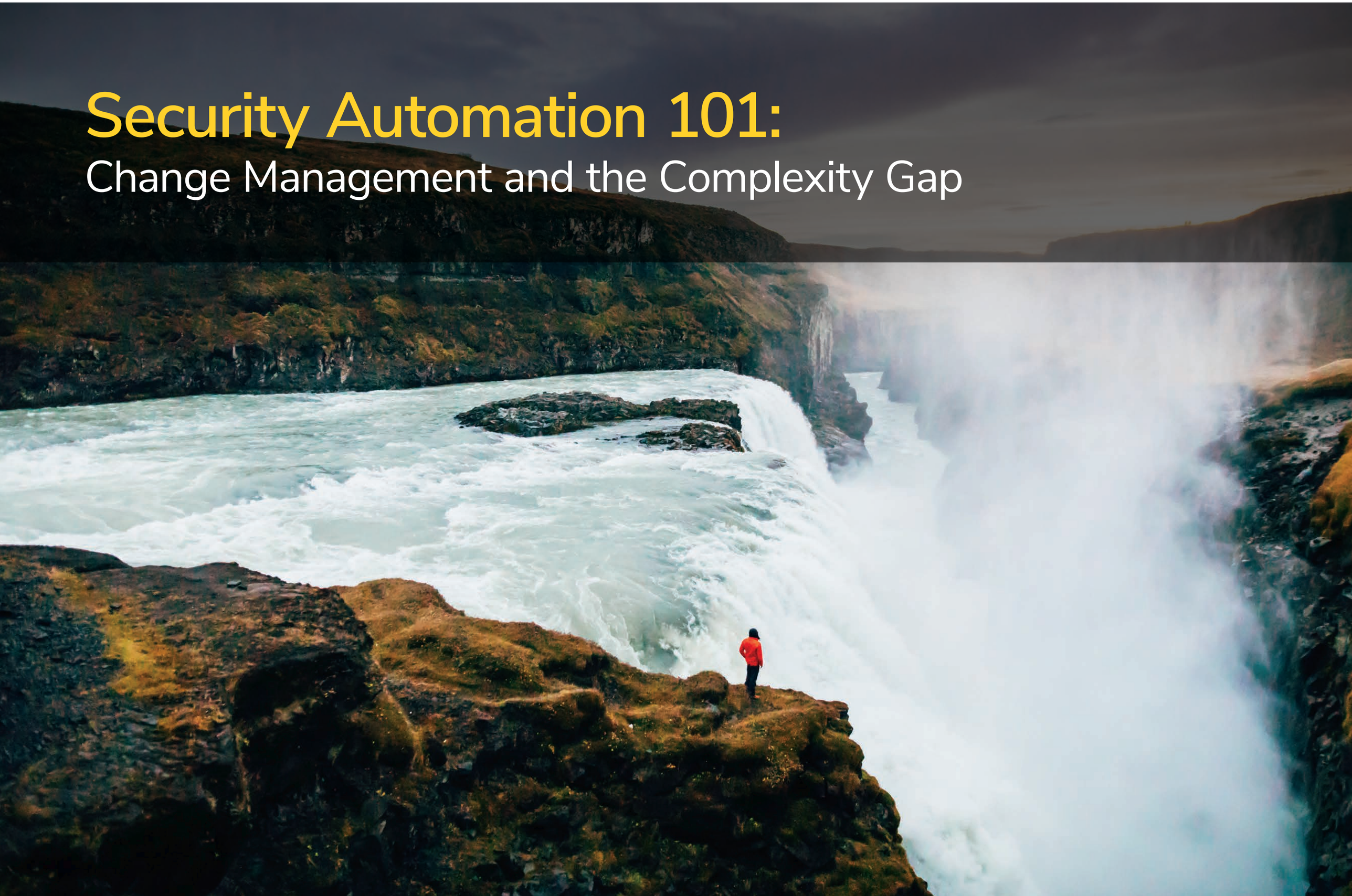
FIREMON

Security Automation 101:

Change Management and the Complexity Gap



The result is a complexity gap where emerging network and cloud technologies outpace security teams' ability to secure and manage their expanding enterprise perimeters.

Executive Summary

Today's threat landscape is constantly evolving. Sophisticated cyber threats are becoming smarter and faster, leading to an increase in security breaches and unprecedented fines for non-compliance. Simultaneously, organizations are rushing to embrace digital transformation, driven by emerging technologies like mobility, cloud computing, large-scale virtualization, software-defined networking, and the hyperconnected Internet of Things. Yet, organizations worldwide face an inability to hire and retain skilled security professionals, putting additional strain on lean security teams and increasing their security risk.

The result is a complexity gap where emerging network and cloud technologies outpace security teams' ability to secure and manage their expanding enterprise perimeters. Organizations find themselves at a crossroads – they must ensure that security doesn't slow down innovation and that innovation doesn't compromise security. Closing the complexity gap at scale requires automation of network security functions to replace manual, error-prone processes, maintain regulatory and internal compliance, and reduce overall security risk. This will increase the efficiency and efficacy of security teams, drive business innovation, and improve the bottom line.

This eBook describes how the complexity gap is impacting organizations and the pivotal role network security policy automation plays in helping organizations reduce risk and enhance their overall security posture.

The Bottom Line:

Automation of key network security functions will provide much needed consistency and control across hybrid network environments required to reduce the complexity gap. It will enhance compliance efforts, reduce risk, and improve productivity for time- and resource-strapped security teams. As a result, organizations can improve their overall security posture, meet regulatory and internal compliance requirements, and keep up with the growing demands of the business.

FIREMON

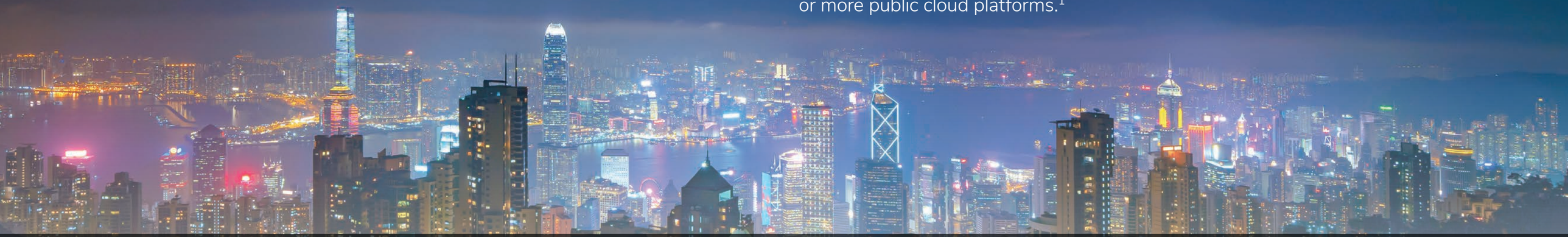
FAST FACTS:

- The rapid pace of digital transformation demands error-prone network security processes be automated.
- It is increasingly difficult to maintain consistent, continuous compliance of network security devices from multiple vendors and eliminate costly misconfigurations caused by human error.
- Security policy enforcement points are not only a vital part of the network security architecture, they are growing in criticality as networks expand in scope and complexity across multiple environments.
- An intelligent network security platform will provide the automation and analysis capabilities needed to tame network sprawl and enable security practitioners to make better-informed decisions based on context and actionable intelligence.
- Centralized management is essential in order to provide real-time visibility and control over the hybrid network and a central policy enforcement point.
- Advanced analytics and security intelligence capabilities will enable better decision making and help detect, prevent, and proactively respond to threats.

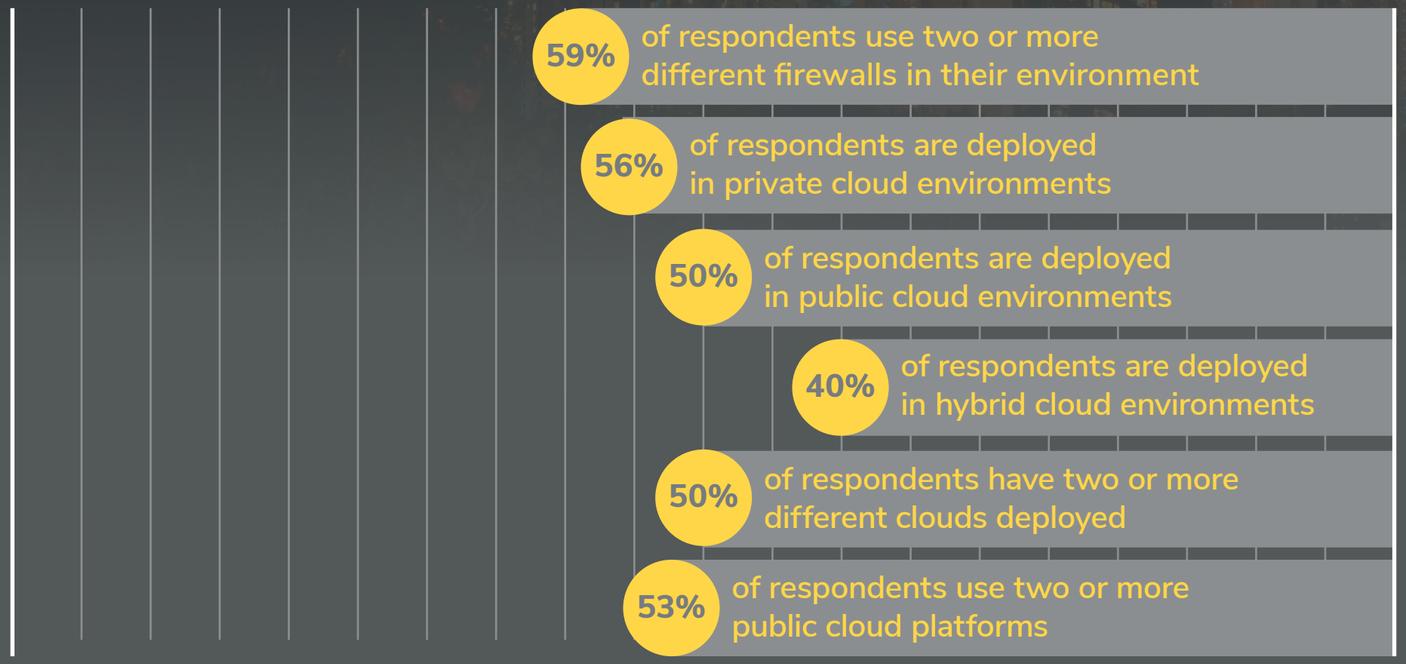
Technology sprawl adds to complexity

Hybrid networks have become increasingly complex, both in terms of the number of endpoints and technologies in use. The explosive growth in the number of mobile devices and the emergence of the Internet of Things (IoT) has massively accelerated endpoint proliferation. Cloud-based applications and services have also grown in popularity, driven by the flexibility, speed, and convenience they offer.

Because organizations tend to use multiple security vendors in a hybrid cloud environment, they may be unintentionally, or intentionally, adding to the complexity of managing and securing their networks. The FireMon 2019 State of Hybrid Cloud Security report showed that 59% of respondents use two or more different firewalls in their environment, with 67% of those using two or more firewalls also using two or more public cloud platforms.[1]



(FIGURE 1) NETWORK COMPLEXITY



Source: FireMon 2019 State of Hybrid Cloud Security Report

CLOUD ADOPTION OUTPACING SECURITY

of respondents say cloud business initiatives are accelerating faster than security teams' ability to secure them

Source: FireMon 2019 State of Hybrid Cloud Security Report

FIREMON

TECHNOLOGY SPRAWL INCREASES COMPLEXITY

- **1995** Stateful, packet inspection firewall is introduced. Most organizations deploy only a handful of devices at the perimeter.
- **2001** Impact of WAN, DMZs, and multiple ingress/egress points begins to increase device counts.
- **2005** Virtualization and mobility lead to erosion of the perimeter and proliferation of network segments.
- **2009** Virtualized infrastructure combined with PCI-DSS standards drives more network segmentation.
- **2016 and beyond** Enterprises operate hybrid infrastructures and security begins to adapt through methodologies including, but not limited to, microsegmentation and containerization.

Other technology trends that increase complexity include software-defined networking (SDN) and microsegmentation. SDN increases agility and flexibility, offering central automated provisioning and control that enables organizations to accommodate rapid changes in their network design. But SDNs lack a central policy enforcement point and can potentially broaden the attack surface . According to the FireMon 2018 State of the Firewall report, 41% of organizations are adopting an SDN solution[2]. Microsegmentation eliminates a “flat” network and brings software-defined security into a virtual environment where physical security devices would impact performance. The rise of the Internet of Things (IoT), Industrial Internet of Things (IIoT) and Operational Technology (OT) may be the reason for rising interest in microsegmentation, which enables organizations to separate insecure IoT devices from the rest of the network.

(FIGURE 2) TOP FIVE SECURITY TECHNOLOGIES BEING CONSIDERED OR IMPLEMENTED

Source: FireMon 2018 State of the Firewall Report (Respondents could select more than one technology)

77%

of organizations are still operating with only limited cybersecurity and resilience

Limited Visibility Equals Increased Complexity

Increasing complexity reduces visibility across and into hybrid networks, making threats more difficult to identify and contain. Organizations that use multiple security tools across their physical and cloud environments may find that they lack a holistic view of their network infrastructure, hindering threat hunting efforts as well as prioritization of remediations. According to EY, 77% of organizations are still operating with only limited cybersecurity and resilience. They may not even have a clear picture of what and where their most critical information and assets are — nor have adequate safeguards to protect these assets.[3]

Lack of network visibility is also problematic for organizations who cannot manage and patch devices that have not been detected. These unknown devices increase the probability of leak paths, which can cause corresponding policy or segmentation violations. Leak paths also include unauthorized or misconfigured internet connections from any part of an enterprise network—including the cloud—that allow traffic to be forwarded to a location on the internet. Leak paths can be especially hard to detect in cloud environments, where there is less network visibility and fewer security controls.

Shortage of Security Skills Delivers an Abundance of Complexity

Adding to the challenge of improving an organization's security posture is the lack of qualified security personnel. With many estimates as high as 3.5 million cybersecurity job openings by 2021[4], organizations will continue to see their security teams being asked to do more with less, with no relief in sight.

CONSEQUENCES OF COMPLEXITY

- Inability to integrate and orchestrate disparate security technologies across different environments
- Sluggish time-to-market for innovative line of business applications
- Lack of consistent policies and governance practices across the enterprise
- Inadequate endpoint visibility across hybrid environments
- Insufficient visibility of vulnerabilities across the hybrid enterprise
- Difficulty articulating the organization's security and vulnerability management strategies to senior management
- Decline in productivity and lack of training of IT security staff
- Lack of accountability for security practices

A cooperative research project by ESG and ISSA showed that one-third of survey respondents (as shown in Figure 3) believe that the global cybersecurity skills shortage has had a significant impact on their organizations, while 41% say the skills shortage has impacted their organizations somewhat. In addition, a three-year research trend clearly indicates organizations are not improving their ability to deal with the cybersecurity skills shortage.[5]

Increasing technology sprawl and the lack of availability of skilled personnel has created a complexity gap, as shown in Figure 4. The number of devices and associated rules has risen exponentially over the years, while the number of skilled staff has not.

(FIGURE 3) THE CYBERSECURITY SKILLS SHORTAGE IMPACT

67% say the skills shortage has increased the workload on existing staff

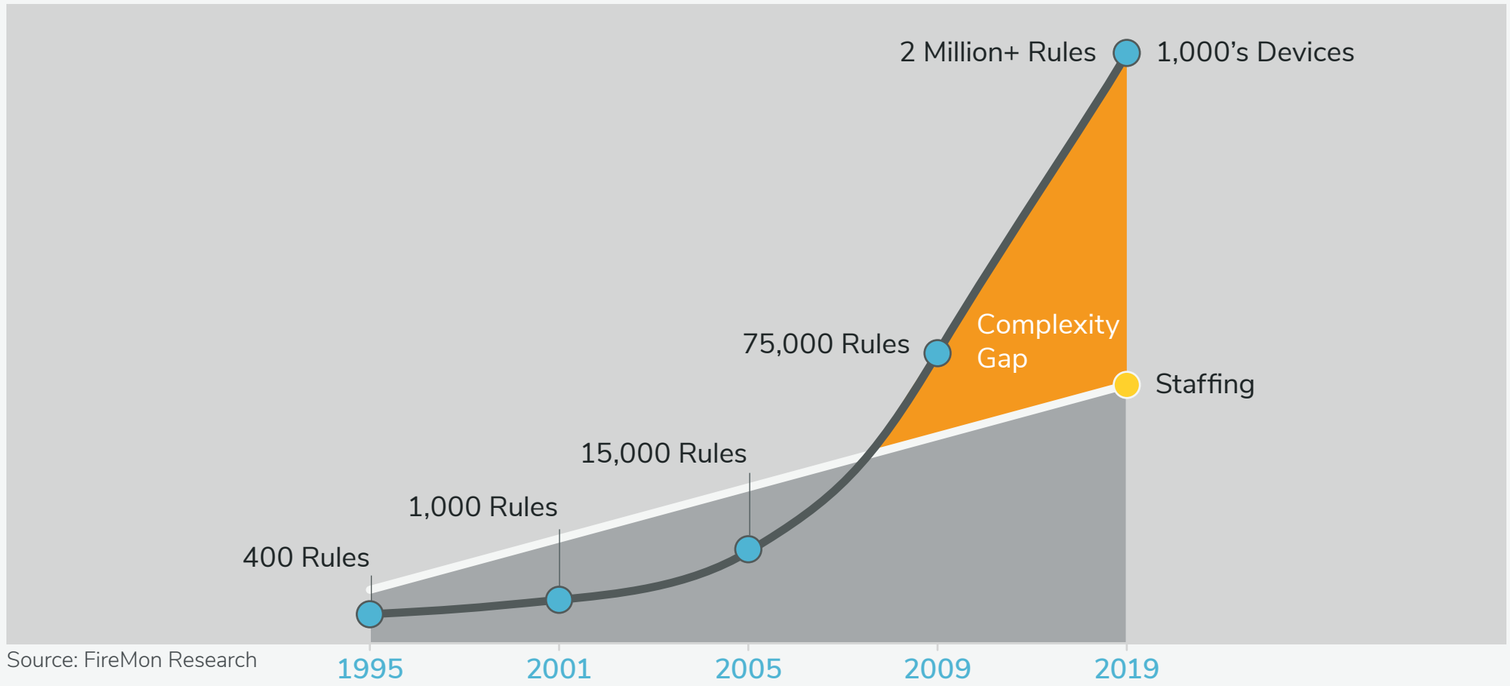
47% report an inability to fully learn or utilize some of their security technologies to their full potential

41% say that their organization has had to recruit and train junior personnel rather than hire more experienced infosec pros

40% claim that cybersecurity staff has limited time to work with business managers

Source: ESG/ISSA

(FIGURE 4) THE COMPLEXITY GAP



Source: FireMon Research

Automation is Essential

Given the growing complexity gap caused by all these factors, automation is essential. Manual processes are time-consuming and error-prone. Misconfigurations have become the main culprit in firewall and cloud breaches as understaffed security teams struggle with too many tools, lack of proper training, and policy complexity. According to FireMon's 2018 State of the Firewall Report, 64% of respondents still utilize manual change management processes despite high volumes of change requests. Some 38% of respondents report that more than 10% of their network changes require rework due to inaccuracies or issues on the network, mostly driven by human error.[6] Ultimately, the lack of automation can result in compliance violations, increased risk, and unplanned outages that can hinder business operations.

As the agility of cloud computing accelerates innovation for DevOps teams, it also increases an organization's potential threat surface. While the importance of security has driven some efforts to shift security left, many DevOps teams have had to sacrifice security for innovation. The 2019 DevSecOps Community Survey found that 48% of developers continue to believe security is important, but don't have enough time to spend on it.[7]

64%

of respondents still utilize manual change management processes despite high volumes of change requests

(FIGURE 5) HOW ORGANIZATIONS ARE UTILIZING AUTOMATION FOR CHANGE MANAGEMENT

39% Firewall change process is part of the IT change process, but rule engineering and pre-change assessments are done outside the IT change management system (tracked in documents, spreadsheets, etc.)

25% Change management process is ad hoc (email requests to firewall admins, spreadsheets, etc.)

22% Change management process, including rule engineering, pre-change assessments and approvals, is automated, but not the technical firewall change

12% Our change management process is fully automated, including automated firewall policy changes (policy push)

2% Other

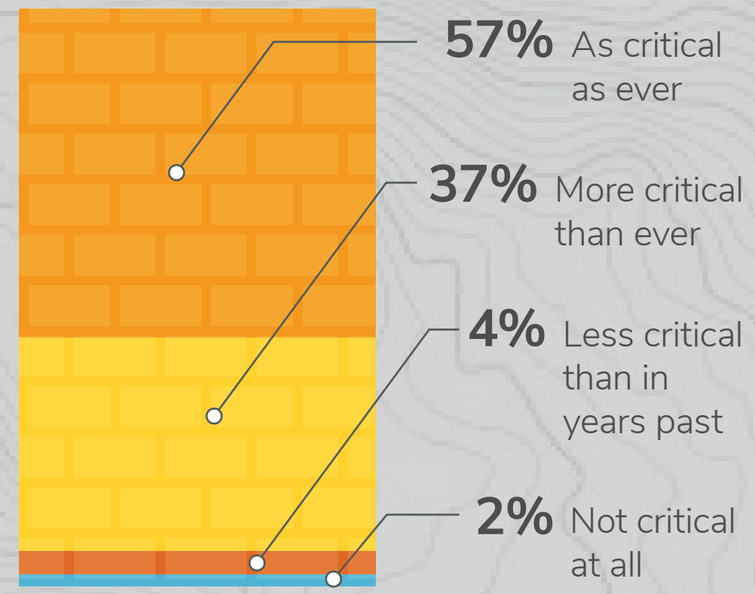
Source: FireMon 2018 State of the Firewall Survey

Network security devices such as firewalls must be able to manage continuous churn and change quickly as new users, applications and devices are granted access. Additionally, they must be able to quickly revoke access as business needs change. Access rights that remain in effect when no longer needed present a significant security risk to the organization.

A major problem in managing firewall deployments, especially on a large scale and across hybrid and cloud environments, is achieving visibility into policies that govern rule sets. Lack of comprehensive visibility makes it difficult to identify rules that are redundant, hidden, shadowed, outdated, or overly permissive.

One of the biggest issues organizations face with firewall change management is handling complexity[8], as shown in Figure 7. At their very core, firewalls filter incoming and outgoing traffic based on a set of user-defined rules. If a firewall is misconfigured, the results can be as catastrophic as not having a firewall at all. Multiply that misconfiguration by the number of disparate firewall devices on premises and in the cloud, and the lack of automated processes, resource-strapped security teams are in for a never-ending battle.

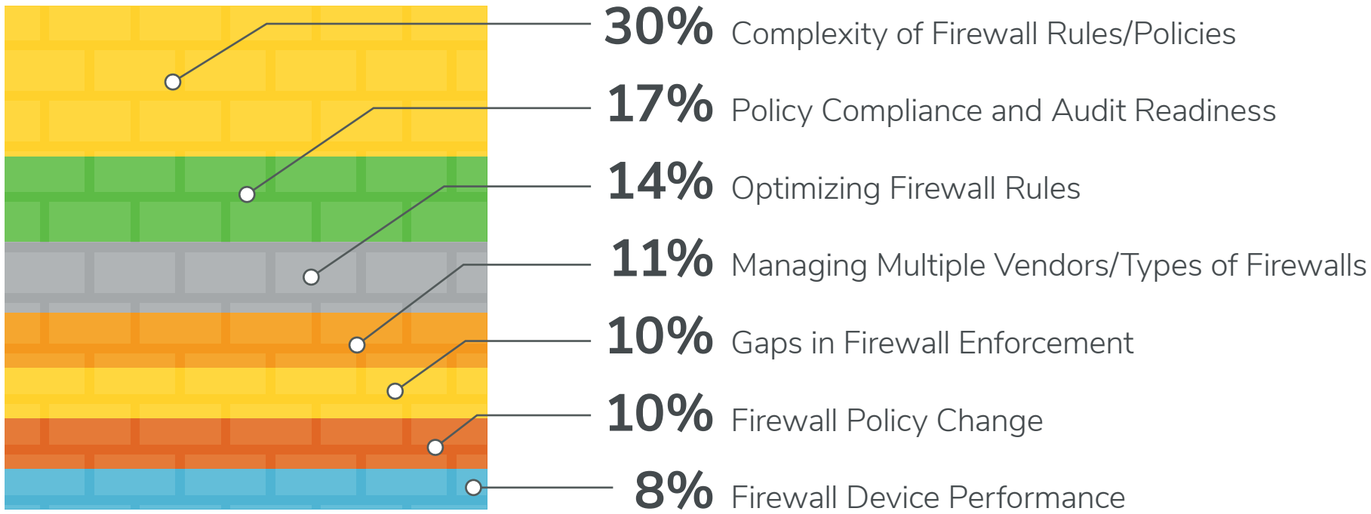
(FIGURE 6) CRITICALITY OF NETWORK FIREWALLS



Source: FireMon 2018 State of the Firewall Report

In addition, as shown in Figure 4 “The Complexity Gap,” not only has the number of devices in use expanded over the years, but the number of rules governing their configuration has skyrocketed. In 2019, a large enterprise may see upwards of two million rules in use, up from just some 400 when firewalls came into regular use in the mid-1990s.

(FIGURE 7) MOST PROBLEMATIC FIREWALL CHANGES



Source: FireMon 2018 State of the Firewall Report

Requirements of Automated Network Security Policy Management

Maintaining a robust security posture is necessary to protect the hybrid network environment from security threats and incidents; achieve audit and compliance requirements; and set the foundation for enabling innovation without compromising security. By automating network security policy management, organizations can reduce security errors, standardize workflows, and make security an enabler to achieve their business objectives.

A primary requirement of an automated network security policy management platform is real-time and comprehensive visibility across the entire network infrastructure, including on premise, private cloud, and public cloud. Centralized management through a single pane of glass must provide the visibility needed into the rules associated with network security devices to determine the state of an organization's current configuration, evaluate the effectiveness of security policies, and scope the impact of any proposed policy changes on an organization's compliance and security posture. Advanced analytics capabilities help security teams plan and monitor the effectiveness of security policies.

An automated network security policy management platform will provide a centralized point to determine which policies can be enforced to eliminate unnecessary access and security risk. Through comprehensive rule analysis and automated workflows, organizations can remove technical mistakes and misconfigurations, remove unused access, review and refine access to optimize the performance of network devices, reduce policy complexity, and enhance security posture.

Another requirement of an automated network security policy management platform is the flexibility to scale automation to an organization's specific requirements. Robust, open application programming interfaces (APIs) will accommodate an organization's changing infrastructure and security demands and incorporate the critical information necessary to perform conclusive analysis of network security devices, policies and underlying risks.

BENEFITS OF AUTOMATED NETWORK SECURITY POLICY MANAGEMENT

- Gain visibility into all assets across on-premise and cloud environments
- Orchestrate security tools across the entire hybrid network
- Monitor and integrate multi-vendor, hybrid networks from a single pane of glass
- Clean up outdated, unnecessary, and non-compliant policies
- Automate policy change management
- Maintain continuous compliance
- Facilitate the migration or onboarding of new network security devices
- Manage vulnerability and risk
- Improve change management SLAs
- Incorporate automated security controls into CI/CD pipeline
- Improve workload portability

FIREMON

Summary

As organizations leverage technologies like cloud computing, virtualization, software-defined networking, and the hyperconnected Internet of Things (IoT), they are also dealing with an inability to hire and retain skilled security professionals. This results in a complexity gap where digital transformation is moving faster than the ability of security teams to secure and manage it.

To overcome the complexity gap, automation is essential. Deploying a network security policy management platform that automates manual functions will reduce misconfiguration errors and risk exposure and enable greater productivity for resource-strapped security teams. With automation, organizations can meet and maintain their compliance requirements, strengthen their security posture, and keep up with the growing demands of their business.

[1]FireMon, LLC. “State of Hybrid Cloud Security: 2019.” February 26, 2019.

[2]FireMon, LLC. “2018 State of the Firewall.” August 2018.

[3]EY. “EY Global Information Security Survey 2018-2019.” October 10, 2018.

[4]Cybersecurity Ventures and Herjavec Group. “Cybersecurity Jobs Report 2017 Edition.” May 31, 2017.

[5]ESG and ISSA. “The Life and Times of Cybersecurity Professionals 2018.” April 2019.

[6]FireMon, LLC. “2018 State of the Firewall.” August 2018.

[7]Sonatype. “DevSecOps Community Survey 2019.” March 4, 2019.

[8]FireMon, LLC. “2018 State of the Firewall.” August 2018.

FIREMON

ABOUT FIREMON

FireMon is the #1 security automation solution for hybrid cloud enterprises. FireMon delivers persistent network security for multi-cloud environments through a powerful fusion of real-time asset visibility, compliance and automation. 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.