EE4758/IM3003 COMPUTER/INFORMATION SECURITY TUTORIAL NO. 1

1. What is computer security?

□ Computer security means protection of computer based resources such as:

- ➔ **Hardware**
- ➔ **Software**
- ➔ **Data**

□ **FROM UNAUTHORIZED**

- ➔ **Use**
- ➔ **Modification**
- ➔ **Theft**
- ➔ **EXAMPLES**: John uses Internet to copy Mary's data and then crashed her system.
- ➔ Henry spoofs Julie's IP address to gain access to her computer.
- ➔ John steals ABC banks data and sales to A-government for $2 millions.

□ Thus, Computer Security refers to the policies, procedures, and technical measures that can be applied to prevent unauthorized access, alteration, theft, or physical damage to computers and information systems.

2. If an attacker breaks into a corporate database and deletes critical files, against what security goal is this attack aimed?

- **INTEGRITY**: Because the information is changed.
- **ALSO AVAILABILITY:** It is no longer available to the firm.
- **WHAT ABOUT CONFIDENTIALITY?**
  - ➔ If the attacker was not allowed to read the data then **YES**.
  - ➔ In case it was an internal attacker and was allowed to read the data then **NO.**
- ❑ It takes just 15 minutes to break into your account according to a study published in the UK in May 2011.
- ❑ A group of volunteers including TV producers, baker and retire people followed online tutorial and were able to hack into someone's account within 15 minutes.
- ❑ Today there are 100, 000 online videos teaching users how to hack into social networks, e-mails, smartphones and PayPal.
- ❑ In year 2012, 6.5 million LinkedIn passwords were stolen and published on Russian social network.
- ❑ In 2014, 1.2 billion passwords were stolen.
- ❑ In 2015,$575 billions were lost due to cyber crimes.
- ❑ In August 2016, 200 million Yahoo accounts were compromised.

3. Suppose that a network computer virus is designed so as soon as it is copied onto a computer, X, it simply copies itself to six of X's neighboring computers, each time using a random file name, so as to evade detection. The virus itself does no other harm, in that it doesn't read any other files and it doesn't delete or modify any other files either. What harm would be done by such a virus and how would it be detected?

- □ This problem is based on the true story of the Cornell graduate student, Robert Morris.
- □ His virus (which is more properly called a “worm") brought the entire Internet to its knees.
- □ The reason is that when the virus copies itself to X's neighbors, they will copy it back six times to X, which then copies 36 copies to its neighbors, and so on.
- □ Soon all of X's disk memory is full of copies of the virus and X crashes. So this is a type of denial of service attack.
- □ This sort of attack is very easy to launch and as recently as August 2011, this method has been successfully employed, particularly via Gmail, Hotmail and other similar services.
- □ The detection is basically done by looking for unusual activities regarding mail, speed etc.

4. It has been claimed that with the emergence of state of the art computer security technology and the awareness of security threats, the number of online attacks have decreased significantly. Do you agree with the above statement? Justify your answer.

□ Although the technology and the awareness helps, the overall online security situation hasn’t had a dramatic change.

□ Two groups called “Anonymous” and “LulzSec” have been very prominent and are believed to be behind many attacks.

□ More users, more data, more devices, and more clouds are creating a perfect security storm of threats and vulnerabilities.

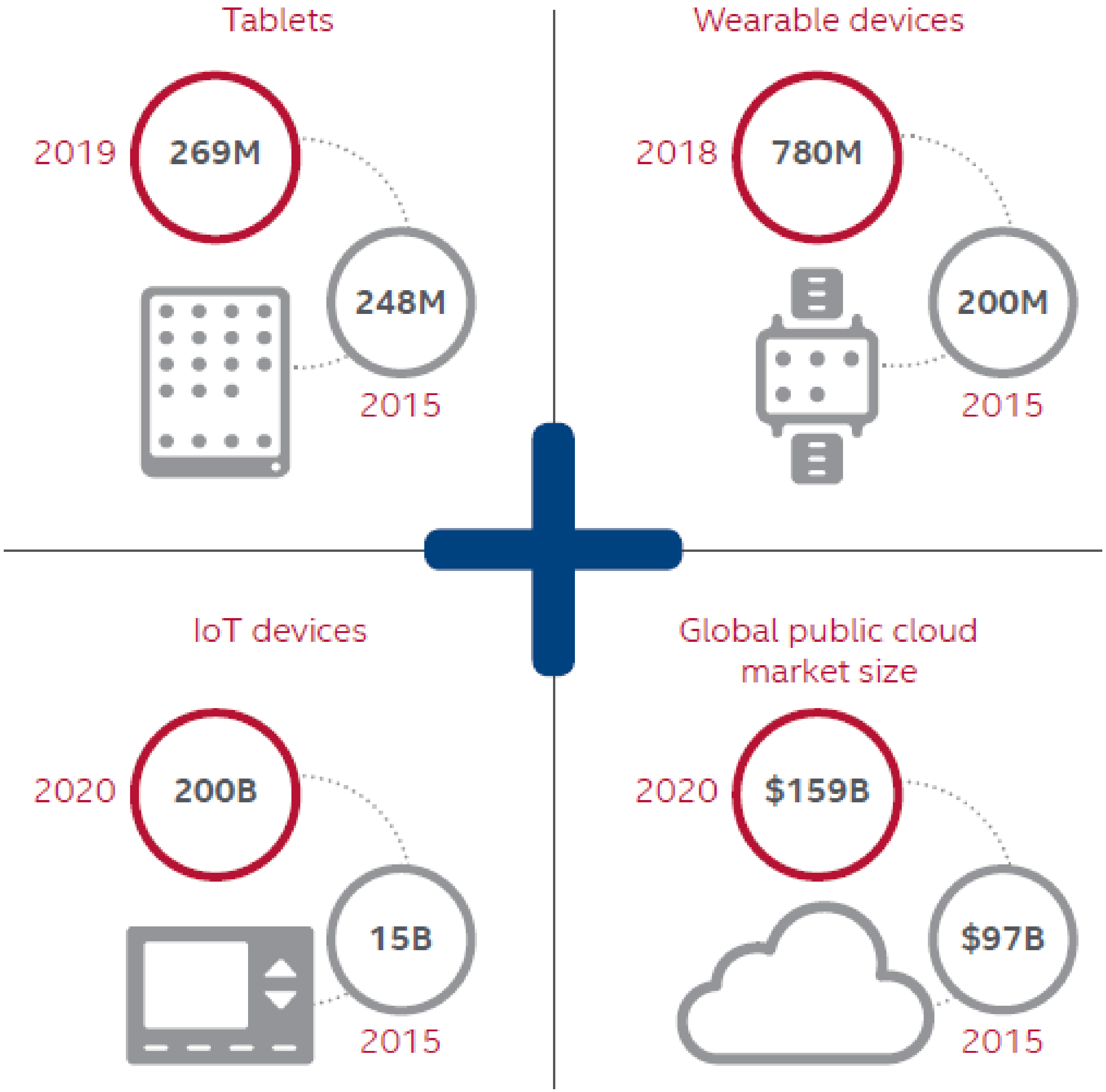
□ Devices will continue to grow in volume and variety, and the forecast for connected devices by 2020 is now 200 billions.

□ MacAfee predicts that the rise of ransomware that started in the third quarter of 2014 will continue in 2016.

□ According to the Business Insider “The Connected-Car Report,” there will be 220 million connected cars on the road by 2020.

□ Currently 16% cars are connected to internet.

New Device Types



Tablets

2019 269M

248M 2015

Wearable devices

2018 780M

200M 2015

IoT devices

2020 200B

15B 2015

Global public cloud market size

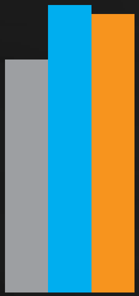
2020 $159B

$97B 2015

Source: McAfee Labs, 2015.

BIG NUMBERS

BREACHES



Total Breaches

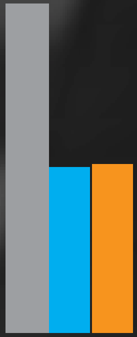
2013	2014	2015
253	312	305
–	+23%	-2%

Breaches With More Than 10 Million Identities Exposed

2013	2014	2015
8	4	9
–	-50%	+125%

Total Identities Exposed

2013	2014	2015
552M	348M	429M
–	-37%	+23%



Average Identities Exposed per Breach

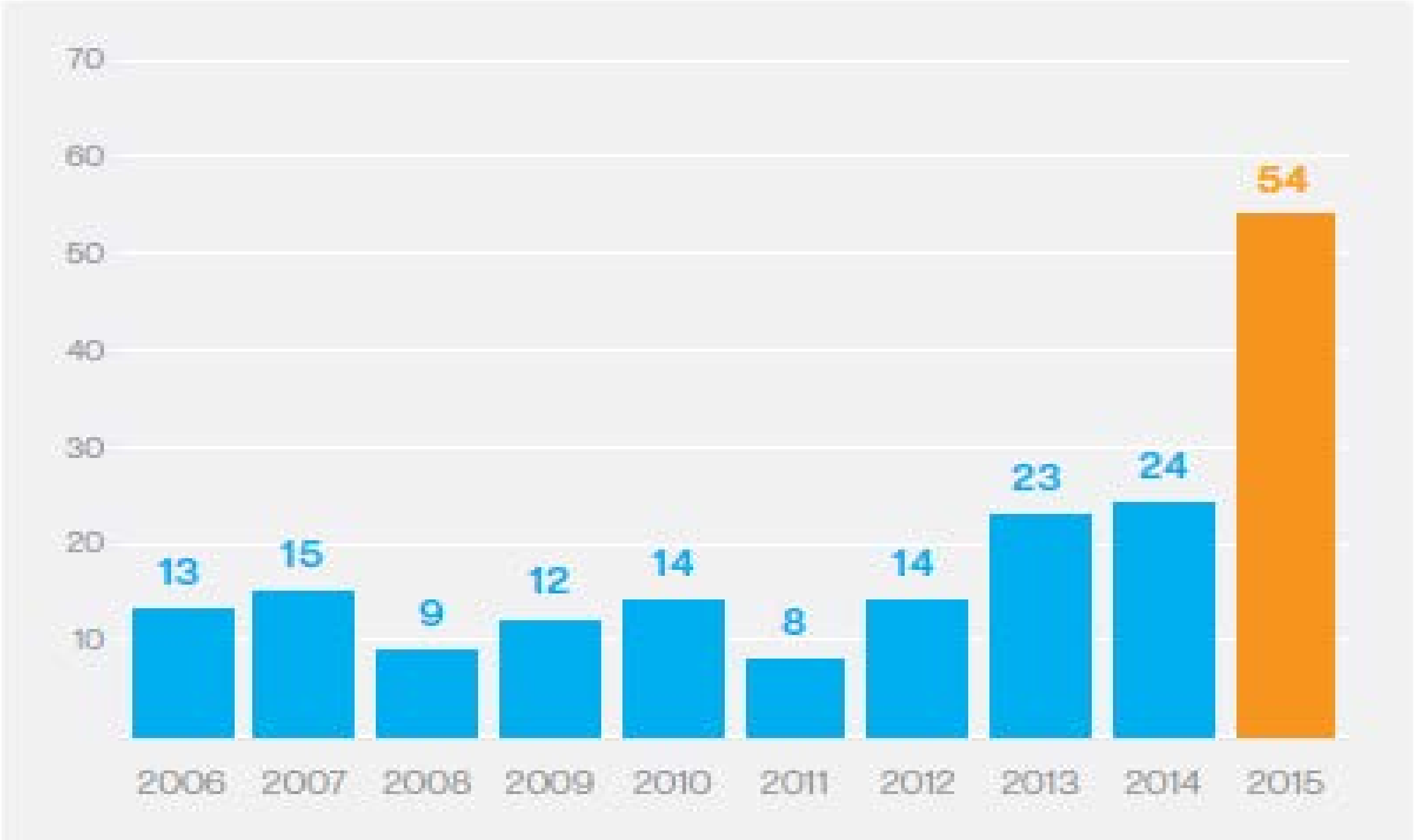
2013	2014	2015
2.2M	1.1M	1.3M
–	-49%	+21%

Median Identities Exposed per Breach

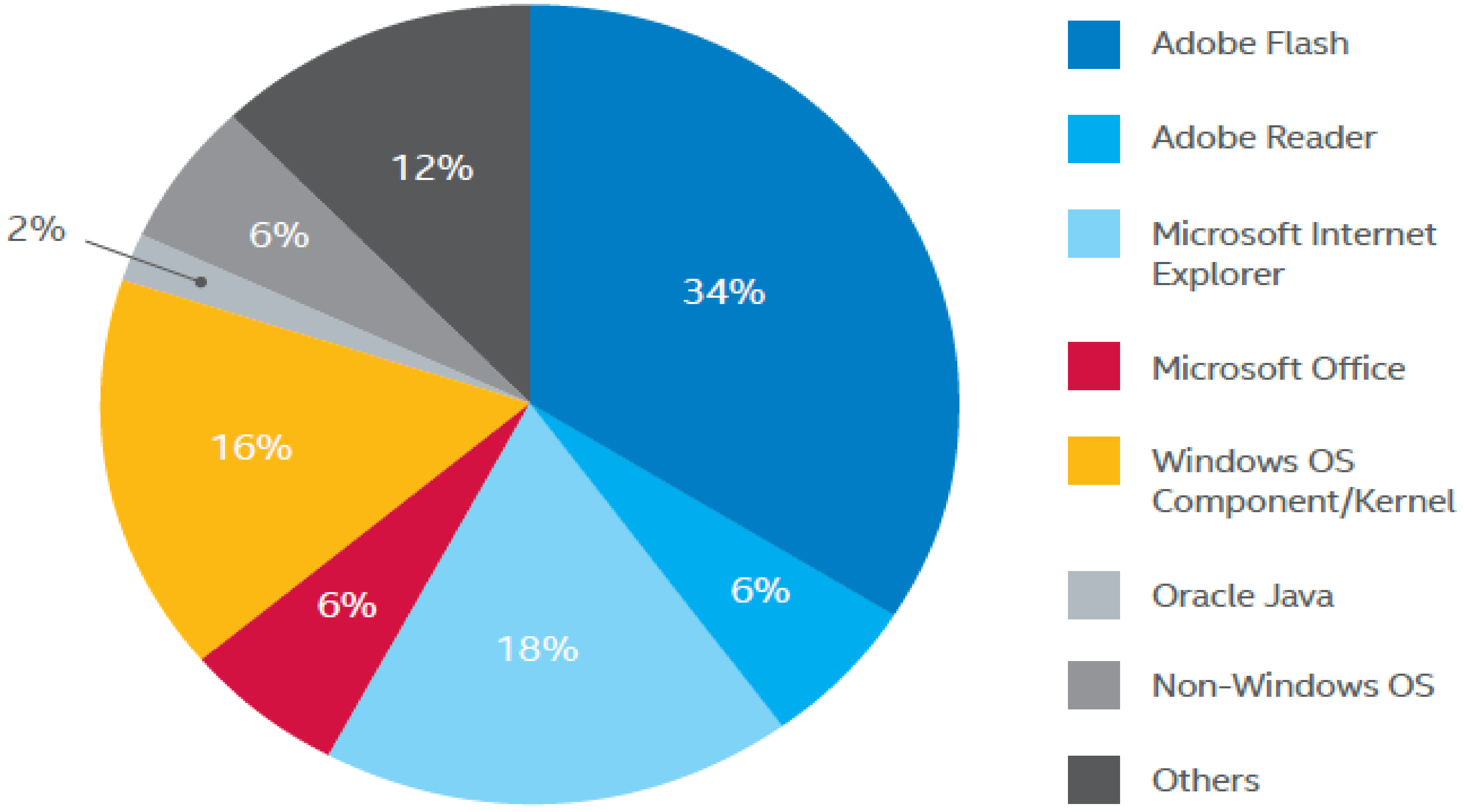
2013	2014	2015
6,777	7,000	4,885
–	+3%	-30%

Zero-Day Vulnerabilities, Annual Total

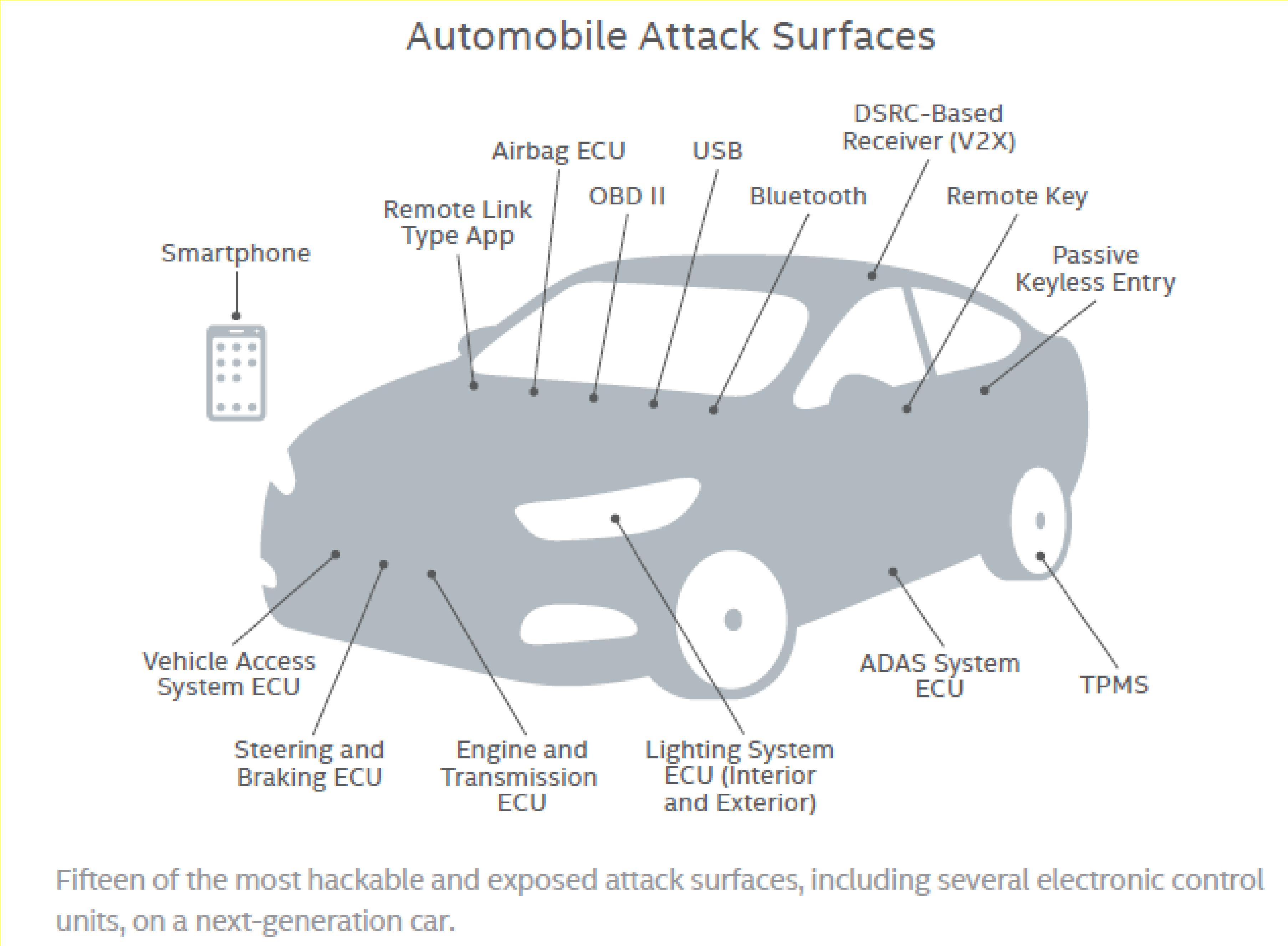
▶ *The highest number of zero-day vulnerabilities was disclosed in 2015, evidence of the maturing market for research in this area.*



2014–2015 Zero-Day Attacks by Vulnerable Application



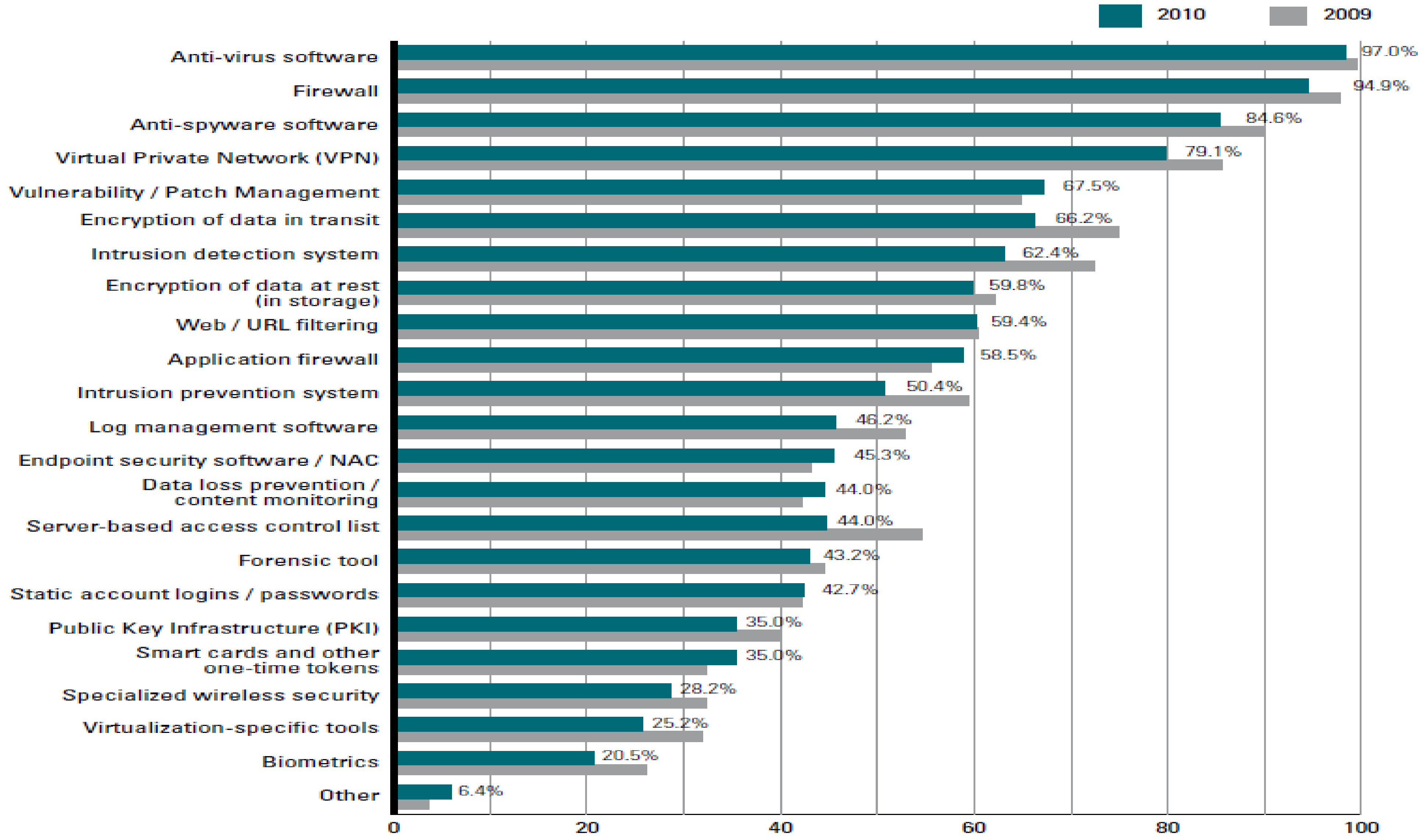
Source: McAfee Labs, 2015.

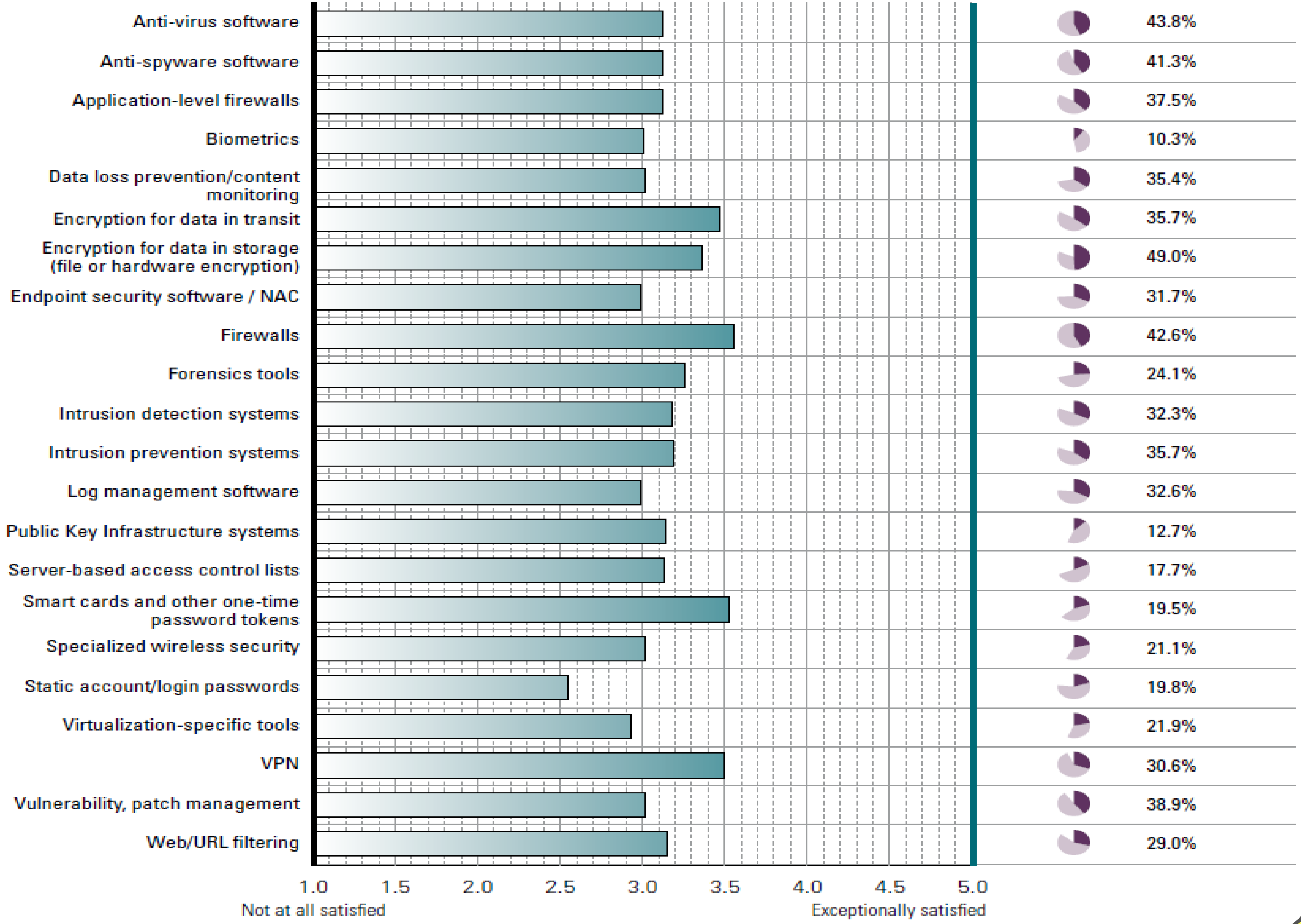


Automobile Attack Surfaces

Fifteen of the most hackable and exposed attack surfaces, including several electronic control units, on a next-generation car.

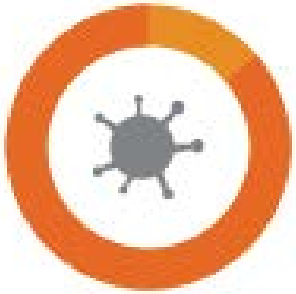
5. What are the most popular security technologies used by industries and individuals to safeguard their assets stored on the computer connected to the Internet



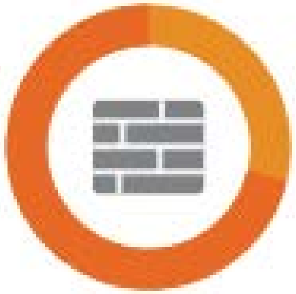

Anti-virus software
43.8%
Anti-spyware software
41.3%
Application-level firewalls
37.5%
Biometrics
10.3%
Data loss prevention/content monitoring
35.4%
Encryption for data in transit
35.7%
Encryption for data in storage (file or hardware encryption)
49.0%
Endpoint security software / NAC
31.7%
Firewalls
42.6%
Forensics tools
24.1%
Intrusion detection systems
32.3%
Intrusion prevention systems
35.7%
Log management software
32.6%
Public Key Infrastructure systems
12.7%
Server-based access control lists
17.7%
Smart cards and other one-time password tokens
19.5%
Specialized wireless security
21.1%
Static account/login passwords
19.8%
Virtualization-specific tools
21.9%
VPN
30.6%
Vulnerability, patch management
38.9%
Web/URL filtering
29.0%
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0
Not at all satisfied
Exceptionally satisfied

Top Types of Security Solutions Used:

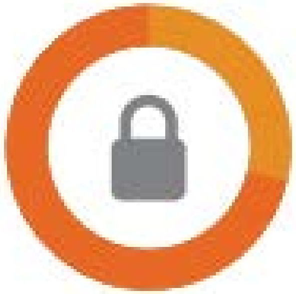
(Asked of those who have security solutions for desktops/laptops. Worldwide percentages are reported below.)



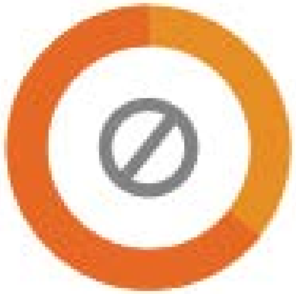
82%
Antivirus/
malware



72%
Firewall



71%
Authentication/
passwords

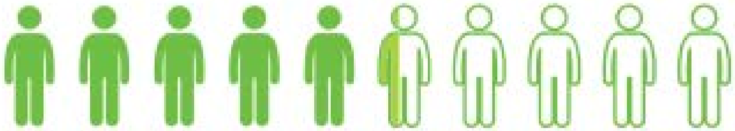


61%
Internet filtering/
blocking

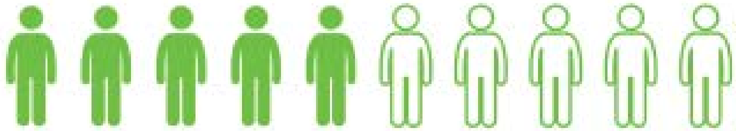
Security Solution Effectiveness:

(Respondents with security solutions for desktops/laptops who selected very effective on a 3-point scale)

54% rated their security solution as very effective at preventing untrusted apps and malware from entering the system.



50% rated their security solution as very effective at stopping security threats during the boot process.



❑ QUIZ

A. ----------------- is the principle in security whose goal is to ensure that data is only modified by individuals who are authorized to change it.

❖ **Integrity**

B. ------------------ is the process used to ensure that an individual is who they claim to be.

❖ **Authentication**

C. What is the most common form of authentication used

I. Smart card
II. Tokens
III. Username/Password
IV. Retinal Scan

❖ **Username/Password**

D. The CIA security triangle of security includes

I. Confidentiality, Integrity, Authentication
II. Confidentiality, Integrity, Availability
III. Certificates, Integrity, Availability
IV. Confidentiality, Inspection, Authentication

❖ **Confidentiality, Integrity, Availability**