy Planner and Immediate Insight—that integrate seamlessly into the application. The Risk Analyzer, Policy Optimizer and Policy Planner are optional add-on modules that customers can add to their system to extend the capabilities, while Immediate Insight is a standalone application that can be deployed with or without the Security Manager platform. Immediate Insight helps organizations search data to identify any unseen threats and risks in an organization. It collects and correlates IT data to help analysts and operations staff increase visibility into the data and reduce the time and effort spent on incident triage. "By bringing in data from an unlimited number of sources, whether it's from applications, hosts firewalls or network logs from packet captures or email boxes, users can discover events within the organization and respond immediately," says Brazil.



While taking care of the security at one end, "making changes in security policies always open up your organization to risks," says Brazil. As such, the Policy Planner module automates the firewall change process with an intelligent workflow solution that solves unique challenges associated with firewall change management. "We help automate the change process not only to make the changes faster, but more importantly to make the right changes," says Brazil.

While security devices, firewalls in particular, are made of a series of rules which determine the flow of traffic in an enterprise, the Policy Optimizer module transforms security infrastructure management by automating the change review process—from rule analysis to policy modification, as well as recertification and documentation. "It enables organizations to stay accurate, up-to-date, and effective. Rules that are no longer necessary to the business or rules that expose the organization to excessive risks can be quickly identified and remediated," says Brazil.

Additionally, the Risk Analyzer module evaluates the effectiveness of the security infrastructure by analyzing the exposure of identified system vulnerabilities in the context of network access controls. Using the results of vulnerability scanners and the network and security data from Security Manager, "we create a picture of potential attack paths through existing defenses," says Brazil. "Effectively, our risk module is a roadmap of all the attack vectors that allows enterprises to identify where they need to focus."

> We understand where the weakness lies and help clients efficiently and effectively secure their enterprises

Delivering Real Impact

The philosophy behind FireMon has always been to provide real-time enterprise security management intelligence that gives security experts the key insights needed to reduce risk and provide appropriate levels of access. "This helps organizations efficiently manage their enterprise, regardless of the industry," extols Brazil.

By deploying FireMon's solutions, customers have reported a measurable improvement in the overall state of their network security. For instance, a large financial institution had over 1000 firewalls, and as the number of devices and rules exploded, they were finding it difficult to manage the complex environment. The client wanted to reduce the amount of time taken to make a change in enabling new access to any applications. The client was expecting to bring the usual 30 day change period to 10 days. They also wanted to maintain the same control infrastructure that existed. All the changes had to be approved by the same number of people and had to go through the same number of checks for verification before they could be implemented.

FireMon provided its Security Manager platform as well as Policy Planner to address the client's needs. Security Manager provided the infrastructure for continuous monitoring of their critical devices—including Check Point, Cisco and Palo Alto Networks. The platform helped the client reduce the complexity of their current environment. By deploying Policy Planner and implementing a custom workflow that integrated with the client's ticket managing system, the solution helped automate many stages of the client's process—from change identification, change request, risk evaluation, to verification. In the end, FireMon was able to reduce the change time from nearly 30 days to less than 10 days, exceeding the client's expectations.

Continuing with the Tradition

The uniqueness of FireMon lies not only in delivering comprehensive products but also in the way it develops the products. "We start with the customer problem, and every decision that we make—the features to build, the products to bring to market next—always starts with the customers' need," informs Brazil. Drawing the line between themselves and the competition, this remains as the DNA of FireMon today. "It is the core tenant in how our company functions," said Brazil.

Subsequently, as new pieces of technology such as cloud, network virtualization, and Software Defined Networking (SDN) arrive on the scene, FireMon is focused on reinforcing its leading role in the network security market through innovation and focusing on solving the complex security problems of their customers. CR