Industry Experts Speak Out: The Network Performance and Security Trade-Off

Zeus Kerravala
ZK Research

Neil Campbell
Dimension Data

Rik Turner
Ovum

Dr. Jim Metzler
Ashton, Metzler & Associates

Ray Maurer
Perket Technologies

Robert Smithers
Miercom

What's Next

Presented by Intel Security

intel Security

McAfee is now part of Intel Security.

Industry Experts Speak Out: The Network Performance and Security Trade-Off

What's Next

Presented by Intel Security

The Experts

Zeus Kerravala
Founder,
ZK Research
@zkerravala

Zeus Kerravala is the founder and principal analyst at ZK Research, where he provides research and advice to end-user IT and network managers and vendors of IT hardware. Prior to ZK Research, Zeus Kerravala was senior vice president and distinguished research fellow at Yankee Group. Before Yankee Group, Kerravala held a number of technical roles, including a senior technical position at Greenwich Technology Partners (GTP), where he worked with Johna Till Johnson, the founder of Nemertes Research. Kerravala holds a bachelor of science in physics and mathematics from the University of Victoria in British Columbia, Canada.

Rik Turner
Senior Analyst
Ovum

Rik Turner is a senior analyst on the infrastructure solutions team at Ovum, focusing primarily on security. Rik joined Ovum in January 2005 as European bureau chief of its ComputerWire daily IT news service. He covered fixed, wireless, and mobile networking and security. In February 2007, he became an analyst on the financial services technology team, initially covering retail banking and writing reports on online and branch banking. More recently he has developed a specialization in capital markets infrastructure. Prior to joining Ovum, Rik spent six years as an IT journalist and, before that, was a foreign correspondent for 16 years in Latin America, writing regularly for publications such as the *Financial Times, The Economist, The Independent,* and *Business Week.*

Neil Campbell
Group General
Manager, Security
Dimension Data

Prior to his current role, Neil was director of solutions for Dimension Data Australia. In that capacity, he was responsible for establishing and executing the national solutions strategy across all the Dimension Data business units, including network, communications, data center, security, and end-user computing, as well as establishing and managing all vendor and partner alliances. Neil joined Dimension Data in 2002 as security general manager and was instrumental in growing the security business unit to the point where it is now recognized by clients, analysts, and partners as a leader in the Australian market.

Dr. Jim Metzler

Founder
Ashton, Metzler & Associates
@AshtonMetzler

Dr. Jim Metzler has created software tools to design customer networks for a major IXC, has served as an engineering manager for high-speed data services for a major telecommunications company, and has been a product manager for network hardware. In addition, he has managed networks at two Fortune 500 companies and has directed market research at a major industry analyst firm. Jim's current interests include application delivery and software-defined networking (SDN). In July 2014 he published an e-book entitled *The 2014 Guide to Application and Service Delivery,* and in November 2014 he will publish an e-book entitled *The 2014 – 2015 Guide to Software Defined Networking and Network Function Virtualization*.

Ray Maurer

Chief Technology Officer, Perket Technologies
@raymaurer

As CTO, Ray is responsible for establishing and maintaining the security and information technology practices within Perket Technologies. Throughout his career, Ray has held senior technical positions, including senior lead network engineer for a large county government, project manager and senior engineer working with Fortune 1000 companies, senior engineer for the leading education technology company in the northeast, CIO for a start-up ISP, and CIO of a Fortune 500 company. While in these positions, he was responsible for the security and network practices and maintaining mission-critical departments, such as 911 emergency response.

Robert Smithers

President and CEO, Miercom
@Miercom

Robert Smithers is president and CEO of Miercom, a leading network consulting and product-testing lab. Rob has authored test reviews and articles featured in many leading business and trade publications. As CEO, Rob directs Miercom's involvement in testing the latest business technologies, including information security, next-generation firewalls, 40GE switch, contact centers, unified communications, and business continuance products and services. Robert enjoys sharing his practical expertise in assessing products with network equipment manufacturers and service providers and conducting needs analysis and installations for enterprise customers. He offers strategic consulting in the form of advanced testing and product selection services for Fortune 500 and Global 100 companies.

1 Impossible Tradeoffs

In Star Trek, it always seemed as if one second, Kirk was asking Scotty to divert more power to the shields and the next, he was demanding more power to the engines. As it turns out, this scenario isn't all that different from those regularly faced by network and security teams at large organizations.

Businesses of all types demand high performance speeds for their employees and customers. When a network goes down or is running slowly, it can mean anything from an overwhelmed IT help desk and reduced productivity to lost data and transactions.

Often, the solution is to disable some of the firewall's security features to increase throughput. However, with a different security breach making headlines each month, many organizations are learning this is no longer a risk worth taking.

Still, our survey showed nearly half of IT professionals continue to make this tradeoff, and if you believe our experts, that number is being under-reported based on what they're seeing.

> "There has always been a delicate balance. It's well known. A kind of unwritten rule, but really, there's a feeling there's not much you can do about it."
>
> Zeus Kerravala

Expert insights

Rik Turner

It's a given. One of the first things you learn is that there's a tradeoff between how secure a network is and how fast the performance is. Everyone lives with the tradeoff.

Ray Maurer

I've had so many arguments with network security guys. They are more concerned with getting somewhere in a timely fashion instead of safely.

Dr. Jim Metzler

They may well value security, but not if it means that users are unhappy with performance. This, by the way, is a classic tradeoff—people want security, but they don't want it to unduly impact the user.

44%

of IT professionals agreed or strongly agreed with the following statement:

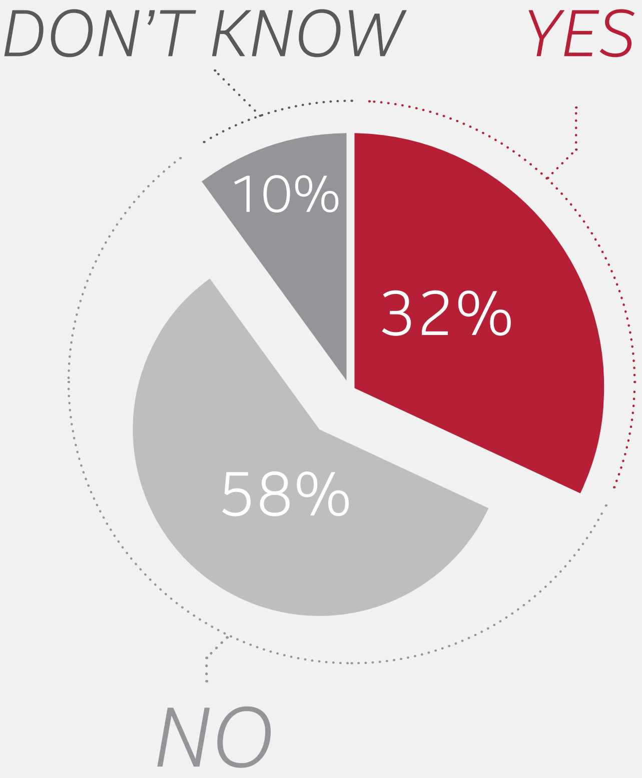
My organization must make trade-offs between network performance and security.

2 All Risk, No Reward

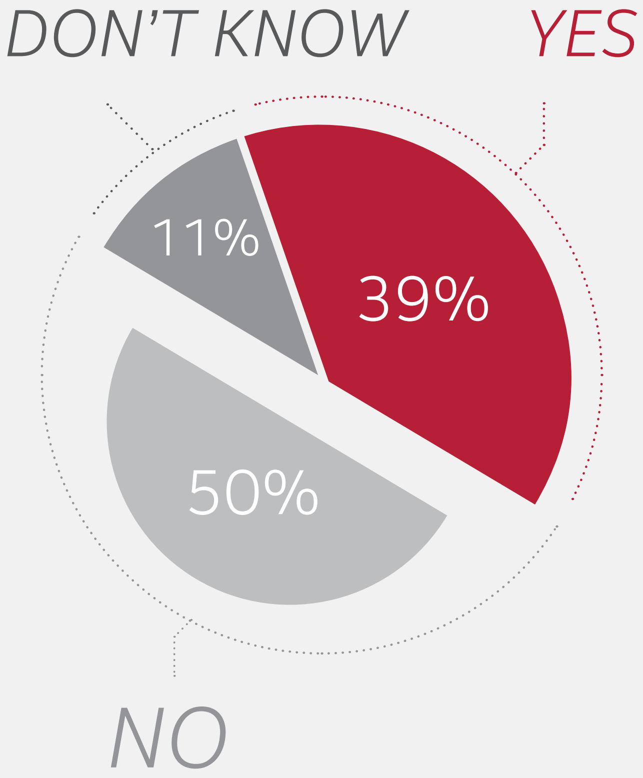
We know what would happen to the starship Enterprise if its shields were down and it were attacked by the Romulans. But what is the risk to a company when firewall features are turned off in order to boost performance?

We asked our experts. While you can likely predict their answers, it's worthwhile to hear them again, given that our survey showed a significant number of people are still choosing to turn off or never even turn on certain firewall functions.

Has your organization turned off certain firewall functions because they were impacting network performance?



Has your organization declined to enable certain firewall functions to avoid impacting network performance?



Expert insights

Ray Maurer

I get concerned about many customers and companies—that if they turn off a simple layer of protection closest to the source they will have a data leak. Depending on the type of data that is leaked, it could be devastating. Not everyone has the ability to be Target or Home Depot and withstand a huge shot to consumer confidence.

Rik Turner

Essentially, you're dumbing down your defenses in the name of faster throughput, which is a bit like removing security checks at airports so folks can board airplanes more quickly—it's great, until a plane gets hijacked.

Dr. Jim Metzler

When the company's first line of defense is not operating at full strength, the company is even more vulnerable than usual to an attack from the outside. Trading security for performance is sustainable until there is a major security issue. Then companies tend to re-think things.

Zeus Kerravala

Data theft has become a significant problem over the past few years, and this could be done much easier with some firewall filters turned off. In essence, turning off some firewall features may be akin to just turning off the firewall.

"Take a look at the current news—organizations are being more reactive than proactive when it comes to security. It's pretty obvious what will happen when DPI and other security techniques are not used. I can't fathom the quantity of data loss for organizations hit."

Robert Smithers

3 You Turned Off What?

Today's firewalls have a wide range of features, many of which are not being used to full advantage to minimize network security risks. Our survey asked respondents to identify which features they have turned off. While you might have guessed the top answer to be antivirus or something else that won't lead to a front page disaster, deep packet inspection (intrusion prevention systems, or IPS) was the top choice. IPS is what makes a next-generation firewall earn its designation as "next-generation," so our experts were in a quandary as to why a company would pay for such a valuable feature only to turn it off.

Which features below has your organization disabled in a security product to avoid impacting network performance?

DPI:
31%

Antispam:
29%

VPN:
28%

Data Filtering:
28%

Antivirus:
28%

URL Filtering:
27%

User Visibility:
23%

Application Awareness:
23%

Other:
4%

Expert insights

Rik Turner

Turning off DPI is clearly not a desirable outcome in that it implies a weaker security posture, though it is understandable that companies might do this in the name of faster throughput. There should be a way of fine-tuning IPS so it is less disruptive. Machine-learning would also be highly advantageous—an IPS system could actually improve over time as it learns more about what is and isn't threatening to a particular organization.

Ray Maurer

Hearing this sends shivers down my spine. When I hear about people turning off security they paid for because of performance decreases—this upsets me so much. I get a bad feeling knowing I had to remove security in the name of performance. I have a hard time sleeping because it is not a matter of *if* a network will be compromised, but *when*.

Neil Campbell

Turning off the DPI is an outrageous decision in concept—again, it may be a conscious decision, in which case why did the company spend the money buying such a capable firewall only to disable it, only to cripple it?

Zeus Kerravala

Turning off DPI may seem attractive from a performance perspective, but there are lots of potential risks, including loss of network security, compliance risks, and poor application performance, to name a few.

> "Turning off DPI means your IT security professionals will not be able to do the type of sophisticated analysis that is needed to stop a sophisticated hack."

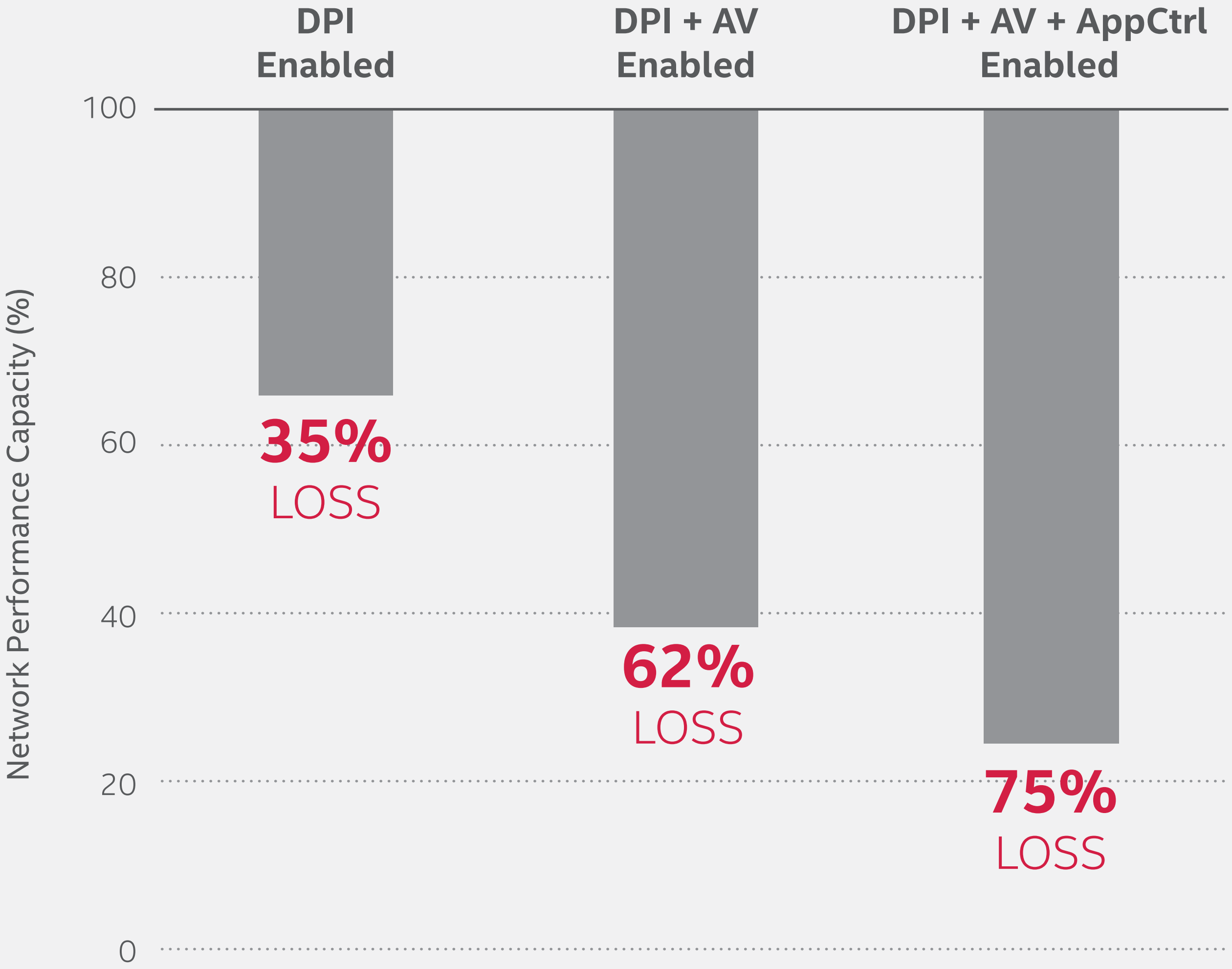
Jim Metzler

4 The Network Performance Penalty

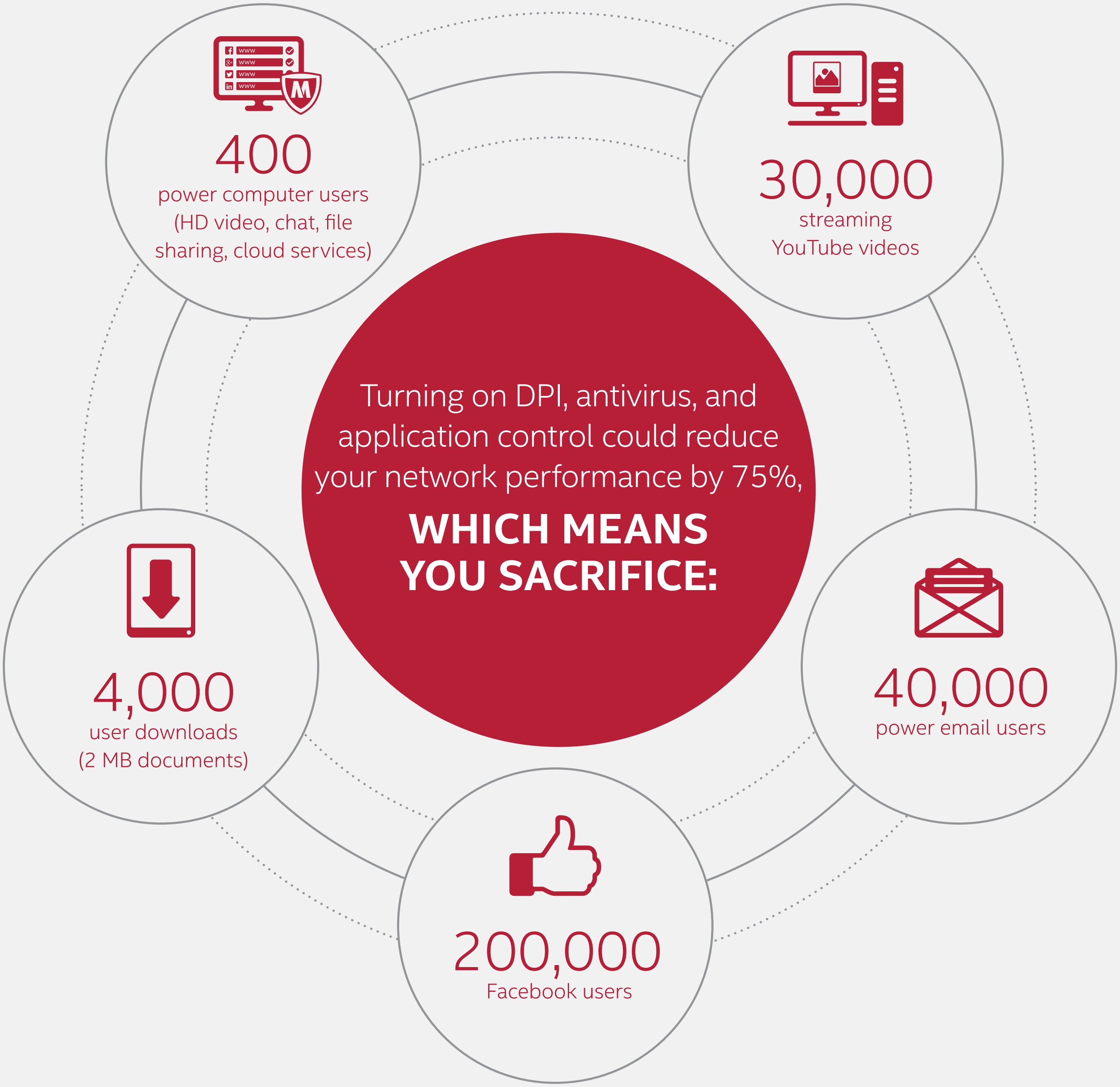
Clearly organizations are taking a sizable risk when they begin disabling security features, yet every day these decisions continue to be made and accepted. To understand the business impact that drives these decisions, we asked Robert Smithers of Miercom to quantify the impact on performance and throughput in simple terms, based on the number of firewalls he has tested.

Network Performance Loss

Firewall Performance Degradation with Features Enabled*



*Based on industry averages from *Miercom Throughput and Scalability Report* (2014). Does not include McAfee Next Generation Firewall.



Turning on DPI, antivirus, and application control could reduce your network performance by 75%,

WHICH MEANS YOU SACRIFICE:

400
power computer users
(HD video, chat, file sharing, cloud services)

30,000
streaming
YouTube videos

4,000
user downloads
(2 MB documents)

40,000
power email users

200,000
Facebook users

The above calculations are based on 75% performance reduction on a 40 Gbps firewall

5 Business Demands and Bureaucracy

The variety of answers we received illustrates the complexity of the issue—even before we address the challenges surrounding the technology.

> “A large number of enterprise companies don’t even have a designated CISO—just a CIO, who is responsible for both network and security, which contributes to the issue.”
>
> Rik Turner

Expert insights

Robert Smithers

They don't do it intentionally to be less secure, they do it because their business demands a certain level of quality of experience with usable bandwidth so the business can maintain high levels of transaction and POS orders.

Zeus Kerravala

Most CIOs don't know the extent of the issue. They have a high level understanding of the threat landscape. I don't think they are aware of the bind most of their IT reports find themselves in. Security is tough though because it's a specialized discipline.

Dr. Jim Metzler

A number of IT shops I deal with often don't have common [internal] goals. The organizations that comprise the IT organization often have different goals. You're focused on your goals and your bonus, and everyone else is focused on theirs. It's kind of fractured. There's always conflict. And there are different measurements. In some cases, bonuses may be tied to specific metrics, and people may get good-sized bonuses based on network availability.

Ray Maurer

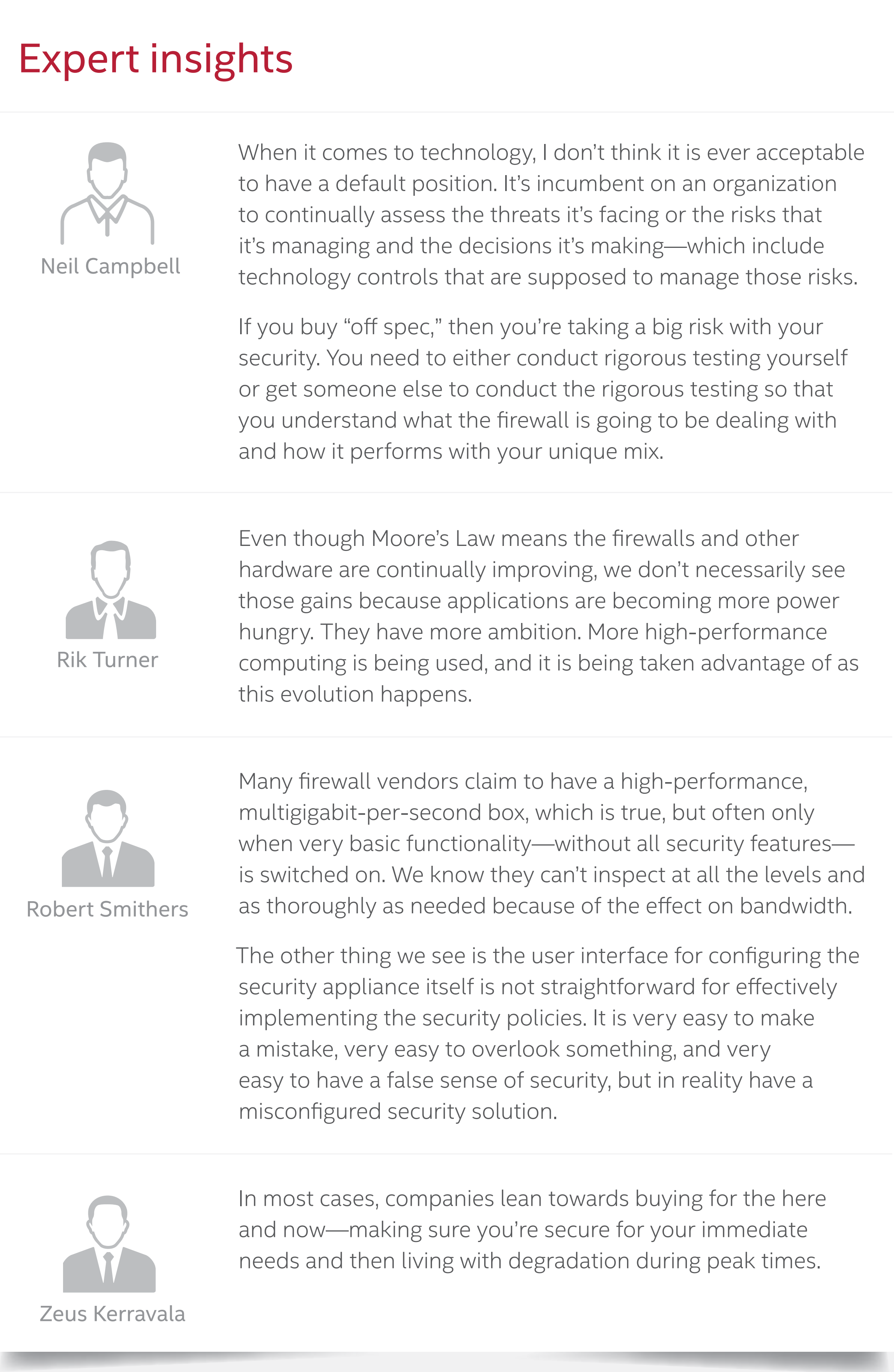
Perceived speed of business. We are all driven by a "do more with less" mandate, and the information security group is always the office of "no." IT and security need to work as one unit, and in the business environment, they should not be pitted against each other. This is a team management problem, and both IT and security need to focus on users, customers, and protecting the vision and reputation of the company.

6 Technical Challenges

When our experts were asked to define the technological issues that contribute to organizations having to choose between network security and performance, they pointed to vendors who over-promise and under-deliver, and at the customers who take vendors at their word. Other problems our experts identified: companies who think short term; power-hungry applications; poor interfaces; and, perhaps most troubling of all, organizations that fail to properly size and test their firewalls before buying.

"People think security is 'set and forget.' Many believe that all the products do what the vendors say they do. Some customers don't even check. They just turn on the firewall, and end up being surprised down the road. Or they assume they have to purchase a larger box to get everything working optimally."

Ray Maurer



Expert insights

Neil Campbell

When it comes to technology, I don’t think it is ever acceptable to have a default position. It’s incumbent on an organization to continually assess the threats it’s facing or the risks that it’s managing and the decisions it’s making—which include technology controls that are supposed to manage those risks.

If you buy “off spec,” then you’re taking a big risk with your security. You need to either conduct rigorous testing yourself or get someone else to conduct the rigorous testing so that you understand what the firewall is going to be dealing with and how it performs with your unique mix.

Rik Turner

Even though Moore’s Law means the firewalls and other hardware are continually improving, we don’t necessarily see those gains because applications are becoming more power hungry. They have more ambition. More high-performance computing is being used, and it is being taken advantage of as this evolution happens.

Robert Smithers

Many firewall vendors claim to have a high-performance, multigigabit-per-second box, which is true, but often only when very basic functionality—without all security features—is switched on. We know they can’t inspect at all the levels and as thoroughly as needed because of the effect on bandwidth.

The other thing we see is the user interface for configuring the security appliance itself is not straightforward for effectively implementing the security policies. It is very easy to make a mistake, very easy to overlook something, and very easy to have a false sense of security, but in reality have a misconfigured security solution.

Zeus Kerravala

In most cases, companies lean towards buying for the here and now—making sure you’re secure for your immediate needs and then living with degradation during peak times.

7 Time to Make a Change

Too many organizations are living under the false assumption that the tradeoff between network performance and security is a fact of doing business. It isn't. The risks, regardless of your choice, are far too high and it eventually becomes unsustainable to live with that level of risk.

We asked Neil Campbell of Dimension Data to describe his approach on finding a firewall that delivers security and performance for your needs without having to overpay for unnecessary features. Whether you're in the market for a new firewall or are being forced to make these tradeoffs, this will help you find the optimal solution.

"You need to understand your risk environment: your tolerance for risk, and the controls you need to put in place. Then you can determine whether the technology will deliver those controls just in theory or in actual practice. Finally, you address affordability. If a certain solution is too expensive, then you need to go through this process again, determine potential gaps with a lower-cost solution, and decide on what you can tolerate and how to mitigate potential issues. This is an iterative process."

Neil Campbell

1 Have we identified the risks that are present in our environment? Do we actually understand these risks?

2 Have we documented what is acceptable and unacceptable in terms of those risks?
Do we understand our appetite for risk?

3 Does the firewall we have chosen or that we are considering mitigate the risks that need to be mitigated?

4 Have we confirmed our concerns about risk mitigation through onsite testing?

5 Finally, do we have the budget? But budget should be the last thing you think about. You need to manage your risk, regardless of your budgetary constraints.

What's Next?

Our experts expressed a wide range of opinions, but there were a number of areas where they unanimously agreed. First, the job of the network and security professionals on the front line isn't an easy one given all of the challenges they face. Second, one of the most critical challenges is navigating the tradeoff between network performance and security. All of our experts agreed the tradeoff was real—and regardless of choice, every day organizations are putting themselves in a position to lose.

In today's environment you simply cannot afford to sacrifice network performance or security and hope to be successful. Fortunately, our experts believed the tradeoff could be avoided altogether. Neil Campbell outlined his recommended approach to finding a better solution through proper risk analysis and rigorous testing. When it comes to minimizing risk and ensuring security, remember what Star Trek's Captain Picard would say: "Make it so!"

WHAT DO YOU THINK?

Join the discussion
#NGFW

For more information visit
www.mcafee.com/ngfw-hub

About McAfee

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com.