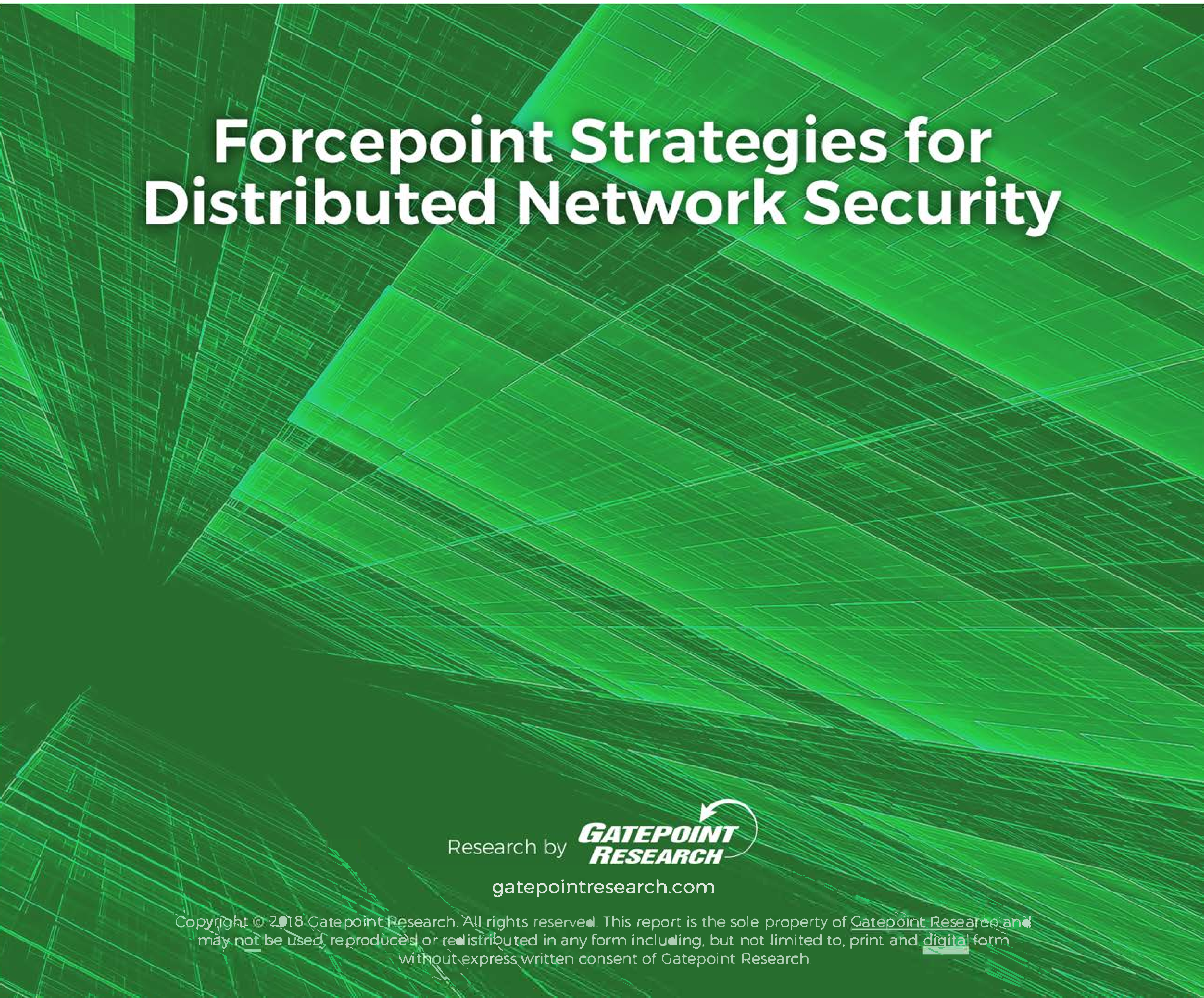
FORCEPOINT

POWERED BY Raytheon

Protecting the human point.



Forcepoint Strategies for Distributed Network Security

Research by GATEPOINT RESEARCH

gatepointresearch.com

1. Table of Contents

2. Executive Summary

Financial institutions are facing increasing challenges as their organizations become more distributed, applications move to the cloud, and threats rapidly evolve. In today's hyper-competitive world, businesses are undergoing a digital transformation in order to stay relevant. Successful digital transformation demands 100% connectivity, agility, security and efficiency.

For networking executives, connecting and protecting a highly distributed organization today keeps getting more complicated requiring evermore boxes, overhead, complexity, and risk. This is neither agile nor efficient. Traditional fragmented network capabilities that are labor intensive and inconsistent to operate, manage, and secure. And it's holding you back. You need a better way.

Gatepoint Research surveyed senior IT executives in the financial services industry on their strategies for distributed network security.

Respondents were asked to report:

- How good is their network security expertise at distributed locations?
- How many (and what types) of firewalls do they have deployed? How effective are they at blocking threats?
- What factors are important in evaluating firewalls from a management standpoint?
- What are their biggest challenges in managing firewalls in distributed locations?

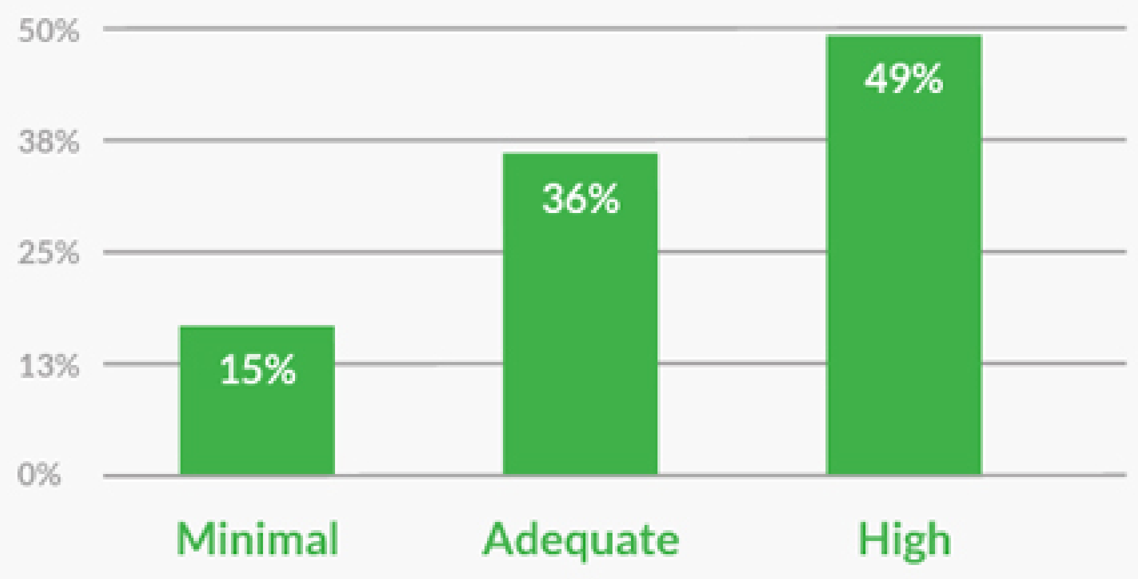
Forcepoint is focused on enabling highly distributed financial institutions to safely and efficiently handle stiff requirements for data security compliance and the scrutiny that come with it. With each new threat and every new location, reputations are on the line. One failed audit or media report of a data breach can cause irreparable harm.

To remain competitive, financial services organizations must continue to innovate and adopt new technology. Forcepoint's security solutions provide distributed enforcement combined with centralized management and visibility, helping financial services organizations to strike the right balance of proactive protection, innovation and growth.

3. Survey Results

Network Security Expertise

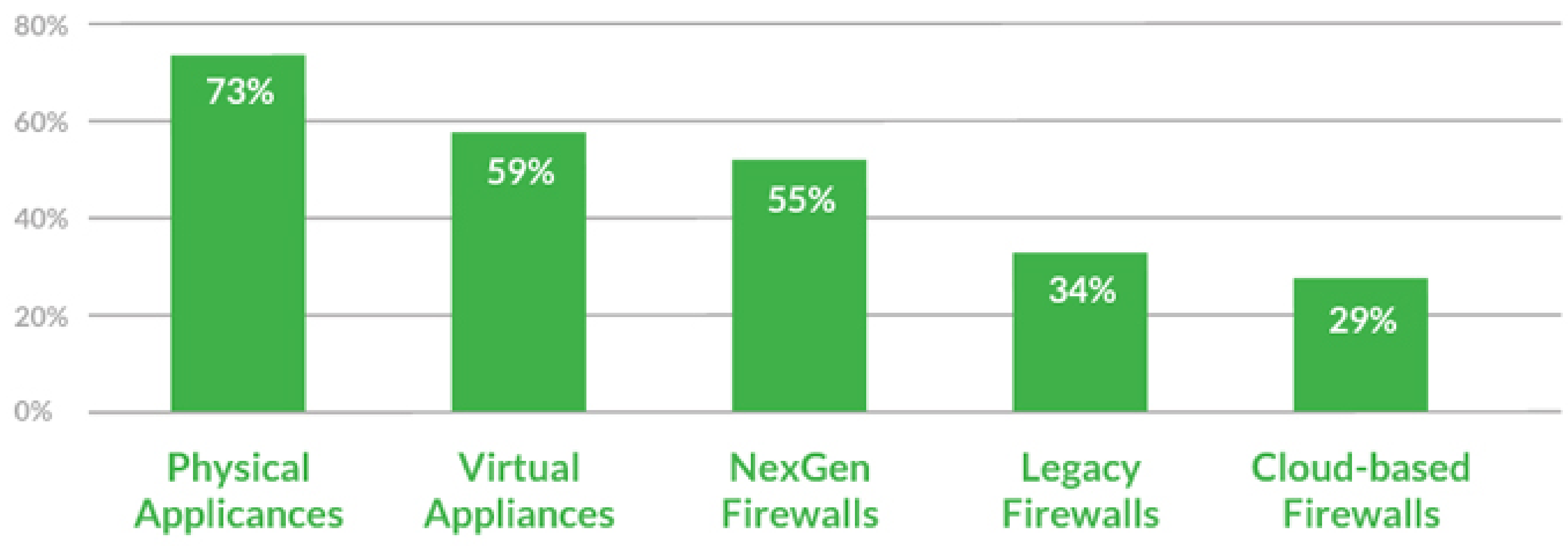
What is the level of network security expertise in your organization's distributed locations, on average?



Although almost half of survey respondents characterize the level of network security in their distributed locations as high, 36% say it is just adequate, and 15% confess it is minimal.

Firewalls Overview

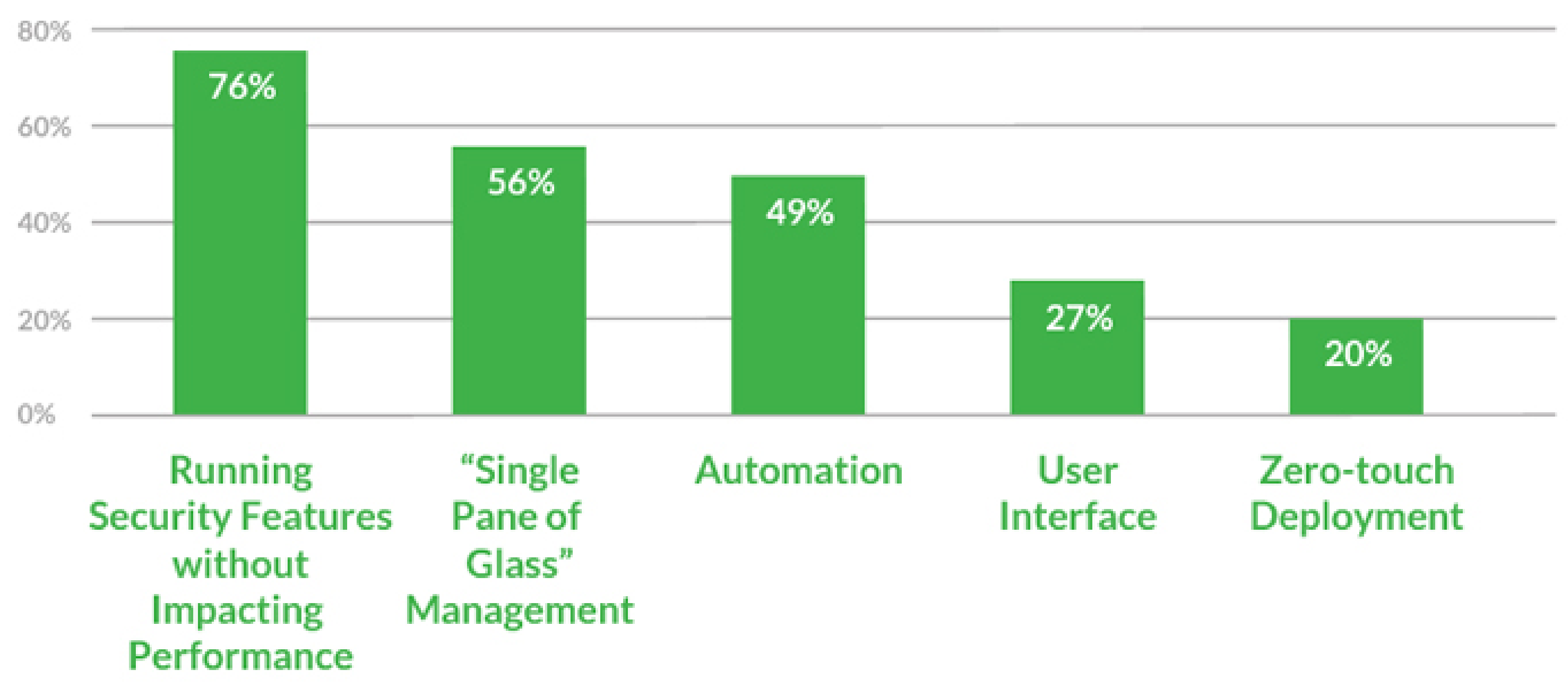
What types of firewalls do you have deployed?



When asked about the firewalls in use today, 34% of those surveyed report using legacy firewalls, which could be a significant security issue. Cloud-based firewalls are gaining converts (29%) especially in the financial sector, where many organizations are migrating to the cloud.

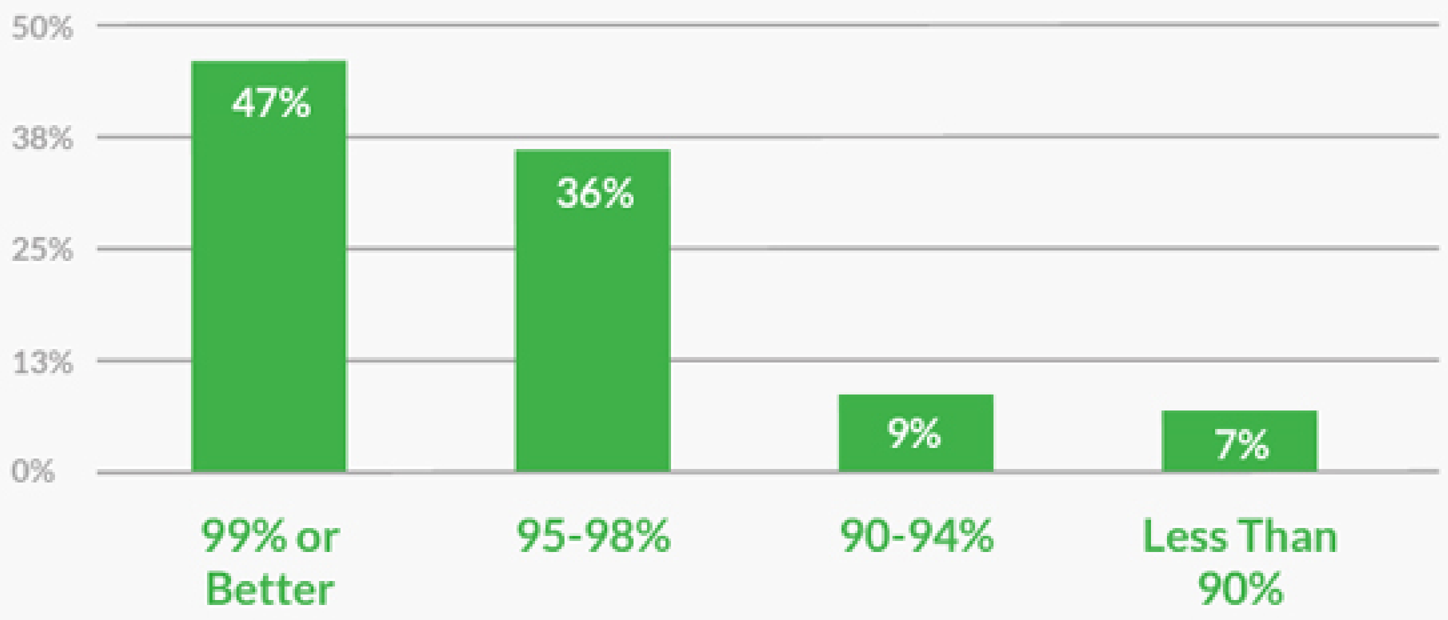
3. Survey Results
continued...

What factors are most important in firewall management?



When asked what is important in firewall management, respondents most often cite security features that do not compromise performance (76%). Other desirable factors are "single pain of glass" management capability (56%) and automation (49%).

How effective are your firewalls in blocking threats, on average?



Nearly half of those surveyed say their firewalls block threats with a 99% efficacy rate. However, latest NSS labs NGFW test results indicate that this level of confidence may be overstated–the average firewall tested had an efficacy of 67% as many NGFWs tested had significant vulnerabilities for blocking evasions.

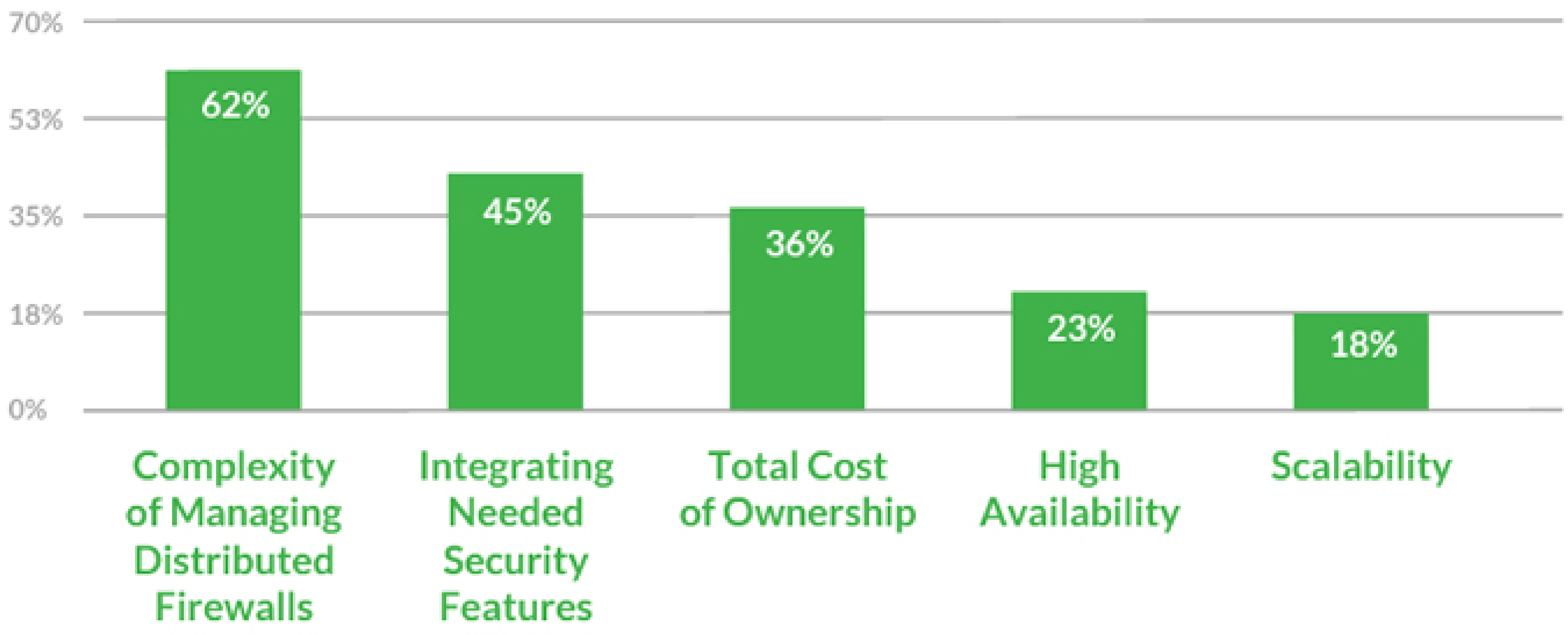
The 2017 NSS Labs' NGFW test shows execs surveyed may not be aware of holes in their firewall security leaving financial networks exposed.

3. Survey Results
continued...

Firewall Management Challenges

Most respondents (62%) rate the complexity of managing distributed firewalls as their biggest challenge. Other challenges that rank highly include integrating security features (45%) and cost (36%).

What are the main concerns in managing distributed firewalls?



4. The Forcepoint NGFW Solution

Forcepoint Next Generation Firewall (NGFW), part of its Human Point System, combines enterprise-grade SD-WAN and network security into a single solution that is centrally managed even at cloud scale. It helps financial services organizations connect and protect users and their data throughout data centers, edge, branches, and the Cloud – all with the industry's #1 security, manageability and availability.

Enterprise SD-WAN

Forcepoint enables distributed organizations to connect their branches, stores, and remote locations to the Internet efficiently and securely. It provides dramatic cost savings over traditional MPLS-based "hub-and-spoke" networks, enabling financial firms to take advantage of the latest commodity broadband links. In addition, it enables multiple technologies and Internet Service Providers to be used at each location, significantly improving resilience and availability in today's always-on world. With Forcepoint, organizations can seamlessly, securely and efficiently operate more than a thousand sites from a single pane of glass.

Strongest Security

Forcepoint's network security solutions offer the industry's top-rated security efficacy for both Next Generation Firewalls (NGFW) and Next Generation Intrusion Prevention Systems (NGIPS) according to NSS Labs' 2017 tests. Forcepoint defeats evasions, exploits and malware that attackers use to penetrate and spread throughout enterprise networks. In addition, it provides high-speed, granular inspection of encrypted traffic that protects financial institutions from modern attacks while also maintaining users' privacy. These capabilities, as well as its pioneering proxy technology for defending mission-critical applications, are tightly integrated, providing strong security that efficient to deploy and manage, even in highly distributed branch environments.

Smartest Manageability

Forcepoint's centralized, policy-based approach enables business processes to be turned into security controls accurately and efficiently. Policy updates and even software upgrades can be deployed to hundreds of systems – throughout data centers, offices, branches, and multi-cloud environments – in minutes, not hours. IDC Research found that customers that switched to Forcepoint NGFW were able to cut the IT burden of securing their network by 53% and reduce incident response time by 70%.

5. Success Stories

Sword Apak (visit website)

> **“Forcepoint NGFW gave us the opportunity to explore upgrades to our system but still run on known hardware platformsthat we already had installed. Everything we use, and then some, is now supported by Forcepoint. It is just an overall great solution.”**
>
> **Adrian Grimshaw**
> **Technical Consultant, Sword Apak**

Sword Apak has been developing and implementing global software solutions since 1979.

For years Sword Apak operated using strictly a proxy-based firewall. Moving to a packet inspection firewall represented a completely different design as employed in the Next Generation Firewall (NGFW) products. Ideally, one single point of failure at a network node, should not fail an entire system. However, the dated firewall systems would not support this kind of functionality. Sword Apak’s strict, proxy-based firewall began to fail as it lacked the features necessary to support a growing infrastructure.

Forcepoint NGFW was originally implemented at Sword Apak, partially, as a ‘ customer compliance project’ back in 2006. Successful implementation and overall customer satisfaction from the project stemmed multiple, additional Forcepoint NGFW projects.

Forcepoint NGFW engines have dynamically improved and load balanced individual connections between Sword Apak firewall nodes. Sword Apak has relied on the Forcepoint solutions since 2006.

5. Success Stories
continued...

Avency (visit website)

Design. Development. Data.

> **"The results with Forcepoint NGFW have been extraordinary – outstanding performance, lower costs, and, most important, considerably fewer invasions."**
>
> **Hendrik Walter**
> **IT Director, Avency**

Avency is a B2B digital services provider based in Telgte, Germany. The company hosts more than 1,200 websites/applications and 7,000 domains for a wide range of businesses. Naturally, high availability and security were large concerns, particularly with regard to intrusion prevention and data loss prevention.

Avency chose to implement Forcepoint NGFW with the Forcepoint Security Management Center (SMC). Through Forcepoint NGFW's multitenancy capabilities, Avency is able to provide each client with its own secure, separate domain that is inaccessible to other clients. Customers can access the SMC to manage their own firewalls, or they can contract with Avency to provide firewall management as needed.

Through its Forcepoint NGFW reseller services, Avency actively monitors the customer firewalls around the clock and contacts the clients when critical events occur. Avency has relied on Forcepoint solutions since 2012.

5. Success Stories

continued...

Carglass (visit website)

> **“Forcepoint NGFW and Security Management Center provide the scalability and management features that make our new network infrastructure possible.”**
>
> **Christophe Hazemann**
> **Head of IT Production, Carglass**

Carglass is a subsidiary of Belron, a leading vehicle glass repair and replacement company operating in more than 35 countries around the world.

In order to maintain its market leadership, Carglass launched an innovative business expansion in 2013 consisting of new mobile service centers modeled on shipping containers and conveniently located at retail sites such as private area or supermarket parking lots.

Carglass established stringent requirements for network security and management. To meet its enterprise security requirements, Carglass sought an integrated solution that could provide network continuity, protect on-premise customer data, improve performance, and help accelerate future expansion projects.

After receiving decisive feedback from multi-site users of Forcepoint NGFW and SMC, reinforced by presentations from the Forcepoint team, Carglass chose the solutions to replace some of the legacy routers and the firewalls within its distributed network with an initial outlay of 50 firewalls.

Carglass (visit website)

CARGLASS®

With the deployment of Forcepoint NGFW, Carglass has met and exceeded its requirements on both a business and a technological level. The company can now proceed with its mobile business expansion in confidence, based on a streamlined and secure network infrastructure that provides advanced routing and firewall capabilities for continuous performance and security.

Moving forward, Carglass will continue to expand its NGFW deployments as the company's mobile operations grow, and the company is evaluating other solutions in the Forcepoint portfolio. Carglass has relied on Forcepoint security solutions since 2013.

6. Conclusion

Forcepoint Next Generation Firewall (NGFW) is an industry-leading network security platform that blocks malicious attacks and prevents the theft of data and intellectual property while transforming infrastructure and increasing the efficiency of your operations.

Forcepoint network security solutions are seamlessly and centrally managed, whether physical, virtual or in the cloud. Administrators can deploy, monitor and update thousands of firewalls, virtual private networks (VPNs) and intrusion prevention systems (IPSs) in minutes, all from a single console – cutting network operating expenses by as much as 53%. Advanced clustering for firewalls and networks eliminates downtime, and administrators can rapidly map business processes into strong, accurate controls to block advanced attacks, prevent data theft and properly manage encrypted traffic – all without compromising performance.

Learn how Forcepoint can connect and protect your users and the data they use throughout your enterprise network. **Sign up** for a free trial or demo.

Source: *Strategies for Distributed Network Security, August 2017*

Research sponsored by

FORCEPOINT
POWERED BY Raytheon

Research by GATEPOINT RESEARCH

gatepointresearch.com