The State of Network Security 2013: Attitudes and Opinions
An AlgoSec Survey
Executive Summary

A survey of 179 network, security and risk and compliance professionals finds that the pace of adoption of next-generation firewalls (NGFWs) has accelerated markedly in the last year. Whether using NGFWs or traditional firewalls, organizations face increasing operational and security challenges. The most significant of these challenges come from internal sources— the need for business agility and the accidental or malicious behavior of employees.

- **Change management poses greatest challenge.**
  Three-fifths of respondents noted that poor processes and visibility create significant risk in managing network devices.
  - Those risks have become real problems for many organizations—four out of five experienced network or application outages as a result of out-of-process changes, a nearly 40% increase from last year.
  - An equal number have suffered outages or impaired performance from application-related rule changes. IT departments are caught between the need to respond to business imperatives and the risk of running afoul of complex rules and bringing down their systems.

- **Adoption of next-generation firewalls up sharply; increasing work for most organizations.** The number of respondents using NGFWs rose 40% from last year, with most still motivated by improved security. While the number of respondents reporting that next-gen firewalls increased their workload declined from last year, most said the new firewalls created more work. Even as organizations centralize their firewall management, time spent managing policies and making changes continues to tax IT departments as complexity rises.

- **Insider damage dwarfs outside threats.** Two-thirds of respondents rated the threat from within—whether from accidental data leakage or malicious employees—as the greatest risk to security. The same proportion expressed concern that allowing employees to “bring your own device” increased the risk of security breaches. Policies and processes that focus on intrusion and other external threats fail to address the biggest risks facing most organizations—employee errors and malice, non-corporate devices, poor visibility and manual processes.

- **Future of cloud security remains hazy.** Less than 20% of respondents said that the majority of their organization’s security controls were in the cloud. And, the larger the organization, the less likely it was to have cloud-based security. The cloud is out there, but most organizations remain reluctant to count on it for security.

**About the Survey**

The “State of Network Security 2013” survey was conducted to analyze security risks and operational challenges, and gauge the effects that next-generation firewalls are having upon IT security professionals' workload.

179 respondents completed the survey, which was targeted to members of Network Operations departments (28.7% of respondents), Security Operations departments (50.6% of respondents) and Risk and Compliance departments (20.8% of respondents). There were no statistically significant differences in the responses from these three groups.

The survey was administered on the show floor at RSA Conference 2013 US, held at the Moscone Center in San Francisco, CA from February 25-28, 2013.
IT Security, Network Operations and Risk and Compliance teams struggle to balance the out-of-process changes undertaken to maintain business agility and the control needed to ensure system security and stability using their current processes. At the same time, poor visibility and complex rules continue to expose organizations to the risk of outages and security breaches, often caused by their own employees and processes. Even those that have adopted NGFWs and centralized policy management find that the increased security still comes at the price of more changes, more policies, and more complexity.

Managing Changes: The Process Is the Problem

Outages and security breaches represent major problems and when it comes to managing network security devices, the greatest challenge is poor process. According to 60% of respondents, time-consuming, manual processes, lack of visibility into policies, and poor change management, are the real challenges to effectively managing network security devices (Figure 1).

Drilling down further into this issue, increasingly complex applications and growing demands for business agility make ad hoc or manual changes riskier than ever.

Out-of-process changes caused more problems for IT departments this year than in 2012. Last year, 54.5% attributed system outages to these changes, whereas this year 76.1% said that they caused application or network outages, a 39% increase (Figure 2).
Outages were the dominant issue associated with out-of-process changes; they occurred three times more often than data breaches and five times more frequently than audit failures. Overall, the percentage of respondents who did not experience an event remained stable at about 25%, but the total number of negative events reported rose.

Application-related rule changes create similar trouble for organizations (Figure 3) with 80% saying they have experienced outages or impaired performance as a result. Application-related rule changes bring down applications about as frequently as out-of-process changes (30.7% versus 32.5%) and cause system outages for about 30% of respondents. More alarmingly, application rule changes caused 20% more security breaches than out-of-process changes, impairing security for 26.4% of respondents.
Next-Generation Now Dominates

Next-generation firewalls (NGFWs) are clearly gaining acceptance. The number of respondents who have adopted NGFWs reached nearly 57% in 2013, up from 41.2% in 2012 (Figure 4).

Of those who have adopted NGFWs, a majority, 56.5%, report that their objective is to improve protection from attacks. Other reasons for adopting NGFWs are significantly less popular; ranking second is reducing IT spend at only 39.1%, and gaining more control over access to external applications at 30.4%.

It is no surprise that with concern about attacks dominating the reasons for adopting NGFWs, over half of users, 53.8%, turn on intrusion protection systems (IPS). When asked what NGFW features they use, the top three are IPS, application control (44.1%), and URL filtering (41.9%).

In exchange for the increased security of NGFWs, IT professionals often must work harder (Figure 5). The majority of respondents (56%) that had adopted NGFWs said they added more work to the firewall management process, down from 76% last year.

![Figure 4: Adoption of Next-Gen Firewalls](image)

![Figure 5: Have Next-Gen Firewalls added more work to your firewall management processes?](image)
Interestingly, even with the 80% increase in organizations that have centralized their firewall management processes, from 24% of respondents in 2012 to more than 44% in the current survey, nearly half (46%) of respondents report they must make more changes and more than half say they spend more time managing policies.

As organizations mature in their experience with NGFWs, the amount of work associated with them will gradually decline. The complexity of these systems, however, will likely mean additional work for many organizations for several years to come.

Still, change management issues plague organizations with NGFWs; one-third consider them to be their biggest challenge with next-gen firewalls (Figure 6).

Little wonder: when asked how the number of changes to NGFWs compares to the number of changes on traditional firewalls, 46.7% stated that they make more changes, with 28.9% making greater than 20% more changes. Only 21.2% make fewer changes, and 32.2% make about the same number of changes.

Many organizations continue to experience a disconnect between their goals and reality with NGFWs. Although nearly 40% of NGFW-users said that reducing IT spend was a motivating factor in implementing the next-gen firewall, the majority of respondents find that NGFWs require more work—and therefore more costs—to manage processes and changes. While the trend is positive, more organizations need to centralize and automate their processes to see the hoped for cost reduction along with improved security.
The Greatest Risk? Employees

While much of the focus of IT Security, Network Operations and Risk and Compliance teams is on external threats, like last year, this year’s respondents were most worried about internal perils (Figure 7).

Employees accidentally jeopardizing security through data leaks or similar errors ranked as the greatest concern for 40.5% of this year’s survey respondents. Malicious insider threats ranked second, with nearly a quarter of respondents listing it as their greatest risk. In light of the recent Matthew Keyes case, organizations may be keenly aware how easily trusted employees with access can become hackers with an agenda.

Employees’ devices create additional challenges for IT departments. Two-thirds of respondents said that permitting employees to connect their own devices to the corporate network increased the risk of security breaches and 55% said it increased network security complexity (Figure 8).

About 40% reported that employee devices increase the risk of network or application outages; the same percentage expressed concern about compliance issues with devices brought from home.
With a more fluid flow between home and work for many employees, risks from inadvertent exposures and errant devices are likely to increase in importance for many organizations. Consequently, IT departments may want to turn their attention more toward automated processes that can defend a network against rogue or careless employees and questionable devices.

**Partly Cloudy for the Foreseeable Future**

Cloud security may be the way of the future, but relatively fewer respondents count on it in the present. Almost 60% of respondents said less than 25% of their security controls are in the cloud and less than 10% had more than 75% of their security controls cloud based (Figure 9). In general, the larger the organization, the less likely it was to rely on the cloud for security. The most enthusiastic adopters had fewer than 100 employees, but even among those, only 28% had more than 50% of security controls in the cloud. So far, the cloud-based security has been more a topic of conversation than adoption.

![Figure 9: Percent of Security Controls in the Cloud, by Company Size](image)

**Conclusions**

This year’s survey reinforces the conclusions reached in the 2012 analysis: the biggest challenges for IT Security, Network Operations and Risk and Compliance teams continue to be lack of visibility, manual processes, and poor change management. In this environment, out-of-process changes are fraught with risk, with outages and security breaches among the most serious—and disturbingly common—possible negative outcomes. Changing application rules to boost productivity or otherwise improve operations has the opposite effect for many organizations as those changes also inadvertently cause outages, impaired performance and security breaches.

The greatest threats for organizations are also increasingly from within: employees accidentally causing a data breach or security problem, malicious insiders, and unsecured or non-compliant employee devices.
In the 12 months since our last report, two related trends have emerged. Next-generation firewalls are rapidly gaining acceptance, even dominance, and more organizations have centralized firewall management processes. Very likely the added process complexity of NGFWs has encouraged this streamlining. Still, the majority of organizations find that the increased security of NGFWs comes at the price of more policies and more changes to manage.

Organizations adopt NGFWs for two primary reasons: to improve security and reduce costs. Moving away from manual processes and toward automated, centralized management of processes and policies will position IT organizations to fully realize the potential of NGFWs to do both.
About AlgoSec

AlgoSec is the market leader in network security policy management. AlgoSec enables security and operations teams to intelligently automate the policy management of firewalls, routers, VPNs, proxies and related security devices, improving operational efficiency, ensuring compliance and reducing risk.

More than 1000 of the world’s leading enterprises, MSSPs, auditors and consultancies rely on AlgoSec Security Management Suite for unmatched automation of firewall operations, auditing and compliance, risk analysis and the security change workflow.

AlgoSec is committed to the success of every single customer, and offers the industry’s only money-back guarantee.

For more information, visit www.AlgoSec.com.