



tufin

Making Security Manageable

Annual Firewall Survey Report

Insights on the state of firewall management

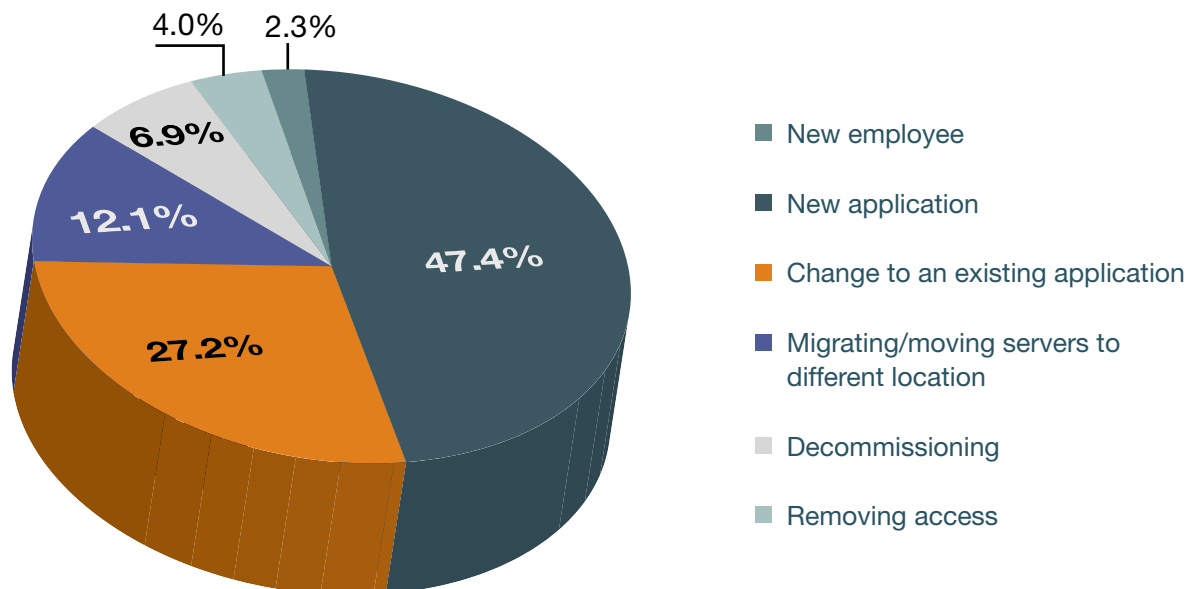
Annual Firewall Survey Report

Tufin conducted its annual firewall management insight survey amongst 200 network security professionals. The study found that 93.6 percent of all firewall change requests are application-related, validating that the function of firewalls has evolved to include secure application connectivity, in addition to their traditional role of perimeter security.

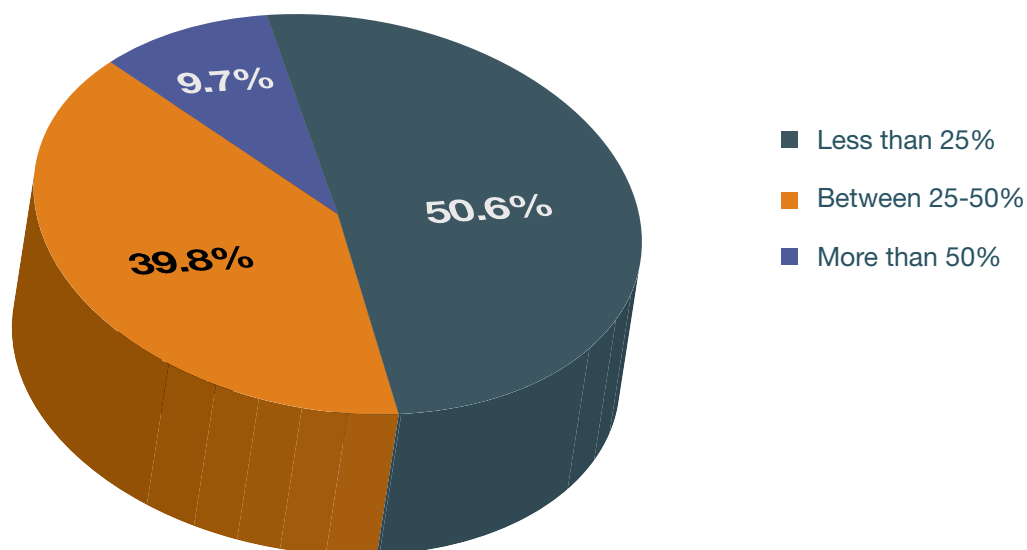
- Almost half of respondents audit their firewalls only once a year and 15% never audit their firewalls; 50% spend up to a week or more per quarter on firewall audits.
- Almost 1/5 reported they knew of someone who cheated on an audit because they either felt the audit was a waste of time (39.3%) or they did not have enough time/resources (35.6%).
- Almost 1/5 of the sample has no idea how current their firewall policy is.
- 40% have no way to know when a rule needs to be expired or recertified.
- 30% never test configuration changes before they are implemented.
- 90% of the sample has to redo up to half of all network security changes because they do not meet design requirements.

While survey data indicates firewalls are becoming increasingly relevant outside of their established function in security operations, their role have expanded - not shifted. Firewall management processes can have a significant impact on an organization's risk posture.

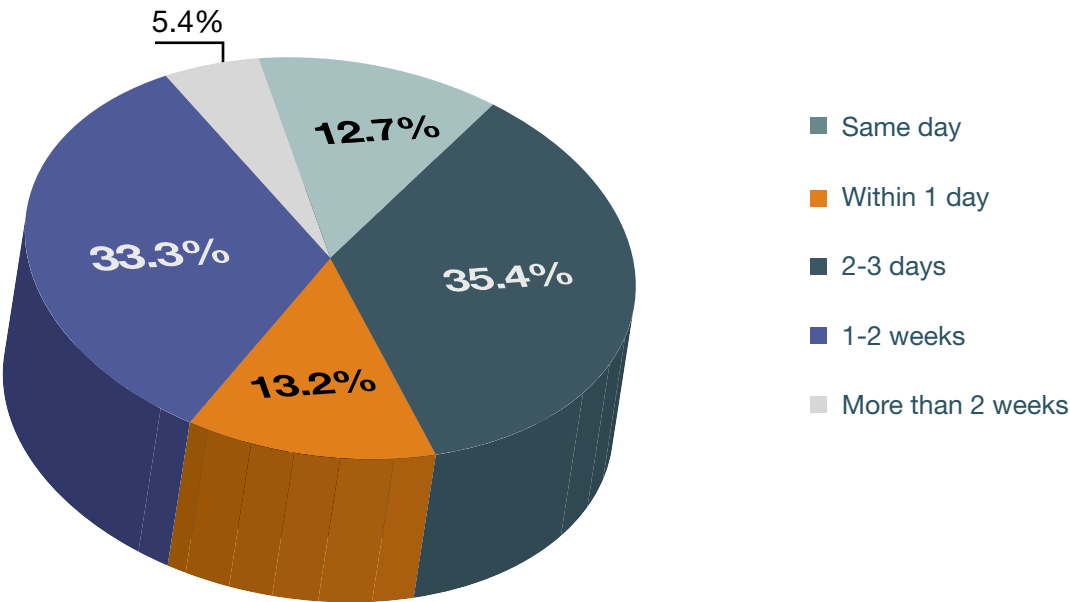
Q. What is the most common cause for a firewall change request?



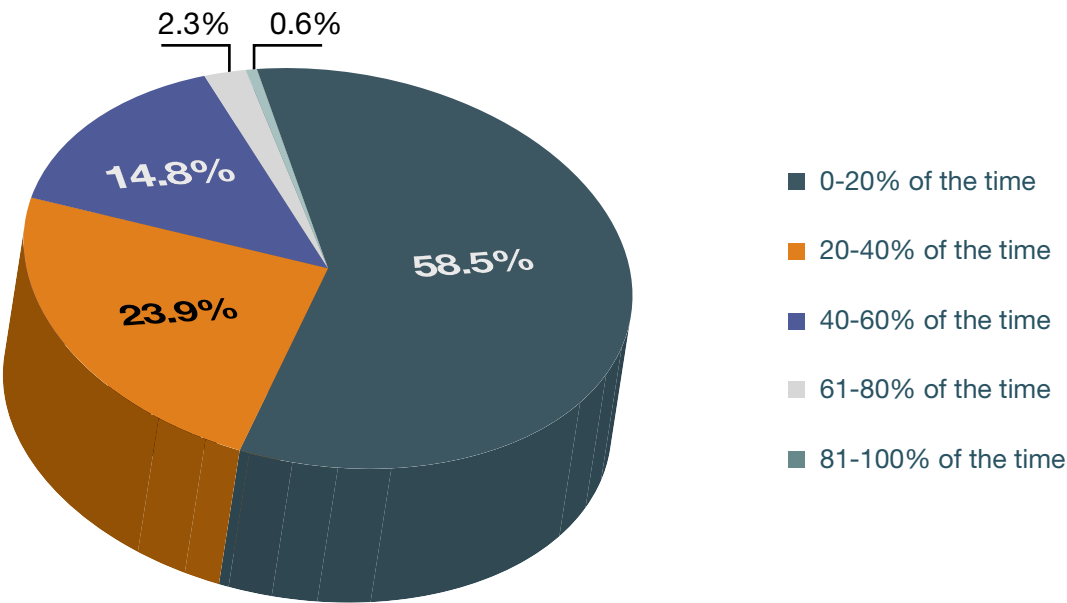
Q. What percentage of network security changes implemented need to be modified because the design does not meet the requirements?



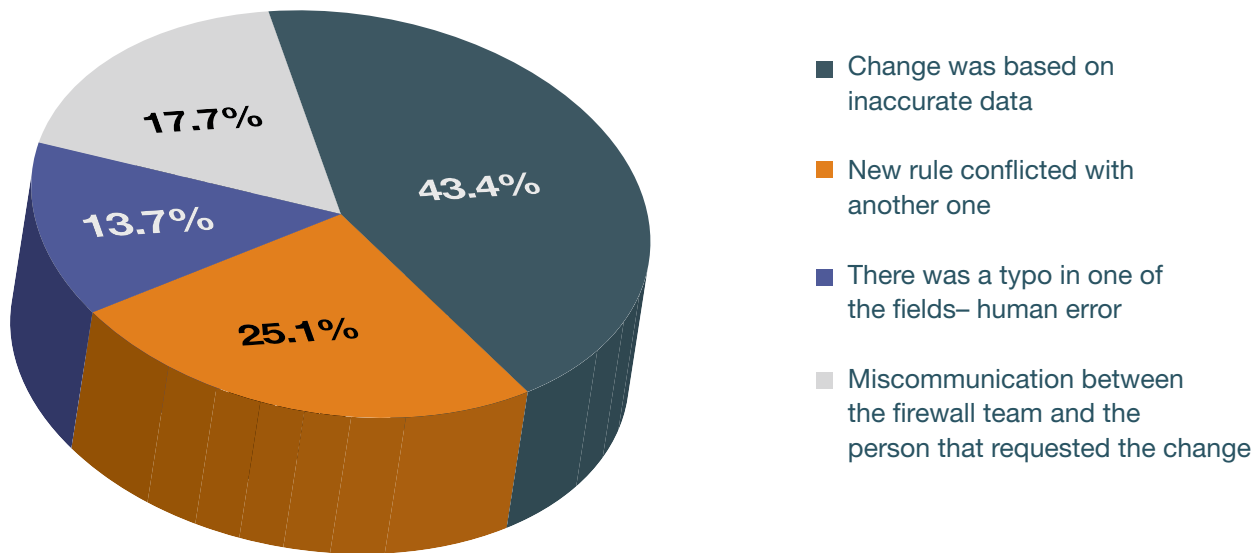
Q. How long does it take from the time a change request is submitted until it's completed (in production)?



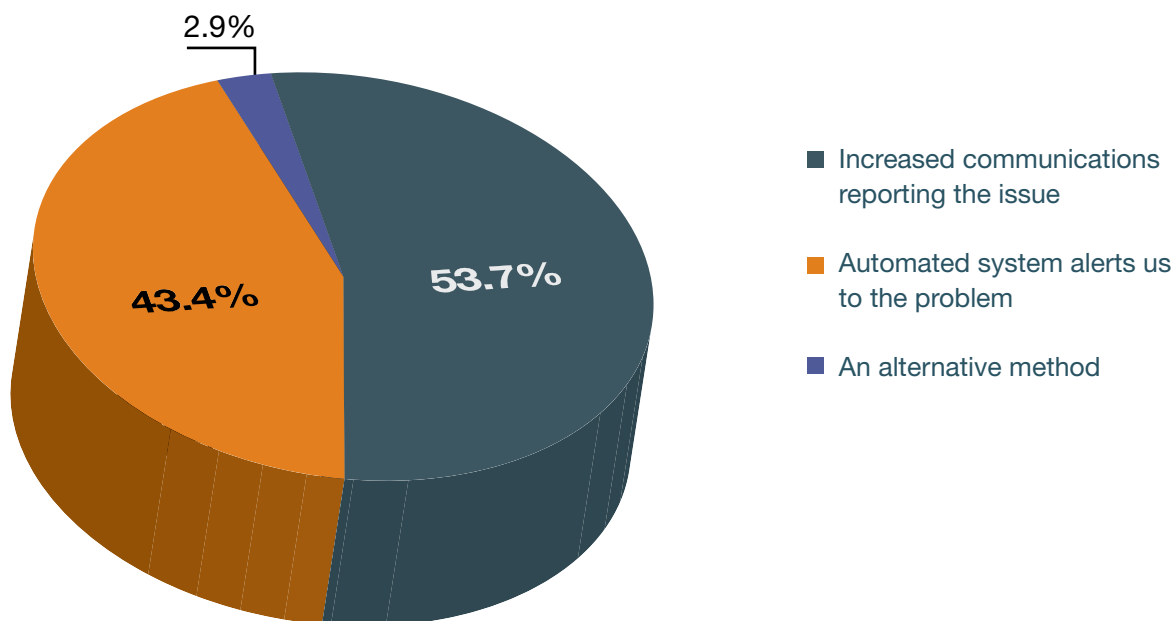
Q. How often does a firewall change need to be redone?



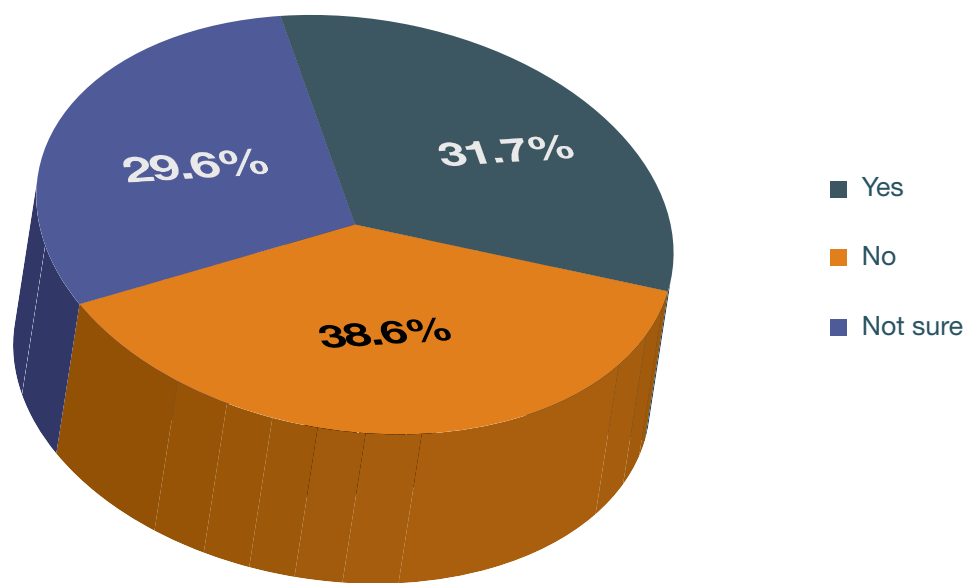
Q. Why do firewall changes need to be redone?



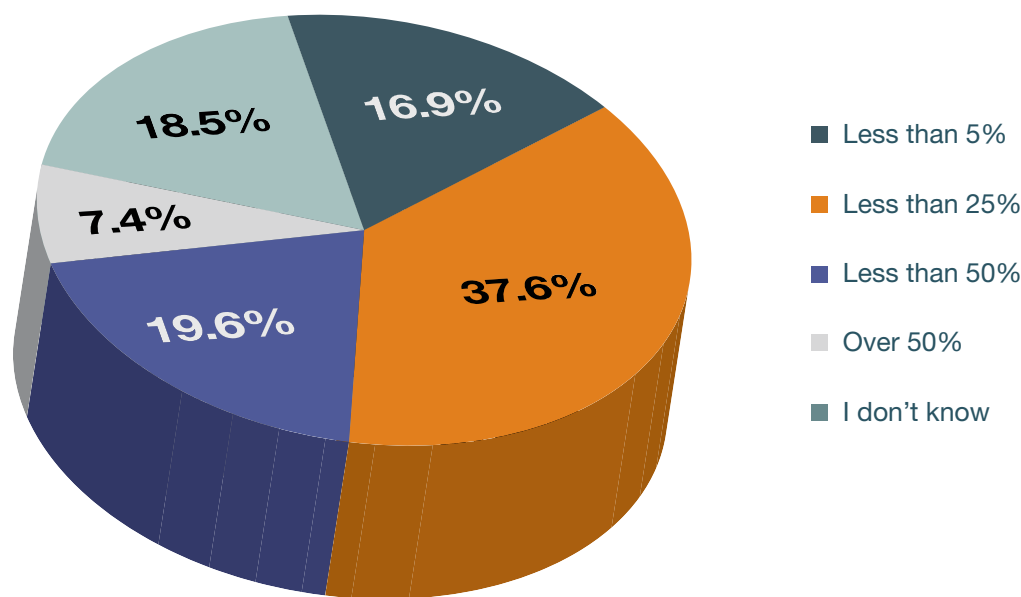
Q. How do you know when a firewall configuration change causes downtime?



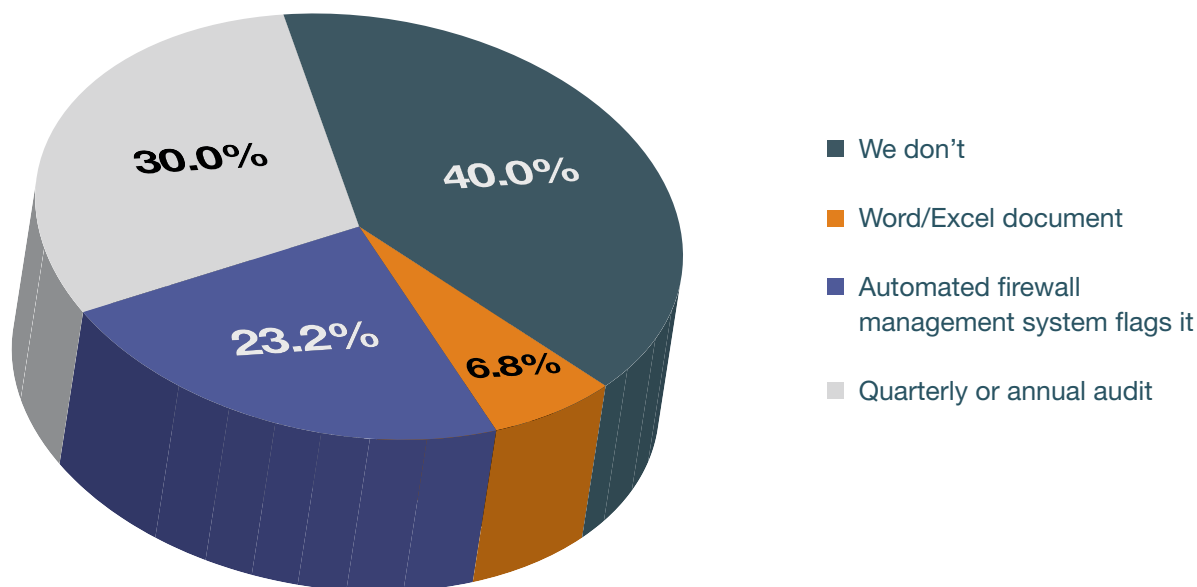
Q. Do you think your current change management processes put you at risk of a security breach?



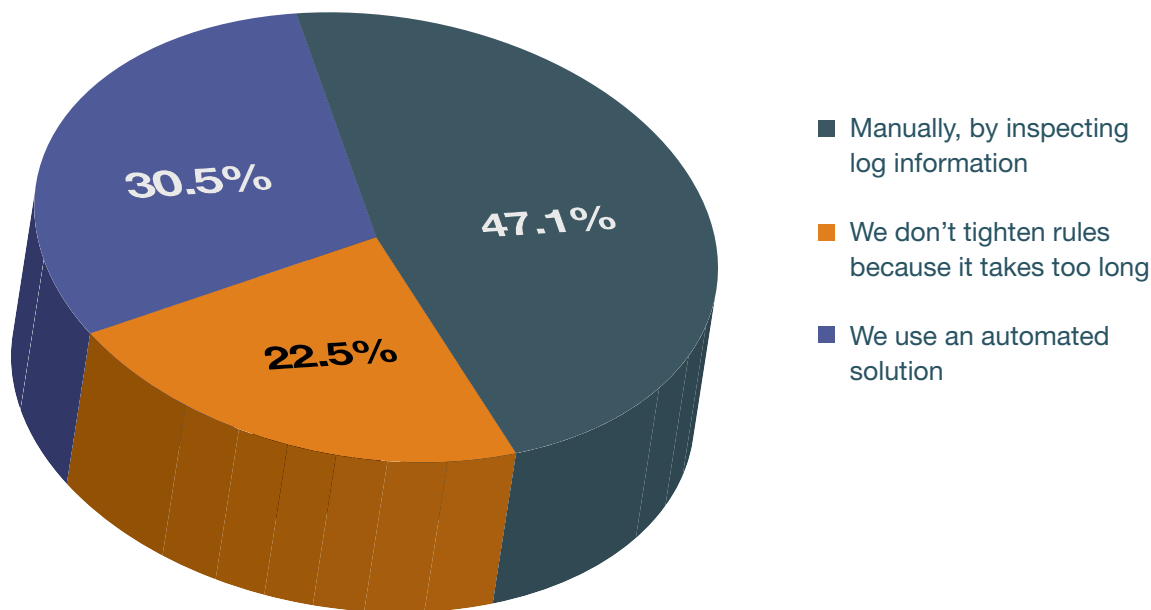
Q. What percentage of your rule base is obsolete (unused, or no longer required)?



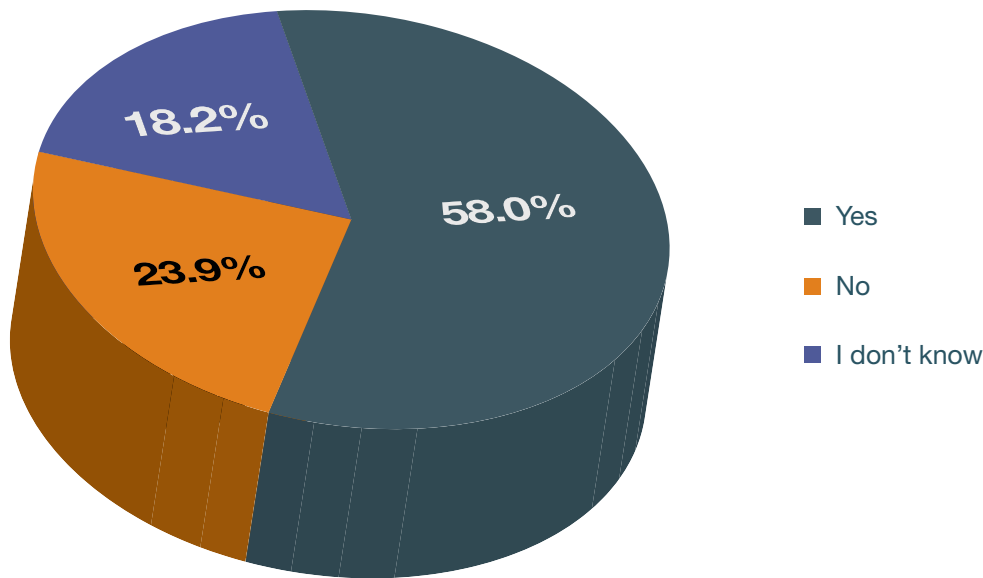
Q. How do you know when a firewall rule needs to be recertified or decommissioned?



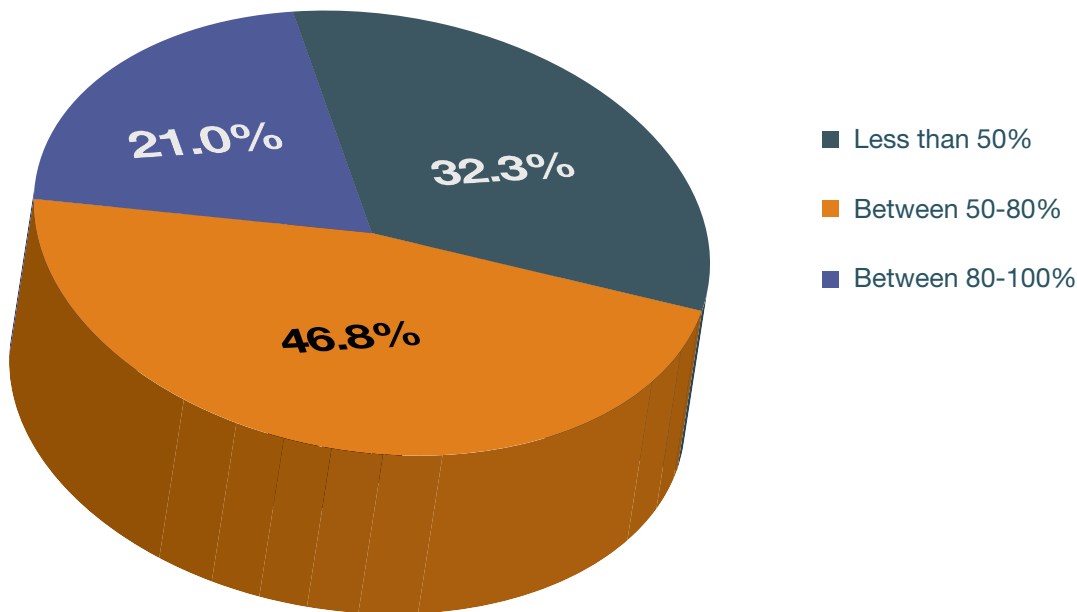
Q. How do you tighten overly permissive firewall rules?



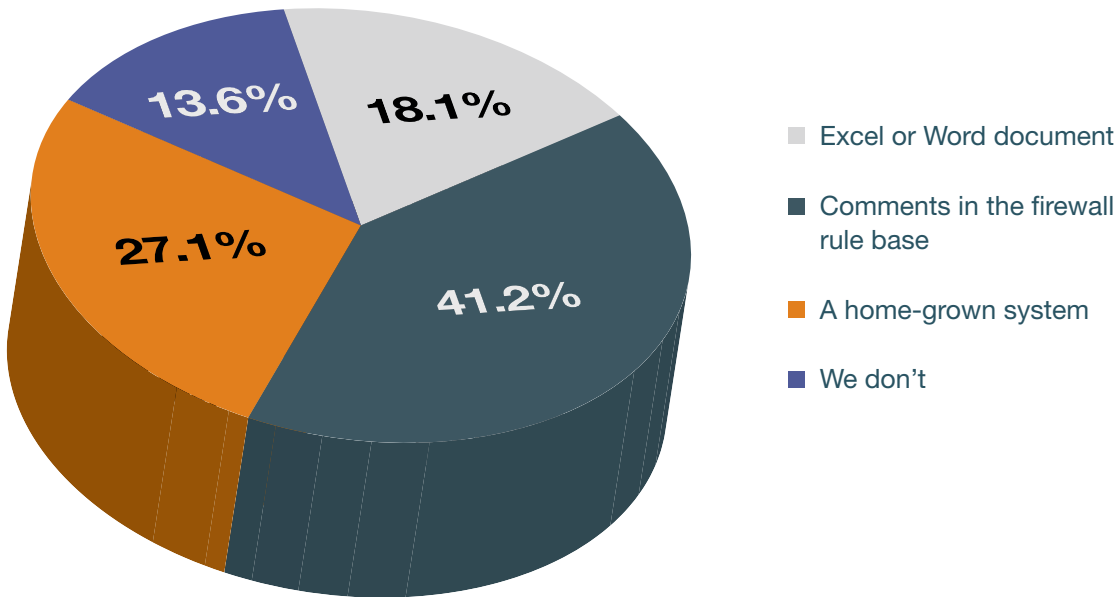
Q. Have you, or any of your colleagues, ever been asked to make a rule/configuration change against your better judgment?



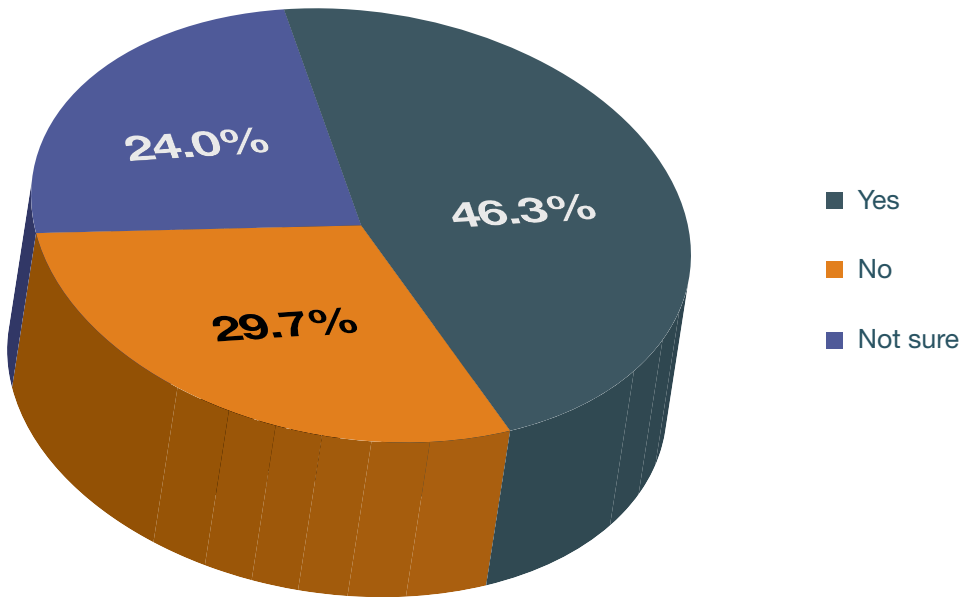
Q. What percentage of your organization's total firewall changes are application-related?



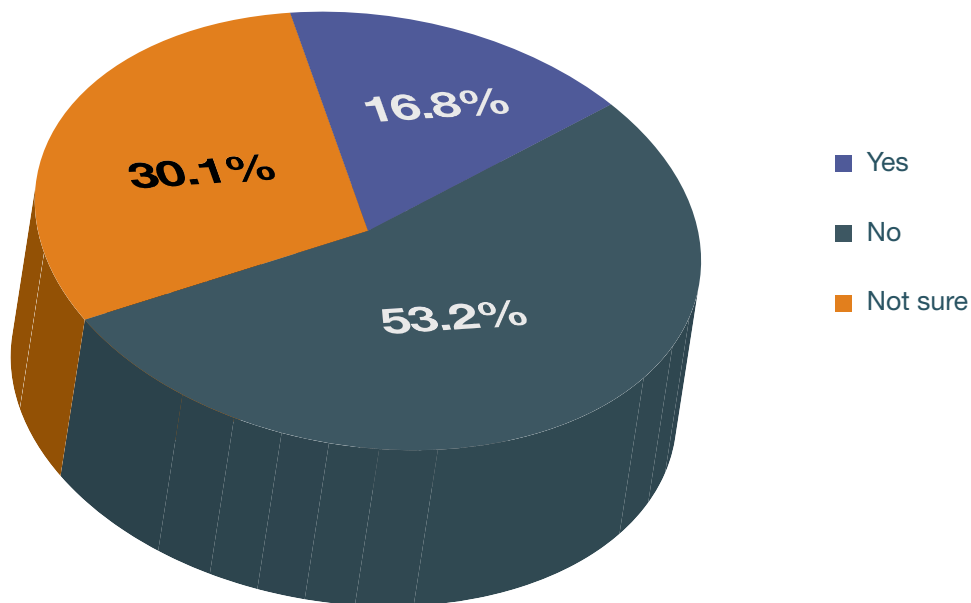
Q. How does your organization keep track of application connectivity requirements?



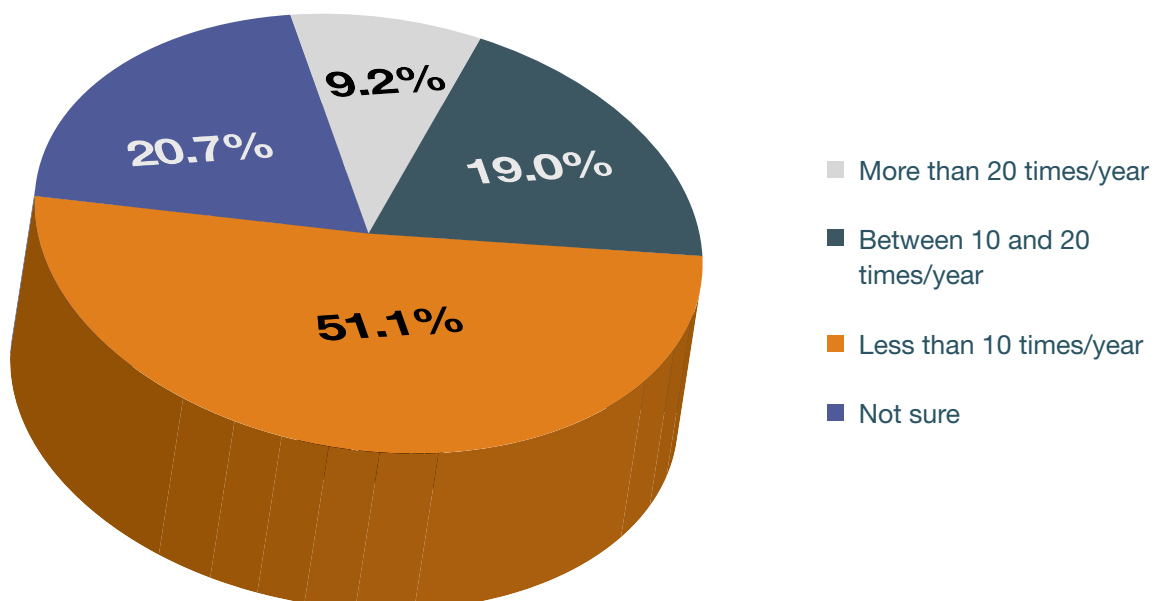
Q. Are you confident that as a team, you only open the ports required by your business?



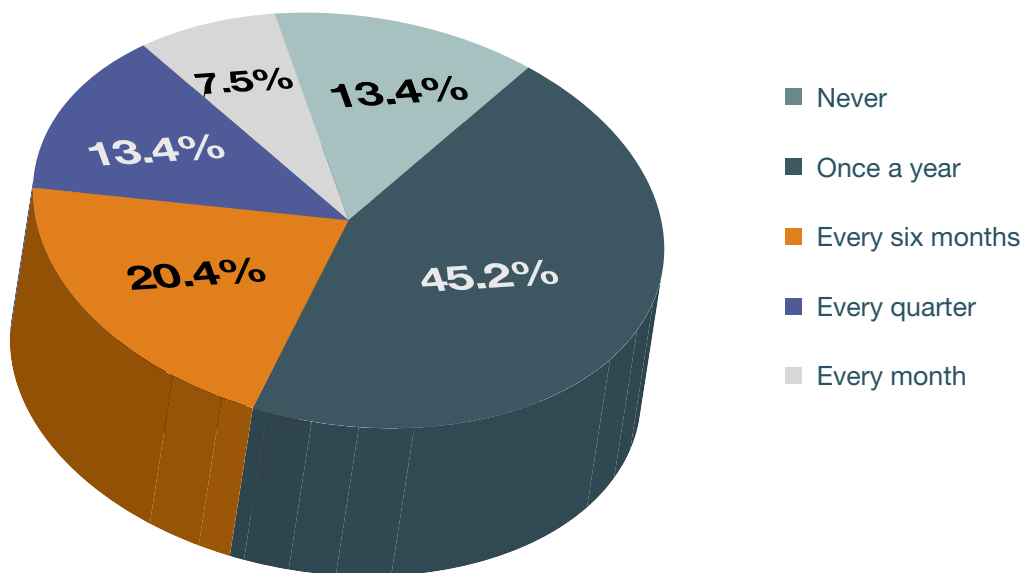
Q. Has your organization had a security breach due to an application-related rule change?



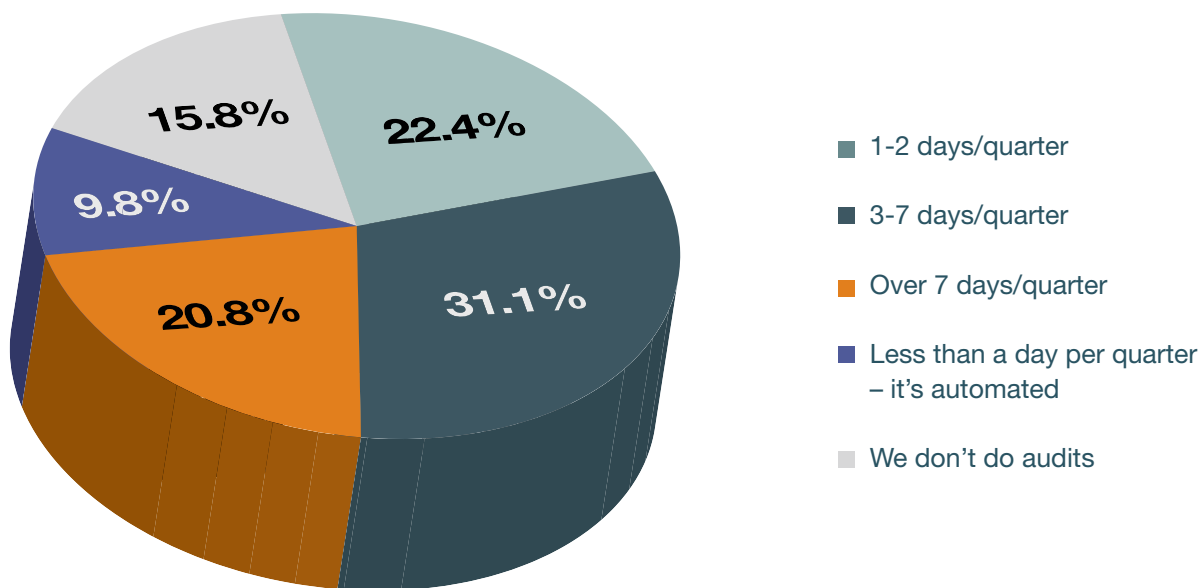
Q. How often has your organization experienced application service disruptions due to network configuration changes?



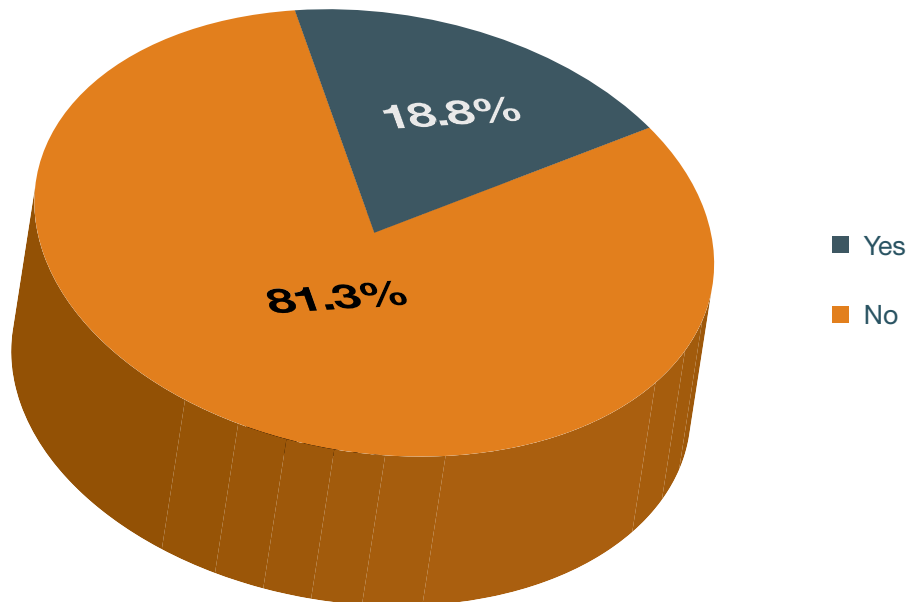
Q. How frequently do you perform corporate and /or regulatory audits?



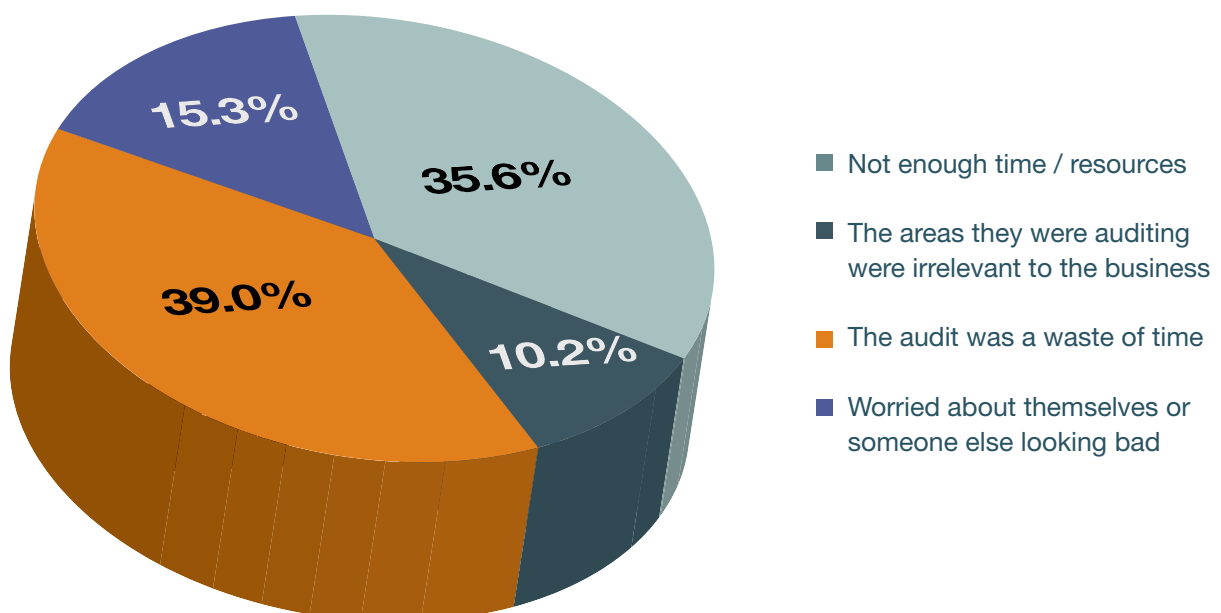
Q. How much time does the network security team spend on firewall audits, both in preparation and in the audit itself?



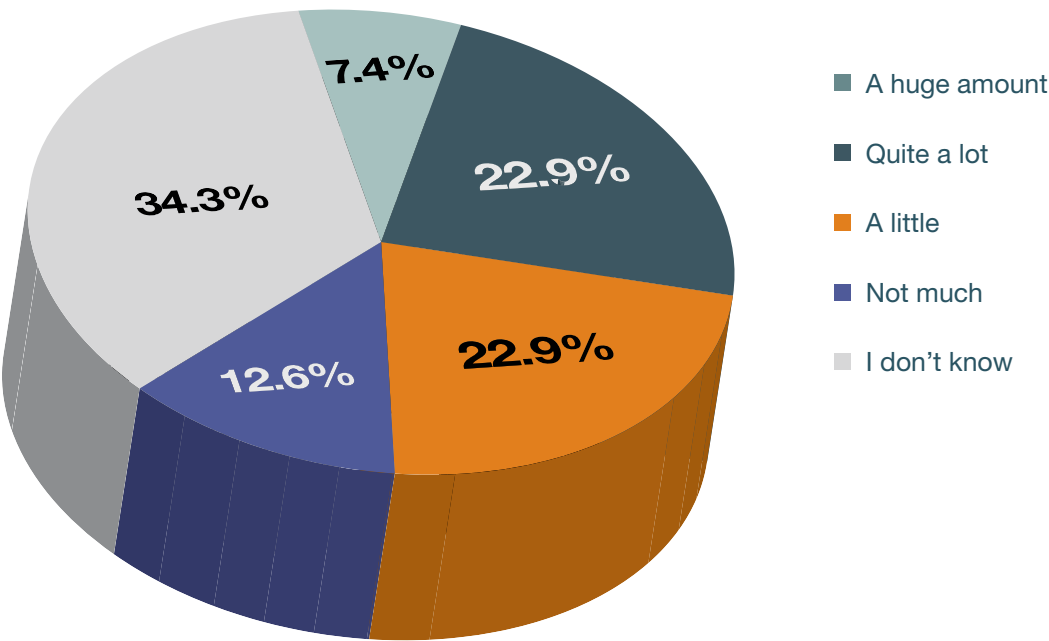
Q. Do you know anyone who ever cheated on an audit?



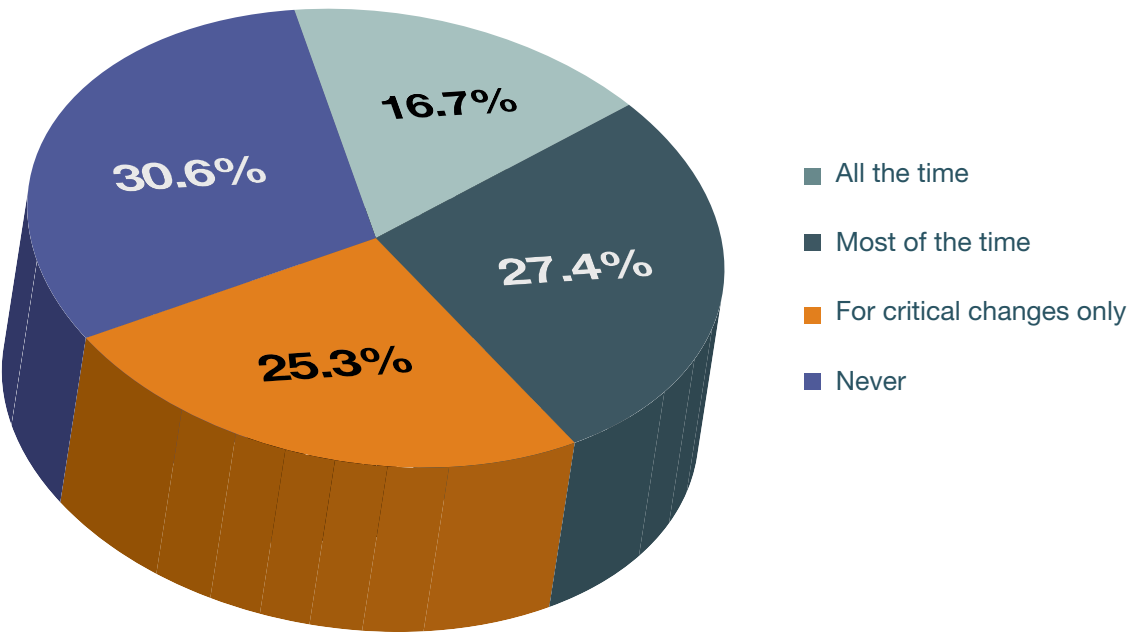
Q. If you answered “Yes” to the previous question, please explain why



Q. What percentage of your security budget is spent on items that don't improve security?



Q. Do you test or simulate configuration changes for potential risk and compliance violations before you implement them in production?



Conclusions

This report reveals that the role firewalls play in managing application connectivity is both a cause and effect of sweeping trends in enterprise IT. It is clear that more needs to be done in terms of education and understanding of the advantages that firewall security automation brings to the business efficiency table and how it allows the right set of organizational processes between the relevant stakeholders to be defined and implemented.

Learn more about how Tufin has addressed these enterprise IT trends from the 2012 launch of SecureApp, to the new release of Tufin Security Suite (TSS), its award winning Security Policy Management solution.

Read the SIX Group case study to learn how – with SecureApp – they can now report dramatic improvements in application connectivity-related change management processes.

Join the discussion about this report, or any other security policy management issues.

Your Opinion Matters

Twitter: <http://twitter.com/TufinTech>

Facebook: <http://www.facebook.com/Tufintech>

Google+: <https://plus.google.com/s/tufin>

LinkedIn: <http://www.linkedin.com/companies/tufin-technologies>

YouTube: <http://www.youtube.com/user/Tufintech>

The Tufin Blog: <http://www.tufin.com/blog>

About Tufin Technologies

Tufin™ is the leading provider of Security Policy Management solutions that enable companies to cost-effectively manage their firewall, switch and router policies, reduce security and business continuity risks, and ensure Continuous Compliance with regulatory standards. The award-winning Tufin Security Suite provides security teams with powerful automation that slashes the time and costs spent managing change and successfully passing audits. Founded in 2005, Tufin serves more than 1,100 customers in industries from telecom and financial services to energy, transportation and pharmaceuticals. Tufin partners with leading vendors including Check Point, Cisco, Juniper Networks, Palo Alto Networks, Fortinet, F5, Blue Coat, McAfee and BMC Software, and is known for technological innovation and dedicated customer service.

© 2008, 2009, 2010, 2011, 2012, 2013 Tufin Software Technologies, Ltd. Tufin, SecureChange, SecureTrack, SecureApp, Automatic Policy Generator, and the Tufin logo are trademarks of Tufin Software Technologies Ltd. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.