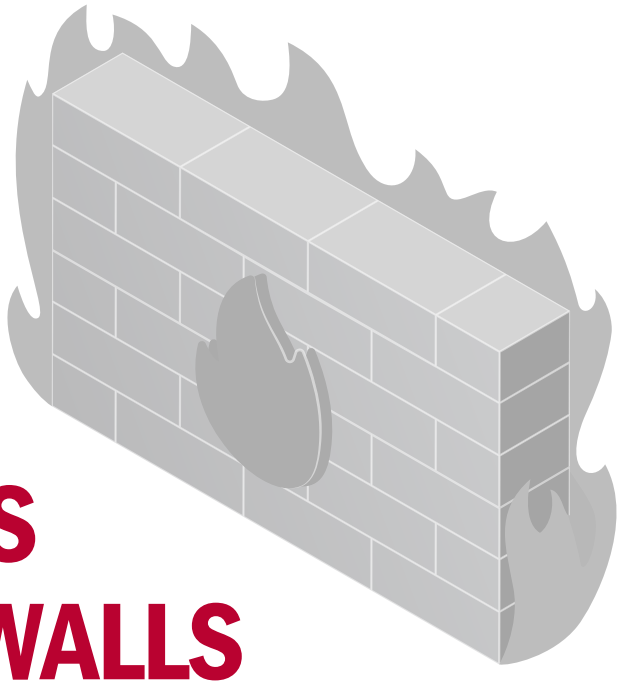
SOPHOS
Cybersecurity made simple.

LOC LES OLSON I.T. COMPANY



THE DIRTY SECRETS OF NETWORK FIREWALLS

Results of an independent survey of 2,700 IT managers in mid-sized organizations, sponsored by Sophos.

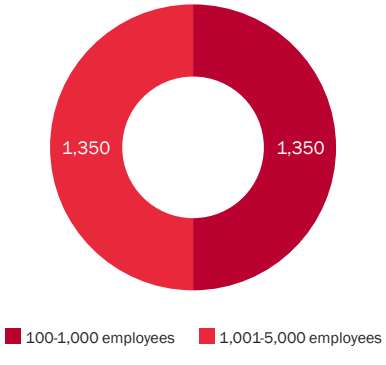
Introduction

In late 2017, Sophos sponsored an independent research study into the state of network security in mid-sized organizations across the globe. This research program explored the experiences, concerns, and future needs of IT managers, with particular focus on firewalls and network defenses.

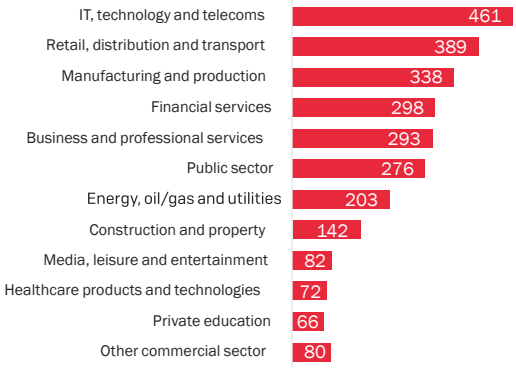
Conducted by leading UK research house Vanson Bourne, the study surveyed 2,700 IT managers in organizations of 100 to 5,000 users in 10 countries, and across five continents.

Respondent country

Organization size



Organization sector



This resulting paper reveals the dirty secrets of today's firewalls, exposing how they are failing organizations in key areas of protection, visibility, and threat response, and the impact of these failures have on IT managers across the globe.

DIRTY SECRET 1

FIREWALLS ARE FAILING TO DELIVER THE PROTECTION ORGANIZATIONS NEED

Executive Summary

- Organizations suffer on average 16 infected computers per month.
  - An average of 13 per month for 100-1,000 user organizations.
  - An average of 20 per month for 1,001-5,000 user organizations.
- 79% of IT managers want better protection from their firewall.
- Better protection is the #1 desired firewall improvement for nearly half of IT managers (48%).

Multiple infections per month is now the norm

Your firewall is the gateway between your network and the internet. Often it is also the gateway between different parts of your IT environment — for example, your DMZ and servers, various LAN segments, wireless networks, and trusted and untrusted zones. Together with your endpoint protection, it's an integral pillar of your security infrastructure.

As a result of this pivotal position, it's also your essential first line of defense against malware threats, stopping them before they can make their way onto your network, and blocking them from moving laterally or spreading across your environment — for example, if they came in on an infected USB device.

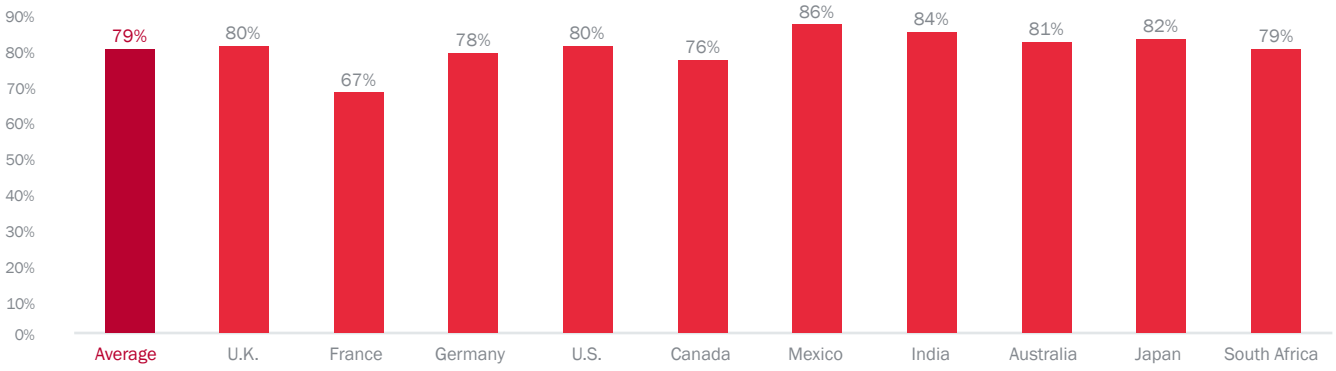
Despite the importance of its role in your threat defenses, the survey revealed that firewalls are failing organizations when it comes to delivering the protection they need. Organizations suffer, on average, 16 infected computers every month. Smaller organizations (100-1,000 users) face 13 infected computers each month, while larger ones (1,001-5,000 users) experience 20.

> 16 Infected computers per month

In light of these ongoing infections, it's unsurprising that nearly four out of five IT managers (79%) want better security from their firewalls. Indeed, better protection was the #1 desired firewall improvement for almost half of IT managers (48%). This desire for better security encompasses both perimeter security — to keep threats out — as well as internal protection to stop them spreading if they do get in.

Insufficient protection is, sadly, a global issue, with at least two-thirds of IT managers wanting better protection in every country surveyed.

% RESPONDENTS WHO WANT THEIR FIREWALL TO DELIVER BETTER PROTECTION



DIRTY SECRET 2

IT MANAGERS CAN'T TELL YOU HOW 45% OF THEIR BANDWIDTH IS CONSUMED

Executive Summary

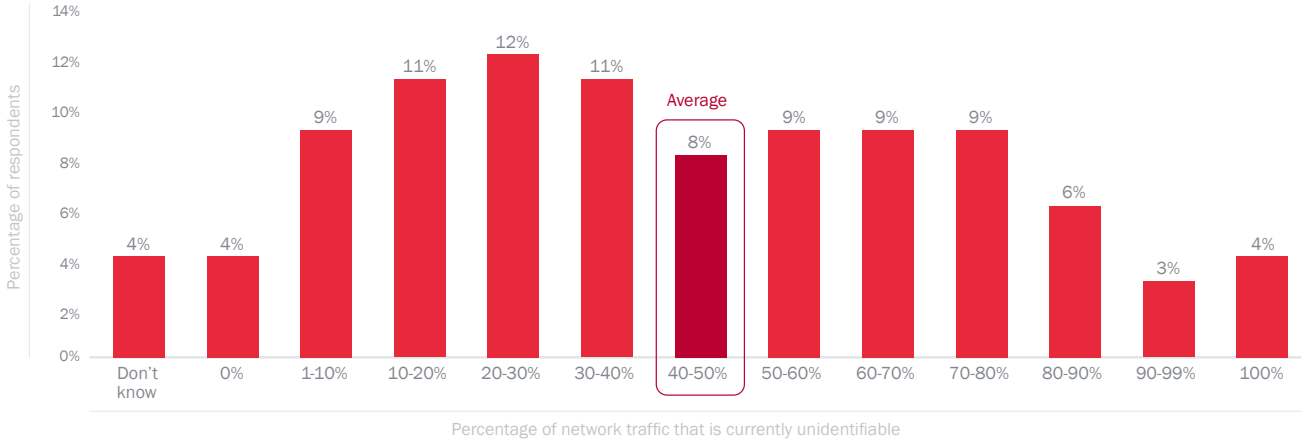
- On average, 45% of network traffic is going unidentified. As a result, it cannot be controlled.
- 70% network traffic can't be identified for nearly one in four IT managers (23%).
- Lack of visibility into network traffic leads to multiple areas of concern:
  - 84% are concerned about security.
  - 52% are concerned about productivity.
  - Four in 10 are concerned that they can't account for how their bandwidth is consumed.
  - 42% are concerned about legal liability or compliance due to potentially illegal or inappropriate content.
  - 50% have invested in custom apps that they cannot prioritize.
- Healthcare struggles most with custom applications with two-thirds (67%) having custom apps they can't identify.
- 85% of IT managers want their firewalls to deliver better visibility.

You can't control what you can't see

Controlling network traffic is an essential role of every firewall. You need to be able to prioritize the essential apps, limit non-work apps, and block malicious apps such as BitTorrent clients. The problem is if you can't see what's running on your network, you can't control it.

The survey revealed that 45% of network traffic currently can't be identified, so can't be controlled. So-called 'application control' simply isn't possible on nearly half the traffic. And nearly one in four IT managers (23%) face a much greater challenge with 70% or more of their network traffic unable to be identified.

WHAT PERCENTAGE OF YOUR NETWORK TRAFFIC IS CURRENTLY UNIDENTIFIABLE?



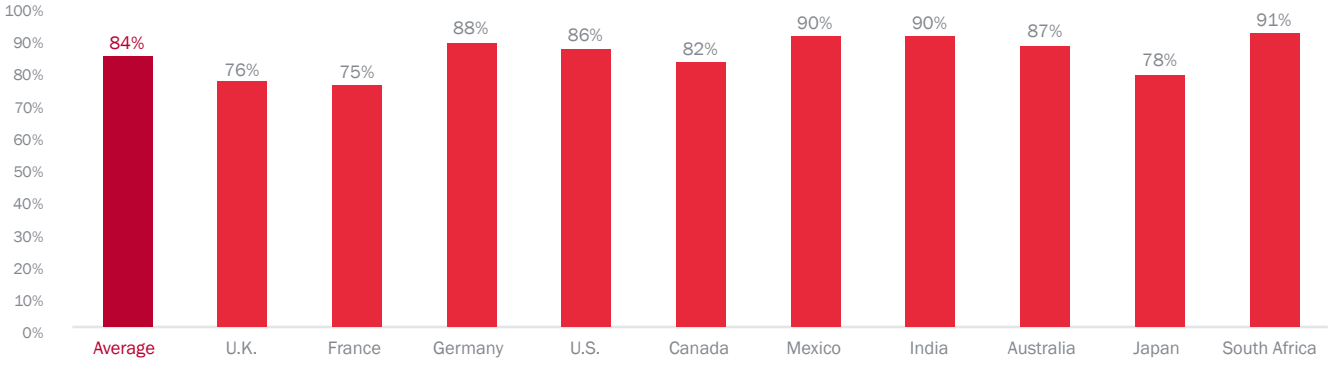
This is because the vast majority of conventional firewalls identify applications using signature-based detection, in the same manner that traditional antivirus software works. This brings with it the same issues as traditional AV — in this case applications that haven't previously been encountered and cataloged, simply cannot be seen, and even if they have a signature, many applications go out of their way to alter their networking patterns to evade detection. What's more, many applications have simply resorted to masquerading as web browsers to avoid control since nearly every firewall enables internet access for web surfing.

Like lack of protection, visibility is also a global issue, although India suffers most with 57% of its network traffic unidentifiable. Conversely, Japan is the least impacted with one-third of its traffic unable to be identified – this is likely due to stricter policy controls, a lower propensity to use SaaS/cloud applications that are often encrypted, and a lower propensity to use non-authorized applications.

Lack of visibility leads to multiple areas of concern:

Security. If you can't see what's on your network, how do you know if it is malicious, suspicious, or high risk? And how can you tell if you have any rogue users whose behavior is putting the organization at risk of a malware threat or breach? That's why security is a concern for 84% of respondents.

% RESPONDENTS THAT AGREE THAT LACK OF EFFECTIVE APPLICATION IS A SERIOUS SECURITY CONCERN



Productivity. If you can't see what's consuming your bandwidth you can't prioritize the mission-critical productivity applications and de-prioritize non-work related applications. You also don't get any insight into what people are using; productivity loss from unwanted or unnecessary apps is a concern for just over half (52%) of the organizations surveyed.

Accountability. In today's 'internet everywhere' era and prevalence of cloud-based apps, bandwidth has become both a critical business asset as well as a significant financial overhead. Organizations look to their IT teams to account for how this valuable resource is being used, but the lack of visibility into network traffic makes this all-but impossible. As a result, on average, four in 10 IT managers worry that they are unable to account for how their bandwidth is being consumed.

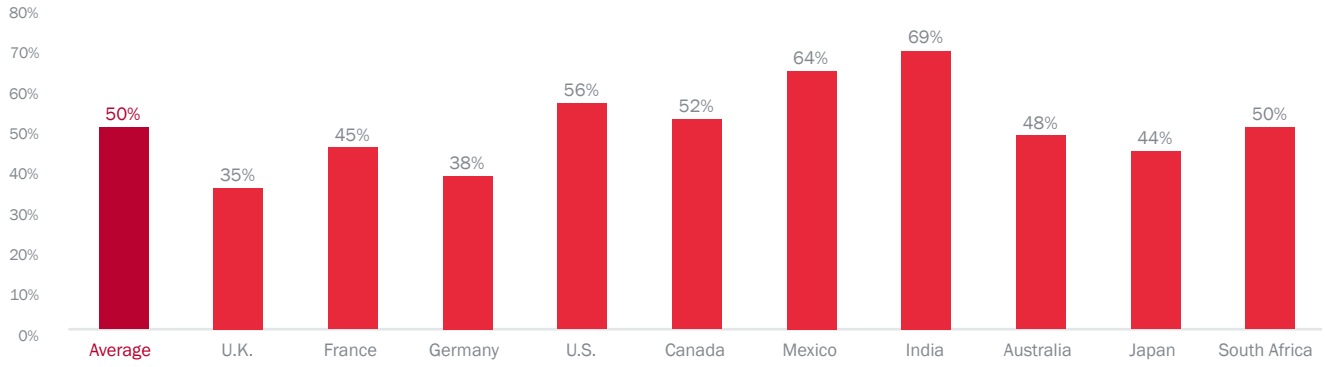
The survey revealed significant regional variations when it comes to accountability. IT managers in India (61%) and South Africa (55%) worry most on this score, while conversely those in Japan (28%) and Germany (30%) worry least. This likely reflects differing business practices around the globe, as well as different expectations around adherence to company policies.

Legal liability and compliance. While IT managers in the countries surveyed face differing legal and compliance obligations, they are united in worrying that they may be downloading, hosting, or distributing illegal or inappropriate content. On average, 42% share this concern, with India (52%) and the UK (47%) topping the list. Without the ability to see what's running through the network, IT managers can't ensure that it's all above board, putting their organizations at risk of non-compliance.

Return on Investment (RoI). Custom vertical or business applications are increasingly common and a significant investment for any business. They range from programs that have been tweaked to meet a particular business need to 100% bespoke applications custom-built for one organization. The survey revealed that 50% of organizations have custom networked applications that their firewall cannot identify. As a result, they are unable to prioritize them, limiting their ability to maximize their RoI from the application and keep their users working at top efficiency.

RoI is another area where we see huge fluctuation between regions. India, Mexico, and the U.S. have an above average number of custom apps they can't identify, while the U.K. is bottom of the list with just 35%. This variation likely reflects differing propensity to invest in custom apps rather than off the shelf, as well as visibility issues.

% RESPONDENTS WITH CUSTOM APPS THE FIREWALL CAN'T IDENTIFY



All industries struggle with custom business applications that they can't identify, but healthcare suffers more than most. Two-thirds of healthcare organizations have custom applications that their firewall can't identify, and therefore they cannot control. This is likely a result of healthcare organizations having a higher propensity to have custom networked applications to support specialized needs, as well as an aging infrastructure.

85% agree: Visibility is a top priority

As we've said, you can't control what you can't see. That's why 85% IT managers agree that they want their firewalls to deliver better visibility. This would enable them to:

- Reduce security risk by identifying risky users and applications.
- Increase productivity by controlling non-work related application traffic.
- Optimize bandwidth for business use.
- Minimize legal liability and compliance concerns by blocking illegal or inappropriate content.
- Maximize RoI on custom business applications.
- Account for their network traffic.

> 85% Want their firewall to deliver better visibility

DIRTY SECRET 3

INEFFECTIVE FIREWALLS ARE COSTING YOU TIME AND MONEY

Executive Summary

- It takes on average 3.3 hours to identify, isolate, and remediate infected computers.
- On average, organizations are spending seven working days per month remediating infected computers.
  - Smaller organizations (100-1,000 users) spend on average five working days a month on remediation.
  - Larger organizations (1,001-5,000 users) spend on average 10 working days a month on remediation.
- 99% agree it would be useful if the firewall could isolate infected machines automatically.
- 97% would likely get their endpoint and firewall protection from the same vendor if it improved detection rates and automated incident response.

Over one week every month is lost to remediating infected computers

As we've already seen, firewalls are failing to deliver the protection that organizations need. As a result, IT teams are spending significant time and effort fixing infected computers. To ascertain the extent of the issue the survey asked two key questions:

1. How long does it take, on average, to identify, isolate, and remediate infected machines?
2. On average, how many infected computers does your organization deal with each month?

The results were startling.

On average, it takes 3.3 hours, or nearly half a working day, to identify, isolate, and remediate an infected computer. Interestingly, smaller organizations took less time than larger ones, with an average of 2.9 hours for 100-1,000 user organizations, going up to 3.9 hours for 1,001-5,000 user organizations.

> 7 days spent remediating infected computers each month (based on 7.5 hr day)

Organizations experience, on average, 16 infected computers per month. Based on a 7.5 hour day, this means that they are spending 7 working days each month remediating infections.

Organization site	# Infected computers per month	Hours to clean up a computer	Total clean up hours per month	# days per month (7.5 hour = day)
100 – 1,000	13	2.8	36.4	4.9
1,001 – 5,000	20	3.9	78	10.4
Average	16	3.3	52.8	7.04

When considering the implications of this clean-up time we need to look at both the immediate time and resource cost, as well as the opportunity cost — what could the IT team have been doing instead? IT teams are under ever-growing pressures, both from increasing demands on their time as well as a significant shortage of IT security expertise. 70% of cybersecurity professionals claim their organization has been affected by the cybersecurity skills shortage [i]. Most can ill-afford to spend seven days every month fixing infected computers.

Given the time and cost implications of fixing infected computers manually, it's not surprising that 99% IT managers want their firewall to automatically isolate compromised systems, with 90% agreeing that it would be 'extremely' or 'very' useful. A similar percentage (97%) would likely get their endpoint and firewall protection from the same vendor in order to enjoy improved detection rate and automated response.

Conclusion

The dirty secrets of today's network firewalls are now out in the open: they are failing to deliver key capabilities organizations need. From network protection, to visibility, and response, the current experiences of IT managers falls well short of what they want and need to secure their organizations. In light of this, it's time for organizations to take a fresh look at their network security and put in place solutions that better meet their needs.

[i] The Life and Times of Cybersecurity Professionals. The Enterprise Strategy Group, 2017

Further reading

Firewall best practices to block ransomware paper – How recent ransomware attacks like WannaCry and Petya took place and the features firewalls need to stop these types of attack.

Why network admins need complete application visibility paper – An in-depth look at the difficulties of network traffic visibility and what can be done to solve them.

Firewall buyers guide – Key technologies and features to look for when choosing a firewall, as well as questions to ask vendors.

Sophos XG Firewall: Solving the problems with network firewalls

Sophos XG Firewall is built to meet the evolving needs of IT managers, and addresses the key challenges with firewalls today.

Protection. XG Firewall stops unknown threats with a comprehensive suite of advanced protection including deep learning, IPS, ATP, Sandboxing, and Dual AV.

Visibility. XG Firewall exposes hidden risks with visibility of all apps, top risk users, advanced threats, suspicious payloads and much more.

Response. XG Firewall automatically responds to incidents by instantly identifying and isolating infected systems until they can be cleaned up.

See the real-world recognition that XG Firewall has been receiving:

NSS Labs – “Top rated”

SC Media – “Very creative convergence of a lot of solid functionality”

PC Pro – “A highly versatile UTM appliance combining top performance with stunningly good value”

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

4-4-18 NA (TN)

SOPHOS