Examining the Impact of Security Management on the Business

An AlgoSec Survey

algosec Managing Security at the Speed of Business

SHARE THIS RESEARCH:

Executive Summary

A survey of 240 information security professionals, network operations and application owners finds that organizations of all sizes face an increasingly complex interaction between business critical applications and the need to manage security effectively in the data center.

- **Organizations are reliant upon more data center applications, but struggle to deploy them and make updates "at the speed of business".** Nearly one-third of respondents said they had more than 100 critical business applications in their data center (32%) and nearly one in five (19%) had responsibility for more than 200. Adding new data center applications and addressing application connectivity changes pose challenges for the businesses, a quarter of which (25%) must wait more than 11 weeks for a new application to go live, and for the IT groups, the majority of which (59%) spend more than eight hours on each application connectivity change.
- **Most organizations want to understand their risks from a business standpoint.** Nearly half of respondents would prefer to see their exposure presented by business application and another 30% would choose to view risk by network segment.
- **Many organizations plan to migrate business applications to the cloud, despite experiencing application connectivity disruptions in the process.** One in five organizations expects to base more than 40% of their business applications in the cloud even though two-thirds have suffered unexpected outages or disruptions during data center application migrations to public, private or hybrid clouds.
- **Firewall audits consume significant time and resources.** Nearly three-quarters (74%) of respondents say that firewall audits consume more than one man-week each year and one in six (16%) spend more than one month on firewall audits annually.

About the Survey

The "Impact of Security Management on the Business" survey was conducted to determine how security management affected organizations' agility and access to business critical applications.

240 information security, network operations and application owners completed the online survey, conducted in September 2013. Of those respondents, 46% primarily had responsibility for information security, 30% were in network operations, 11% were application owners, 10% were C-level executives, and 2% were auditors. There were no statistically significant differences in the responses from these three groups.

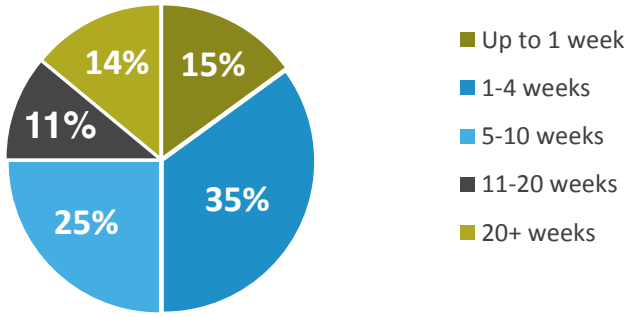
Respondents hailed from 54 countries, making this a truly global survey. Businesses of all sizes participated: 20% of respondents worked for businesses with 1-100 employees, 28% for mid-sized organizations of 101-1000 employees, and 52% for enterprises of more than 1000 employees.

The growing number of critical business applications has increased the complexity of security management and reduced organizational agility. To better support enterprise productivity, information security professionals, network operations and application owners alike need greater visibility into the impact of security changes and cloud migrations on data center applications. Additionally, these teams need to streamline processes for making application connectivity changes and auditing firewalls – to improve the security and compliance posture as well as keeping operations agile enough to quickly respond to changing business needs.

More Data Center Applications, but Less Security and Agility

The ability to efficiently deploy and manage connectivity has not kept pace with the rapid growth in numbers of critical business applications, with serious consequences for business agility. While the majority of organizations (51%) now manage more than 50 data center applications, most organizations (50%) spend more than five weeks on the average application deployment. In 14% of organizations, new critical business applications take more than five months to bring online (Figure 1).

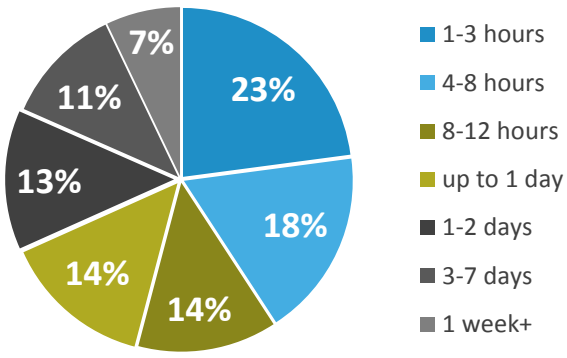
Figure 1: Average time to deploy new data center applications



Challenges with the large number of applications continue long after deployment, particularly with the high number of connectivity changes requested each week and the lack of visibility to the impact of those changes. Today 11% of organizations must handle more than 40 application changes specifically related to connectivity each week and 44% of organizations manage more than 11 application connectivity change requests weekly.

All those connectivity related changes create a significant load for IT teams. Forty-five percent of organizations measure time to process this type of application change in days, not hours. For 7% of organizations, connectivity related changes typically take more than a week. Only 41% can process connectivity related application changes in less than eight hours on average (Figure 2).

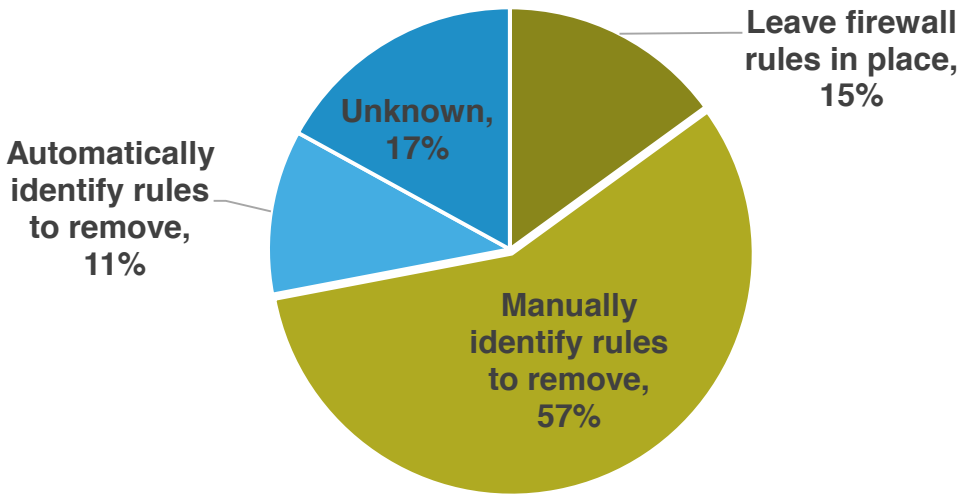
Figure 2: Average length of time to process application connectivity change



Despite the significant amount of time spent managing changes, the majority of IT professionals (53%) report that they have limited visibility into the impact that network security changes have on critical business applications. One in six notes they have poor or very poor visibility and another 37% characterize their visibility as only fair.

While bringing new business applications online takes many organizations weeks or months, most organizations find the process of decommissioning data center applications too risky to undertake at all. Less than 11% of organizations can automatically identify firewall rules that should be removed when decommissioning an application. The majority must undertake the arduous and error-prone method of manually identifying the rules to remove. More than 15% of responding organizations find that process so daunting that they simply leave the firewall rules intact (Figure 3).

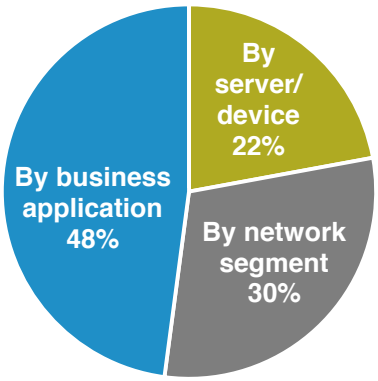
Figure 3: How are firewall rules managed when business applications are decommissioned?



Managing Risk from the Perspective of the Business

Whether from connectivity changes, outdated software, device misconfigurations or other factors, the vulnerabilities associated with business applications abound. IT organizations want to know what their risks are from the business perspective, but most network vulnerability management systems do not offer that view. Given the choice, nearly half of respondents (48%) want to view risk by business application; 30% want to see their exposure by network segment and 22% by server or device (Figure 4). With this type of visibility, security teams can more effectively communicate with business owners and enable them to “own the risk”.

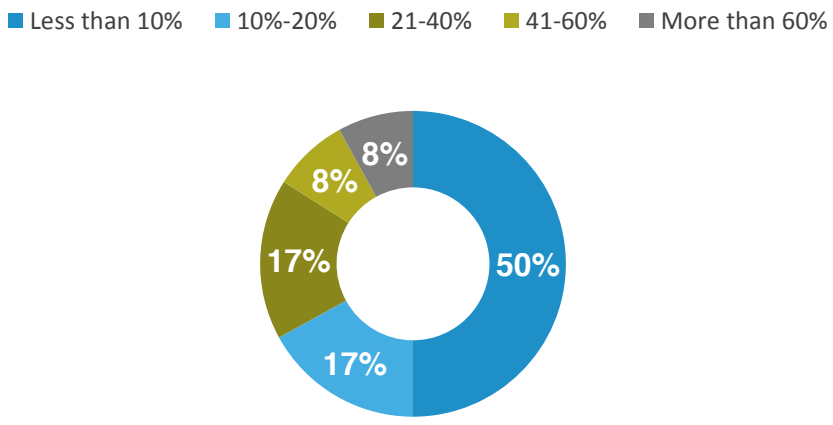
Figure 4: Ideal method for prioritizing network vulnerabilities



Cloud Migration Challenges Lead to Increased Risk

Many organizations have yet to migrate a significant percentage of their business applications to the cloud, though most plan to increase their reliance upon cloud-based applications in the future. In excess of two-thirds of respondents say they will migrate to private (34%) or hybrid (35%) clouds. Just 5% expect to migrate to public clouds and 25% have not defined their cloud strategy yet. Physical data centers dominate today, with 50% of organizations reporting that they have less than 10% of their business applications in the cloud. A third of respondents had between 10% and 40% in the cloud today. Those that have committed to cloud-based applications have done so in a big way, with 16% of organizations having already migrated more than 40% of their applications (Figure 5).

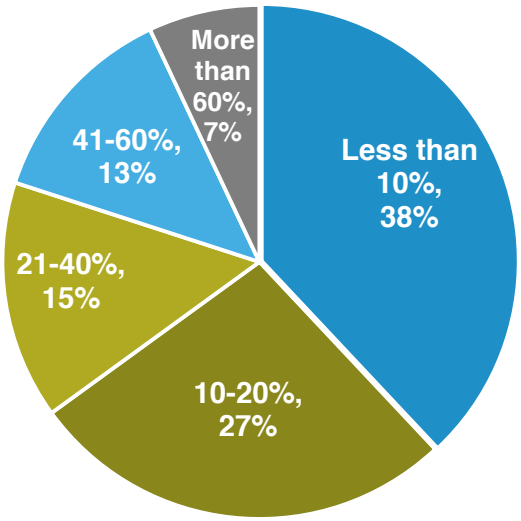
Figure 5: Number of business applications currently in the cloud



SHARE THIS RESEARCH:

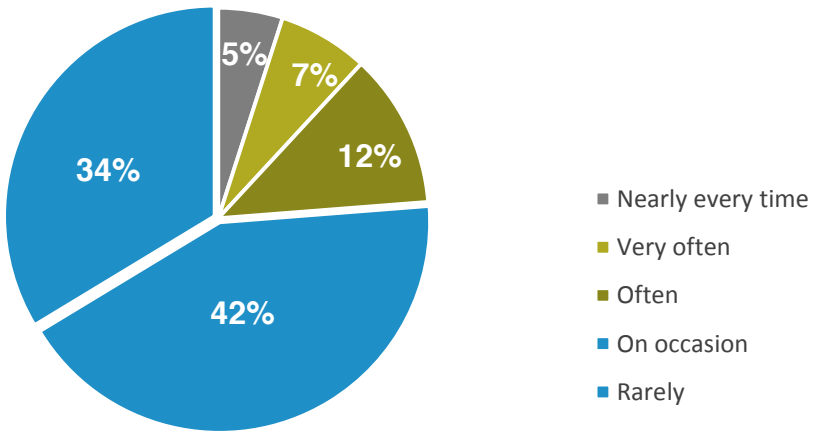
Across the board, IT groups plan to migrate more of their applications, with one in five expecting to have more than 40% in the cloud and more than one-third planning to migrate at least 20% of their applications in the next 12 months (Figure 6).

Figure 6: Percentage of business applications expected to migrate in the next 12 months



For many organizations, the delay in migrating may be due to the challenges experienced in previous efforts to move applications to the cloud. Two-thirds of organizations report that they suffer unforeseen connectivity disruptions or outages in connection with migrating data center applications at least occasionally. For 23%, migration causes unexpected outages or disruptions somewhere at least "often" and 5% are plagued by problems "nearly every time" (Figure 7).

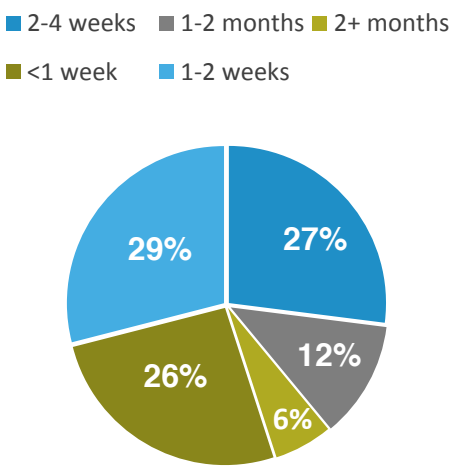
Figure 7: Frequency of unforeseen connectivity disruptions or outages during data center application migration



Firewall Audits Create Barriers to Strategic Contributions

Ensuring the continued security of all those data center-based critical business applications requires ongoing firewall audits, absorbing significant resources in most organizations. Nearly three-quarters of respondents said they spent more than one man-week per year on firewall audits. One in six reported that their organization devoted at least one man-month to firewall audits annually (Figure 8). While firewall integrity is essential to organizational security, a more streamlined process for auditing would free IT professionals to focus on more strategic efforts that advance the goals and productivity of the organization.

Figure 8: Time devoted to firewall audits each year



Conclusions

The current approach to managing security policies and devices is not in alignment with what the business requires. In order to improve both security and agility, security professionals must have the visibility to understand the impact of policies on business applications and then be able to communicate with business owners. The rapid growth of critical applications in data centers creates significant challenges as the length of time required to deploy new applications and/or update existing ones impacts the organizational agility and productivity those applications are presumably designed to enhance.

The explosion of applications, lack of visibility into the effects of connectivity-related application changes and the manual processes required to remove rules for decommissioned applications all compound risk at the application level. Many IT teams are essentially “flying blind” when they make the dozens of changes requested each week and retire applications—exposing businesses to risks of outages and other unexpected consequences. Migrating critical applications to the cloud—which is expected to increase substantially in the next year—exposes businesses to a significant risk of unplanned disruptions and outages. Additionally, network vulnerability management does not present risk from a business perspective, which is what most IT professionals want to see.

IT teams want to contribute more strategically to their organizations and find that the weeks and months often devoted to tasks such as firewall audits and application deployment in environments that still rely heavily on manual processes absorb time and resources that could be better spent advancing the goals of the business and increasing productivity.

About AlgoSec

AlgoSec is the market leader for security policy management, enabling organizations to manage security at the speed of business. The AlgoSec Suite of products automates management of complex policies across firewalls, routers, switches, secure web gateways and more. Bridging traditional gaps between security, network and application teams, the AlgoSec Suite improves business agility, increases security and ensures continuous compliance.

More than 1000 of the world's leading organizations, including 15 of the Fortune 50, rely on AlgoSec for faster security provisioning of business applications, simplified security operations and improved protection against cyber-attacks.

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

SHARE THIS RESEARCH:

265 Franklin Street
Boston, MA 02110
USA

T: +1-888-358-3696
F: +1-866-673-7873
E: info@algosec.com

AlgoSec.com