All Products & Vendors

In 2012, 2,503 vulnerable products were discovered, with a total of 9,776 vulnerabilities in them.
That means there's an average of 4 vulnerabilities per vulnerable product.

There is an increase in vulnerabilities, and a decrease in the number of vendors and products vulnerabilities are discovered in.

How dangerous are the vulnerabilities for all products/vendors?

TOP 50

The Top 50 Portfolio

What is the Top 50 portfolio?

To asses how exposed endpoints are, we analyze the types of products typically found on an endpoint. For this analysis we use anonymous data gathered from scans throughout 2012 of the millions of private computers which have the Secunia Personal Software Inspector (PSI) installed.

PSI users' computers have an average of 72 programs installed on it - from country to country and region to region there are variations as to which programs are installed.

For the sake of clarity, we have chosen to focus on the state of representative portfolio of the 50 most common products found on the computers.These 50 programs are comprised of 29 Microsoft programs and 21 third-party programs.

These are the attack vectors used by attackers to trigger or reach a vulnerability in a program

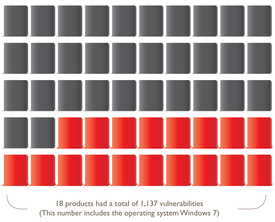
91% Remote network used as attack vector

2% Local network used as attack vector

7% Local system used as attack vector

The majority of attacks are carried out by a hacker from a remote network, where the attacker is not required to have access to the system or a local network in order to exploit the vulnerability.

Vulnerabilities in the 50 most used applications



18 products had a total of 1,137 vulnerabilities
(This number includes the operating system Windows 7)

GOOGLE CHROME	291
MOZILLA FIREFOX	257
APPLE ITUNES	243
ADOBE FLASH PLAYER	67
ORACLE JAVA JRE SE	66
ADOBE AIR	56
MICROSOFT WINDOWS 7	50
ADOBE READER	43
MICROSOFT INTERNET EXPLORER	41
APPLE QUICKTIME	29
MICROSOFT .NET FRAMEWORK	14
VLC MEDIA PLAYER	11
MICROSOFT EXCEL	10
MICROSOFT VISIO VIEWER	7
MICROSOFT SILVERLIGHT	5
MICROSOFT WORD	3
SKYPE	1
MICROSOFT XML CORE SERVICES (MSXML)	1

In the top 50 portfolio the total number of end-point vulnerabilities in 2012 was

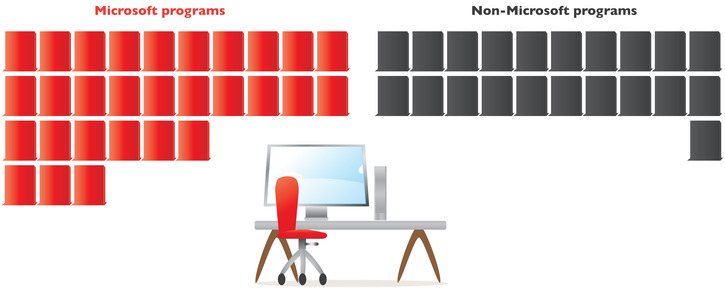
1137

In the 5 year trend, this shows an increase of

98%

The 1,137 vulnerabilities were discovered in 18 of the Top 50 products - an average of 63 vulnerabilities per product.

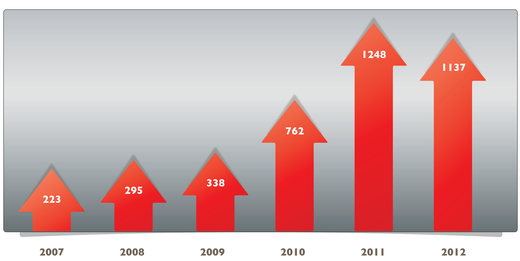
Installed software on a typical endpoint



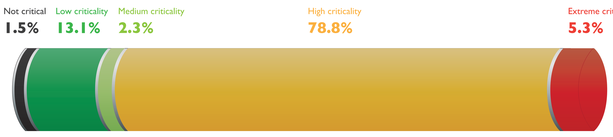
29 Microsoft products are installed on the PC of an average user of Secunia Personal Software Inspector

21 Non-Microsoft products are installed on the PC of an average user of Secunia Personal Software Inspector

The 5 year vulnerability trend



How dangerous are the vulnerabilities in the Top 50 portfolio?

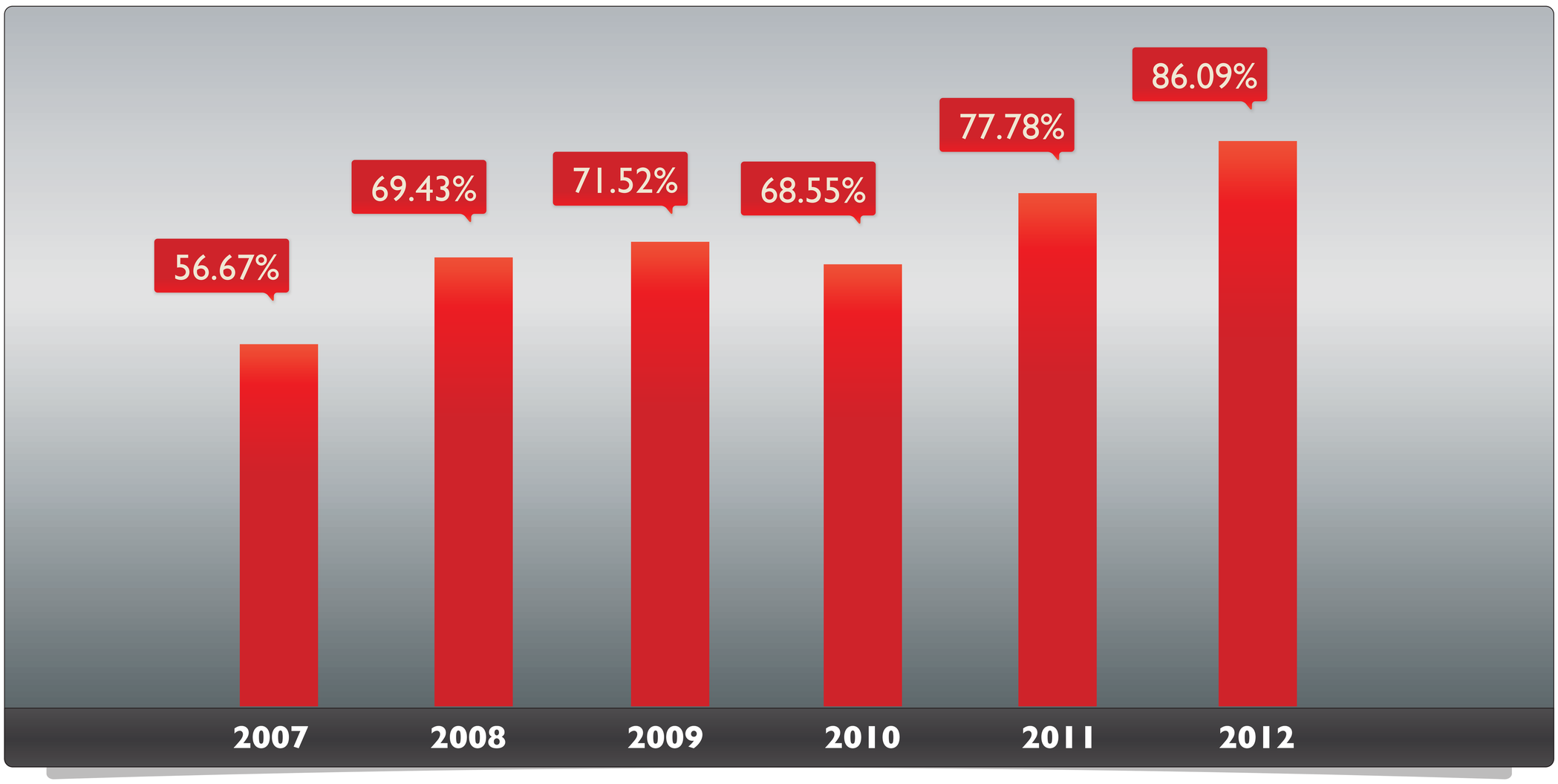


Most of the endpoint vulnerabilities were rated by Secunia as either 'Highly critical' (78.8%) or 'Extremely critical' (5.3%).

Third Party Vulnerabilities

Share of vulnerabilities discovered in third-party programs

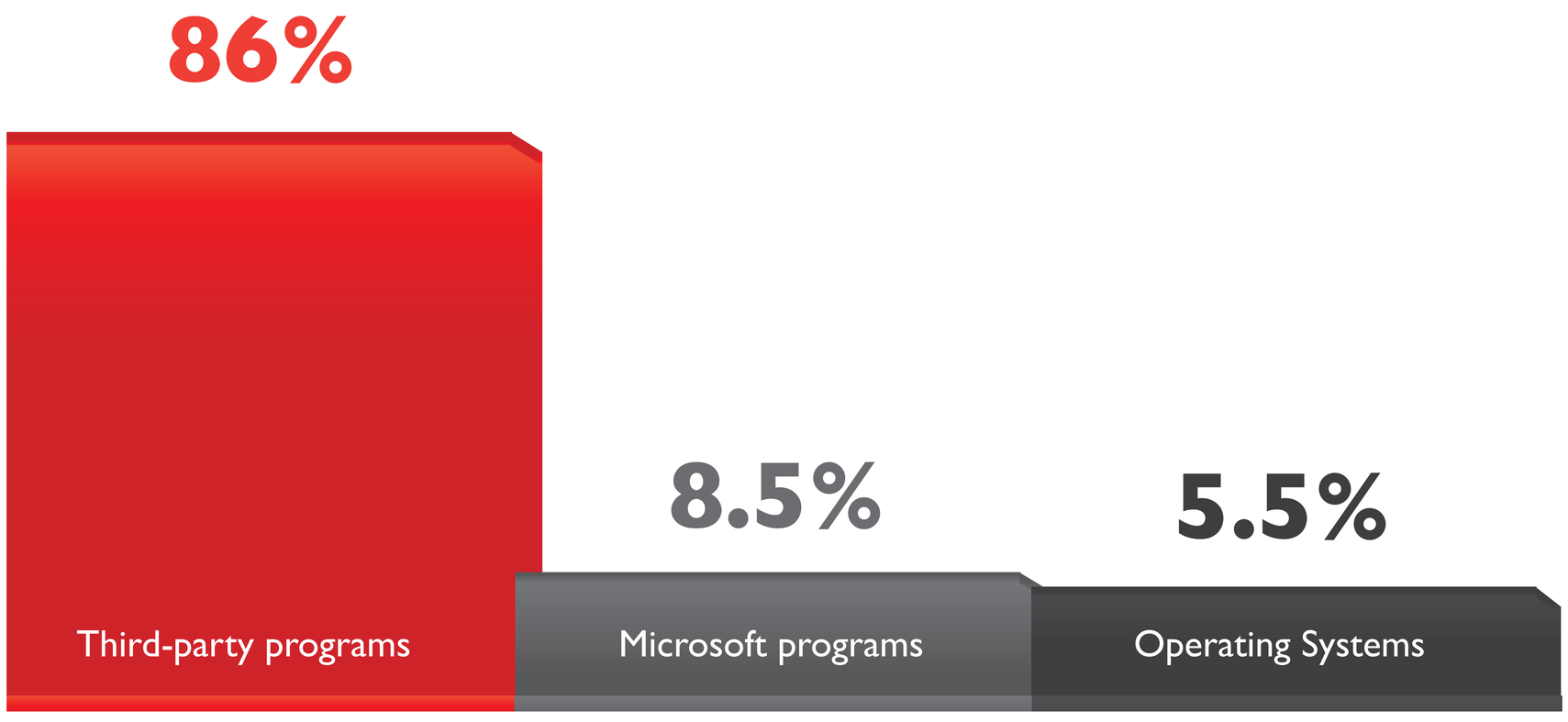
Share of vulnerabilities discovered in third-party programs, rather than in Microsoft programs and operating systems, in the Top 50 portfolio.



Since 2007, the share of vulnerabilites in third-party software has increased by **52%**

Compared to last year, the share of third-party vulnerabilities has increased by **10.7%**

The share of vulnerabilities in Top 50, divided by program types.

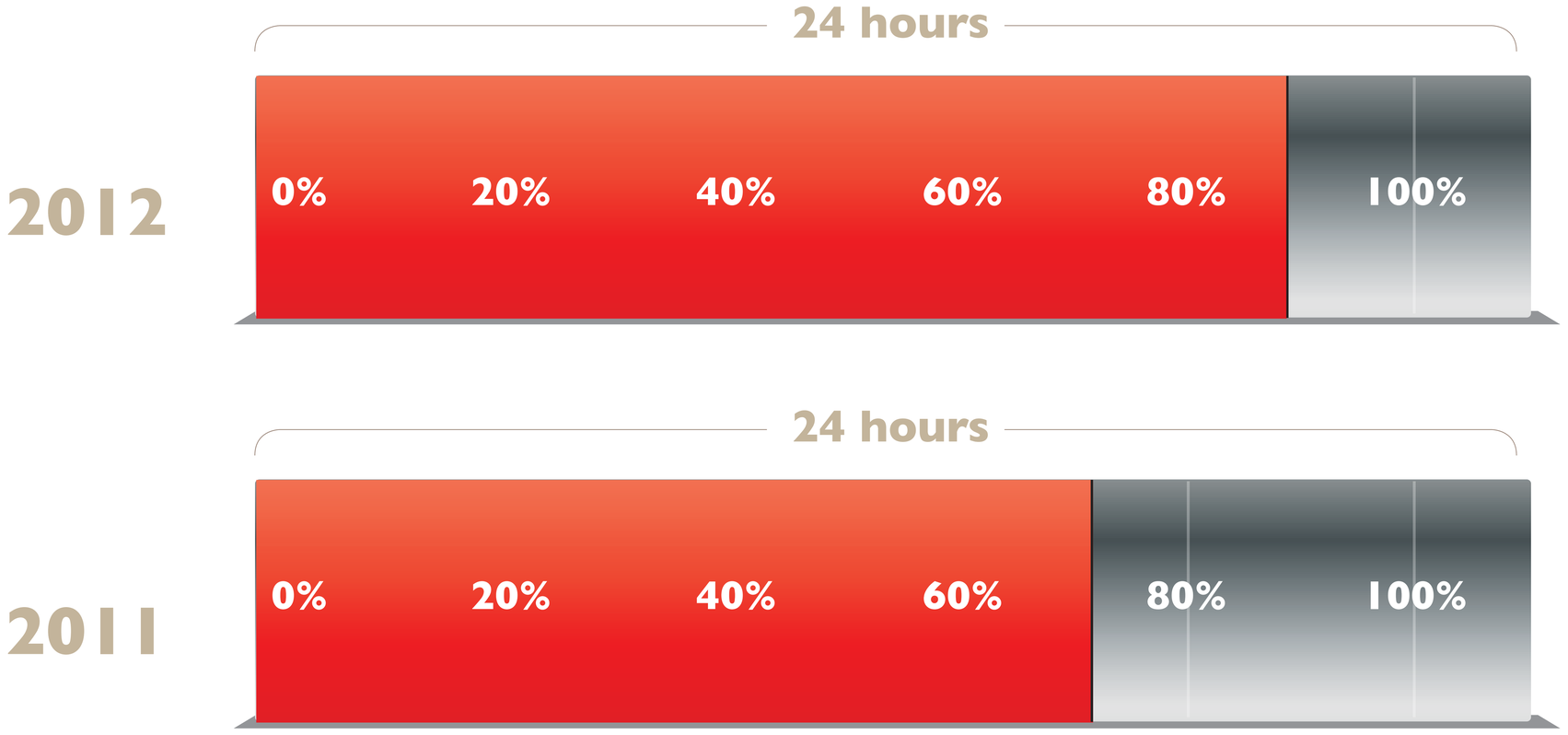


86% of vulnerabilities in 2012 affected third-party programs, outnumbering the 5.5% of vulnerabilities found in operating systems or the 8.5% of vulnerabilities discovered in Microsoft programs.

Third-party programs, rather than programs from Microsoft, are responsible for the majority of vulnerabilities in Top 50.

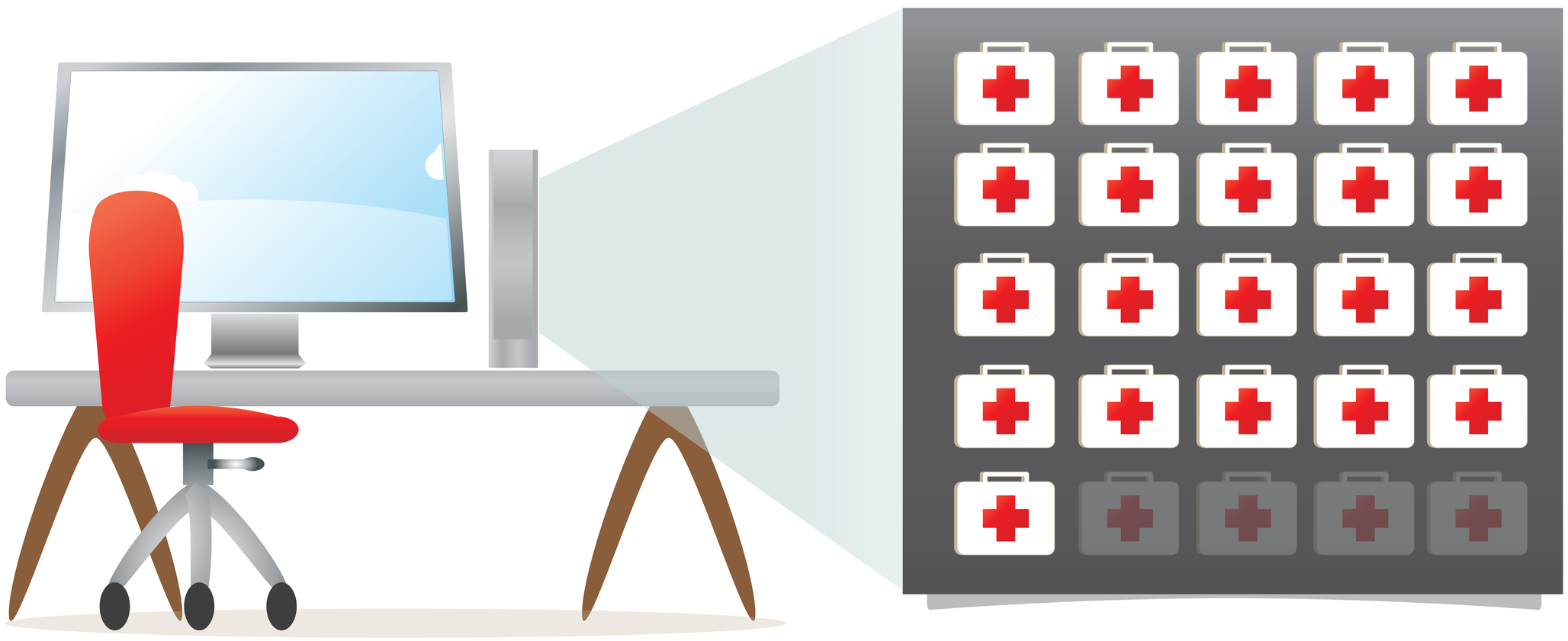
Time to Patch

When are patches available for vulnerabilities in the Top 50 programs?



84% of vulnerabilities had patches available on the day of disclosure in 2012

72% of vulnerabilities had patches available on the day of disclosure in 2011



In 2012, 84% of vulnerabilities had a patch available on the day they were disclosed. This means that it is **possible to remediate the majority of vulnerabilities**, and that organizations and private users alike have a solution available for the root cause of security issues: vulnerabilities in software.

Browser Security

Increase in vulnerabilties in the most popular browsers
(Google Chrome, Mozilla Firefox, Internet Explorer, Opera, Safari)

In 2012 there was an increase in browser vulnerabilities - but a quick time-to-patch rate for all vulnerabilities indicates that vendors are serious about security, which is an overall positive trend.

All browser vulnerabilities found in the last 2 years were patched in less than

30 days

Compared to last year, the number of browser vulnerabilities increased by

17%

Compared to last year, the number of advisories increased by

19%

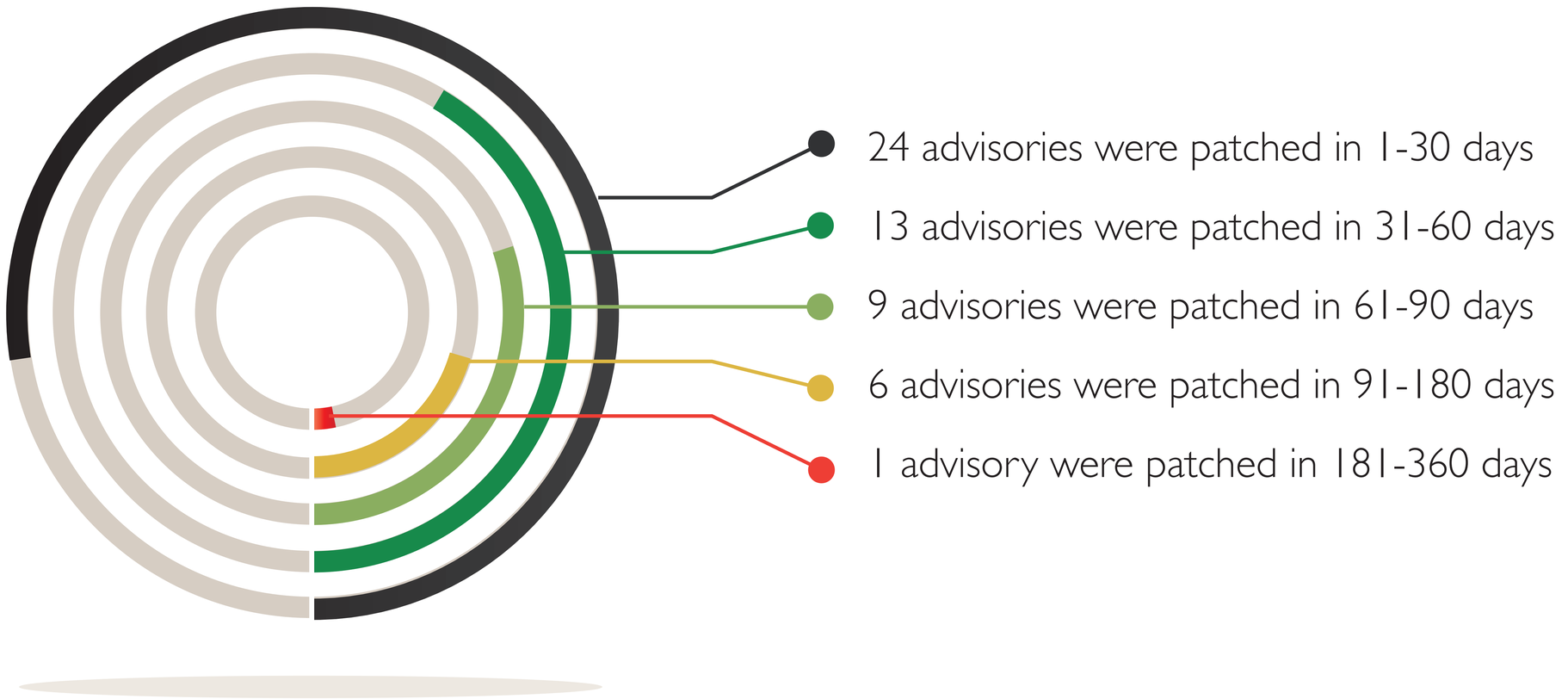
Vulnerabilities in the most popular browsers 2011 and 2012

The evolution of vulnerabilities in the most popular browsers

Google Chrome, Mozilla Firefox, Internet Explorer, Safari and Opera in 2011 and 2012.
Please note: the numbers are incremental.

SCADA

Time-to-patch for SCADA advisories the last 24 months



SCADA software today is at the stage mainstream software was at 10 years ago: security updates are erratic (great variation in how they are handled), compared to what we are becoming accustomed to in mainstream programs.

Many vulnerabilities remain unpatched for longer than 1 month in SCADA software.

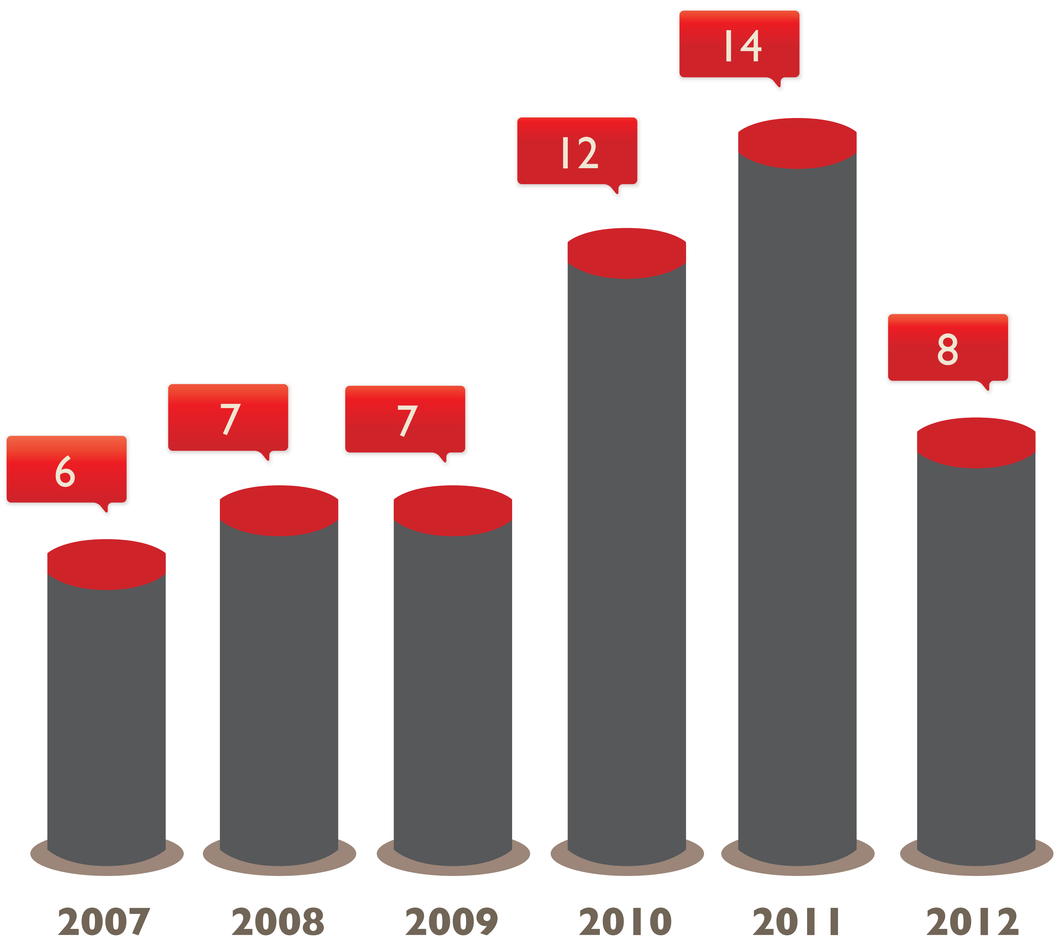
These are the attack vectors used by attackers to trigger or reach a vulnerability in a program

How dangerous are the SCADA vulnerabilities?

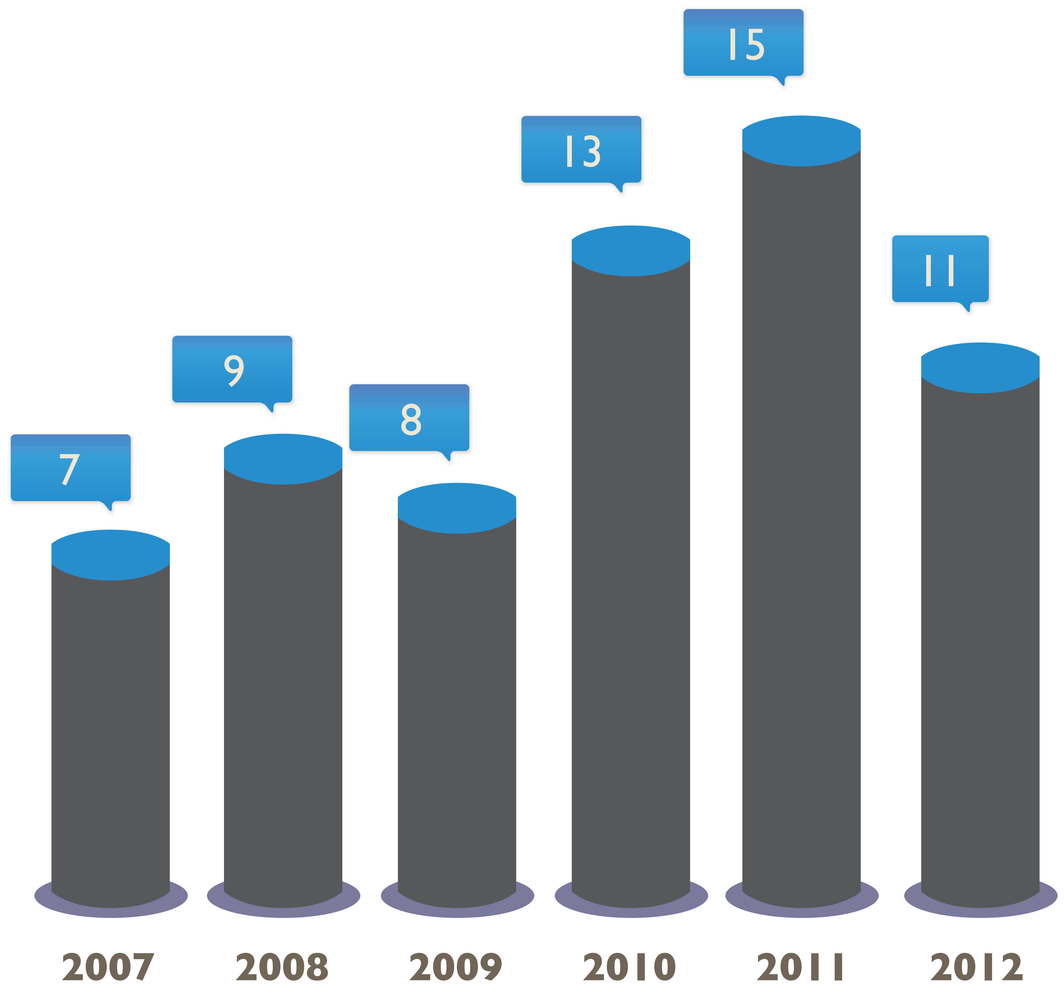
Zero-Days

The difference between the number of vulnerabilities in the Top 25 most popular programs and the Top 400 in negligable, as demonstrated by these graphics.

Zero-Days In the Top 25 portfolio



Zero-Days In the Top 400 portfolio



This means you are not substantially more exposed to zero-days, the more programs you have installed on your systems.

What is a zero-day vulnerability?
A zero-day vulnerability is a vulnerability that is actively exploited by hackers before it is publicly known, and before the vendor has developed a patch for it.

The products used by the most people are the ones zero-days are on. Regardless of the increased focus on security, we have not seen a rise in the number of reported zero-days in popular products.