Overcoming the complexity gap

...the role of automation in optimising network performance and security

author • **Fran Howarth**

Executive summary

The world of network security is changing rapidly. Ever more sophisticated threats are leading to an increase in security breaches and are creating a greater sense of vulnerability among organisations of all sizes and in all industrial sectors. At the same time, technology developments are being made at a dizzying pace, changing the network environment considerably. These include the rise of mobility and cloud computing, large-scale virtualisation, the advent of software-defined networking, the rise of microsegmentation of networks and the hyperconnected work of the Internet of Things. Yet, organisations are facing an inability to hire and retain skilled security professionals on a worldwide basis, meaning that resources are increasingly stretched.

This is creating a complexity gap where technology advances are moving much faster than the ability of security personnel to keep up and manage them. Closing the gap requires automation of network security functions to replace inefficient, error-prone processes with automated intelligence and guidance. This will increase the productivity and efficiency of skilled security teams and free them up to perform higher value tasks. Automation cannot only provide cost savings, through reduced staff and service costs, but can help to reduce the overall risks that organisations face.

This document describes how the complexity gap has come about and how it is impacting organisations. It then describes how automation of network security functions will aid organisations in reducing risk and the technology components that are required for doing so.

Fast facts

- The fast pace of technology change demands that error-prone processes involved in network security be automated.
- Firewalls are not only a critical part of the network security architecture, but are growing in criticality as networks expand in scope and complexity.
- It is particularly problematic to manage network systems such as firewalls, owing to the need to keep configurations in the desired state, which requires tweaking of rules on a regular basis to ensure that they are maintained in line with policy.
- An intelligent network security platform will provide the automation and analysis capabilities needed to tame the sprawl and enable security practitioners to make better informed decisions based on context and actionable intelligence.
- Centralised management is essential for such a platform in order to provide visibility and control over the network and to provide a central policy enforcement point.
- The platform should provide advanced analytics and security intelligence capabilities to enable better decision making and to help in the ability to prevent, detect and proactively respond to threats.

The bottom line

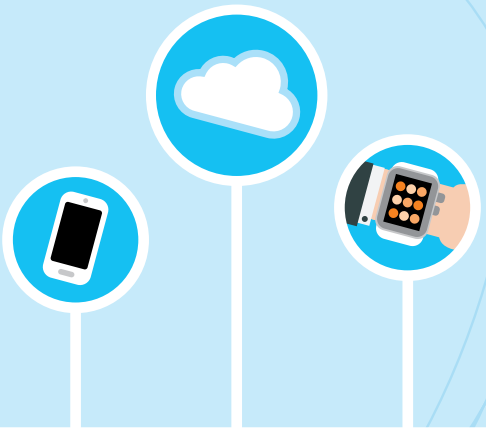
Intelligent automation of network security functions will provide the visibility and control across network devices and functions, covering both internal and external networks, that is required for reducing the complexity gap. It will help considerably to cut the number of breaches and attacks experienced and will improve productivity for time-strapped security teams. As a result, organisations will find that their security posture and their ability to meet compliance objectives is improved considerably.

Technology sprawl adds to complexity

No organisation can afford to be complacent. Every organisation, no matter its size, purpose or line of business can be seen as a viable target for external adversaries and internal threats are no less of a problem. Crowd Research Partners recently found that just 3% of organisations believe that they are not vulnerable to threats emanating from inside their network.

According to research from *451 Research* undertaken in 2017, **68%** of respondents had experienced a data breach in the past year, an increase of **7%** over the previous year's survey. As a result, almost three-quarters are planning to increase their data security budget, up from **54%** in 2015. With security breaches continuing to rise, **88%** report that they feel vulnerable to security threats, with almost one-third reporting feeling very or extremely vulnerable.

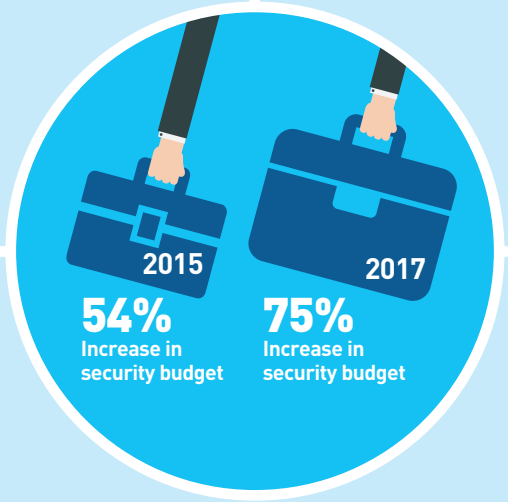
Networks are also becoming increasingly complex, both in terms of the number of touchpoints and the array of technologies that they contain. The network of today is vastly different and more complex than it was 10 years ago.



Endpoints have proliferated in recent years given explosive growth in the number of mobile devices in use, many of which have exceptionally powerful capabilities. Such devices, including those personally owned by users, are increasingly used to access corporate applications and data. Cloud-based applications and services have spiralled in popularity, driven by the flexibility and convenience that they offer. According to *RightScale*, **89%** of organisations are using cloud services in 2017, the majority of which are using multiple clouds. Virtualisation has been a driver behind the rapid growth of cloud, but growth is low owing to the maturity of this market. *Gartner* estimates that organisations have virtualised **75%** of their data centre, rising to **90%** in some cases.

Number of respondents increasing data security budget in 2017

Source: 451 Research



Other technology trends that are contributing to increasing complexity include software-defined networking (SDN) and microsegmentation. The use of SDN brings many advantages, including increased agility and flexibility, central automated provisioning and control, enabling organisations to keep up with the pace of change being seen in networks. According to a recent study from ***FireMon***, **67%** of organisations are adopting an SDN solution. Microsegmentation of networks is also being increasingly seen, made possible by virtualisation. It improves network performance and makes it easier to reduce complexity in SDN where workloads fluctuate. According to FireMon, the rise of the Internet of Things (IoT) may be a key reason behind rising interest in microsegmentation, enabling organisations to cut insecure IoT devices off from the rest of the network to prevent problems that they could cause.

Technology sprawl and complexity

Technology sprawl causing complexity to rise

1995 Introduction of stateful, packet inspection firewall. Most organisations 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 Virtualisation and mobility lead to erosion of the perimeter and proliferation of network segments.

2009 Virtualised infrastructure combined with PCI standards drives more network segmentation.

2016 & beyond Enterprises operate hybrid infrastructures and security begins to adapt through micro-segmentation and asset-centric management.

Source: FireMon

All these factors have caused network complexity to rise exponentially (***See Figure 1***). But there is more to come. For example, ***IDC*** estimates that the use of SDN technologies is currently growing at a cumulative average rate of **54%** annually, at least until 2020. Technology is developing so fast that the network will likely look very different in three to five years time than it does today. Complexity needs to be contained.

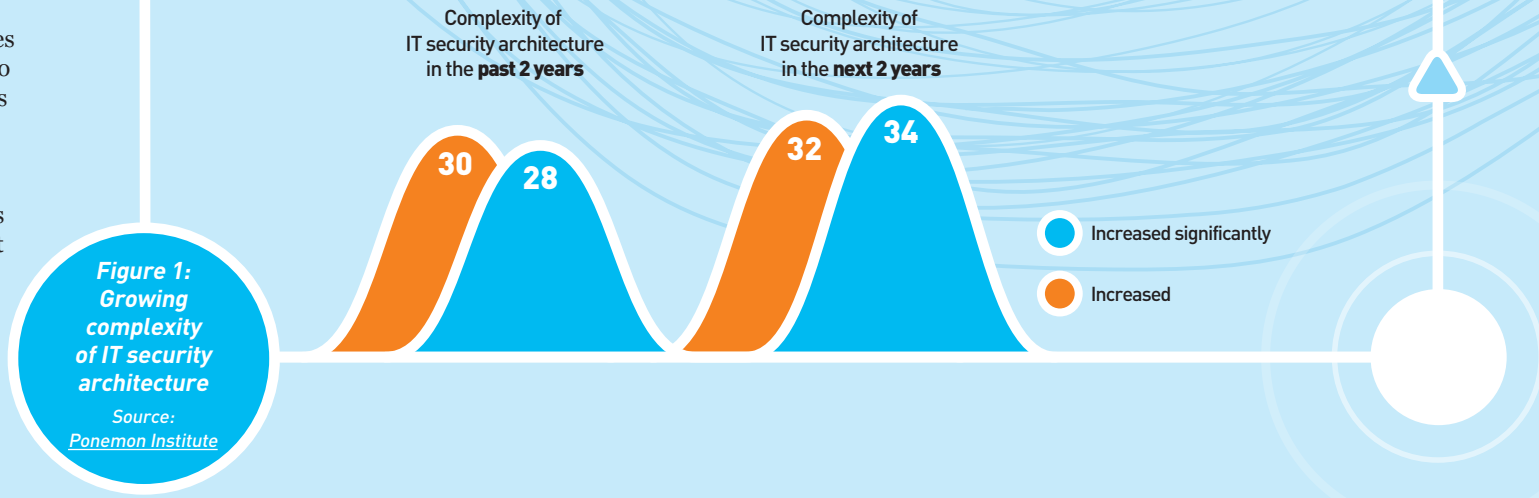


Figure 1: Growing complexity of IT security architecture

Source: Ponemon Institute

If complexity cannot be contained, security risks will multiply (see ***Figure 2***). One of the greatest problems is that complexity reduces visibility into what is happening on the network, making threats harder to identify and contain. Some of the main consequences of security are outlined in the text box "Consequences of complexity."

One factor often cited in the fight to improve an organisation's security posture is the inability to hire qualified and experienced security personnel (see ***Figure 3***). Estimates of the shortage vary. Frost & Sullivan estimates that there will be a shortage of **1.8 million** information security workers by 2022.

Consequences of complexity

- Inability to integrate security technologies across different platforms.
- Inability to ensure policies and governance practices are applied consistently across the enterprise.
- Too many active endpoints.
- Poor investments in overly complex security policies that are difficult to operate and financial loss due to scrapping of these complex technologies.
- Inability to see vulnerabilities in the system.
- Difficulty in communicating the organisation's security strategy and approach to deal with cyber threats to senior management.
- Decline in productivity of IT security staff due to complexity. Lack of accountability for security practices.

Source: Ponemon Institute

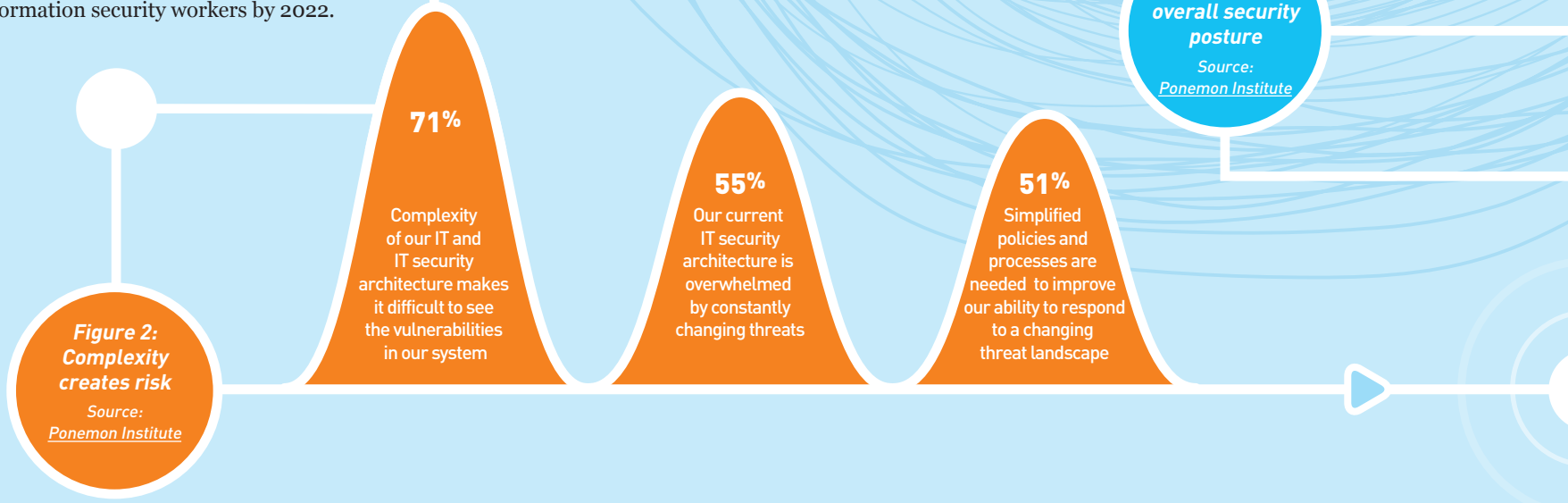


Figure 2: Complexity creates risk
Source: Ponemon Institute

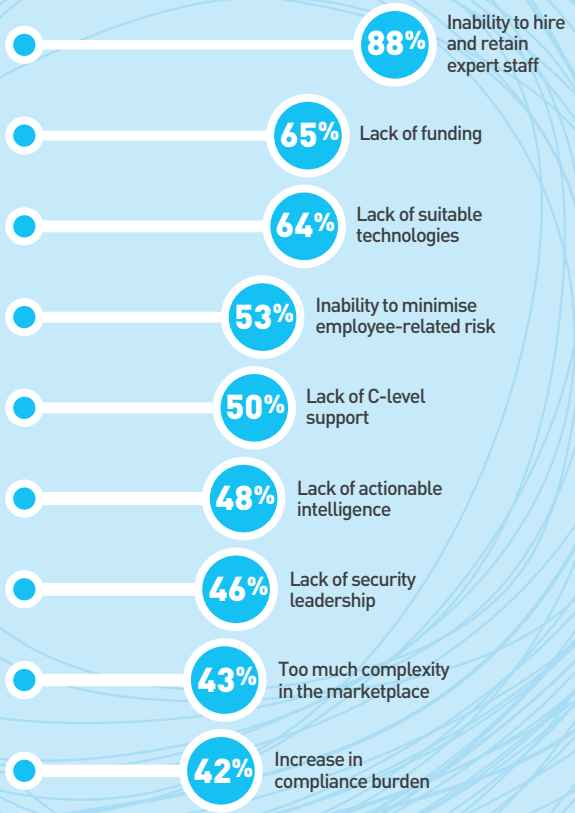


Figure 3: What decreases overall security posture
Source: Ponemon Institute

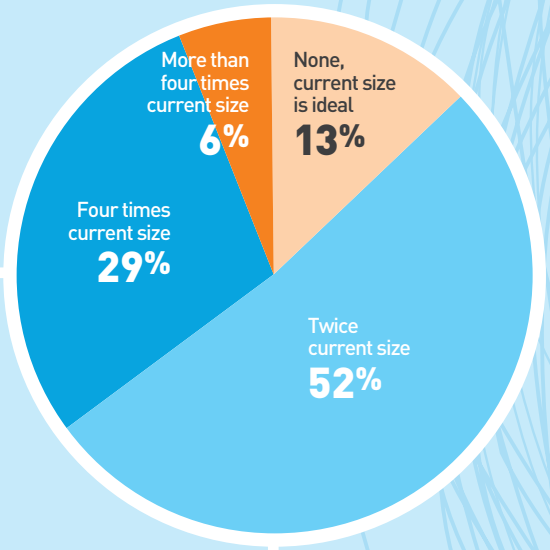


Figure 4: Ideal staffing levels

Source: Trustwave

As shown in ***Figure 4***, this shortage is being felt by multiple organisations, with a full **87%** indicating that they want to hire additional security staff.

The result of increasing technology sprawl and the lack of availability of skilled personnel has created a complexity gap, as shown in ***Figure 5***. That figure depicts how the number of devices and the rules that are in place to govern them has risen exponentially over the years but the growth in the number of skilled staff shows just a gently incline.

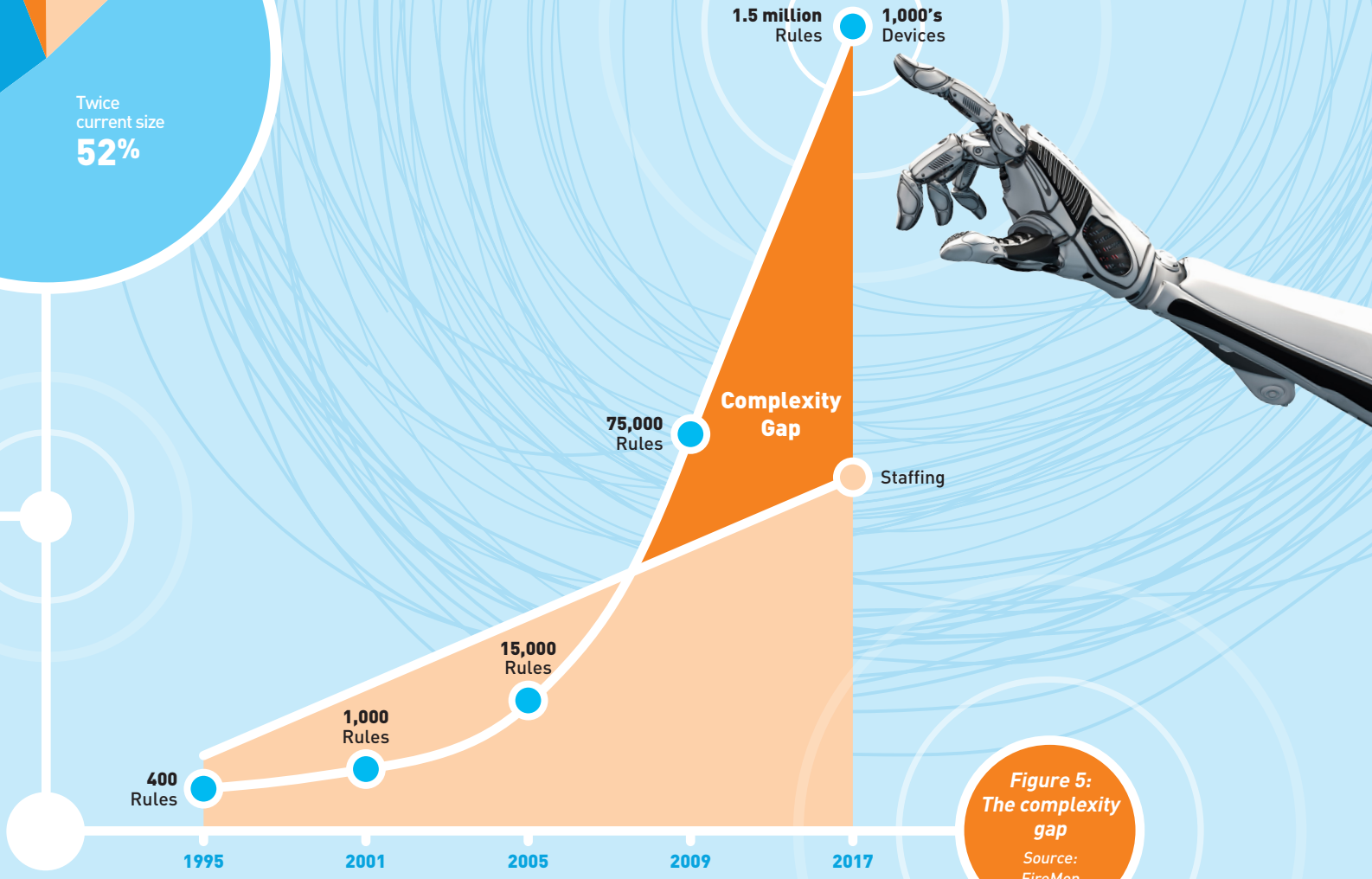


Figure 5: The complexity gap

Source: FireMon

Automation is essential

Given the growing complexity gap caused by all these factors, automation is essential. Manual processes are not only time-consuming to wade through, but are error-prone. IDC recently undertook research to gauge how far organisations are on the journey towards optimisation and transformation of their IT infrastructure through automation, as shown in *Figure 6*. Whilst automation enables gains in productivity and agility, improvements in efficiency, reduced risk and cost savings, just 20% of respondents were fully automated across the infrastructure, resulting in performance, efficiency and cost savings not being maximised, as well as providing metrics for assisting in continuous improvement.

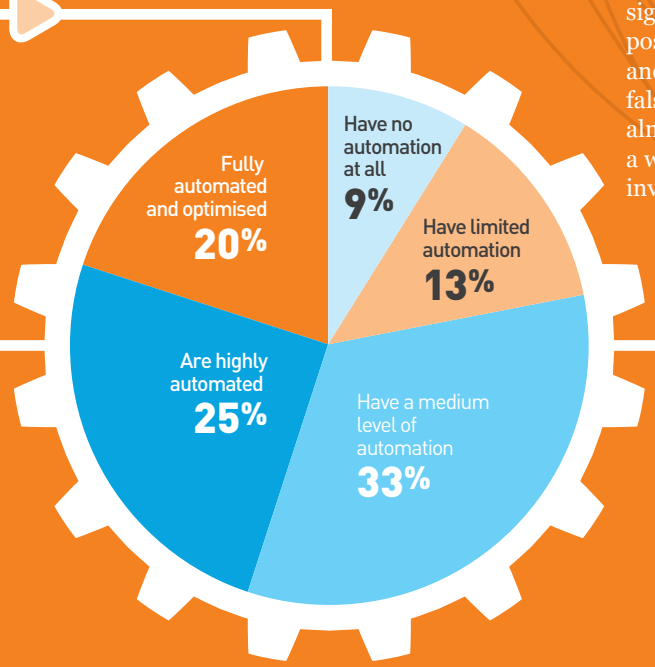


Figure 6: Automation for optimising IT operations
Source: IDC

Effective automation is essential for achieving high levels of security in the network, for increasing security team efficiency and for boosting the ability to prevent security incidents. In its research, IDC found that achieving a high degree of automation enables each staff member to manage up to two-and-a-half times as many network devices as with manual methods, and **15%** more servers.

Yet, many have yet to achieve effective automation. According to research from ***Light Cyber***, half of all time spent by security personnel is wasted through security inefficiency. It found that **68%** spend a significant amount of time dealing with false positive alerts generated by security devices and just **13%** rate their ability to minimise false positives as high. With an average of almost **17,000 false positives** being seen on a weekly basis, it found that just **4%** can be investigated by security personnel.

Firewalls are an essential part of network security, monitoring traffic and access events across the network, including elements that link internal and external networks. They sit at the heart of any network, as well as having expanded up the stack to applications. The number of firewalls continues to expand, driven by factors such as SDN, greater network segmentation and the proliferation of virtual appliances in the cloud. According to ***Aberdeen***, almost half of organisations are faced with the complexity of managing firewalls from multiple vendors across multiple sites. Any organisation can find itself managing multiple firewalls, but a large multinational can be faced with managing thousands or even tens of thousands of firewalls. As shown in ***Figure 7***, firewalls are not only retaining their criticality for organisations, but that criticality is set to increase.

Network devices such as firewalls must quickly be able to manage continuous churn and change as new users, applications and devices are granted access and need to have access rights revoked as needs change. Access rights that are not revoked when no longer need present a significant security risk.

A major problem in managing firewall deployments, especially on a large scale, is achieving visibility into policies that govern rule sets that are put in place. This makes it difficult to identify rules that are redundant, hidden, shadowed, outdated or overly permissive in terms of the access they allow. It is estimated that up to **50% of firewall rules are redundant**.

One of the biggest problems organisations face in firewall management is handling complexity, as shown in ***Figure 8***. The report from which this data is taken from breaks out optimising firewall rules and managing multiple vendors/ types of firewalls for the first time. In previous reports, these were lumped under complexity. When taken together, complexity is seen as far and away the greatest challenge.

Firewall rules are used to verify network traffic according to policy. If a firewall is not configured correctly so that rules adequately reflect policy, the network and the organisation will not be adequately protected. According to ***Gartner***, **99%** of firewall breaches will be caused by misconfigurations, not flaws, through 2020.

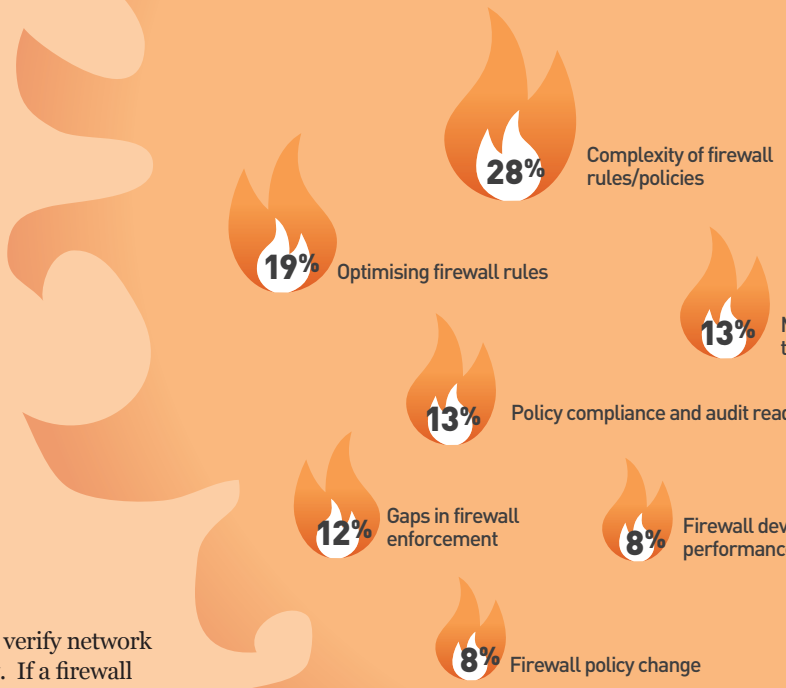


Figure 8: Most problematic firewall challenges
Source: FireMon

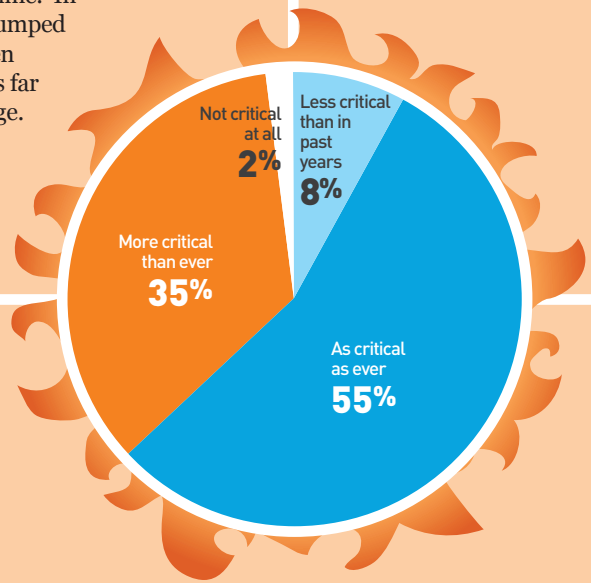


Figure 7: Criticality of network firewalls
Source: FireMon

However, as shown in ***Figure 5*** "The complexity gap," (see page 6), not only has the number of devices in use expanded over the years, but the number of rules governing how they are configured has skyrocketed. In 2017, a large enterprise may see an estimated **1.5 million** rules in use, up from just some **400** when firewalls came into regular use in the mid-1990s.

Requirements of automated network security management technologies

Maintaining a robust security posture is necessary for guarding against security threats and incidents, and for achieving audit and compliance objectives. By automating network security management, those needs are easier to achieve than through traditional staff-intensive methods. *Gartner* estimates that more than 95% of breaches can be prevented through better management of network technologies. Among its recommendations are to remove unused firewall rules, ensure that systems are adequately patched in a timely manner and remove unnecessary administrator rights.

A main requirement is that of a common platform that provides visibility across the entire network infrastructure, both on premise and in the cloud, and the devices that are necessary for keeping it in good running order. That platform should provide centralised capabilities for threat prevention, detection and response. Centralised management will provide a single pane of glass across the myriad of technologies making up the network security environment, enabling more holistic management. This will provide the visibility that is needed into the rules associated with devices such as firewalls so that organisations will be able to gauge the effectiveness of their security policies. It will reduce complexity by automating change management requirements by letting machines take some of the decisions. The platform should contain advanced analytics capabilities to help personnel to plan and monitor the effectiveness of security policies.

The security management platform will provide a centralised point through which policies related to rules and changes to workflow automation can be enforced. It should also enable policies to be optimised through the intelligence gained through the advanced analytics capabilities regarding events that have been monitored across network devices. The platform should also provide the intelligence to proactively hunt for threats and the tools, techniques and procedures used by attackers that are indicative of threats through explorative data analysis, based on context and hypotheses in real time to enable more effective decision making. This will help to ensure that only legitimate alerts are flagged for action.

A prime consideration is that the platform be able to integrate data feeds from a variety of sources, which are automatically analysed to provide the context needed to take better informed decisions regarding changes that need to be made. It will need to provide security practitioners with a clear understanding of what controls are in place, the vulnerabilities that the network faces and the main threat vectors. This requires that it is capable of continuous monitoring and vulnerability mapping, which are essential for identifying issues that matter and reducing the noise from false positives that plague many security implementations. It will help to plan and monitor security policies intended to prevent breaches and to remediate threats identified by security alerts.

Benefits of a security management platform

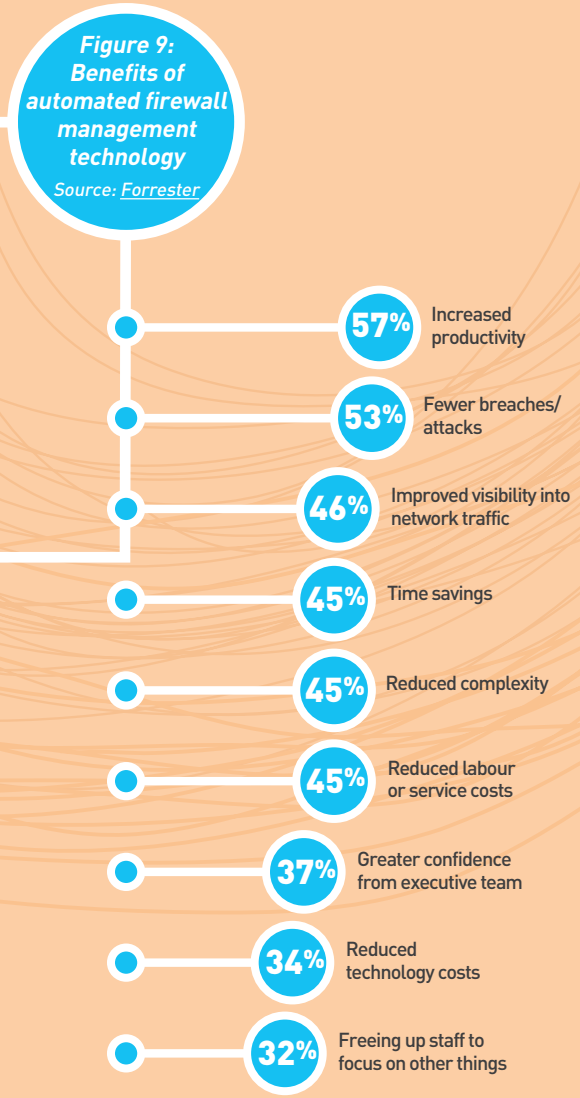
The use of a security management platform include providing visibility across the network infrastructure to guide automated actions and inform security personnel with the actionable intelligence that they need to take action. This will help considerably in cutting through the complexity involved in large-scale, heterogeneous network environments that span both internal and external networks.

It will provide the security intelligence that is required for making better decision making, automating tasks where possible and informing security personnel of suitable actions to take in a proactive manner. This will help greatly in managing vulnerabilities and risks in the network environment and in achieving security and compliance objectives. The prime benefits of using such a platform are shown in ***Figure 9*** and in the text box "The benefits of advanced automation and analysis."

Benefits of advanced automation and analysis

- Monitoring multi-vendor networks from one place.
- Cleaning up outdated, unnecessary of non-compliant policies.
- Automating policy change management.
- Reporting on compliance and preparing for audits.
- Migrating or upgrading security devices.
- Managing vulnerability and risk related to network access.
- Quickly triaging security alerts for response.
- Proactively hunting for threats in the network.

Source: Firemon



Closing summary

The growing sophistication and pace of technology is creating challenges for security personnel-strapped organisations to keep up in the light of ever more determined and better resourced adversaries.

Those technology advances include the rise in mobility and cloud computing, expanding use of virtualisation, the move to software-defined networking and microsegmentation, and the Internet of Things. This is creating a complexity gap that only looks set to get worse. Networks today look vastly different to those of just five years ago and a further sea change will be seen in the coming three to five years.

To overcome that gap, automation is essential. Deploying a network security management that automates manual functions will reduce errors and risk exposure, and enable greater productivity without the need to hire large numbers of scarce security professionals. It will vastly help in improving overall security postures and will help organisations to realise their governance and compliance objectives.

20–22 Wenlock Road
LONDON N1 7GU
United Kingdom

Tel: **+44 (0)207 043 9750**
Web: **www.BloorResearch.com**
Email: **info@BloorResearch.com**