DYNAMIC
GROUP - INDIA
www.dynamicgroup.in | info@dynamicgroup.in
(91) 9025 66 55 66

The State of Computer Security and Software-level Solutions

Table of Contents

Introduction	3
Desktop/laptop security across the globe	4
The lack of multi-factor authentication	6
Challenges to effective security	7
Conclusion	8

Introduction

Every day an average of 30,000 new websites are identified as distributing malicious code to site visitors.[1] This helped contribute to the 43% of U.S. companies that experienced data breaches in 2014 alone.[2]

But not all dangers to computers and laptops come from malicious code picked up over the Internet. A study by IDC and the National University of Singapore revealed that in 2014, businesses worldwide would spend nearly $500 billion to deal with the problems caused by malware on pirated software.[3]

In its 2014 "Data Breach Investigation Report," Verizon found that 40% of "threat events" involved malware, 71% targeted end-user devices, 92% were initiated by outsiders, and 75% were conducted for financial motives.[4]

Organizations know the danger and understand the importance of securing their computers against cyber-attacks and malicious applications. After all, 93% of respondents in a Spiceworks survey of over 650 IT decision-makers in the Americas (US, Mexico and Brazil), EMEA (UK, France and Germany), and APJ (China, Japan and India) said their organizations have security solutions for their desktops and laptops. These solutions are securing on average 84% of their organization's desktops and laptops.[5]

The survey also revealed that many of these organizations are simply using software-level solutions, which are increasingly ineffective—leaving IT professionals unsatisfied. Based on the recent Spiceworks survey, this white paper will explore worldwide trends and pain points in desktop and laptop security solutions and illustrate levels of IT satisfaction and the outlook on security solutions—particularly the software-level solutions most commonly used today.

> A study by IDC and the National University of Singapore revealed that in 2014, businesses worldwide would spend nearly $500 billion to deal with the problems caused by malware on pirated software.[3]

Desktop/Laptop Security Across the Globe

Interestingly, use of security solutions for desktops/laptops is significantly more common in EMEA (95%) and APJ (98%) than in the Americas (89%). However, while APJ organizations have the highest rate of security solution use, they're only securing about three-fourths of them—which is significantly lower than the other regions. This could be a reflection of fewer computers being connected to the Internet, precluding the need for security solutions. The survey reveals that most organizations are relying on software-level solutions rather than considering BIOS, pre-boot and other built-in hardware security features. On average, the most popular security solutions used are antivirus/malware, firewalls, authentication/passwords and Internet filtering, although usage is a bit lower in APJ than in the other regions.

Top types of security solutions used:

(Asked of those who have security solutions for desktops/laptops. Worldwide percentages are reported below.)

82%
Antivirus/malware

72%
Firewall

71%
Authentication/ passwords

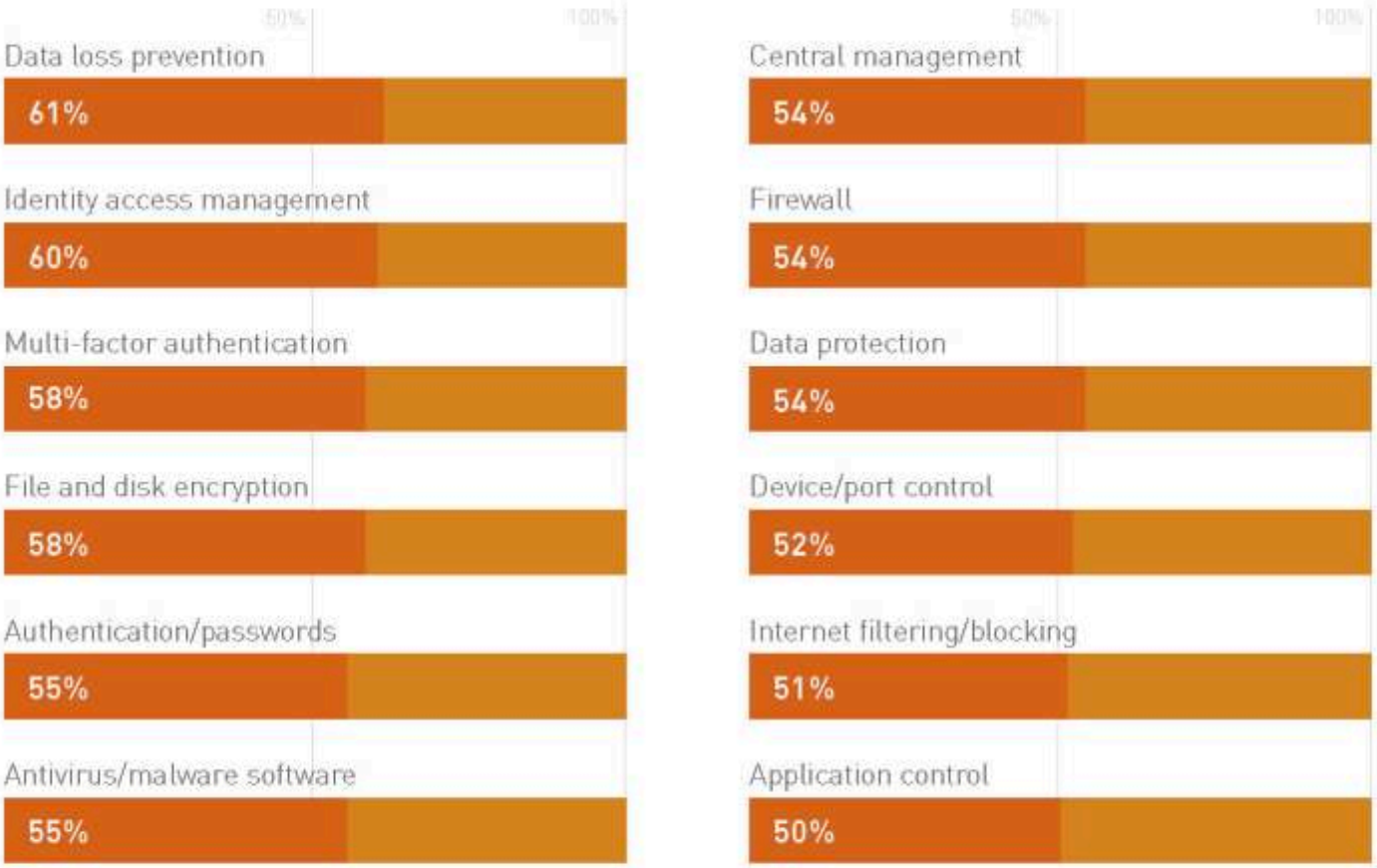
61%
Internet filtering/ blocking

These software solutions may be "the way it's always been done," but they aren't always effective—in fact, only about half of IT decision-makers said their desktop/ laptop security solutions are highly effective. Fifty-four percent said their security solution is highly effective at preventing untrusted apps and executable programs from entering their system; and 50% said their security solution is highly effective at stopping security threats during the boot process.

This relative ineffectiveness is leaving IT professionals wanting more in their security solutions. More than 40% of respondents said they were not completely satisfied with their desktop/laptop security solutions—particularly when it comes to data prevention, firewall antd Internet filtering/blocking.

IT pro satisfaction with security solutions:

(Respondents were only asked about the solutions currently used. The worldwide percentages of those who select 4 or 5 (very satisfied / completely satisfied) on a 5-point scale are included below.)



Those in the Americas are generally less satisfied with their solutions than IT decision makers in EMEA or APJ, most notably for data loss prevention, identity access management, antivirus/malware and central management solutions.

This isn't surprising given that a slightly lower percentage of respondents from the Americas said their security solutions were effective at both preventing untrusted apps and executable programs from entering their systems and at stopping security threats during the boot process.

The Lack of Multi-factor Authentication

Despite more than 40% of respondents not being satisfied with their desktop/laptop security solution, organizations aren't building in redundant security measures to strengthen them. Less than a quarter of respondents said their organizations use multi-factor authentication. Among those who do, the most common type is smartphone/text authentication.

Smartphone/text authentication, customized security tags and fingerprint authentication are more frequently used in APJ. While the Americas and EMEA also mostly use those, they use other methods, as well. For example, fingerprint authentication is much more common in APJ (65%) than in the Americas (39%) and EMEA (38%).

Those who do use multi-factor authentication aren't particularly more satisfied than those who don't: just 58% of those respondents said they were very or completely satisfied, a percentage that's consistent between regions.

Types of multi-factor authentication used:

(Asked of those who use multi-factor authentication. Worldwide percentages are reported below.)

61%
Smartphone/text authentication

52%
Customized security tags

49%
Fingerprint authentication

7%
Other

Challenges to Effective Security

There are always challenges to deploying desktop/laptop security solutions. In the Americas and EMEA, these challenges primarily come from end users who either have limited knowledge regarding risk and security practices or are simply resistant to implementing the measures. In APJ, more respondents report challenges with security threat detection and network complexity, likely due to the fact that more respondents from that region were from larger companies, while some also report challenges with limited end-user knowledge and resistance.

Top 5 security challenges worldwide:

Limited end-user knowledge regarding risk/ security practices

Cost

Impact on device performance

End-user resistance

Time/resources required to deploy/ manage solutions

Because of their reliance on software-level security solutions, organizations don't seem to prioritize security features when purchasing new desktops and laptops. Particularly in the Americas, cost and reliability are far more important, according to respondents.

The Need for a Different Security Approach

Organizations are still relying on traditional add-on software security solutions, solutions that aren't highly effective for nearly half of those surveyed by Spiceworks.[5] Worldwide, organizations seem to be missing an opportunity to beef up security—via built-in hardware security features.

Perhaps it's time to consider a more layered security approach to safeguarding desktops and laptops and the invaluable data they contain. IT professionals can better protect their organizations through built-in, hardware-level security.

HP commercial PCs with Windows 10[1] address security from the inside out.

- HP offers state-of-the-art BIOSphere with Sure Start technology- the industry's first self-healing BIOS-level protection.
- Multi-factor authentication helps protect your device with customized security tags with personalized company logos.
- Protect your data with HP Touchpoint Manager it helps recover lost or stolen devices and safeguards sensitive information if it fall into the wrong hands.

Ready to learn more?

Learn more

Sources

[1] "30,000 Web Sites Hacked a Day. How Do You Host Yours?," *Forbes*, September 2013. http://www.forbes.com/sites/jameslyne/2013/09/06/30000-web-sites-hacked-a-day-how-do-you-host-yours/

[2] "43% of Companies Had a Data Breach in the Past Year," *USA Today*, September 24, 2104. http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/

[3] "The Link between Pirated Software and Cybersecurity breaches: How Malware in Pirated Software is Cost the World Billions." *Microsoft*, March 2014. http://news.microsoft.com/download/presskits/dcu/docs/IDC_031814.pdf

[4] "Data Breach Investigation Report," *Verizon*, 2014. http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf

[5] "HP Security Global Research," a Spiceworks Voice of IT panel survey of 671 respondents from the US, Mexico, Brazil, the UK, France, Germany, China, Japan and India, conducted on behalf of HP, July 2015.

[6] HP BIOSphere with Sure Start is currently available on select HP commercial products only.