A Forrester Consulting
Thought Leadership Paper
Commissioned By Fortinet

July 2015

Your Best Defense: Next-Generation Firewalls Enable Zero Trust Security

Best Practices For Evaluating And Implementing A NGFW

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

Security professionals are tasked with defending their organizations from internal and external threats at a time when those threats are more sophisticated, numerous, and unpredictable than ever before. As customers and employees alike push businesses to deliver new digital experiences, and thus expose the network to an ever-increasing risk of breaches, the security and risk teams must adopt a new approach to network security.

"Trust but verify" — the predominate philosophy among security professionals — is unreliable in this new threat landscape. It protects the perimeter, but if these initial security protections are breached, it is difficult to distinguish "trusted" and "untrusted" network traffic. The only way to ensure a malicious user isn't granted access to your network under the cover of "trusted" traffic is to assume a "Zero Trust" model, in which all network traffic is untrusted.[1]

Security technology is now in a position to deliver this model, with next-generation firewalls (NGFWs) as the cornerstone. NGFWs combine many of the security controls found in individual point products and embed them into a single solution. These appliances allow security professionals the flexibility to place protection at the data level and effectively defend against the rapidly changing threats organizations face today.

Eighty-seven percent of surveyed IT security professionals reported their organizations have experienced at least one breach within the past 12 months.

In May 2015, Fortinet commissioned Forrester Consulting to examine the purchase and implementation considerations, as well as challenges faced, for next-generation firewalls. To explore this topic, Forrester conducted a quantitative survey of 150 IT security professionals at midlevel organizations with next-generation firewall implementations.

KEY FINDINGS

Forrester's study yielded four best practices for organizations considering investing in a next-generation firewall:

- **Conduct an honest internal assessment.** Many of the challenges security professionals cited with implementation and performance of NGFWs can be sidestepped with a comprehensive purchase evaluation process. Before investing, conduct a thorough assessment of the budgetary and resource implications of a NGFW implementation.
- **Test before you buy.** Seventy-one percent of the IT security professionals surveyed with NGFW implementations would do more comprehensive product testing during the purchase evaluation process if they could do it again. Test multiple products for features and performance based on your requirements before you buy, either using third-party test houses or your own internal testing. Get a clear understanding of all NGFW features and how — or if — they will work with your existing point security products in order to optimize NGFW functionality in your network environment.

Seventy-one percent of those with NGFWs deployed would conduct more comprehensive product testing before purchasing a solution if they could do it again; 61% would consider a broader selection of vendors.

- **Identify and vet a wide cast of vendor solutions.** Sixty-one percent of the security professionals surveyed would consider a broader selection of vendors if they could go back in time. Start by doing some research online, reading analyst evaluations, and consulting peers at other organizations. Once you've identified potential vendors, utilize product demos, third-party testing, a proof of concept, and bake-offs to better understand vendor solution functionality.
- **Take a data-centric approach to security.** A critical part of a NGFW implementation is determining where it will be deployed. In following with one of the core tenets of Zero Trust, be sure to protect at the data level, as well as the perimeter. Identify your organization's most sensitive and toxic data, install microperimeters of control, grant security professionals full visibility into these assets, and ensure your team has a clear understanding of how the business uses the data.

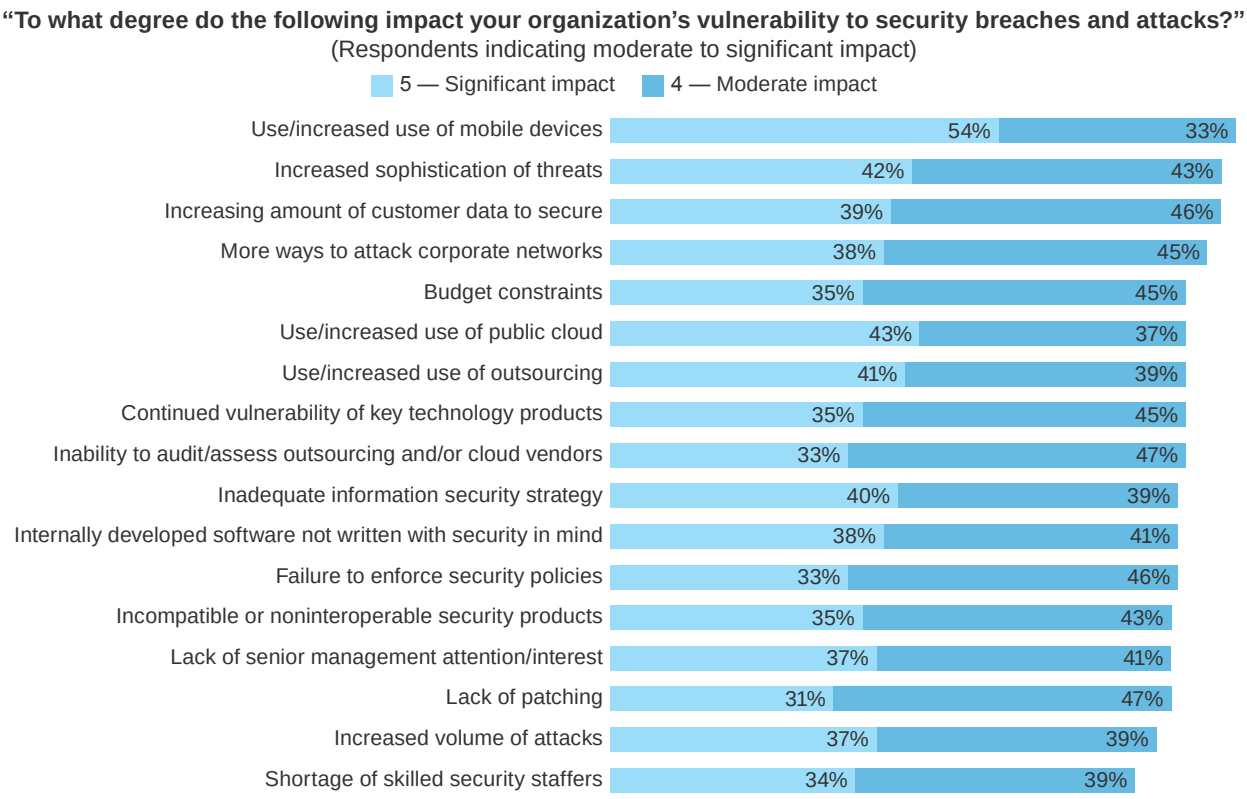
The Mutating Threat Landscape

The current threat landscape isn't evolving; it's mutating. In biology, evolution is a process spanning a period of millions of years as a result of small changes in successive generations. Mutations, in contrast, are rapid, and the changes are often dramatic and harmful.[2] Today's cyberattacks are more complex and sophisticated, and attackers are constantly changing and evolving their methods in order to evade detection and thwart security defenses. Traditional security controls that were once effective are now insufficient to protect organizations from today's highly skilled cyberattackers.

The complexity of the situation is compounded by elemental changes in enterprise networks. Security professionals no longer have clearly defined borders to protect, in the form of a limited and highly restricted user base, with a visible set of threats such as worms and viruses. The increased use of cloud computing and proliferation of mobile and wearable devices with network connectivity mean organizations need to worry about protecting multiple points of attack (see Figure 1). Users now extend beyond the traditional enterprise — customers, business partners, and contractors add a layer of complexity to implementing security measures. This "extended enterprise" is constantly changing with the movement of users, the introduction of new technologies, global expansion, and the integration of new partners and supply chains.[3]

In recent years, high-profile breaches — with far-reaching and devastating consequences — have peppered headlines. In 2013, a national retailer reported a massive data breach that affected nearly 110 million customers, including the theft of 40 million credit card numbers.[4] The fallout was massive: The CIO was fired, the CEO resigned, and earnings and revenue plummeted.[5] Also, the retailer faces a $10 million settlement stemming from a class-action

FIGURE 1
Multiple Factors Contribute To Security Vulnerability



Base: 150 IT security decision-makers at midlevel US organizations that have implemented a next-generation firewall
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2015

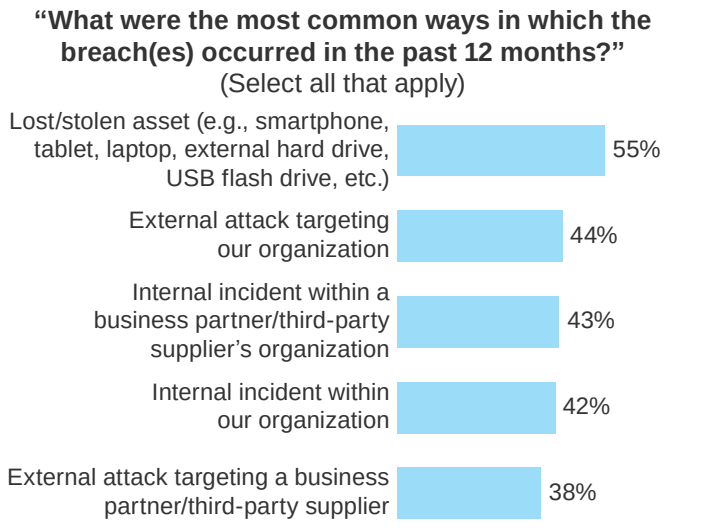
lawsuit.[6] A December 2014 breach at a leading media and entertainment company resulted in online leaks of sensitive employee information as well as full copies of movies yet to be released in theatres.[7] In May of this year, the IRS disclosed that cybercriminals had gained access to the tax returns of approximately 104,000 individuals, using that information to request 15,000 fake refunds totaling $50 million.[8] Breaches perpetrated by insiders captured headlines as well: The Pvt. Chelsea Manning/WikiLeaks and Edward Snowden/NSA data breaches had international implications and consequences. In both of these high-profile breaches, the "trusted user" paradigm was exploited.[9]

The harsh reality of the current threat landscape means security professionals should assume:

› **It's no longer a question of *if* your organization will experience a security breach, but *when*.** Eighty-seven percent of the IT security professionals surveyed said their organizations had experienced at least one breach within the past 12 months; 23% had six or more incidents. But what about the 13% who indicated their organizations were breach-free? They could be very fortunate, but a more likely scenario is that they've actually been compromised and just don't know it yet. Some attacks can extend over several months before being discovered, and in many cases, a third party — not the breached organization — unearths the incident.[10] To say you have never been breached is no longer an honest statement, as most organizations just don't know.

FIGURE 2

Both Internal And External Sources Pose Credible Threats



Base: 130 IT security decision-makers at midlevel US organizations that have implemented a next-generation firewall and have experienced a breach in data security over the past 12 months

Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2015

› **The threat is everywhere.** The "extended enterprise" means cybercriminals have multiple access points through which breaches can occur. Among those organizations surveyed that had experienced a breach within the past year, internal incidents were as likely to be a source of breaches as external attacks (see Figure 2).

› **Continued investment in network security is mandatory.** With constantly shifting threat vectors, more sophisticated attacks, and well-organized attackers, organizations need to invest in security infrastructure and strategies to ensure their organizations are protected. In the study, 96% of the security professionals we surveyed reported increases in their network security and operations budgets for 2015; 67% increased budgets by 6% or more.

Say Goodbye To "Trust But Verify" And Adopt Zero Trust

This rapidly changing threat landscape necessitates a new approach to network security. Protecting the perimeter is not enough — security professionals need to take a long, hard look at the measures they have in place and identify gaps in protection.

THE TRUST MODEL IS BROKEN

For years, security professionals based their network security approach on the premise that as long as they had strong protections in place at the perimeter, malicious forces would not be able to penetrate it. This is no longer an effective way to enforce security. Once attackers get past perimeter security measures, they have access to everything on your organization's network.

Within the network perimeter, it is more difficult to distinguish "trusted" from "untrusted" network traffic. Current security devices are designed with the assumption that "trusted" and "untrusted" network interfaces are easily identified — ports are actually labeled with these designations. But it is a mistake to assume that any user or device within your network perimeter is trustworthy. Furthermore, Forrester has found that while many

organizations say they take a "trust but verify" approach to internal network traffic, most "trust" but fail to "verify" due to the difficulty in actually executing verifications. Hanging your security hat on a "trust but verify" model for internal traffic leaves your network vulnerable — not only from external agents penetrating the perimeter, but to malicious insiders in positions of "trust."[11]

ZERO TRUST IS THE ANSWER

If the current trust model is broken, what can organizations do to fix it? Security professionals must abandon the idea that users, devices, and networks can be classified as "trusted" and "untrusted" and adopt a new approach, where all network traffic is untrusted. Forrester calls this new model "Zero Trust." In a Zero Trust approach to security:

- **Trust is never assumed.** Never assuming trust forces you to constantly monitor all network traffic for questionable activity and classify data and policies based upon the information captured.
- **Sensitive data is always protected.** Zero Trust takes a singular approach to data protection, regardless of device type, location, or user: Devices are securely connected at all times. And just because a device is located on a trusted network, doesn't mean it has unlimited access to data. This approach means security professionals must have more granular control over data access.
- **Security teams fully understand the data they're protecting.** It's impossible to create — never mind enforce — an effective security strategy if you don't have insight into your organization's most sensitive or harmful data. Zero Trust is data-centric: Sensitive data is protected by microperimeters of control, security professionals have full visibility into these assets, and there is an in-depth understanding of how the business uses the data.[12]

Next-Generation Firewalls Are The Cornerstone Of Zero Trust

Advances in firewalls make the Zero Trust infrastructure possible. In a Zero Trust network, next-generation firewalls act as "segmentation gateways," taking security controls found in individual point products (firewalls, intrusion prevention systems, web application firewalls, content-filtering gateways, network access controls, VPN gateways, and other encryption products) and embedding them in a single solution.[13] Unlike traditional firewalls, these powerful appliances can be placed at the center of the network — in front of the data they need to protect — rather than at the edge of the network, which is a core tenet of Zero Trust. This provides visibility into data access and greatly increases your chances of discovering an intrusion before it escalates into a data breach. Survey data reveals that:

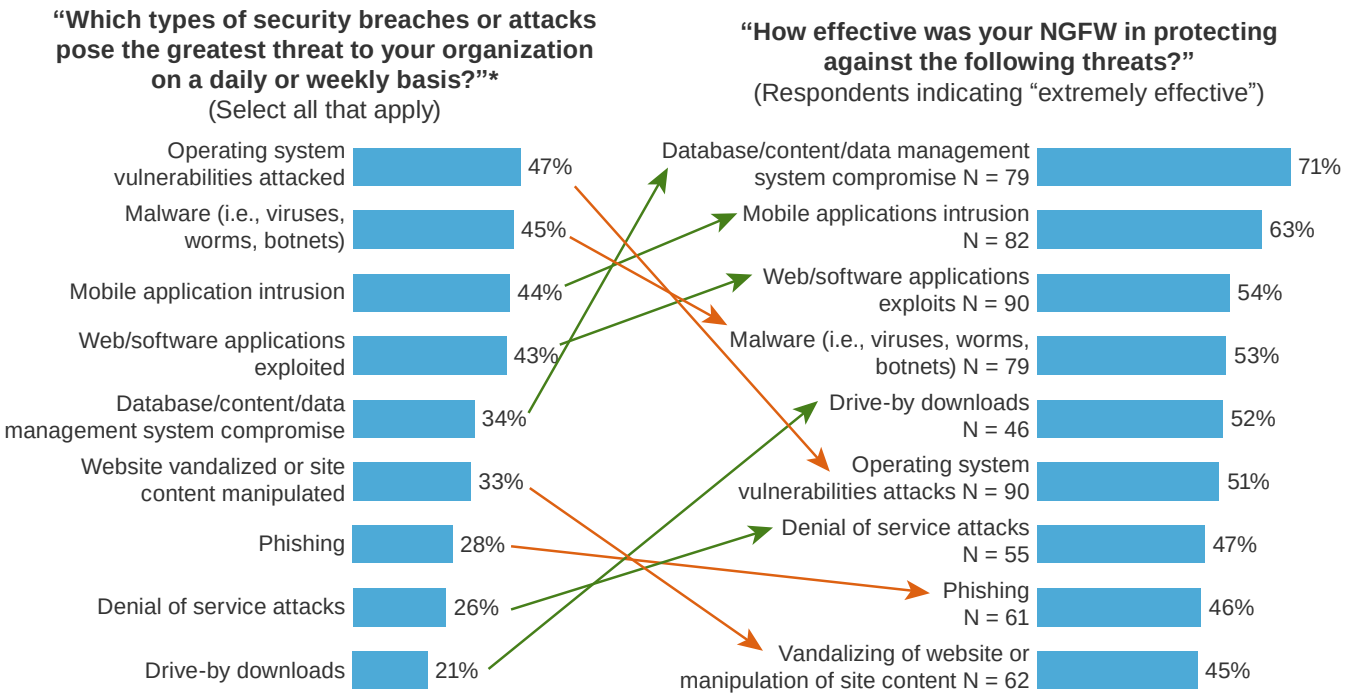
- **NGFW adoption is poised for growth.** According to a 2014 Forrester survey on global security trends, midlevel organizations (defined as 500 to 4,999 employees) in the US are already taking steps toward Zero Trust. While 50% of organizations had implemented NGFWs or had plans to expand their implementation, another 22% planned to adopt NGFWs within the next 12 months.[14]
- **NGFWs provide effective protection against today's security threats.** Today's security teams are challenged with continuously protecting their organizations from a host of threats. Operating system vulnerabilities, malware, mobile application intrusions, web/software application exploits, database/content/data management system compromises, among other types of breaches, threaten enterprise networks every day (see Figure 3). Because NGFWs can be deployed in front of sensitive data, they are very effective in protecting against these threats.

Best Practices For Evaluating A Next-Generation Firewall

To take the first step on the road to Zero Trust, it is critical to lay the groundwork by implementing a NGFW. Before you jump in, however, it is important to weigh business and technology considerations, have in-depth insight into your current environment, and fully evaluate and test vendor solutions. Forrester's study identified the following best practices:

- **Get a clear understanding of the implications of implementing a NGFW on both your infrastructure and staffing and budgetary resources.** It may seem like a no-brainer, but it is important to not only evaluate the technical aspects of a NGFW implementation, but the impact on resources as well. Technical factors, such as performance, security effectiveness, compatibility, and flexibility of the platform, were top of mind among survey respondents when evaluating NGFWs, but they also factored in cost, implementation time, and the IT resources needed to manage the solution (see Figure 4).

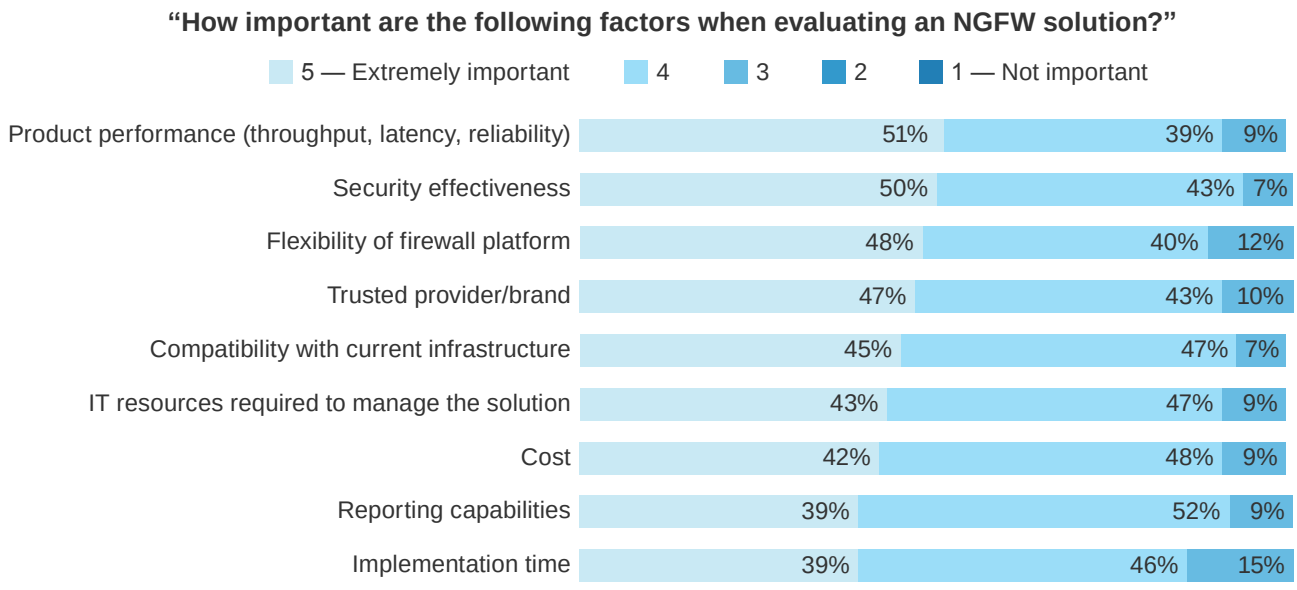
FIGURE 3
Next-Generation Firewalls Combat Multiple Threats



*Base: 150 IT security decision-makers at midlevel US organizations that have implemented a next-generation firewall

Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2015

FIGURE 4
Consider Both Infrastructure And Resource Implications



Base: 150 IT security decision-makers at midlevel US organizations that have implemented a next-generation firewall

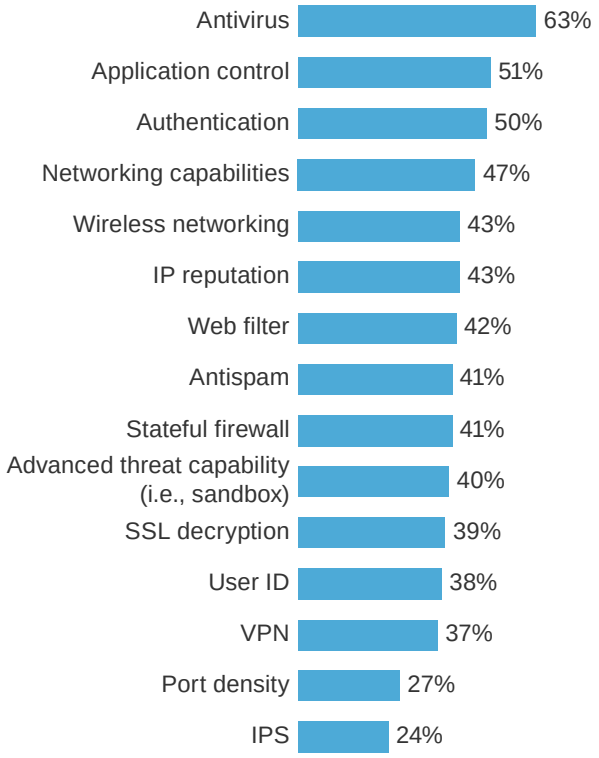
(percentages may not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2015

- **Get the right feature fit.** Failure to understand which features are most appropriate and will provide the best functionality for your organization can lead to challenges and gaps in protection down the line. Next-generation firewalls offer security professionals a single solution for integrating multiple functions traditionally found in standalone products. The vast majority of survey respondents placed high priority (a 4 or 5 rating on a 5-point scale, where 5 was "top priority") on all NGFW product features during the evaluation phase. Once they implemented the NGFW, however, most used just select features (see Figure 5). They pointed to configuration challenges (61%), too much noise (40%), and a slowdown in throughput (39%) as the primary reasons for using fewer features. This implies a limited understanding of NGFW functionality and immature adoption. If you are running point products with capabilities redundant with a NGFW, you may encounter inefficacies. Furthermore, only utilizing antivirus tools and not using advanced threat capabilities, user IDs, and an intrusion prevention system (IPS) will leave your organization open to advanced threats. Make sure your security team is familiar with NGFW capabilities, eliminate redundancies that cause configuration and performance issues, and take full advantage of the available features to ensure your network is protected against the full spectrum of threats
- **Identify the contenders.** Do your homework. Identify the NGFW vendor solutions that best fit your requirements. Sixty-one percent of the security professionals we surveyed would consider a broader selection of vendors if they could do it again. Start by doing some research online, reading analyst evaluations, and consulting peers at other organizations. Once you've identified potential vendors, utilize product demos, a proof of concept, and bake-offs to better understand vendor solution functionality (see Figure 6). Third-party testing will also help generate your shortlist by providing you with unbiased, side-by-side product comparisons. Eighty-eight percent of the security professionals surveyed relied on third-party testing when evaluating NGFW solutions.
- **Test before you buy.** Don't rely on third-party tests alone — be sure to thoroughly test solutions in your own environment. Take a lesson from survey respondents: If they could go back in time, 71% said they would conduct more extensive testing of capabilities. Some key tests to look at are performance, including performance with application controls activated, raw packet processing performance, and "real world" traffic; stability and reliability, such as persistence of data, high availability, and power fail, among others; and security effectiveness, including firewall policy enforcement, application control, user/group identity aware policies, and an IPS. For a detailed list of tests, see Appendix C.

FIGURE 5
Organizations Are Using Limited NGFW Features

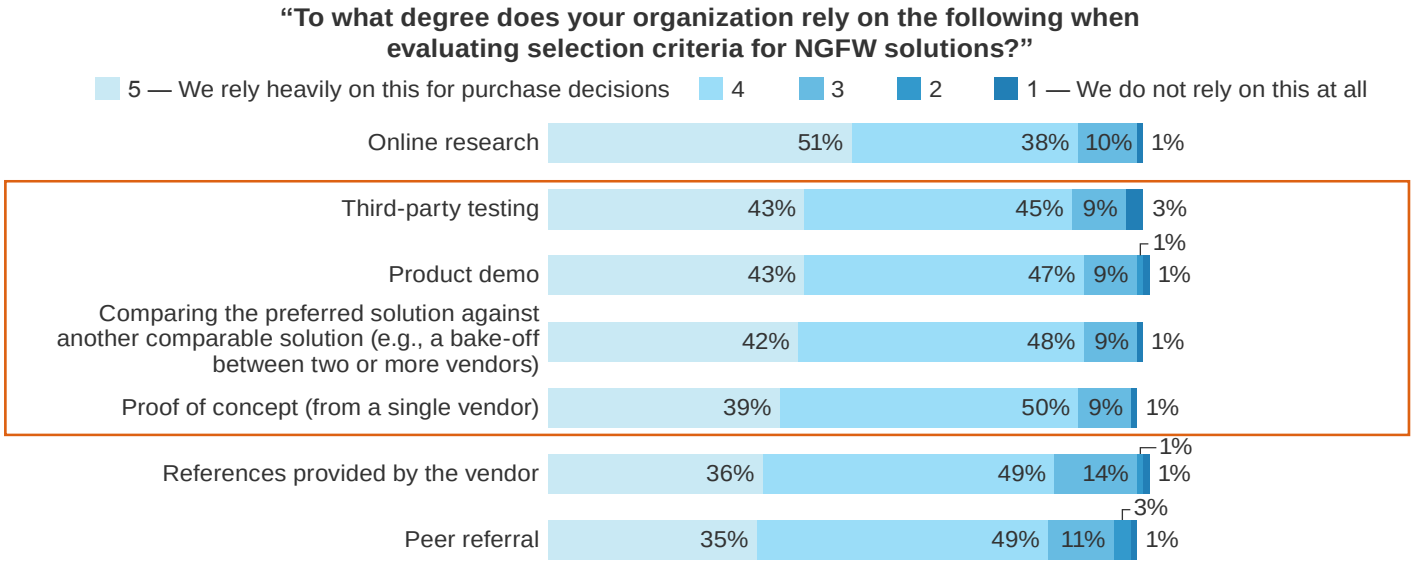
"Once you implemented your NGFW, which of the following product features were actually used?"
(Select all that apply)



Base: 150 IT security decision-makers at midlevel US organizations that have implemented a next-generation firewall

Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2015

FIGURE 6
Do Your Research To Generate A Shortlist

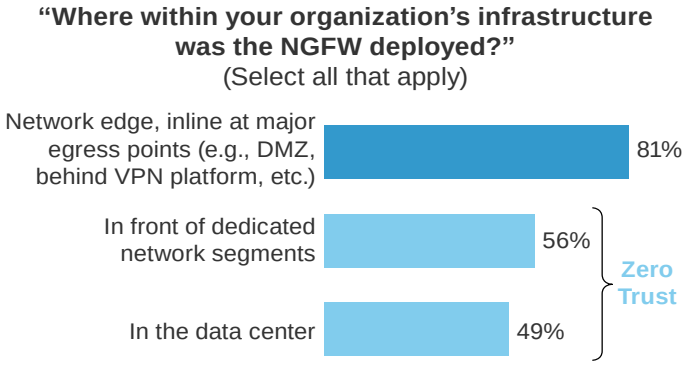


Base: 150 IT security decision-makers at midlevel US organizations that have implemented a next-generation firewall
(percentages may not total 100 because of rounding)
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2015

› **Create data-centric microperimeters.** As you plan your NGFW implementation, it is important to identify key points in your network for deployment. Eighty-one percent of the security professionals surveyed deployed a NGFW on the network edge, protecting against web-based threats (see Figure 7). But a Zero Trust approach means protections need to be placed in the center of the network, in front of your organization's most sensitive data. Fifty-six percent of survey respondents deployed NGFWs in front of dedicated network segments, effectively creating microperimeters, and 49% deployed them in the data center — an indication that midlevel enterprises are well on their way to adopting Zero Trust.

Zero Trust is becoming widely adopted by leading, cutting-edge organizations.[15] As data breaches continue to devastate businesses and governments, more security organizations are under pressure to create new ways of protecting their critical data by turning to a Zero Trust data-centric network security model powered by NGFW technology.[16]

FIGURE 7
Next-Generation Firewall Deployment



Base: 150 IT security decision-makers at midlevel US organizations that have implemented a next-generation firewall
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2015

Key Recommendations

Today's mutating threat landscape renders traditional security controls and approaches ineffective. The definition of "user" now goes beyond the traditional enterprise, to an extended enterprise consisting of customers, business partners, and contractors. In this new world, former notions of trust — including the mantra "trust but verify" — are outdated. Security professionals must abandon the idea that users, devices, and networks can be classified as "trusted" and "untrusted" and adopt a new approach, where all network traffic is untrusted. Forrester calls this new model "Zero Trust." With Zero Trust, you constantly monitor all network traffic for questionable activity and classify data and policies based upon the information captured and require more granular control over data access. In a Zero Trust network, next-generation firewalls act as "segmentation gateways." Unlike traditional firewalls, NGFWs can be placed at the center of the network — in front of the data they need to protect — rather than at the edge of the network, which is a core tenet of Zero Trust. To select your NGFW, consider the following best practices in your evaluation:

- **Evaluate the impact on resources and staff in addition to technical specifications.** Factor in the IT resources needed to manage the solution, what performance you will need, how long it will take to implement, and at what cost. This will help to reduce issues relating to reporting, maintenance, implementation, and performance.
- **Understand which features are most appropriate for your organization.** NGFWs take security controls found in individual point products (firewalls, intrusion prevention systems, web application firewalls, content-filtering gateways, network access control, VPN gateways, and other encryption products) and embed them in a single solution. Determine which capabilities and features you need. This will help to reduce challenges and gaps in protection after deployment, as well as eliminate redundancies with other technology solutions.
- **Consider a broad range of vendors.** Compare and contrast via product demos, a proof of concept, and bake-offs to better understand vendor solution features. Third-party testing can also provide additional insight to help in narrowing down your shortlist and criteria for evaluation.
- **Test multiple solutions before you buy one.** Test and compare solutions in your environment or based on your requirements before you make your choice. Key tests would evaluate performance, stability and reliability, and security effectiveness.
- **Identify key points in your network for deployment.** Deployed on the network edge, your NGFW will protect against web-based threats. To take a Zero Trust approach, deploy your NGFW in front of your most sensitive data, such as in front of a dedicated network segment or data center.

Next Steps

Zero Trust is a fundamentally different approach and way of thinking for information security. Next-generation firewalls are a key enabler for implementing and applying Zero Trust concepts. However, it's more than a matter of just deploying a NGFW. As you embark on your Zero Trust journey and begin to evaluate NGFWs:

- **Evangelize Zero Trust to gain internal support, particularly from executives.** Change how your organization thinks about trust concepts and conventional wisdom about information security. Illustrate why traditional notions are outdated and ineffective in today's threat landscape and extended enterprise. Explain how a Zero Trust strategy addresses traditional security's shortcomings, and the necessary steps involved with implementing this strategy.
- **Start a cross-functional Zero Trust working group.** Involve representatives from security, networking, application development, and enterprise architecture. To implement Zero Trust concepts and technologies that support this model of information security, you will need everyone on board and working together to brainstorm and whiteboard the immediate and long-term uses of a Zero Trust network architecture.
- **Map out your data flows.** Start by identifying and classifying your most sensitive data. Map how this data flows across your network and between users and resources. This initial application flow mapping will illuminate how the flow currently works today, but use this as an opportunity to redesign a more optimal flow if necessary. Your Zero Trust network design is based on how transactions flow across your network and where microperimeters are placed around your most sensitive data. Use a NGFW to enforce this microperimeter.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 150 midlevel organizations (500 to 2,500 employees) in the US to identify the purchase considerations, challenges, and best practices associated with implementing next-generation firewalls. Survey participants included IT/security and enterprise IT architecture decision-makers involved with security technologies. Respondents had to be at organizations with current or past next-generation firewall implementations in order to participate. Questions provided to the participants asked about their organizations' network security strategies and practices and next-generation firewall evaluation and implementation processes. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in April 2015 and was completed in May 2015.

Appendix B: Supplemental Material

RELATED FORRESTER RESEARCH

"Three Technical Innovations Will Ignite Zero Trust," Forrester Research, Inc., May 5, 2015

"Understand The Business Impact And Cost Of A Breach," Forrester Research, Inc., January 12, 2015

"Rules Of Engagement: A Call To Action To Automate Breach Response," Forrester Research, Inc., December 2, 2014

"No More Chewy Centers: The Zero Trust Model Of Information Security," Forrester Research, Inc., October 7, 2014

"Market Overview: Network Segmentation Gateways, Q4 2013," Forrester Research, Inc., December 12, 2013

Appendix C: Next-Generation Firewall Tests

FIGURE 8
Next-Generation Firewall Tests

Performance tests	Stability and reliability tests	Security effectiveness tests
Raw packet processing performance (UDP traffic)	Blocking under extended attack	Firewall policy enforcement
Latency — UDP	Passing legitimate traffic under extended attack	IPS
Maximum capacity	Behavior of the state engine under load	Application control
HTTP capacity with no transaction delays	Protocol fuzzing and mutation	User/group identity (ID) aware policies
Application average response time — HTTP	Power fail	
"Real world" traffic	Redundancy	
With IPS activated	Persistence of data	
With application controls activated	High availability (HA)	
With antivirus activated		
With web filtering activated		
With SSL inspection activated		

Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2015

Appendix D: Endnotes

[1] Source: “Three Technical Innovations Will Ignite Zero Trust,” Forrester Research, Inc., May 5, 2015.

[2] Source: “Defend Your Data From Cyberthreats With A Zero Trust Network,” Forrester Research, Inc., June 11, 2014.

[3] Source: “Defend Your Data From Cyberthreats With A Zero Trust Network,” Forrester Research, Inc., June 11, 2014.

[4] Source: “Rules Of Engagement: A Call To Action To Automate Breach Response,” Forrester Research, Inc., December 2, 2014.

[5] Source: “Understand The Business Impact And Cost Of A Breach, “Forrester Research, Inc., January 12, 2015.

[6] Source: Miles Parks, “Target Offers $10 Million Settlement In Data Breach Lawsuit, NPR, March 19, 2015 (http://www.npr.org/sections/thetwo-way/2015/03/19/394039055/target-offers-10-million-settlement-in-data-breach-lawsuit).

[7] Source: “Understand The Business Impact And Cost Of A Breach,” Forrester Research, Inc., January 12, 2015.

[8] Source: “Quick Take: Fifteen Lessons For Security & Risk Pros From The IRS Get Transcript Breach,” Forrester Research, Inc., May 28, 2015.

[9] Source: “No More Chewy Centers: The Zero Trust Model Of Information Security,” Forrester Research, Inc., October 7, 2014.

[10] Source: “Three Technical Innovations Will Ignite Zero Trust,” Forrester Research, Inc., May 5, 2015.

[11] Source: “No More Chewy Centers: The Zero Trust Model Of Information Security,” Forrester Research, Inc., October 7, 2014.

[12] Source: “Three Technical Innovations Will Ignite Zero Trust,” Forrester Research, Inc., May 5, 2015.

[13] Because of the increasing demand for Zero Trust networks, Forrester envisions the development of a new product category called a network segmentation gateway, a product category that is much more than a "next-generation firewall." A segmentation gateway (SG) takes all of the features and functionality of individual, standalone security products and embeds them into a single solution. By embedding a packet-forwarding engine, a network SG becomes a device that can sit at the center of a Zero Trust network — a streamlined network that segments and protects sensitive data in microperimeters, enables the secure adoption of mobile technology and cloud services, and ensures continuous network analysis and visibility for situational awareness. Source: “Market Overview: Network Segmentation Gateways, Q4 2013,” Forrester Research, Inc., December 12, 2013.

[14] Source: Business Technographics® Global Security Survey, 2014, Forrester Research, Inc.

[15] Source: Steven Norton, “Google CIO: Enterprises Should Build ‘Zero Trust’ Infrastructure,” The Wall Street Journal, April 24, 2014 (http://blogs.wsj.com/cio/2014/04/24/google-cio-enterprises-should-build-zero-trust-infrastructure/) and Lucian Armasu, “Google Adopts Zero Trust Network Model For Its Own Cloud,” Tom’s IT Pro, May 13, 2015 (http://www.tomsitpro.com/articles/google-zerotrust-network-own-cloud,1-2608.html).

[16] Source: “Three Technical Innovations Will Ignite Zero Trust,” Forrester Research, Inc., May 5, 2015.