

The Antivirus Industry: Quo Vadis?

VirusBulletin

October 1, 2008



Sunbelt Software

Our perspective

- AV: An industry under assault?
- A clean slate
 - Our possibly unique perspective through recent development and marketing efforts.



Perception vs. Reality



Comments from the peanut gallery

- “AV is dead.”
- “It’s all going to be free from your ISP.”
- “It’s just a cash cow.”
- “Signatures don’t work.” (duh!)
- “Not an interesting growth space.”



Comments from the peanut gallery

- “With Vista, you don’t need antivirus.”
- “Whitelisting is the future.”
- “Your product didn’t find anything on my system.”
- Overcharging, too many resources, bad support, not enough detection, etc., etc.



The barrage of negativity: Clouds on the horizon?

The screenshot shows a news article on a website. The main article is titled "Texas Bank Dumps Antivirus for Whitelisting" and is dated July 11, 2008. The author is Paul Korzeniowski, a contributing editor at Dark Reading. The article discusses how Brent Rickels, senior vice president at First National Bank of Bosque County, is tired of dealing with antivirus software and has decided to switch to application whitelisting. The article also mentions that the bank had to beat back a tenfold increase in malware in four years. There are several sidebars and navigation menus visible, including "LATEST STORIES", "BEST OF THE BLOGOSPHERE", and "RELATED" articles. A search bar and a "GO" button are also present at the bottom of the page.

Security - eWeek

TECHWORLD Home page | About Techworld | Contact details

AUSTRALIAN IT

Guide to techweb White Papers | Blogs | Video | Events | Webcasts | Briefing Centers | News

ecTech Opinion Best of the Web

Contracts Special Reports

Powered By InformationWeek BUSINESS TECHNOLOGY NETWORK

for security

Font Size: [A] [A+] Print Page: [Print]

Home > Security > Application Whitelisting Gains Traction

LATEST STORIES

- Oracle Says Will Catch Up with SAP
- FCC Proposes Easing Spectrum Bids
- Highlights from Oracle OpenWorld
- Your Guide to the Top 5 Green Energy-Efficie...
- How Many Cloud Computing Platforms Can we Ha...

BEST OF THE BLOGOSPHERE

- iPhone's Mediocre Battery Life Still Beats Rivals
- The Android Developer Revolt
- Google Feels Developers' Pain
- Nokia Launches Location-Aware Chat Client

Security

Application Whitelist

By Jason Brooks
2008-09-25

Article Views: 505
Article Rating: ★★★★★ / 3

The technology, being pushed by vendors as Cisco, is giving IT de a new weapon in fighting malwa Application whitelisting is a goo complement to other anti-virus such as blacklisting, diligent pat user education.

Malicious software is a disease, a conventional-wisdom remedies of patching, anti-virus deployment a education haven't proved potent bring about a cure.

Enter application whitelisting, a d approach to the problem of secur Windows clients. Application whit

First National Bank of Bosque County, which serves the Waco, Texas, area and manages approximately \$100 million in assets, had seen the volume of spam and software it had to beat back increase tenfold in four years. So when it was time for presentation at the company's IT Security Summit in London.

Buyers should take advantage of the competitive environment in the anti-virus software industry to negotiate better prices for such products, he said.

DATE: September 28 - October 6, 2008
LIVE EVENT: SANS Network Security 2008
LOCATION: Las Vegas, NV
More Information

HOME | NEWS | OPINION | VIDEO | TALK | EVENTS | JOB SEARCH | PAID RESEARCH | W

Texas Bank Dumps Antivirus for Whitelisting

Tired of AV and malware, First National Bank of Bosque County adopts application whitelisting instead

JULY 11, 2008 | 1:15 PM

By Paul Korzeniowski
Contributing Editor, Dark Reading

Brent Rickels, senior vice president at First National Bank of Bosque County, had grown tired of dealing with antivirus software. He was tired of regularly updating virus signatures, tired of hackers constantly tweaking malware, and tired of worrying about what users had downloaded onto their PCs. So Rickels dumped the bank's AV software for a whitelisting product and in the process, become one of its first commercial customers.

First National Bank of Bosque County, which serves the Waco, Texas, area and manages approximately \$100 million in assets, had seen the volume of spam and software it had to beat back increase tenfold in four years. So when it was time for presentation at the company's IT Security Summit in London.

Buyers should take advantage of the competitive environment in the anti-virus software industry to negotiate better prices for such products, he said.

DISCUSS
EMAIL
PRINT
LINK/REPRINT
SHARE
RSS

RELATED

VIDEO

Friend Me Satan!
PLAY (15:23)

Typo Squatting Election '08
PLAY (05:10)

Typo squatting and other ways to mess

Subscribe to the Computer & Internet Security newsletter

Recent Computer & Internet

can't manage their own internet security, but the industry is still a long nd reliability at an affordable price.

Bill Snow, computer scientist and retired technical director of the US National Security Agency, likens the technology leap needed to that of the car industry. "A car built in the 1930s looks nice and goes fast, but in an accident, you die," he told the AusCERT 2008 conference on the Gold Coast last week.

"A mid-2000s car has airbags, seatbelts, engineered crush zones, traction control and anti-skid brakes, and in an accident, you probably live."

Companies should be producing "a series of unbroken products", rather than "an unbroken series of products", Snow says.

That will be a challenge, as industry heavyweights s, patching and antivirus software.

ten hackers bulk-harvest in phishing attacks or by keystroke logging, availability there are limited opportunities for patching, and antivirus e of signature variations.

rt advocates a new approach. "Perhaps we should assert what's good, stuff - the things on blacklists," he says.

“The end is nigh
upon us!
REPENT!”

(Spoken recently by the Crazy Drunk Bum Guy down the street.)



Myths and facts about the AV industry



Well...

What's the truth?



The antivirus industry then



The antivirus industry then

- Small group of individuals.
- Extreme secrecy regarding samples, etc.
- Small number of samples.
- One major testing outfit: VB



The antivirus industry...and now

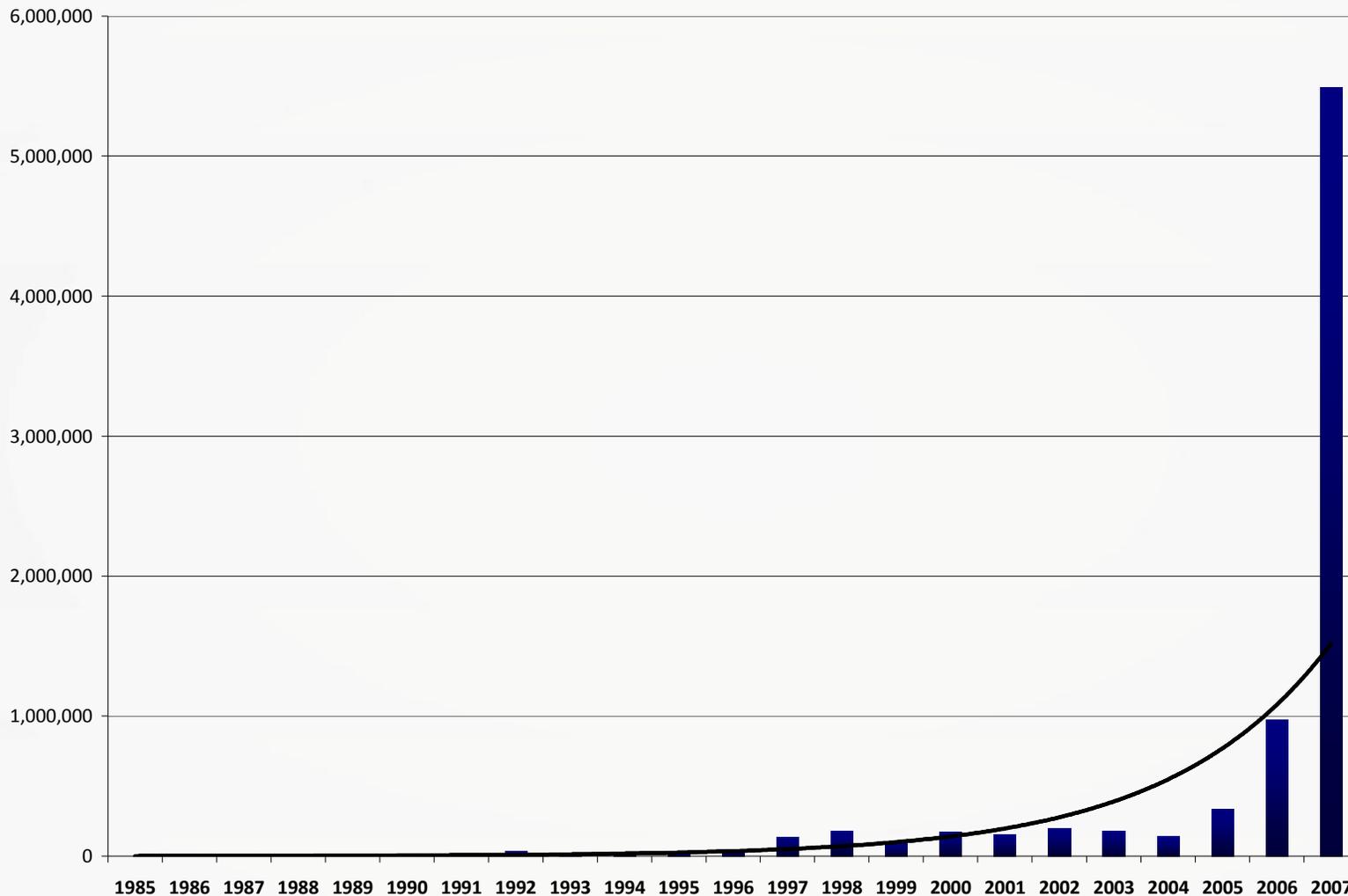


The antivirus industry now

- Large amounts of researchers involved.
- Numerous security lists, vetted and non-vetted.
- Free-flow of information.
- Numerous testing organizations, both professional and non-professional.



Malware is exploding (yes, we all know)



Source: Av-test.org



Sunbelt Software

Malware Overload, Information Overload

- Information overload is a method of obfuscation.
 - Lots of malware, lots of information obfuscates the key priorities.
- Non-linear correlation of size with efficiency.
- Testing methodologies.
 - Prevalence, relevancy.
- Not all of the information is necessarily correct.
 - The VirusTotal/Jotti Syndrome.
- Small amount of malware actually responsible for most damage.



Malware has evolved insanely

- New methods create real problems in detection.
 - Increasingly sophisticated evasion techniques.
 - Anti-dumping, anti-debugging, anti-emulation, anti-intercepting.
- These new techniques, combined with volume, make today's antimalware field extremely challenging.



Malware has evolved insanely

- The “old” style AV company is a thing of the past
 - Carefully writing detections on malware updated only once or twice.
- Now, with money involved...
 - One day’s work on a detection today is useless tomorrow.
 - Malware authors have our tools and write malware that is undetectable upon release.
- Current technologies (static unpacking, etc.) may become obsolete; performance is an issue.



The business case

- This VB will focus on new techniques.
- Let's focus on the business side instead.



The antivirus industry

- Growth is slowing, but still there:
 - Gartner: Worldwide security software revenue will increase from more than \$10.5 billion in 2008 to more than \$13 billion in 2012, a CAGR of 6.8% from 2007 through 2012.



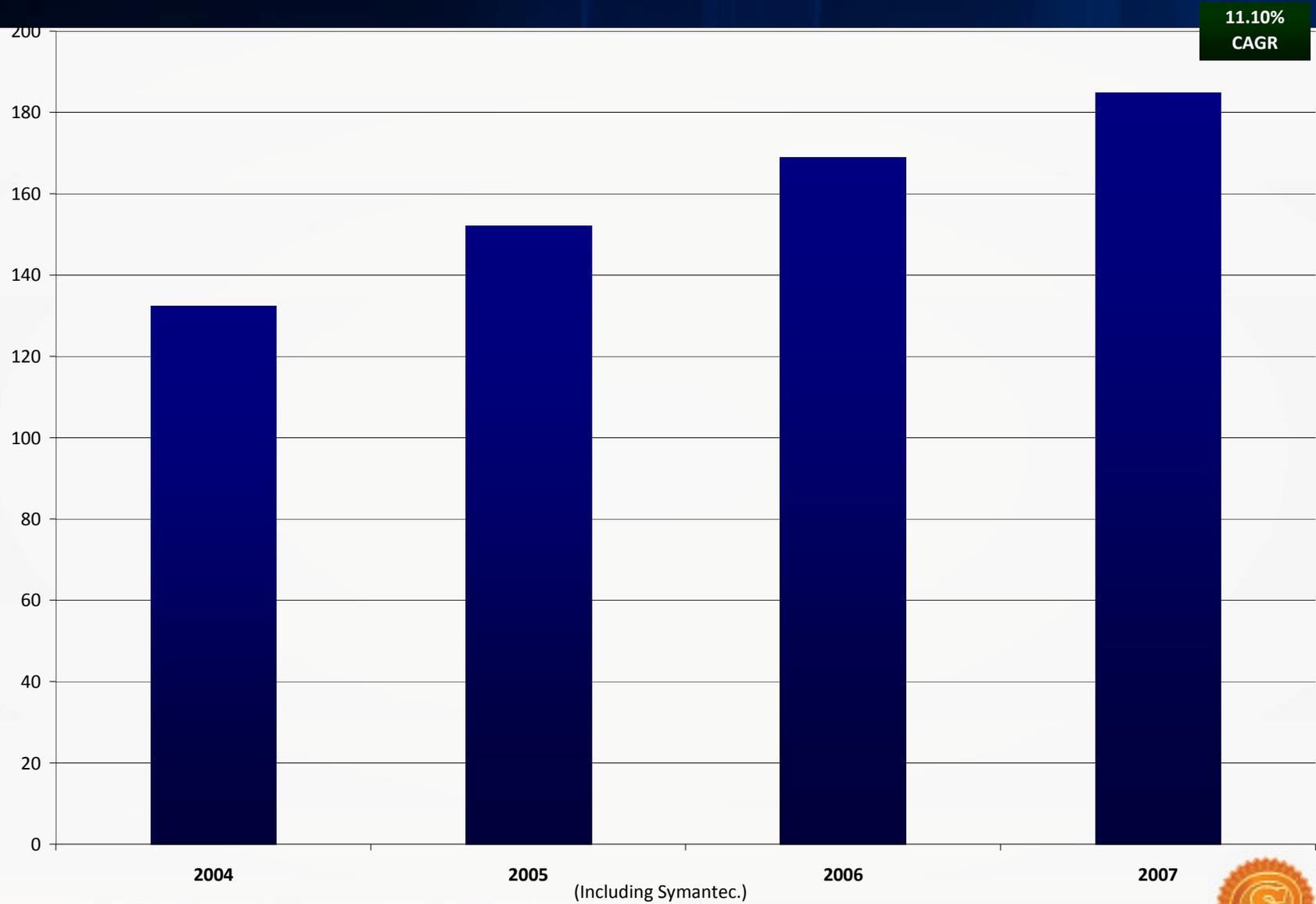
Fun with numbers (and disclaimers)

- Analysis performed on 6 publicly traded security companies: Trend, Sophos, Symantec, McAfee, Norman and F-Secure.
- Numerous disclaimers apply:
 - Did not take into account many FASB/GAAP issues, as well as reporting in different currencies.
 - Security numbers used as a proxy for antivirus, not an entirely accurate method.
- NTSEN* Rule applies.

* Never Trust a Software Executive with Numbers



Revenues



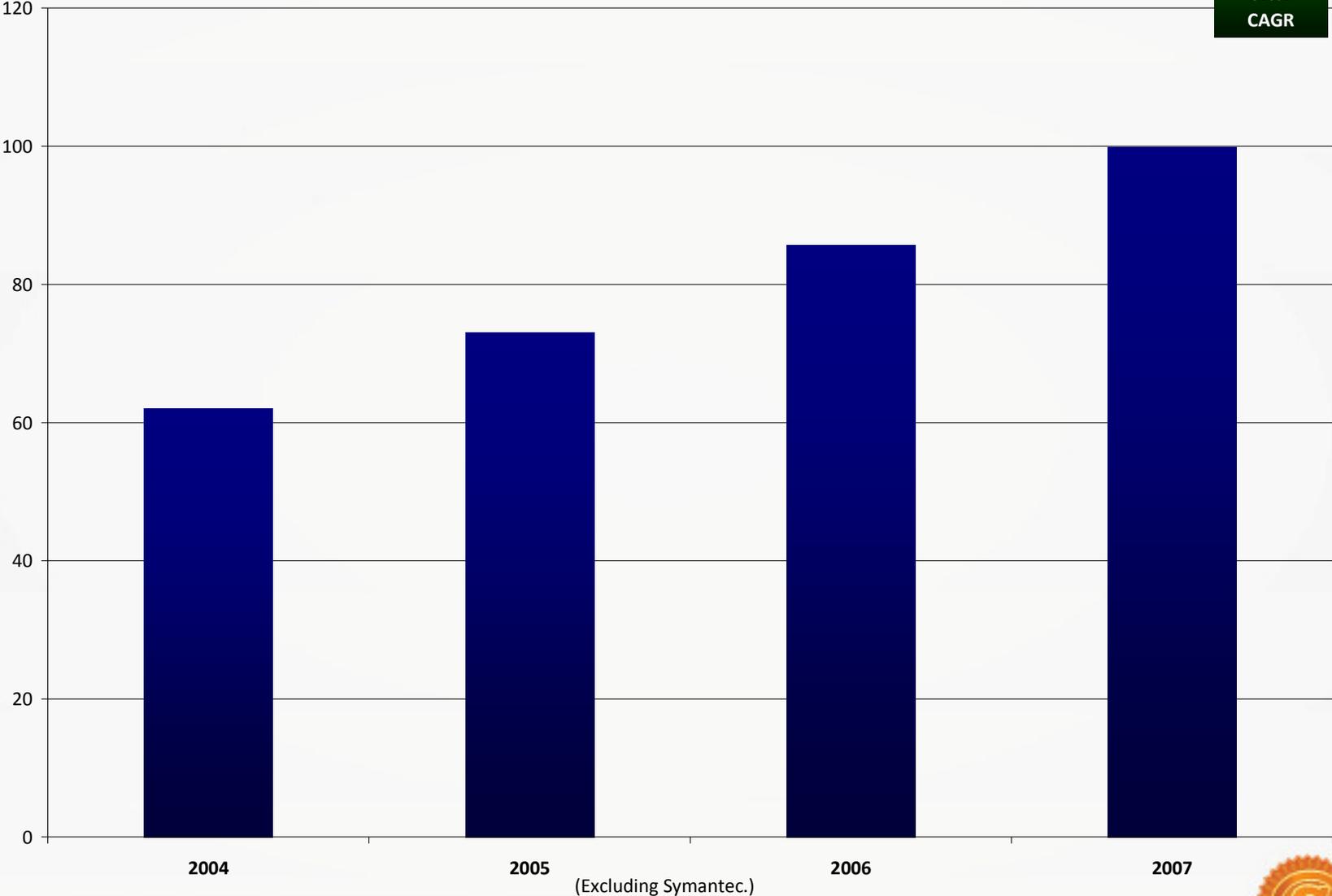
11.10%
CAGR



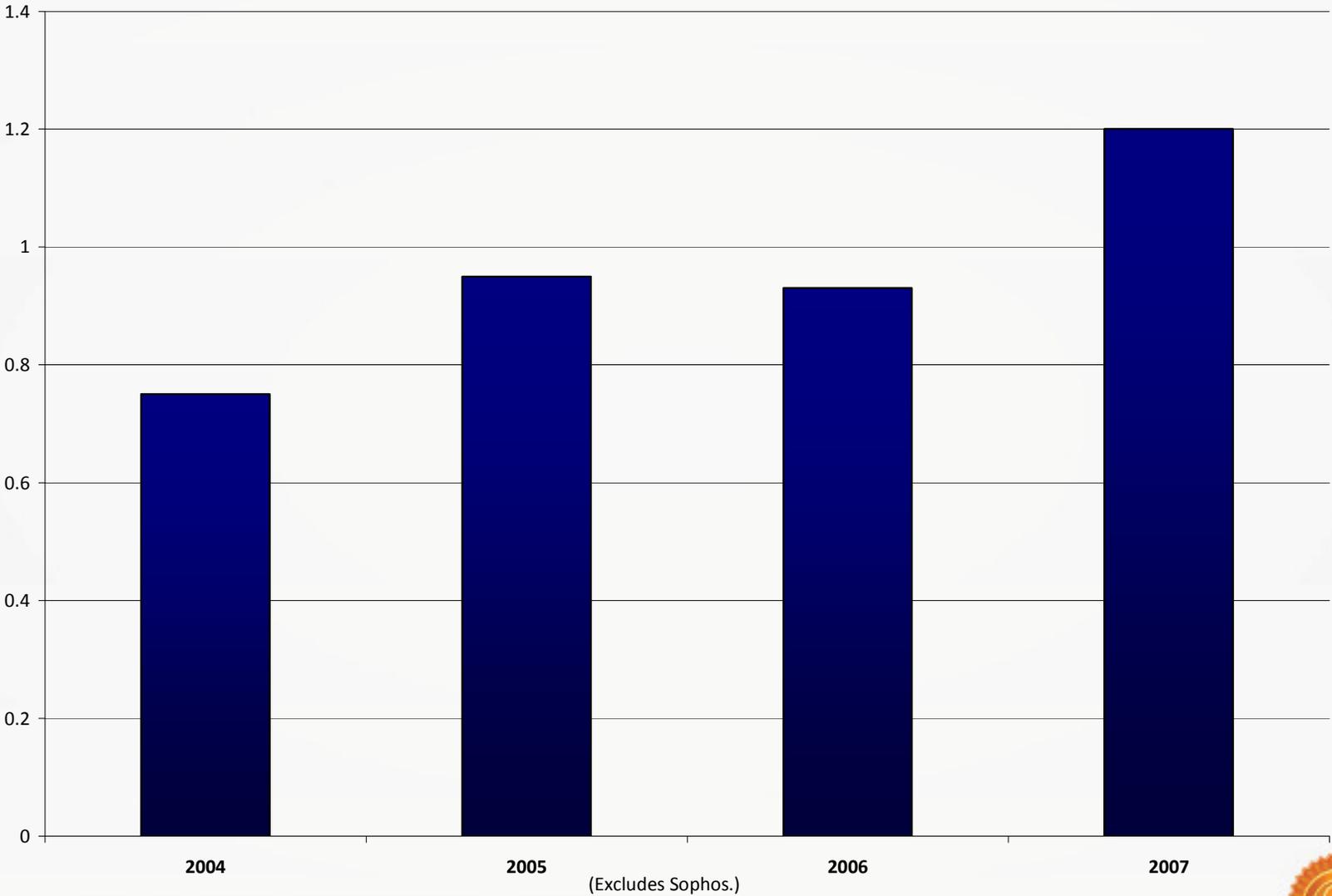
Sunbelt Software

Revenues

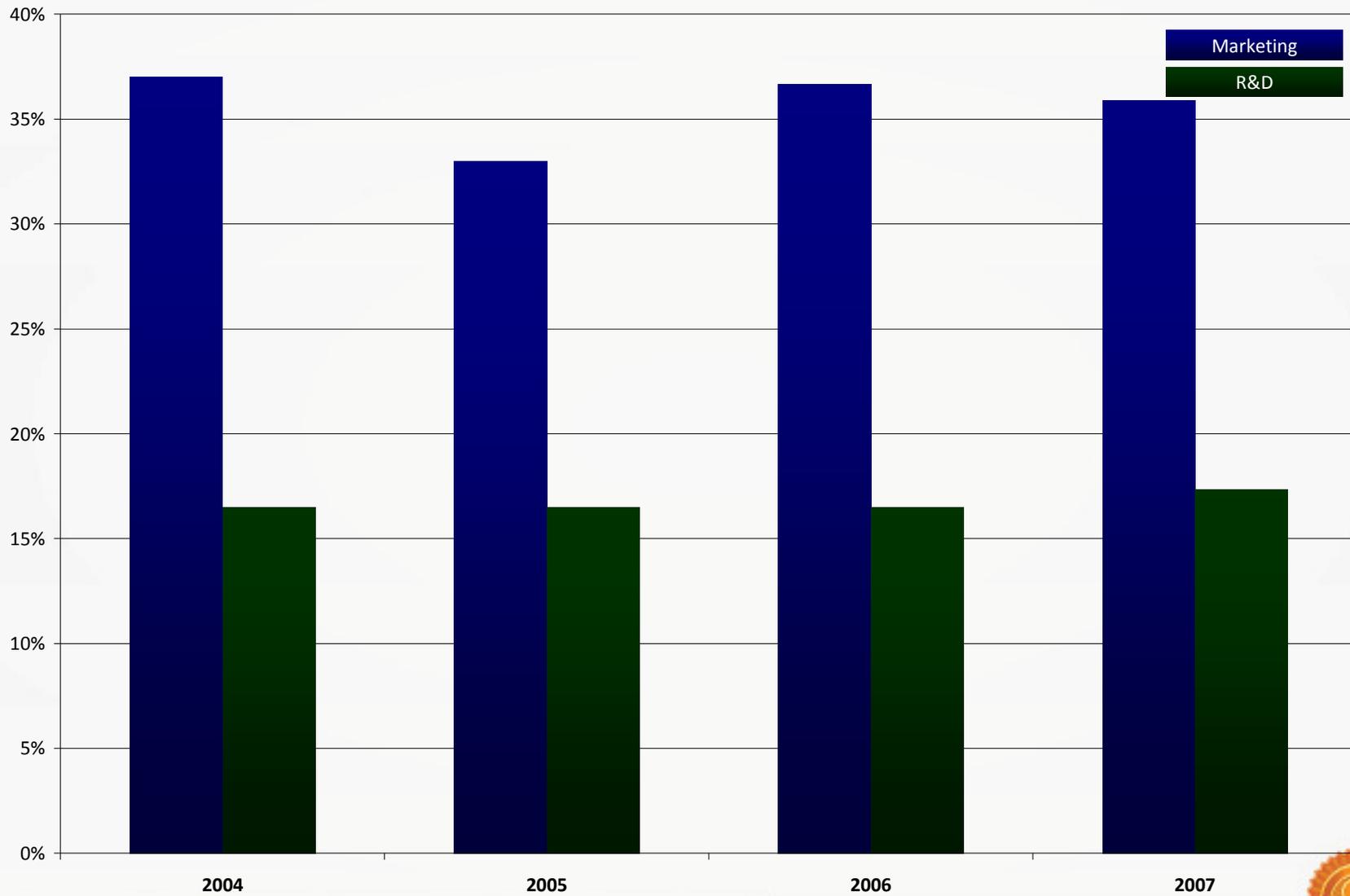
9.6%
CAGR



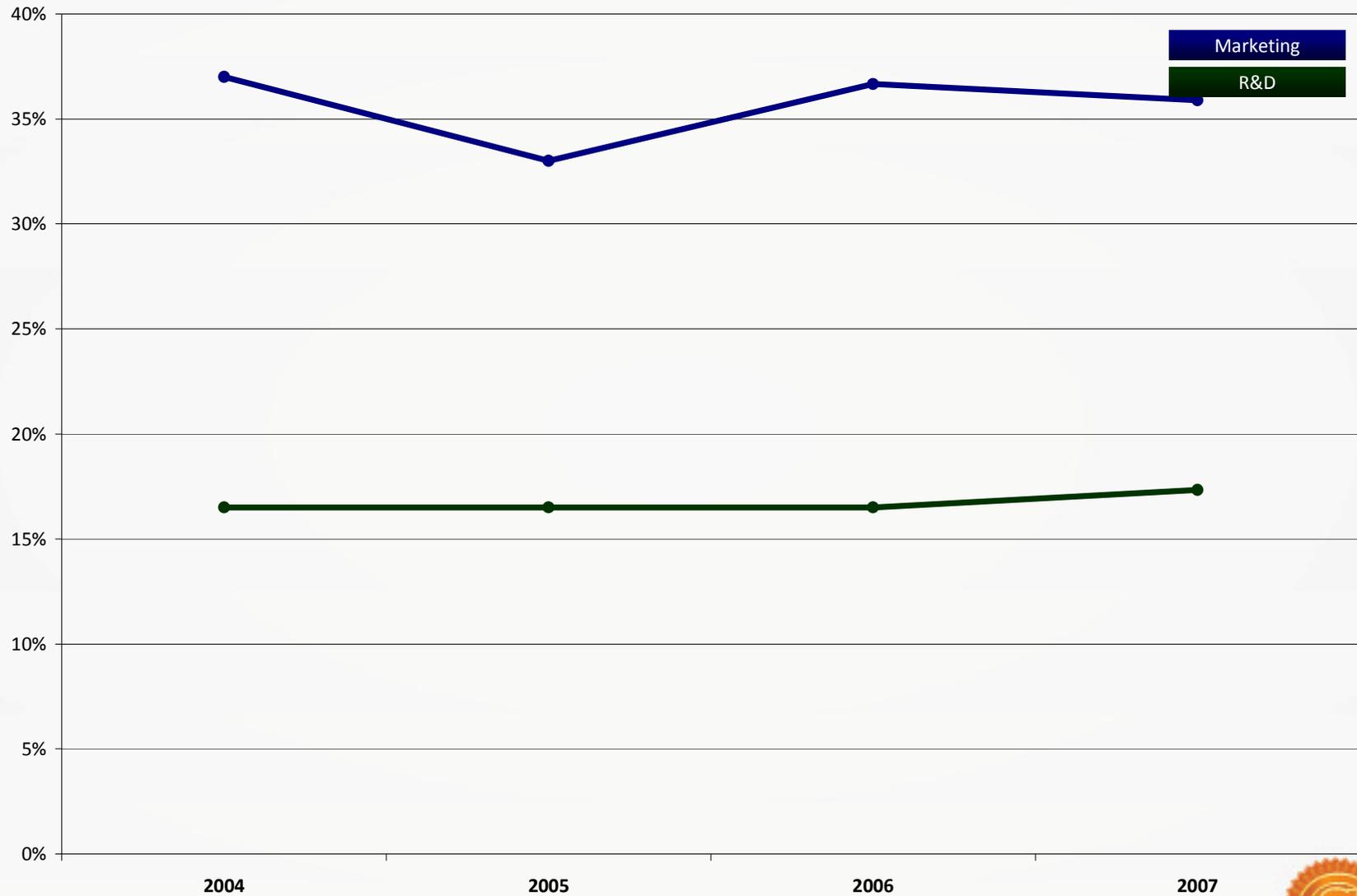
Earnings Per Share Growth



Median expenditures as a percentage of revenue



Median expenditures as a percentage of revenue



Sunbelt Software

What do customers think?



Sunbelt Software

Consumer antivirus user survey

754 surveys taken in September, 2008.

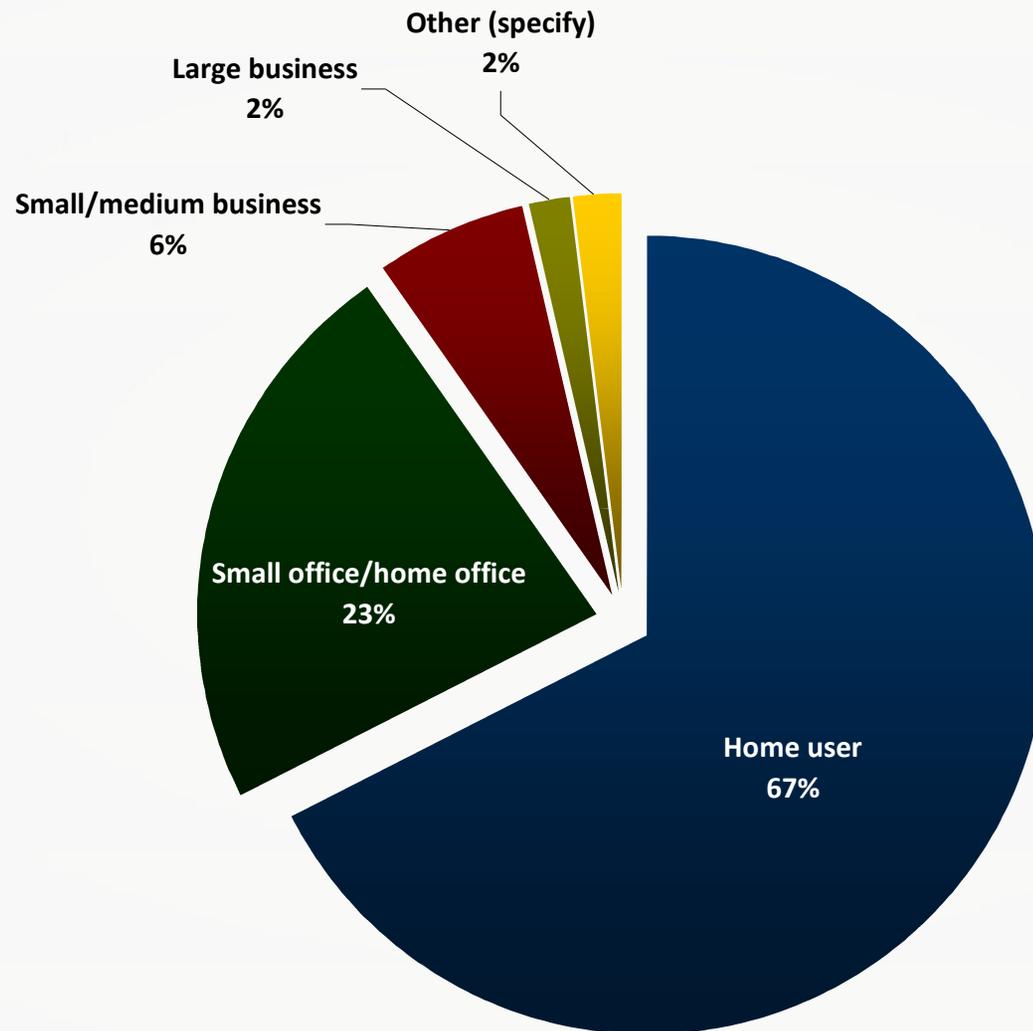
Public was readers of Wxpnews and VistaNews.

Sampling error of 3.6% (95% confidence interval).

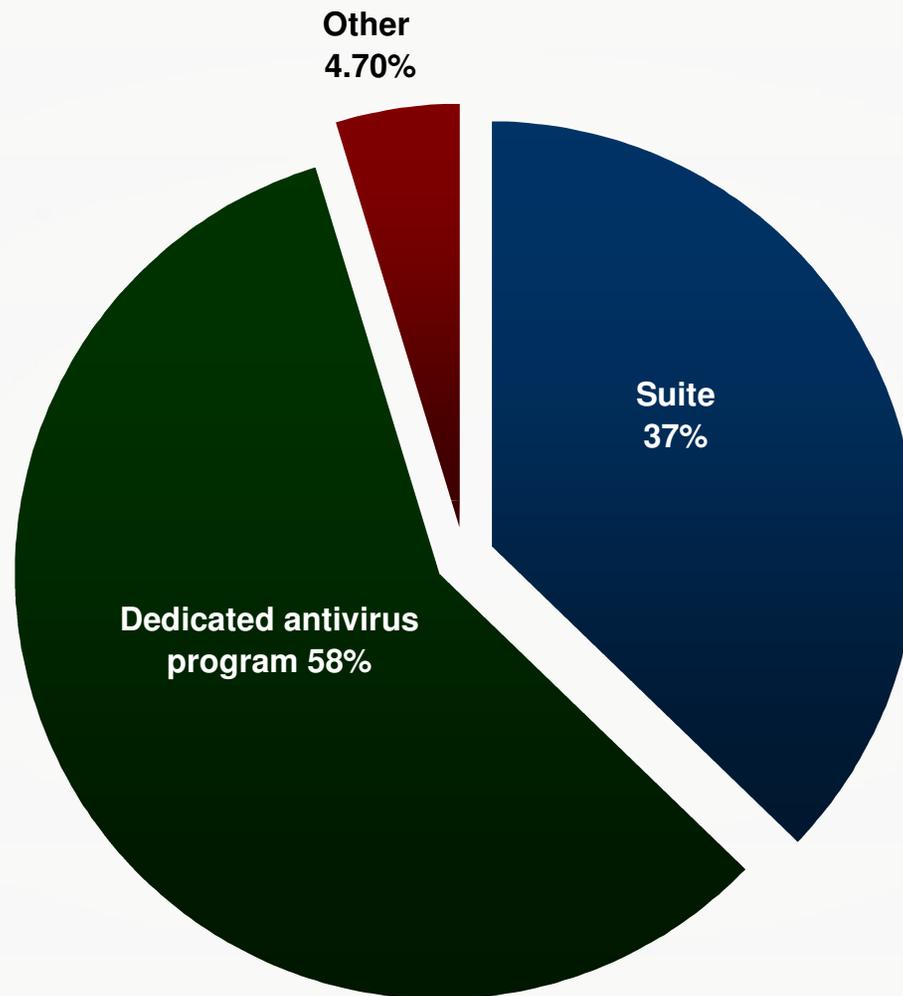


Sunbelt Software

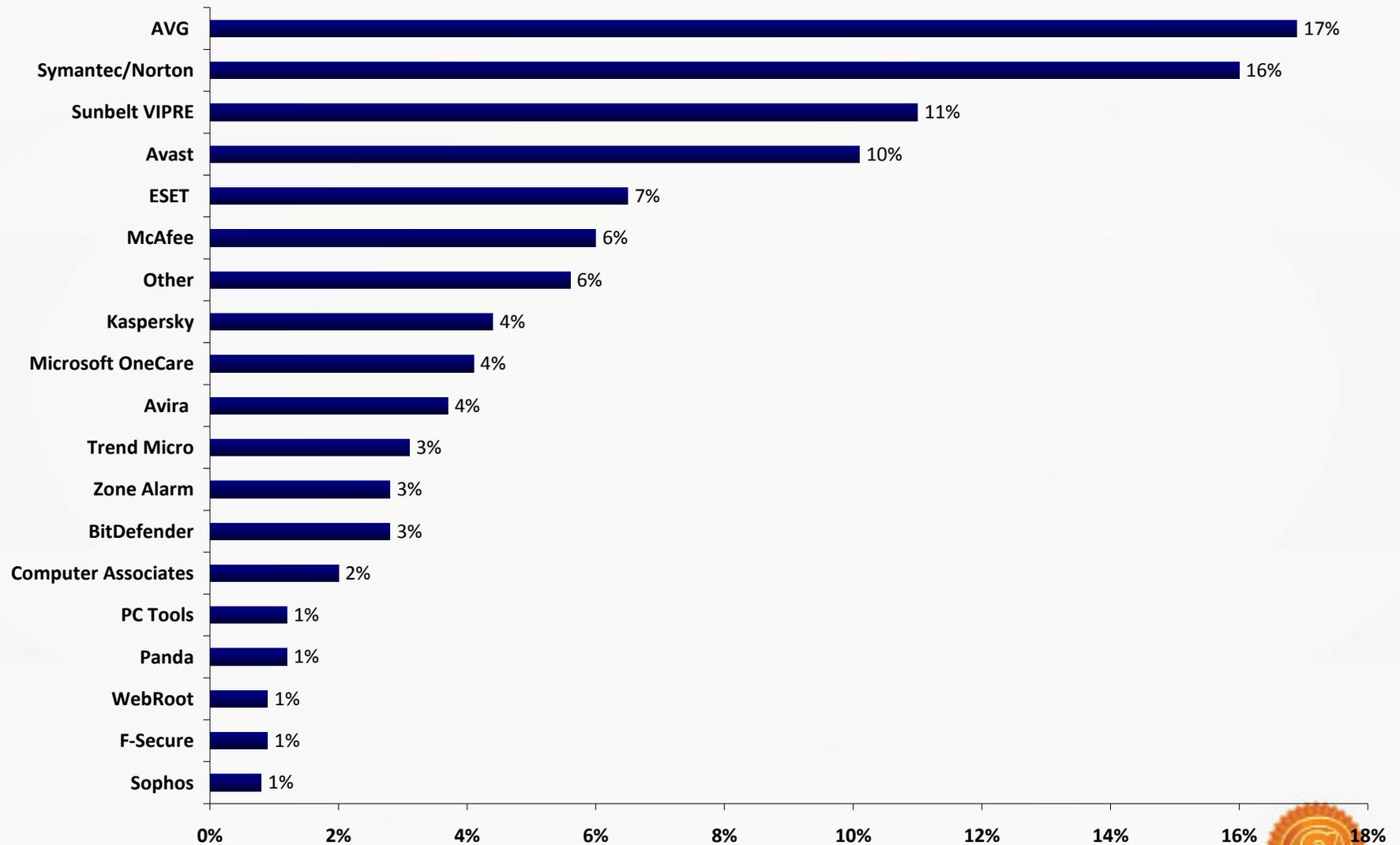
Type of customer



Type of product used

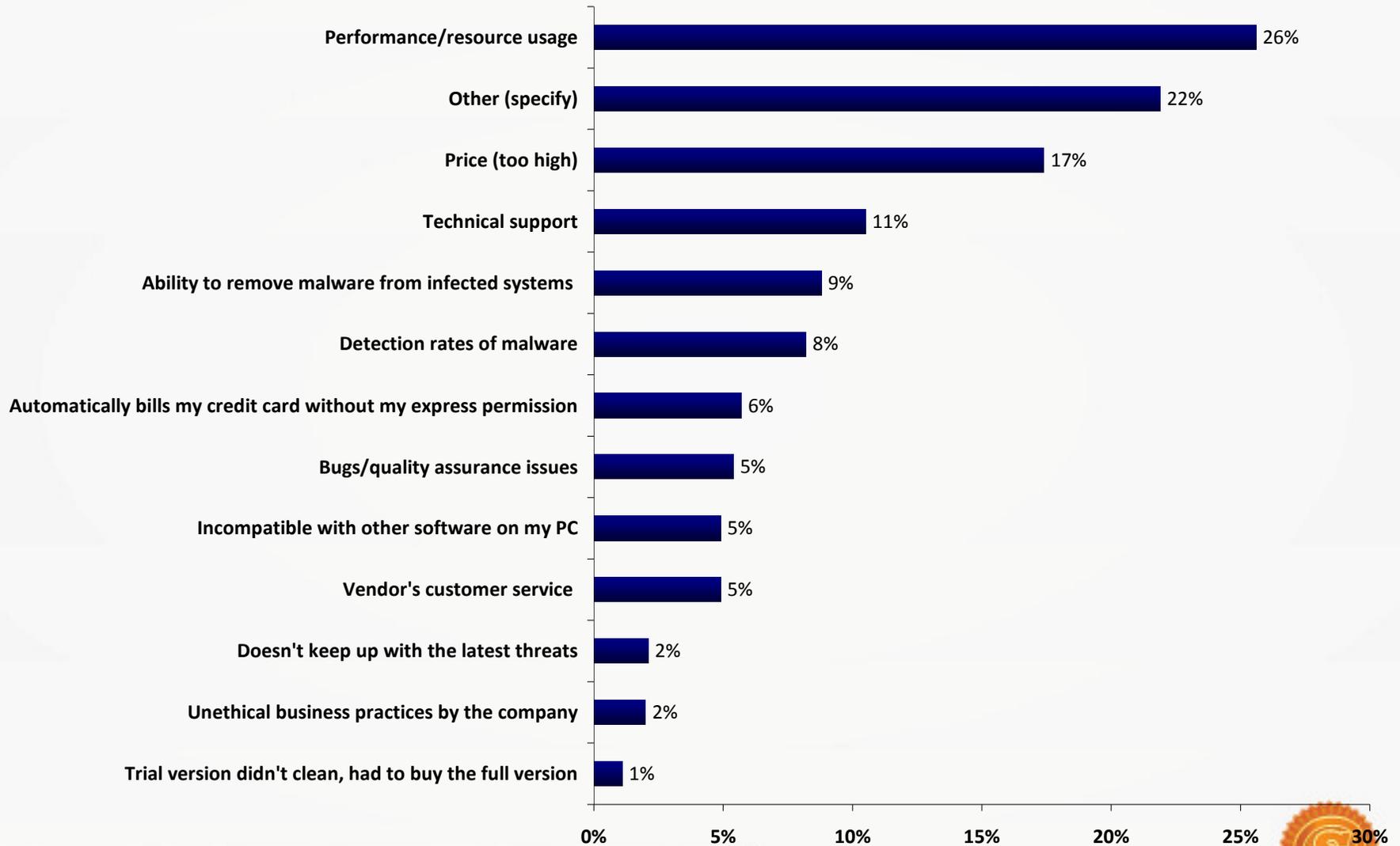


What brand is primarily used

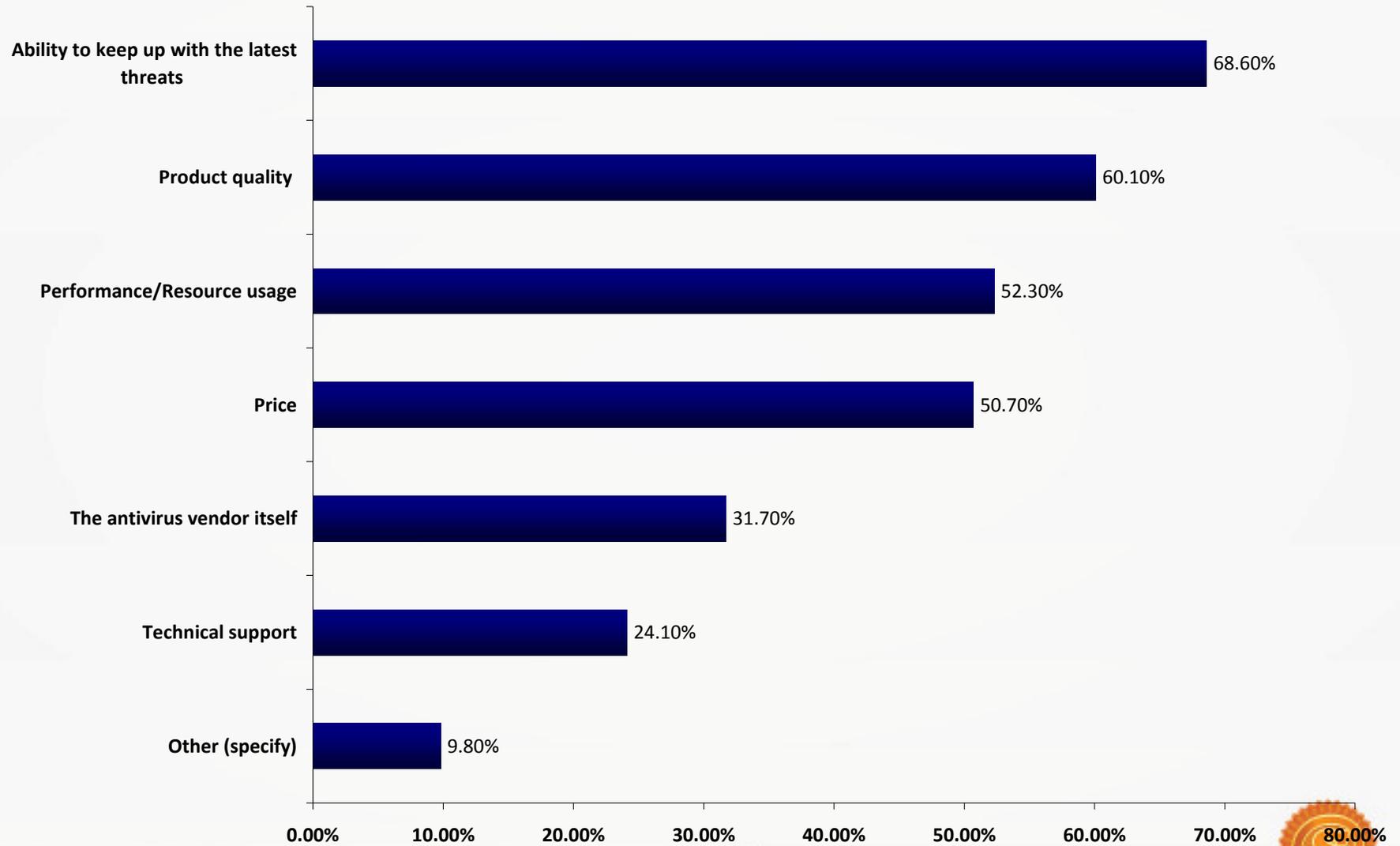


Sunbelt Software

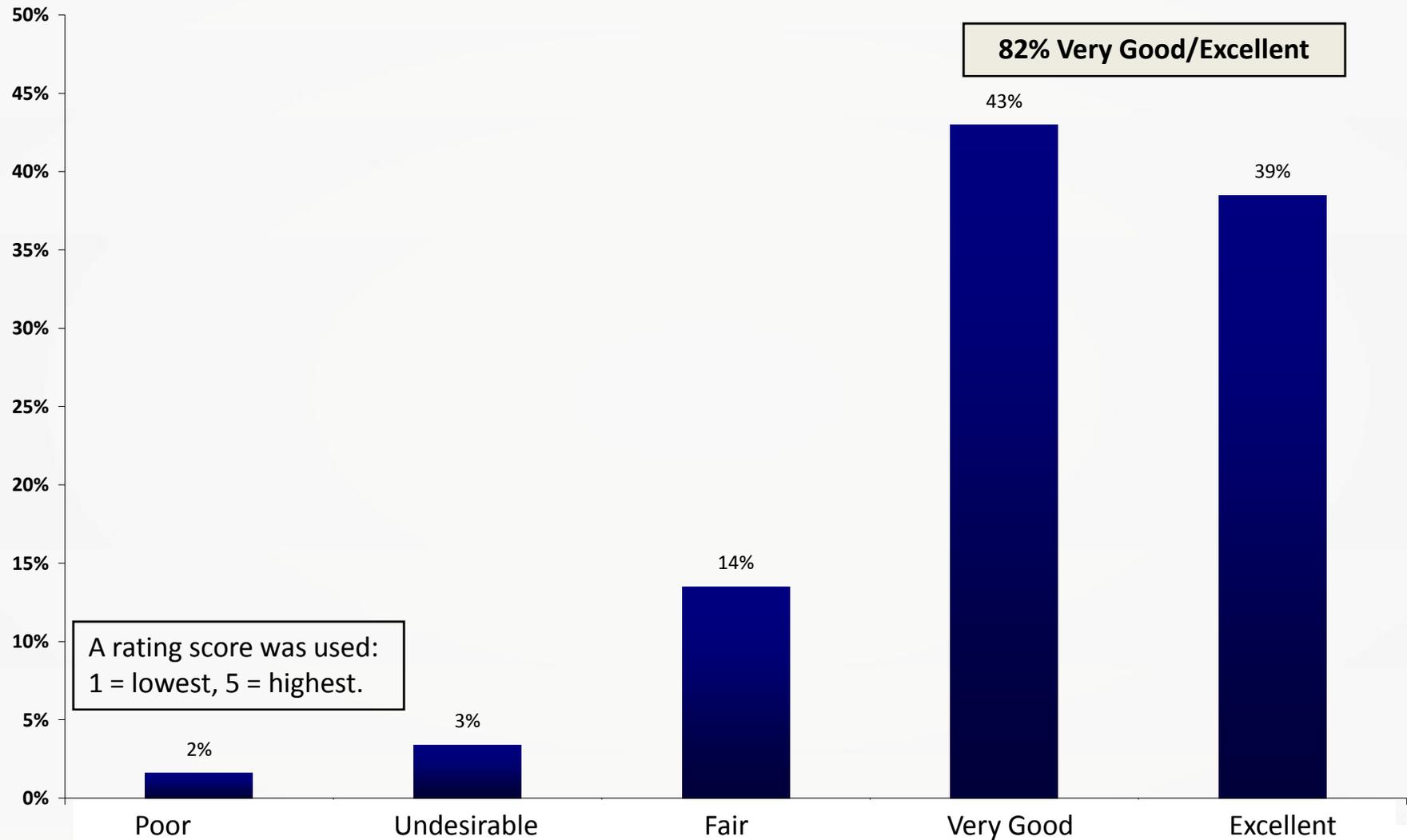
What do you *not like* about your AV program?



What do you *like*?

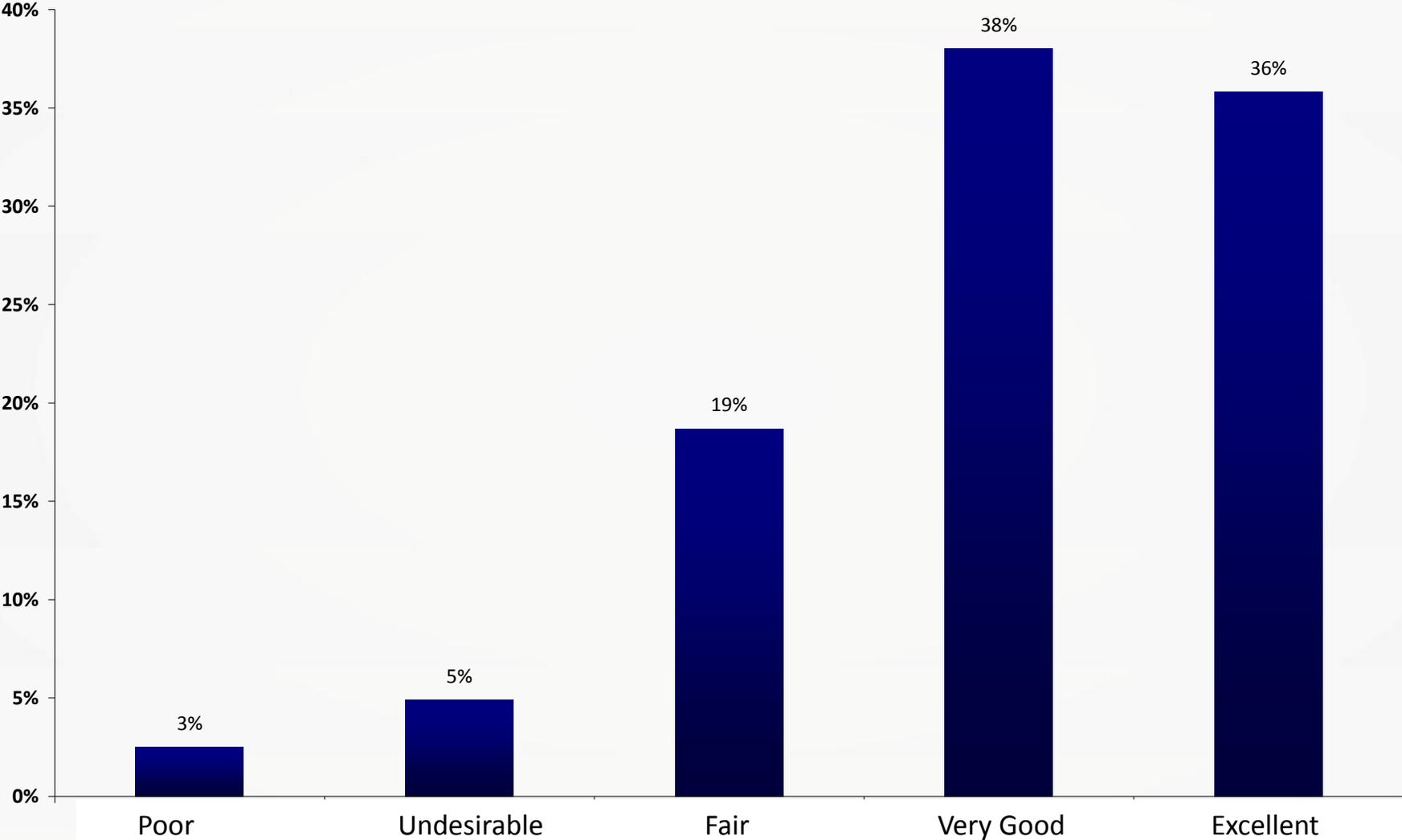


Your overall opinion of your antivirus product?

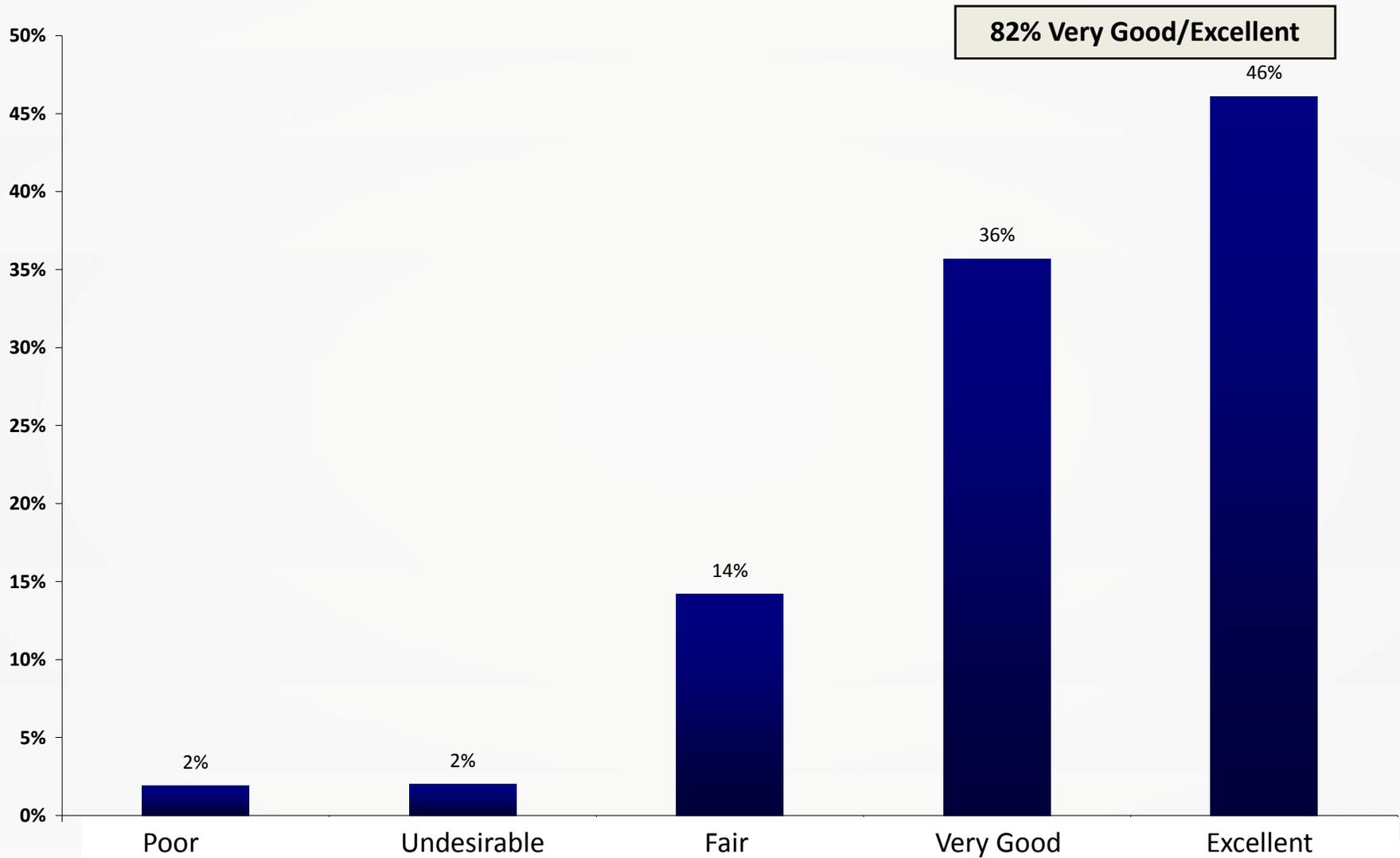


Overall opinion of your antivirus vendor?

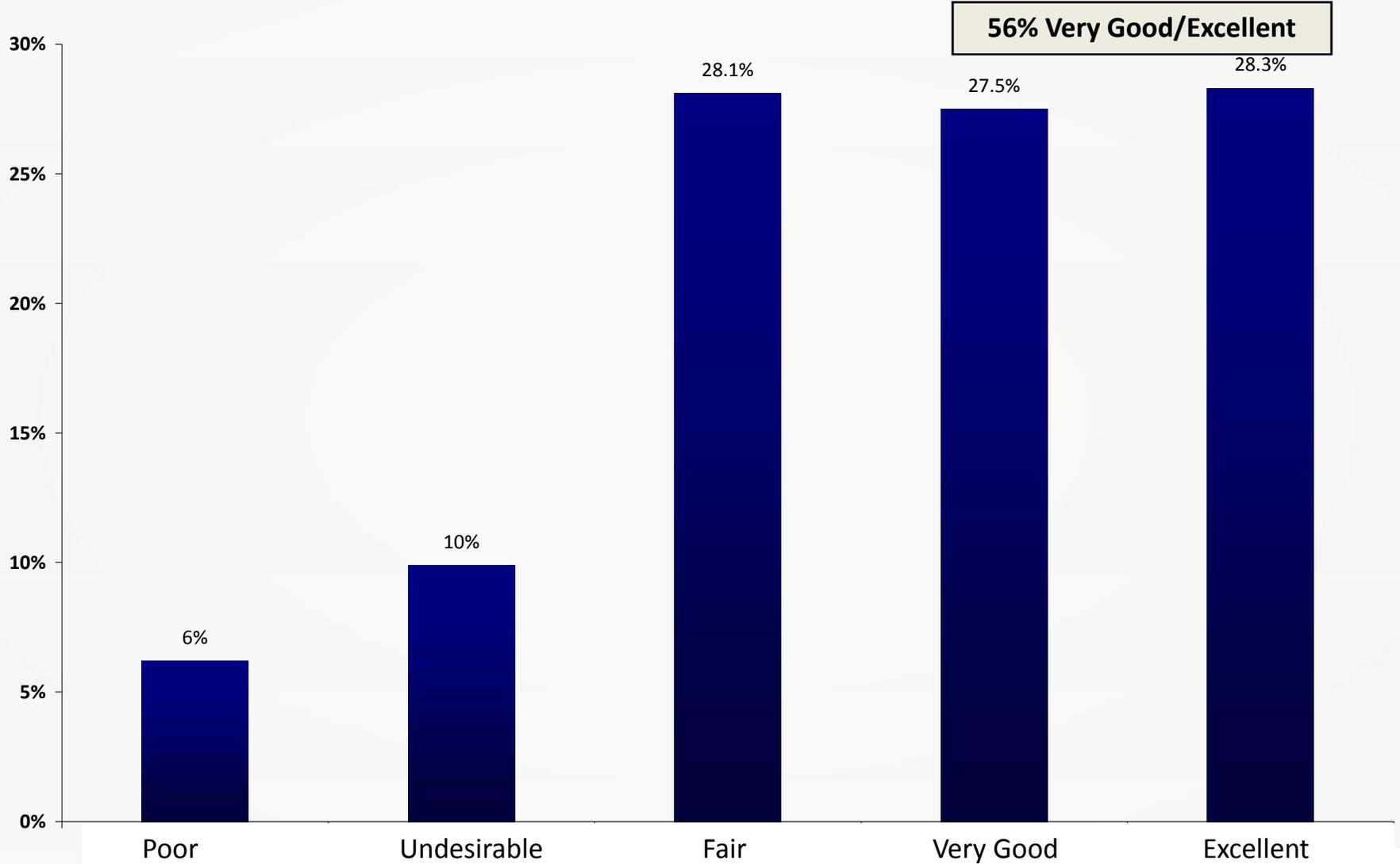
74% Very Good/Excellent



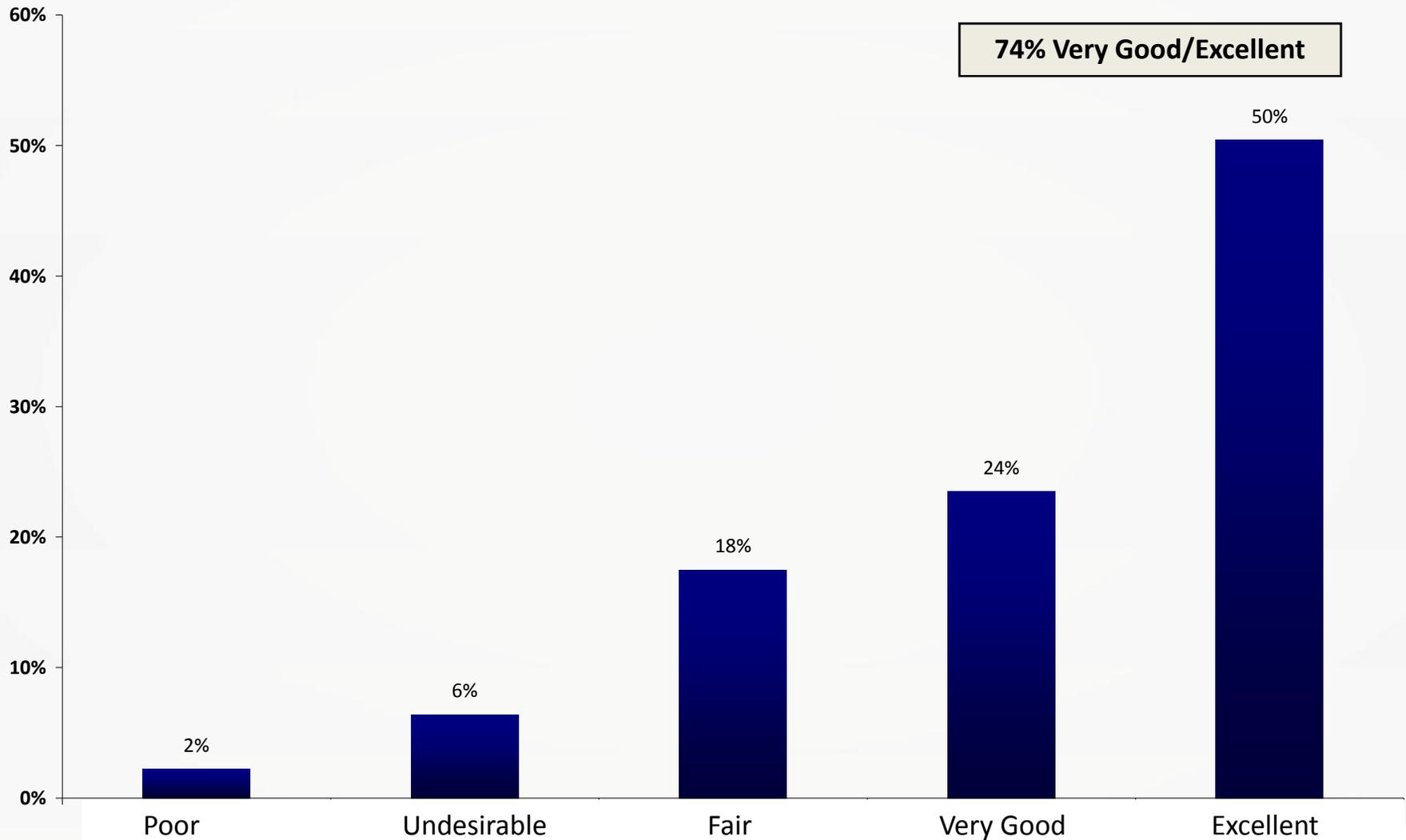
Trustworthiness of your antivirus vendor?



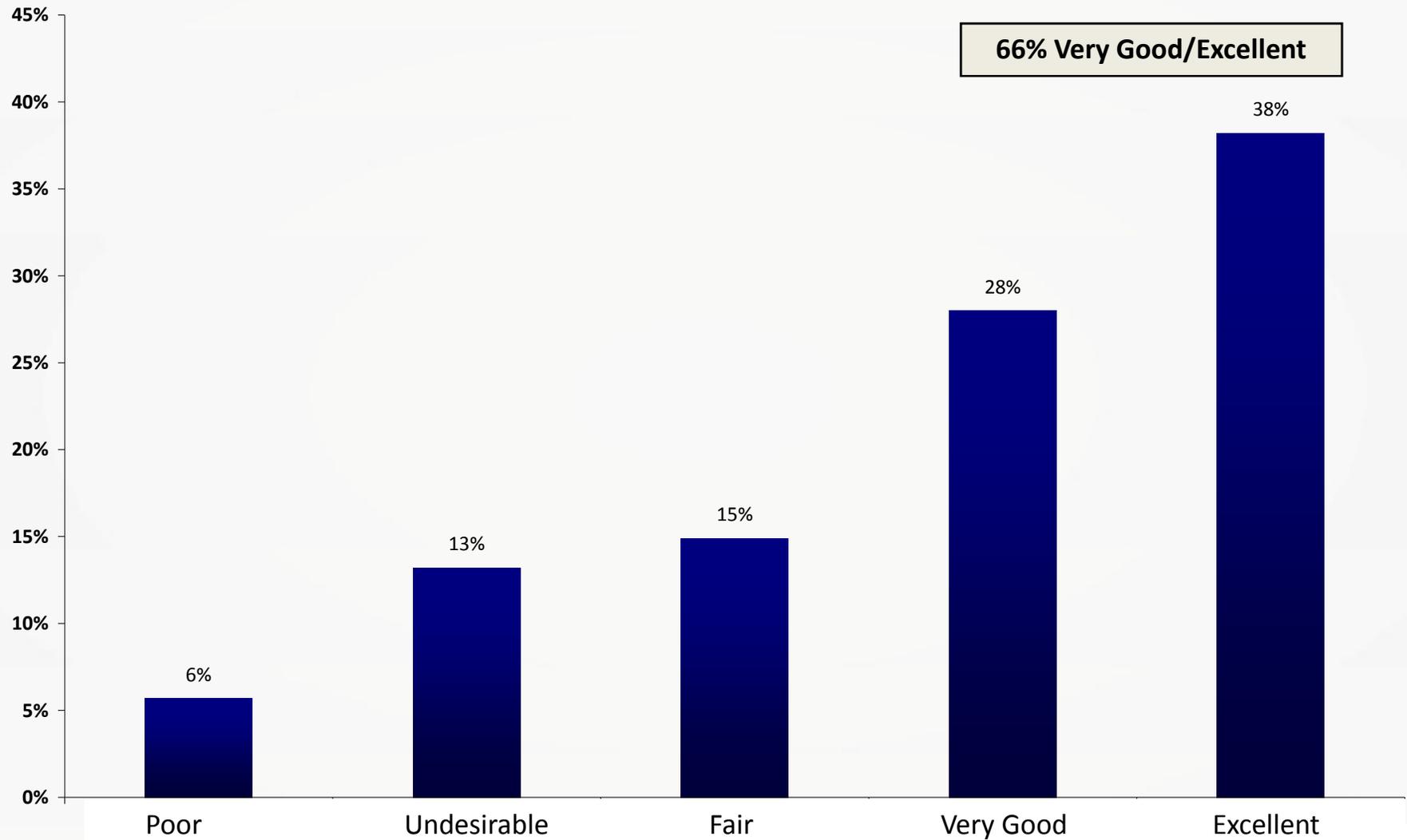
How would you rate the technical support?



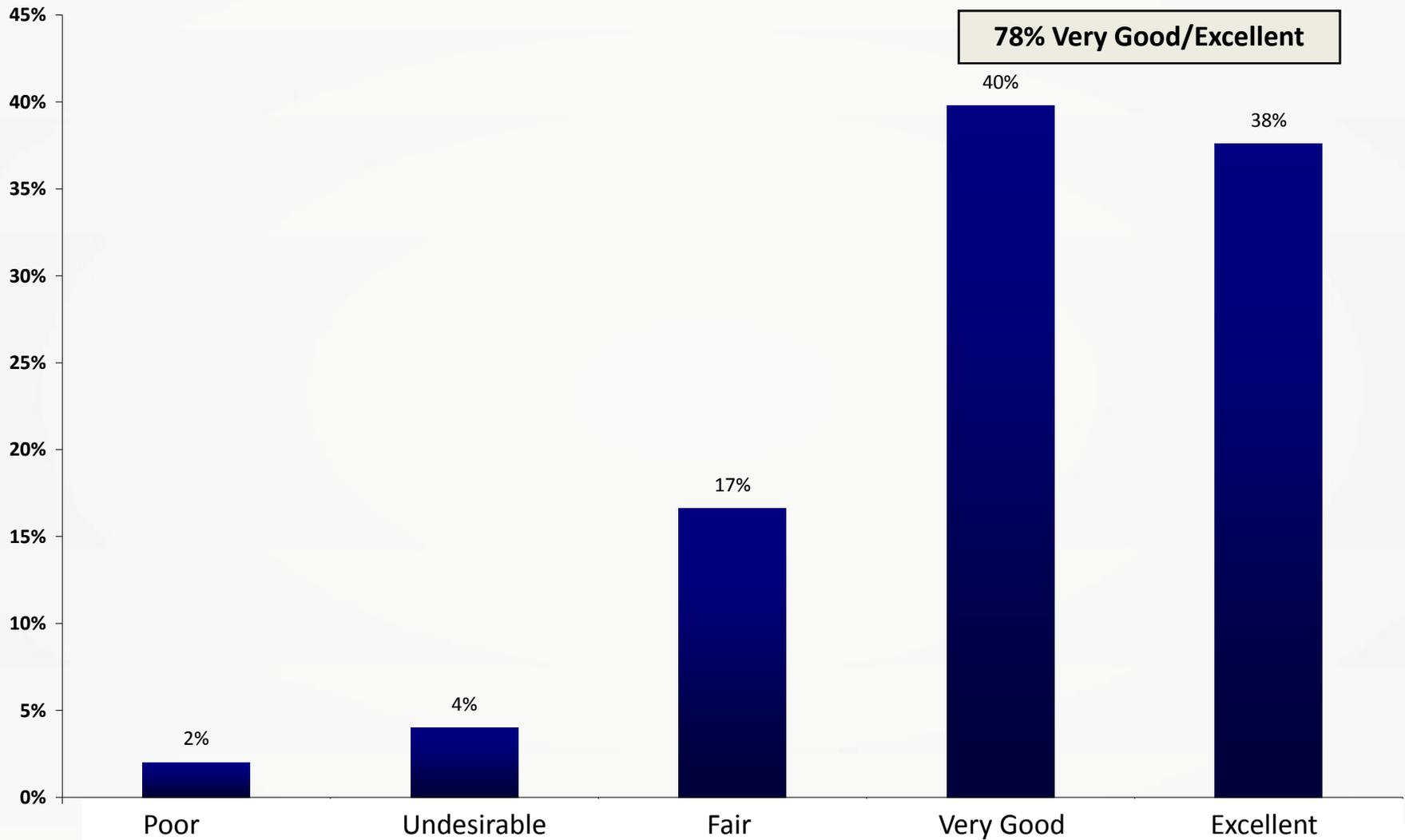
The value for your money of your antivirus product?



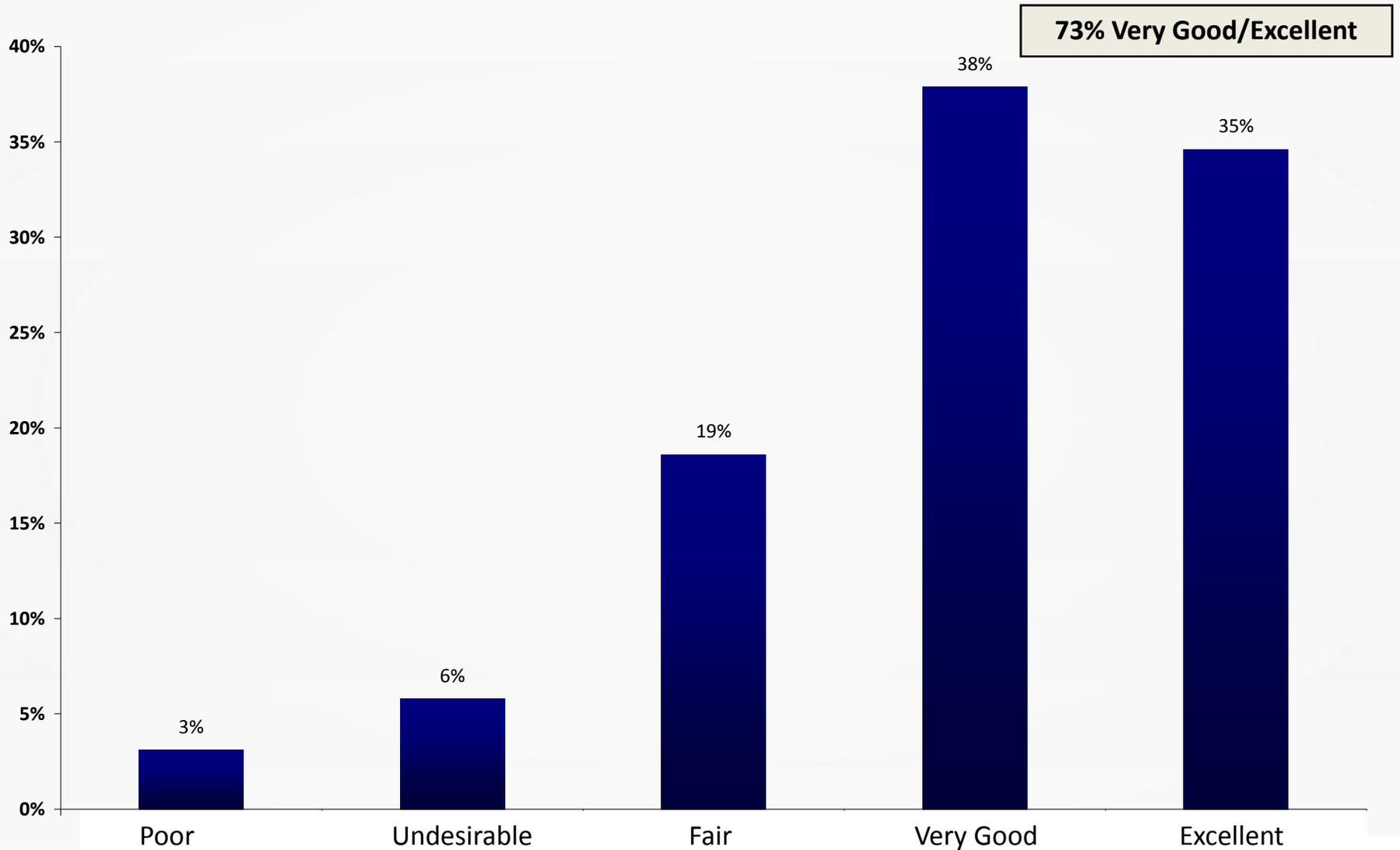
The performance and resource usage?



Ability to protect you against malware?



How well does it clean up malware infections?



Enterprise antivirus user survey

207 surveys taken in September, 2008.

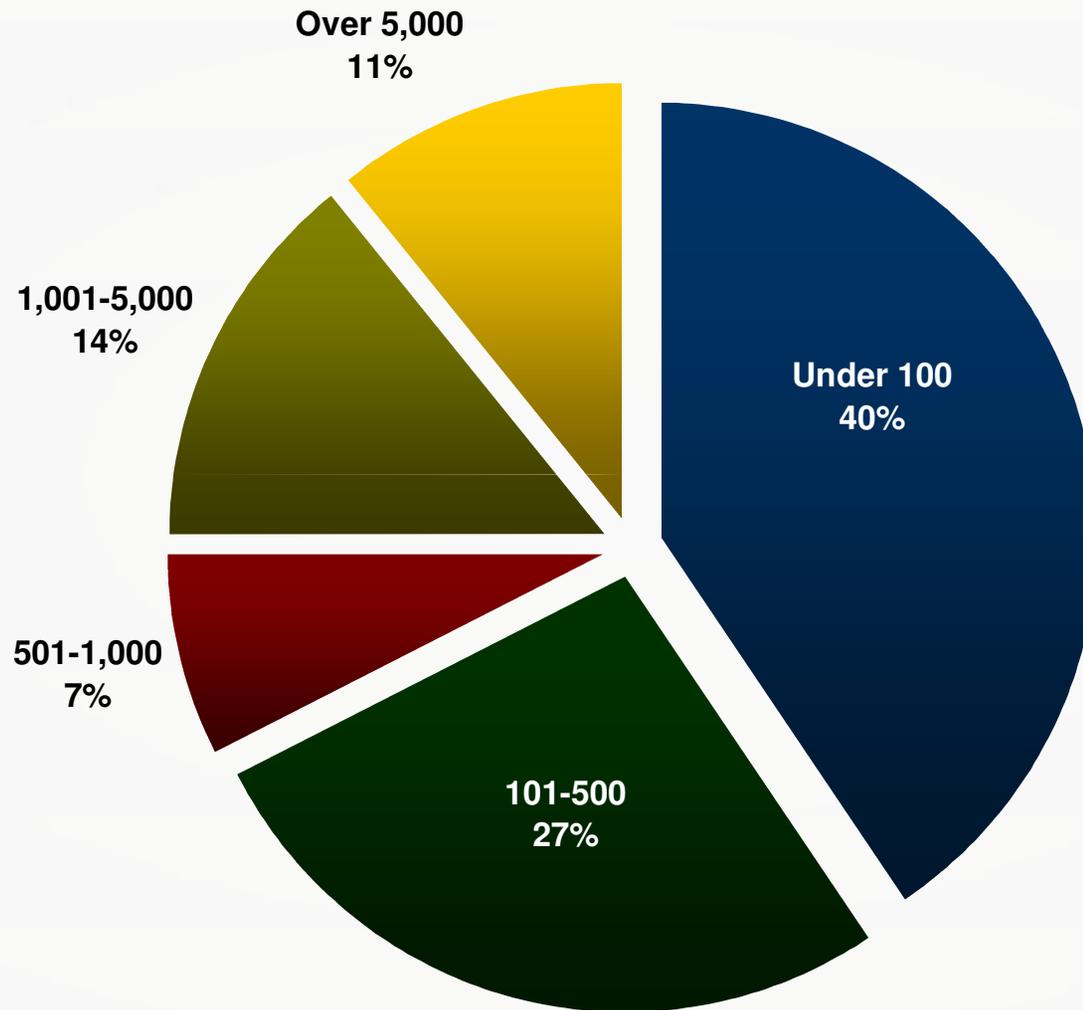
Public was readers of WServerNews and NT
SysAdmin forum.

Sampling error of 6.8% (95% confidence interval).

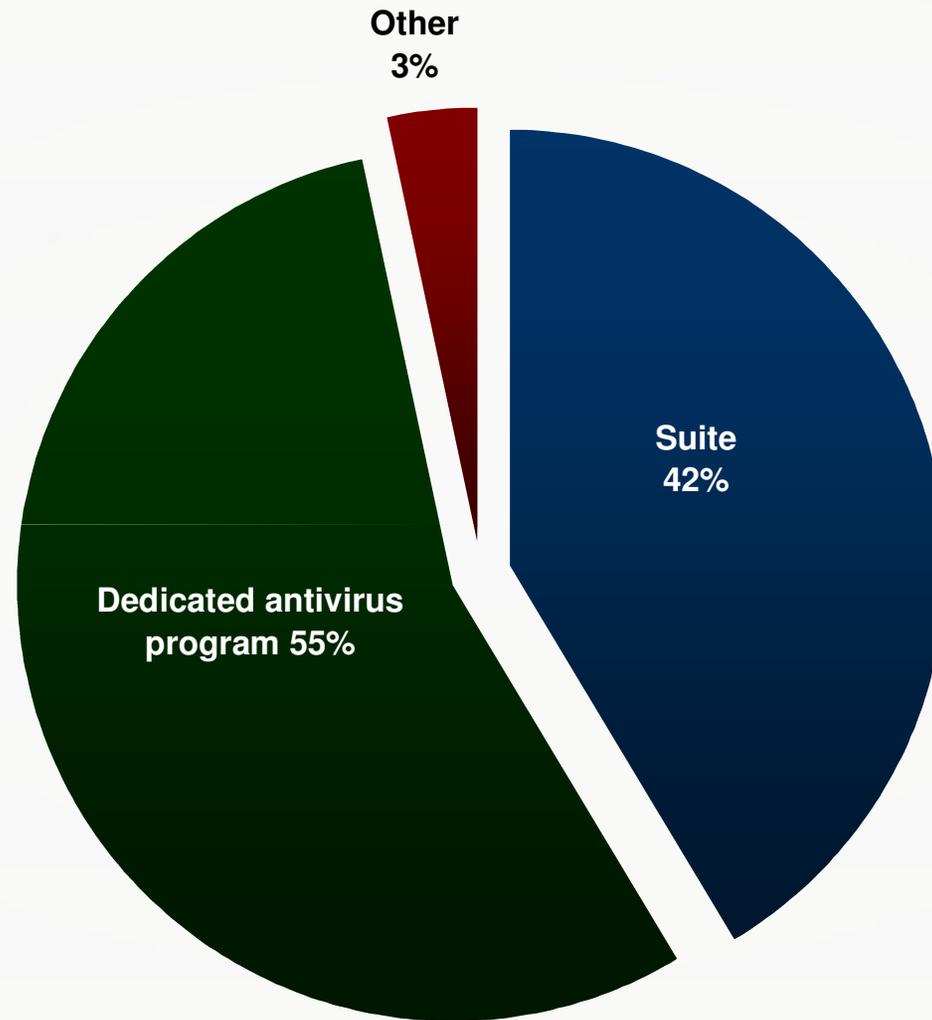


Sunbelt Software

How many seats are there in your enterprise?

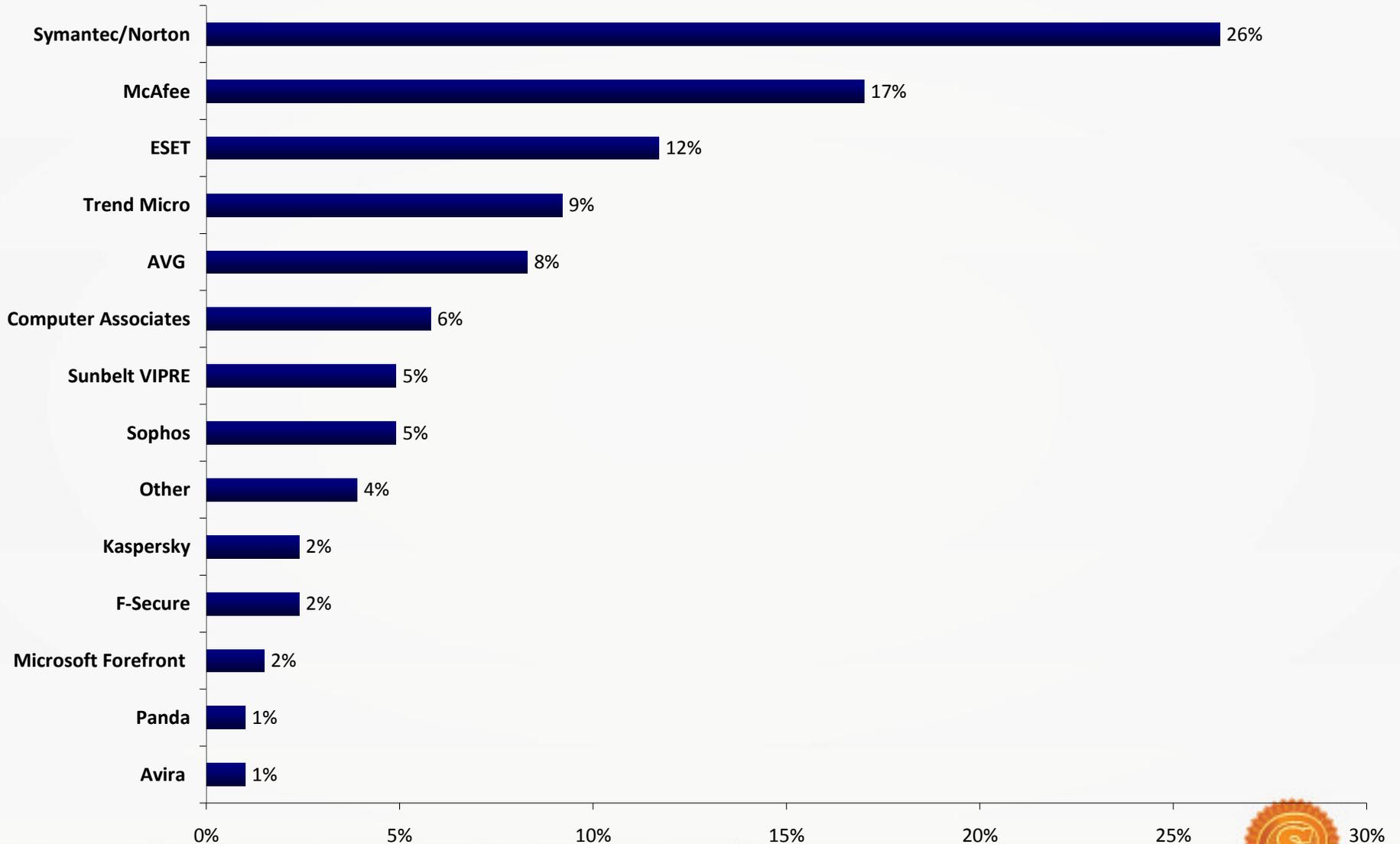


Are you running a suite or a dedicated antivirus program?



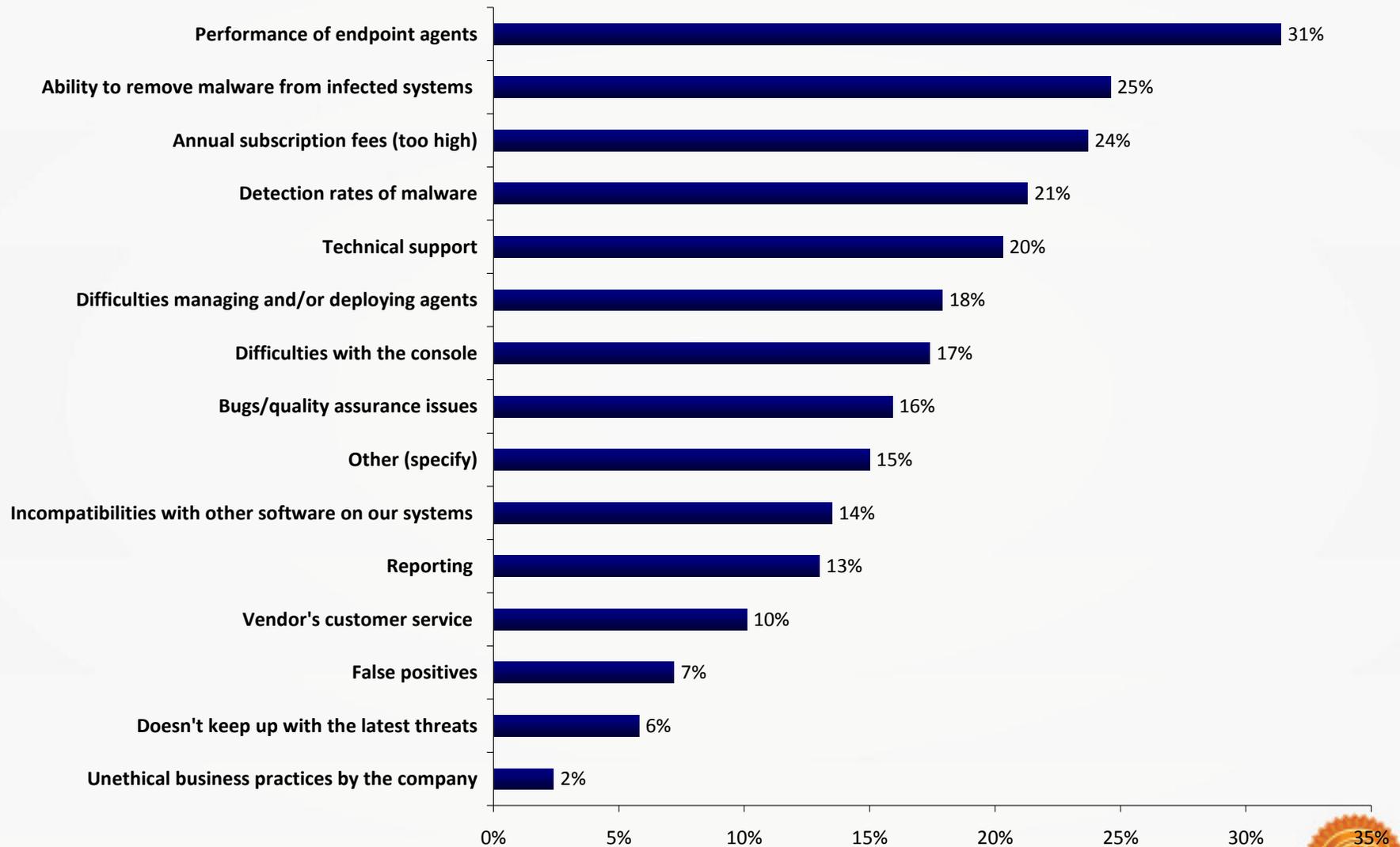
Sunbelt Software

What is your primary antivirus product for endpoints?

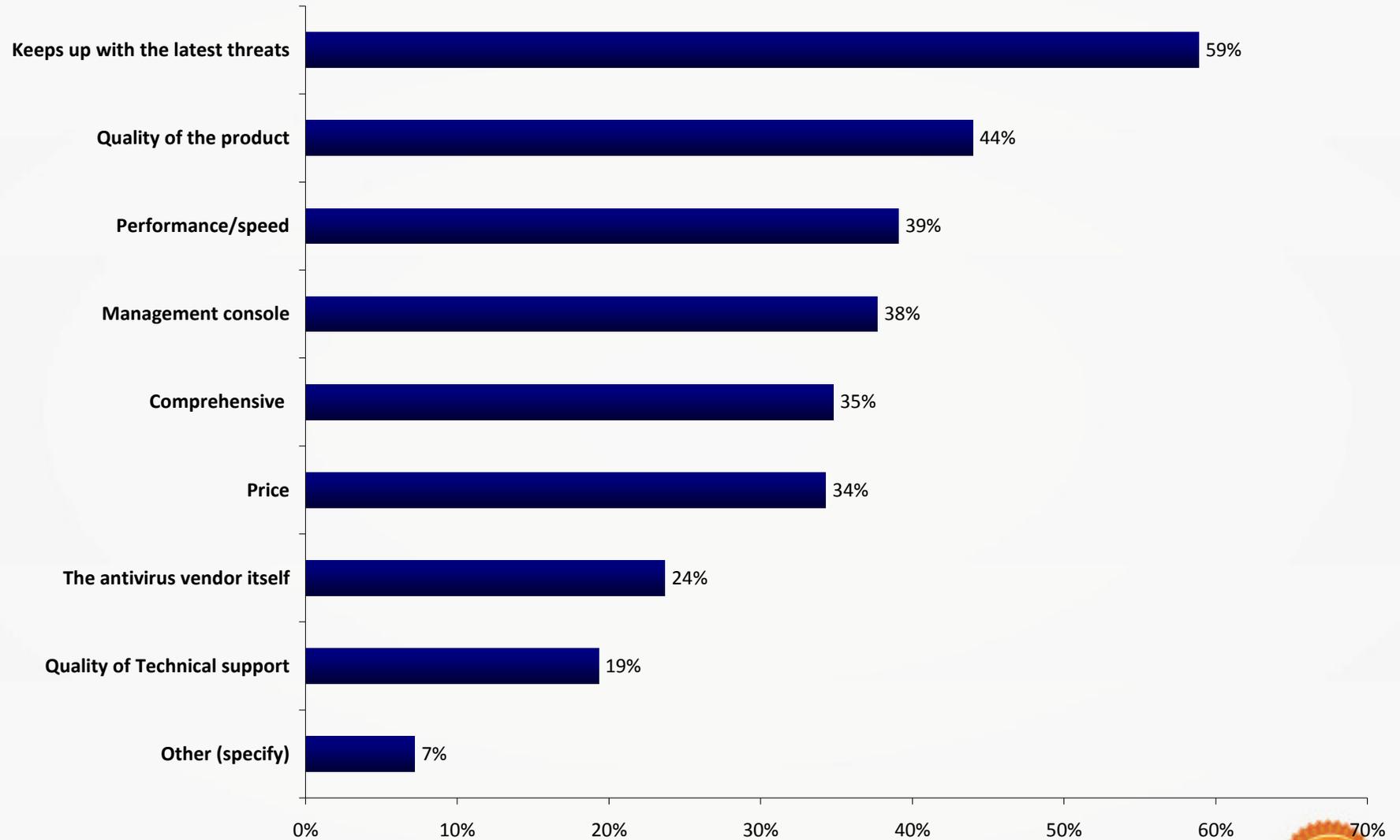


Sunbelt Software

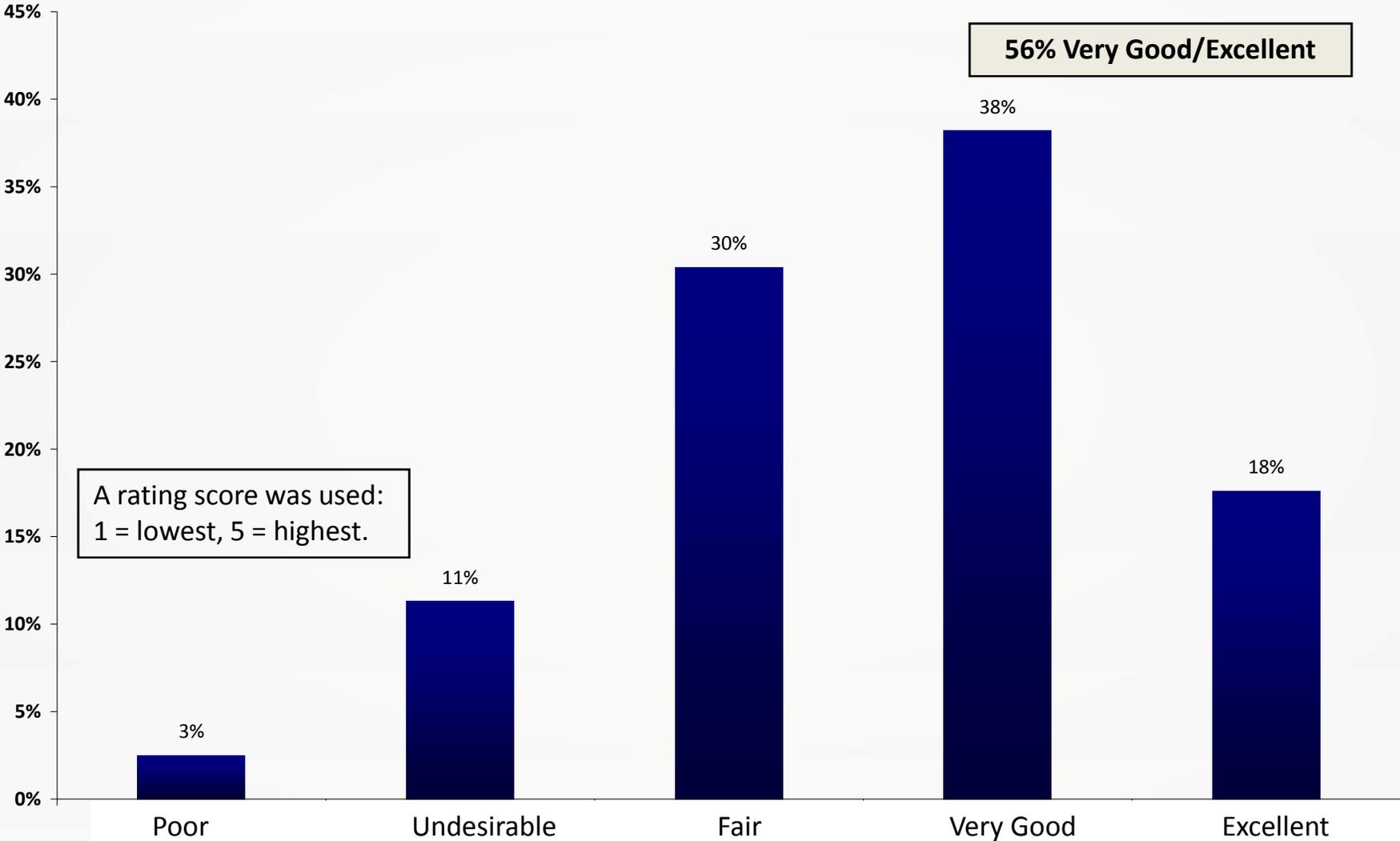
What do you *not like* about your existing antivirus solution?



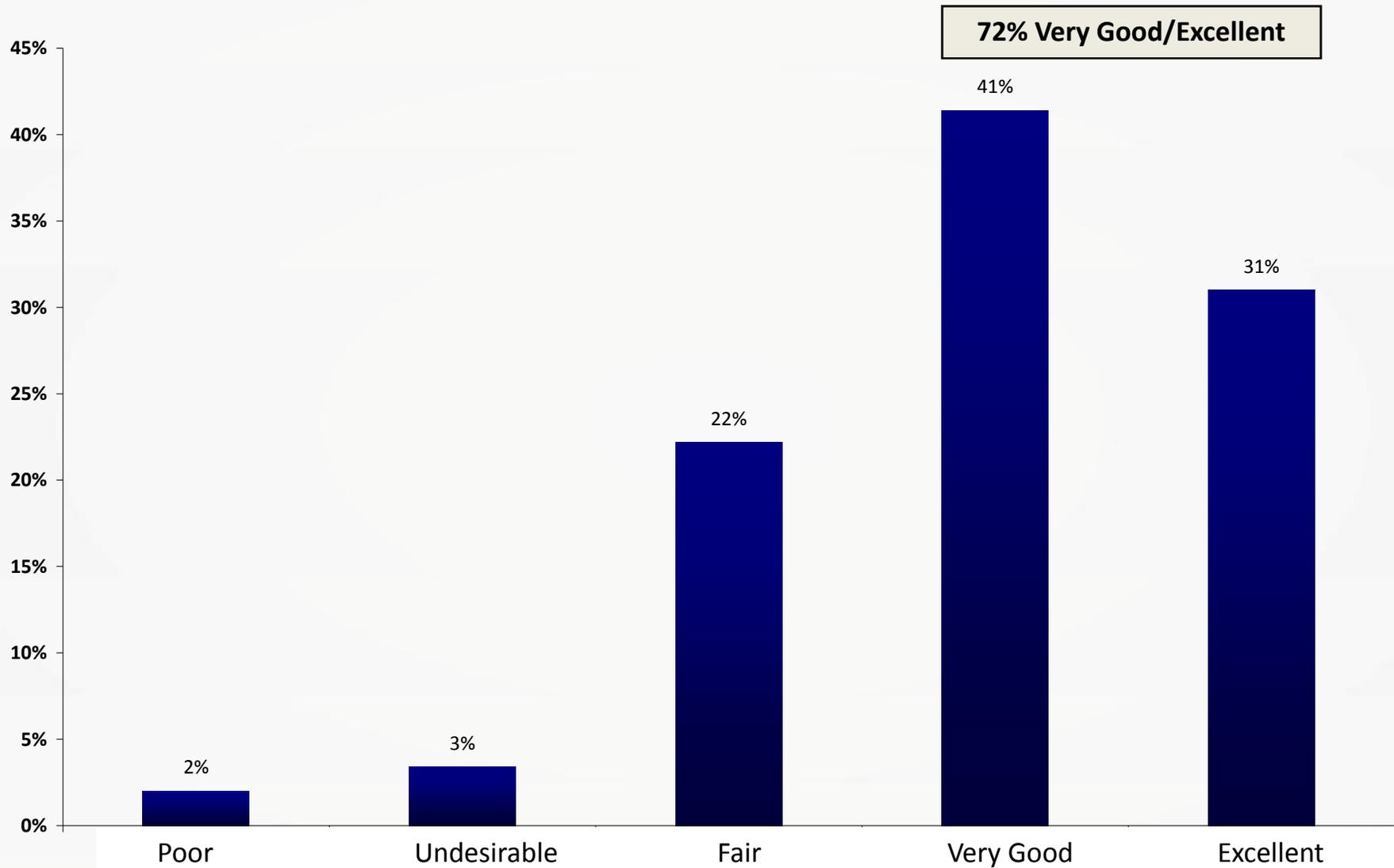
What do you *like* about your existing antivirus solution?



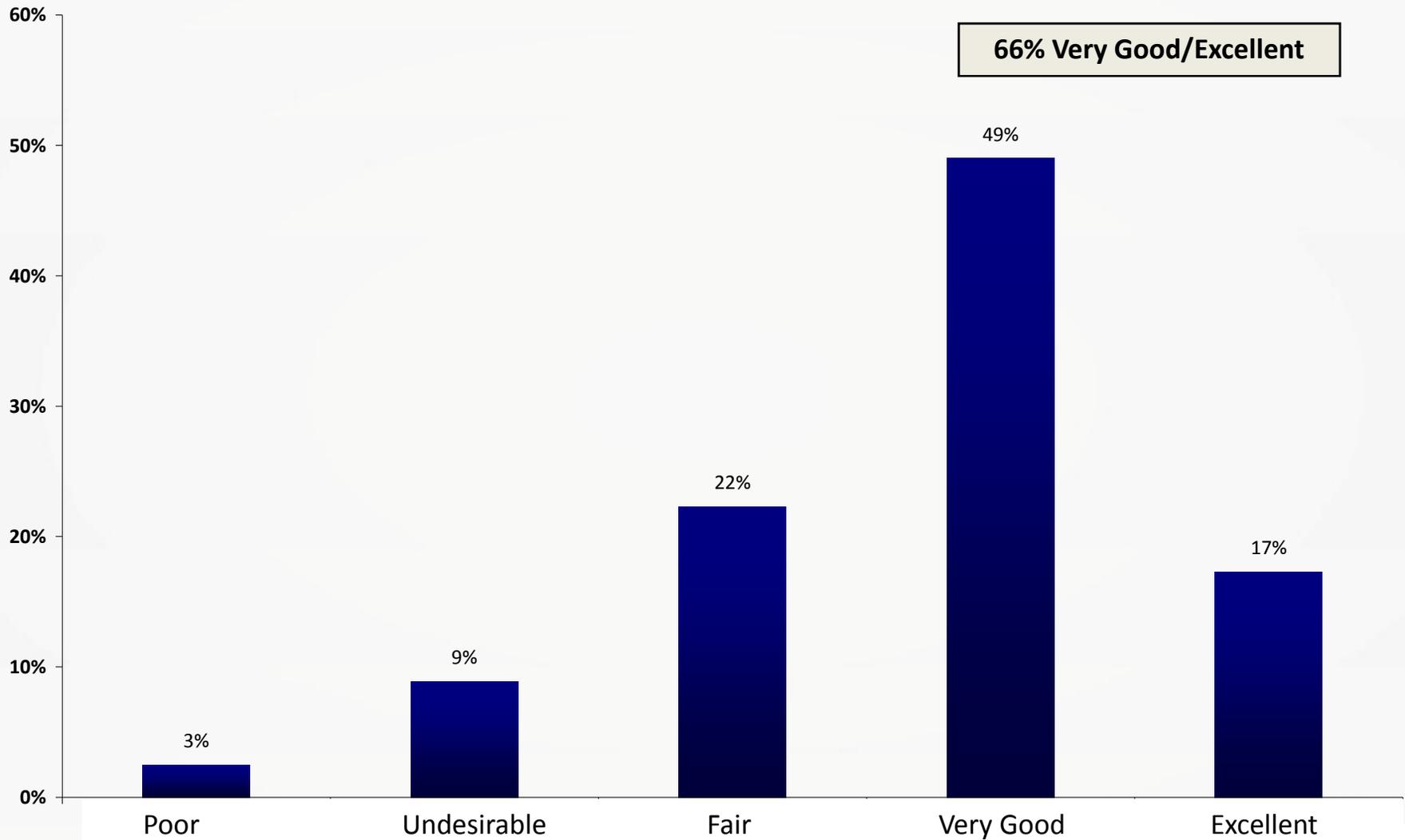
Overall opinion of your antivirus vendor?



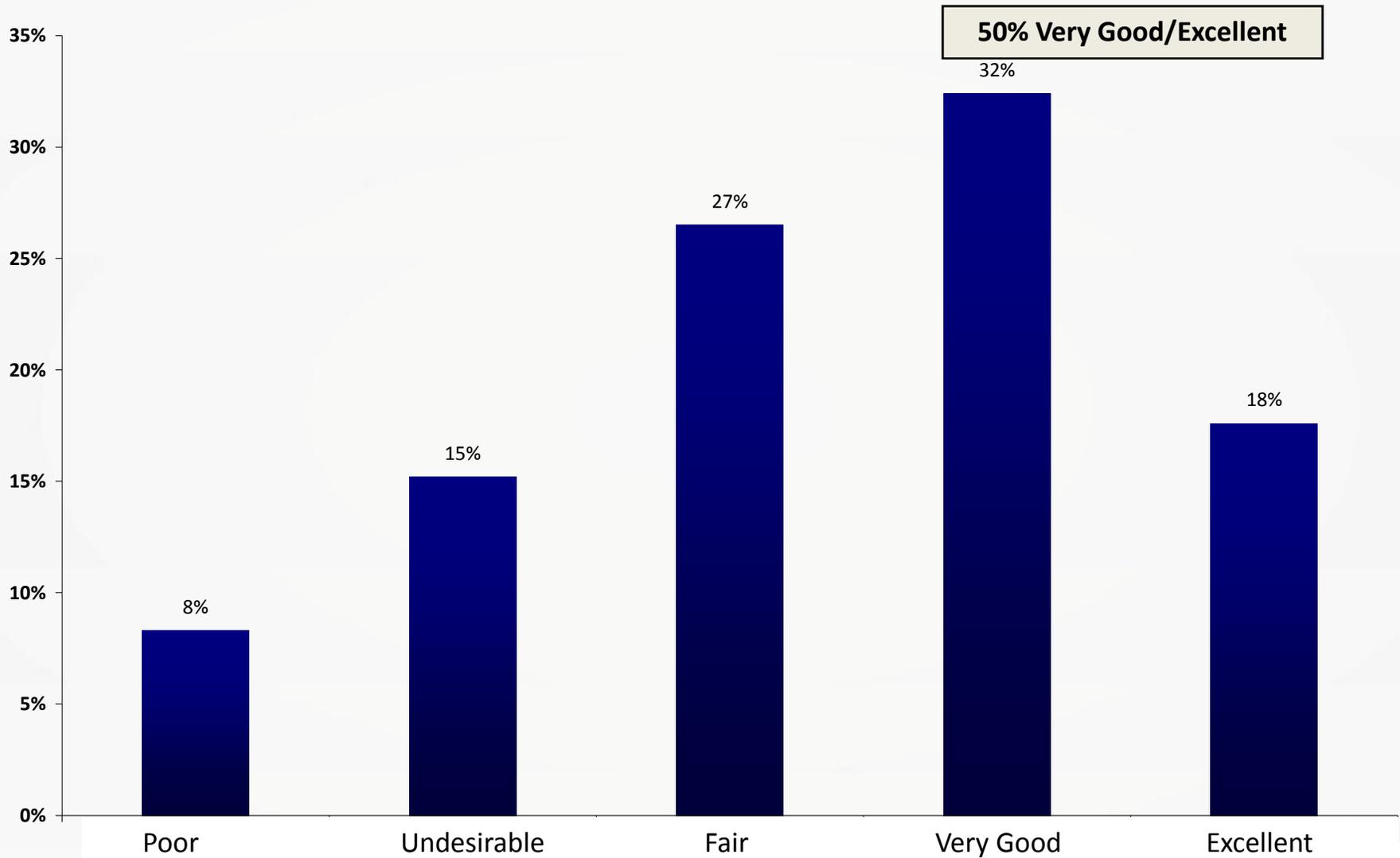
The trustworthiness of your antivirus vendor?



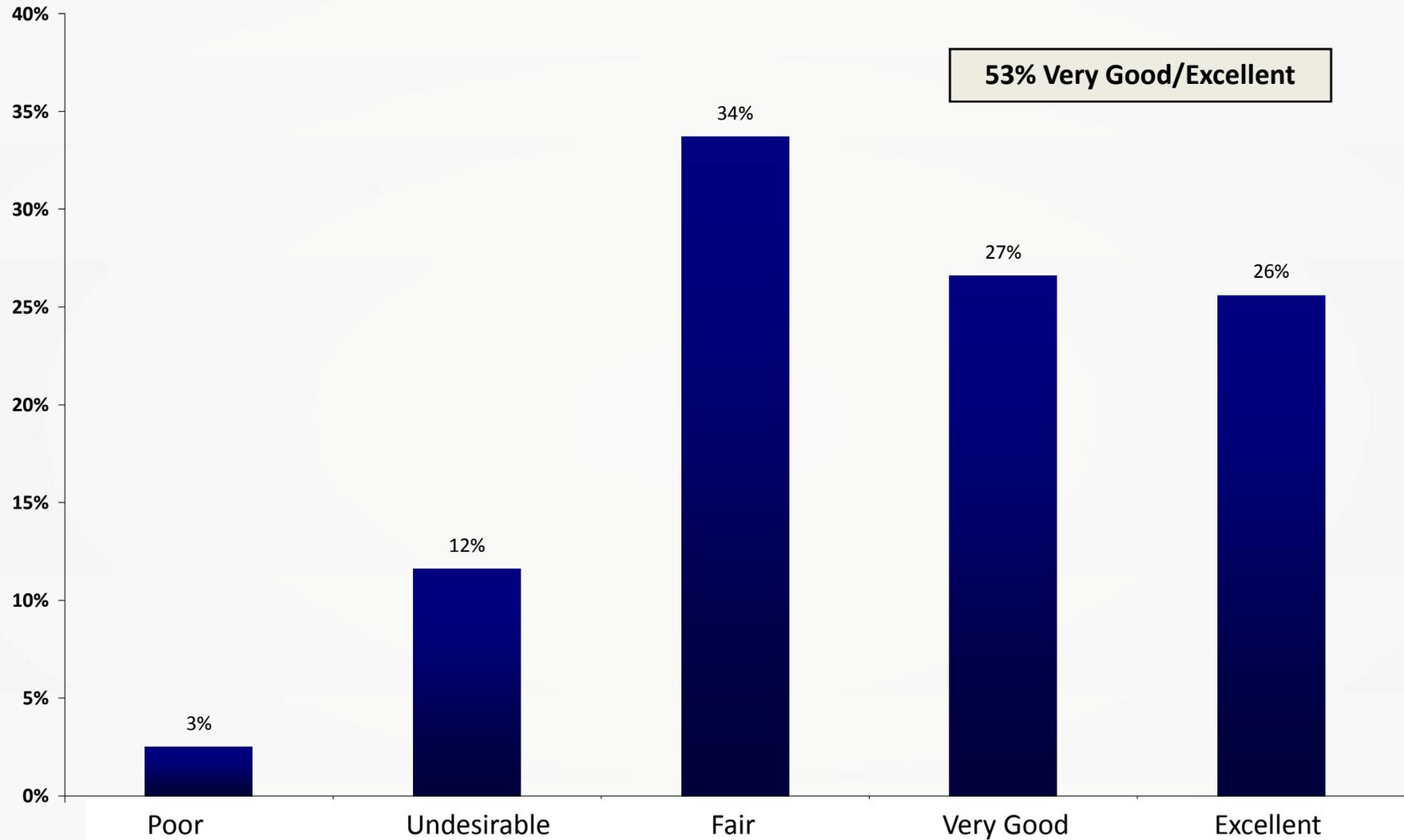
Your overall opinion of your antivirus product?



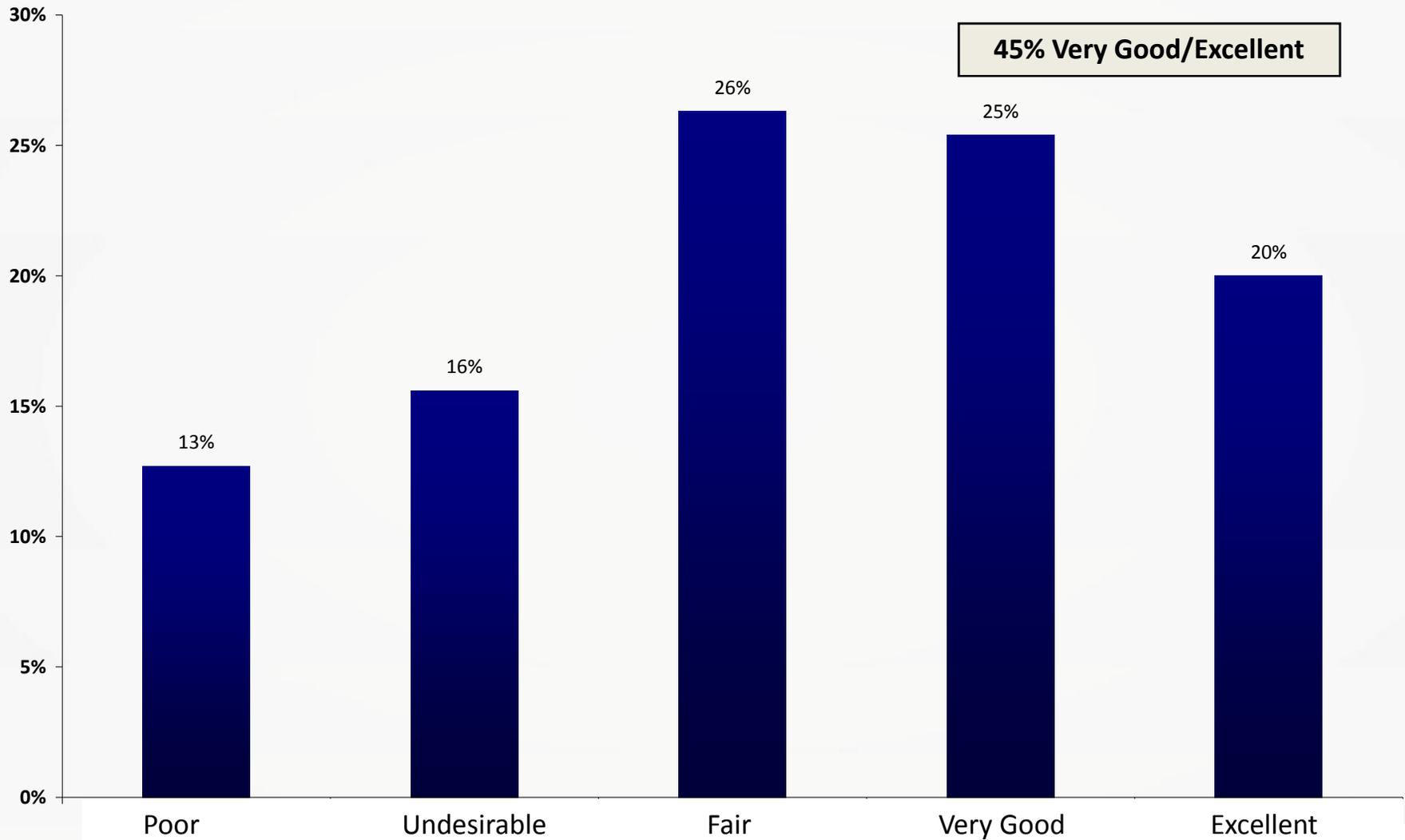
How would you rate the support of your antivirus vendor?



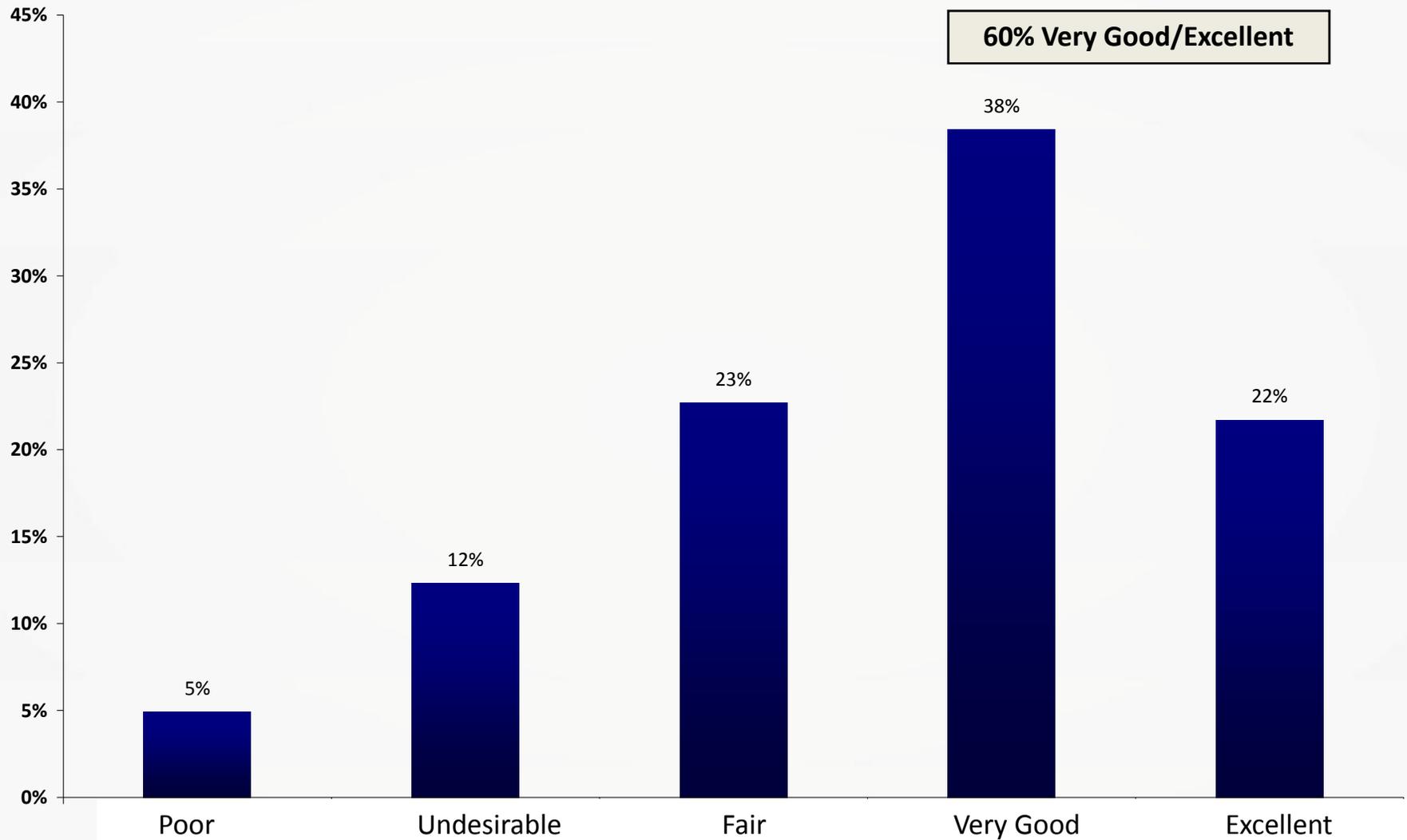
The value for your money of your antivirus product?



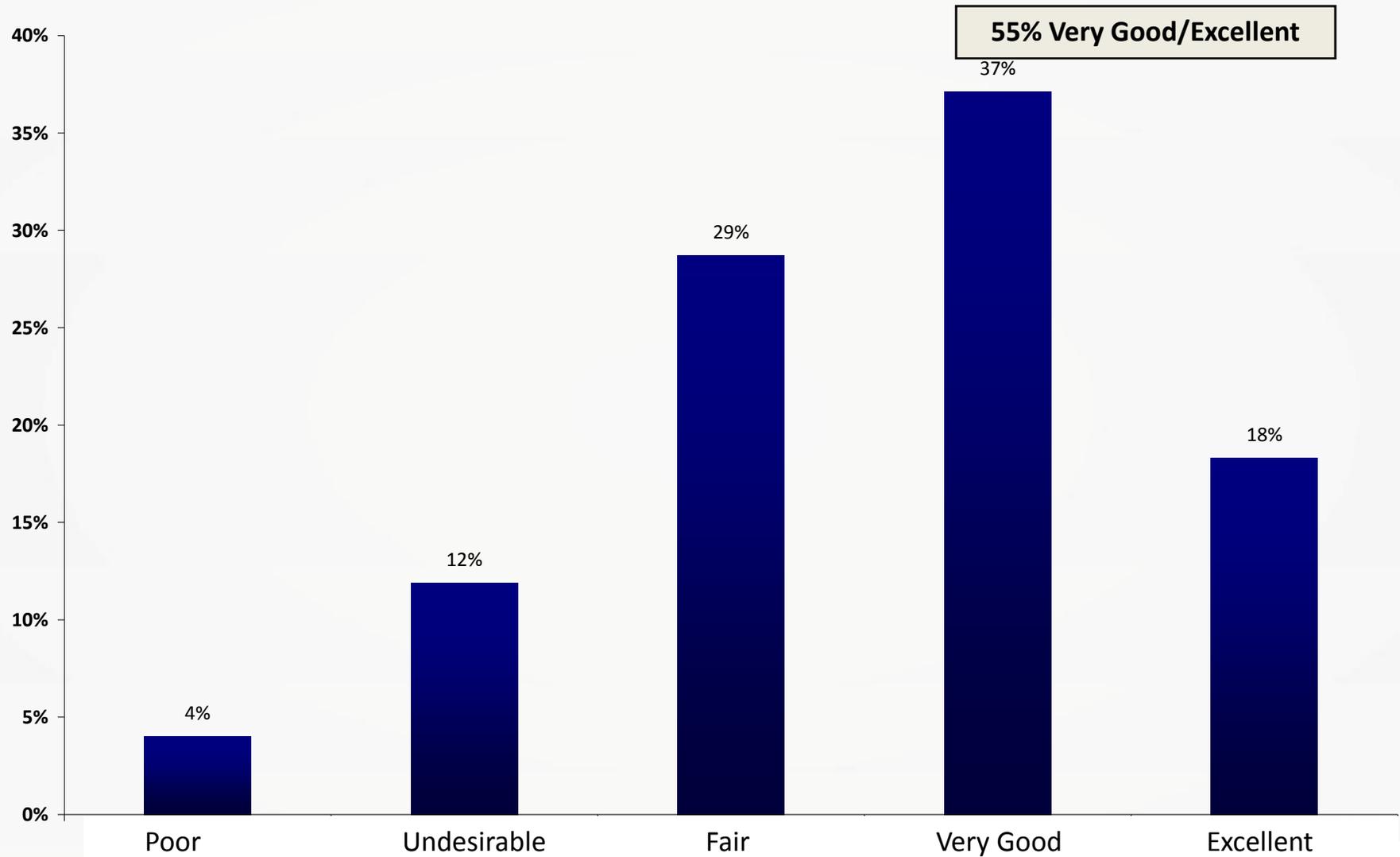
The performance/resource usage of your antivirus product?



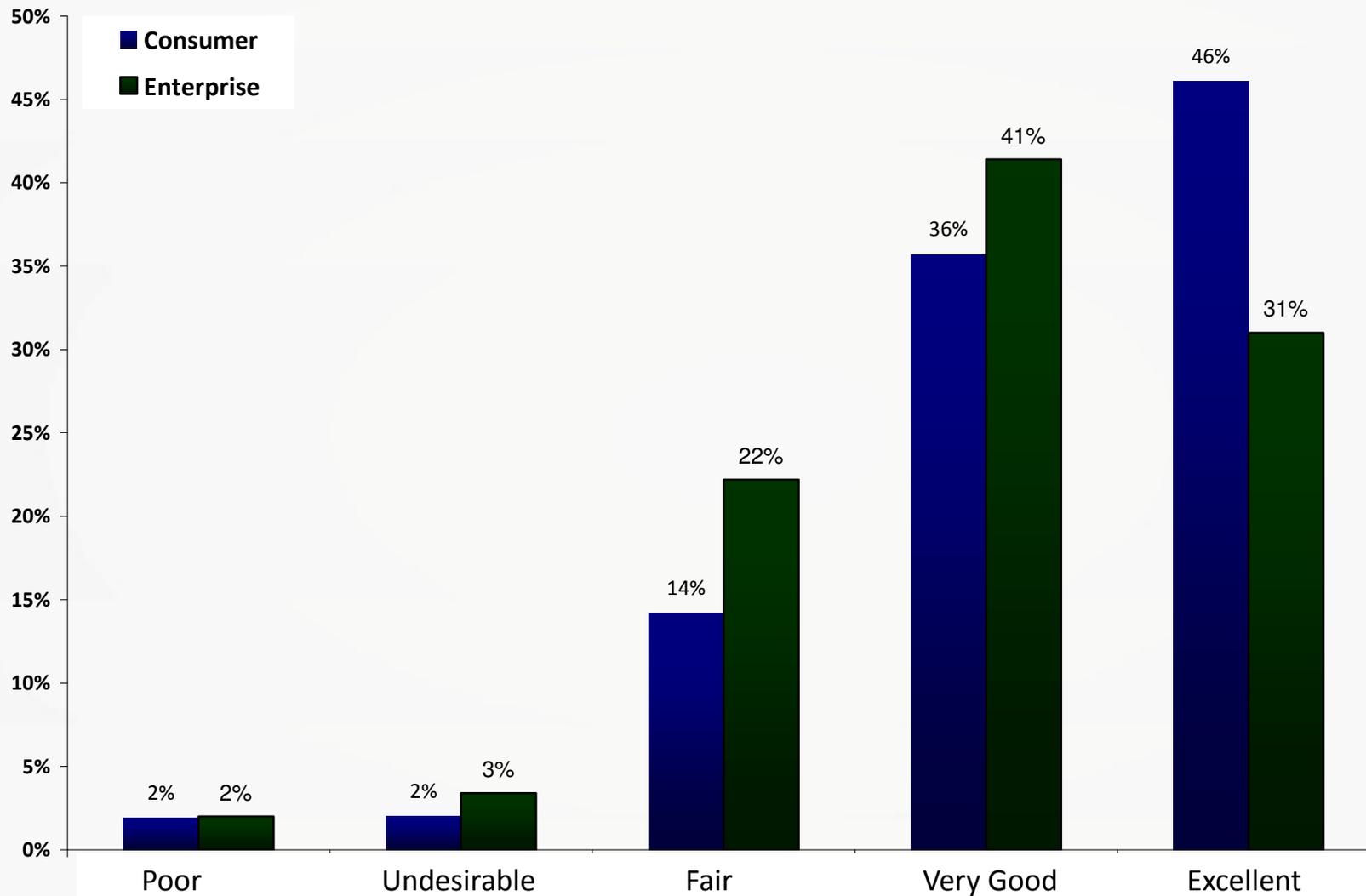
Ability to protect against malware?



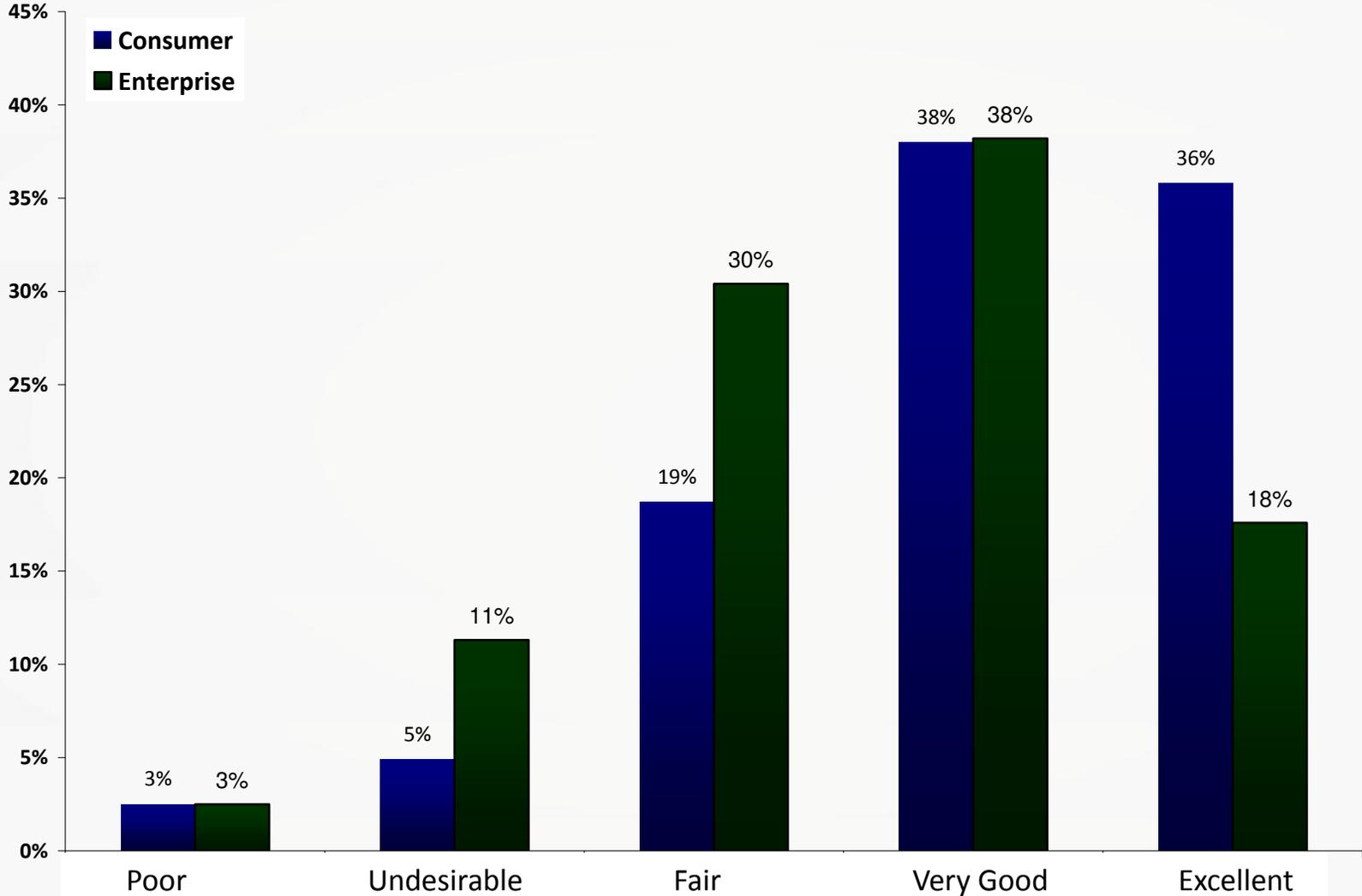
Cleans up infected systems?



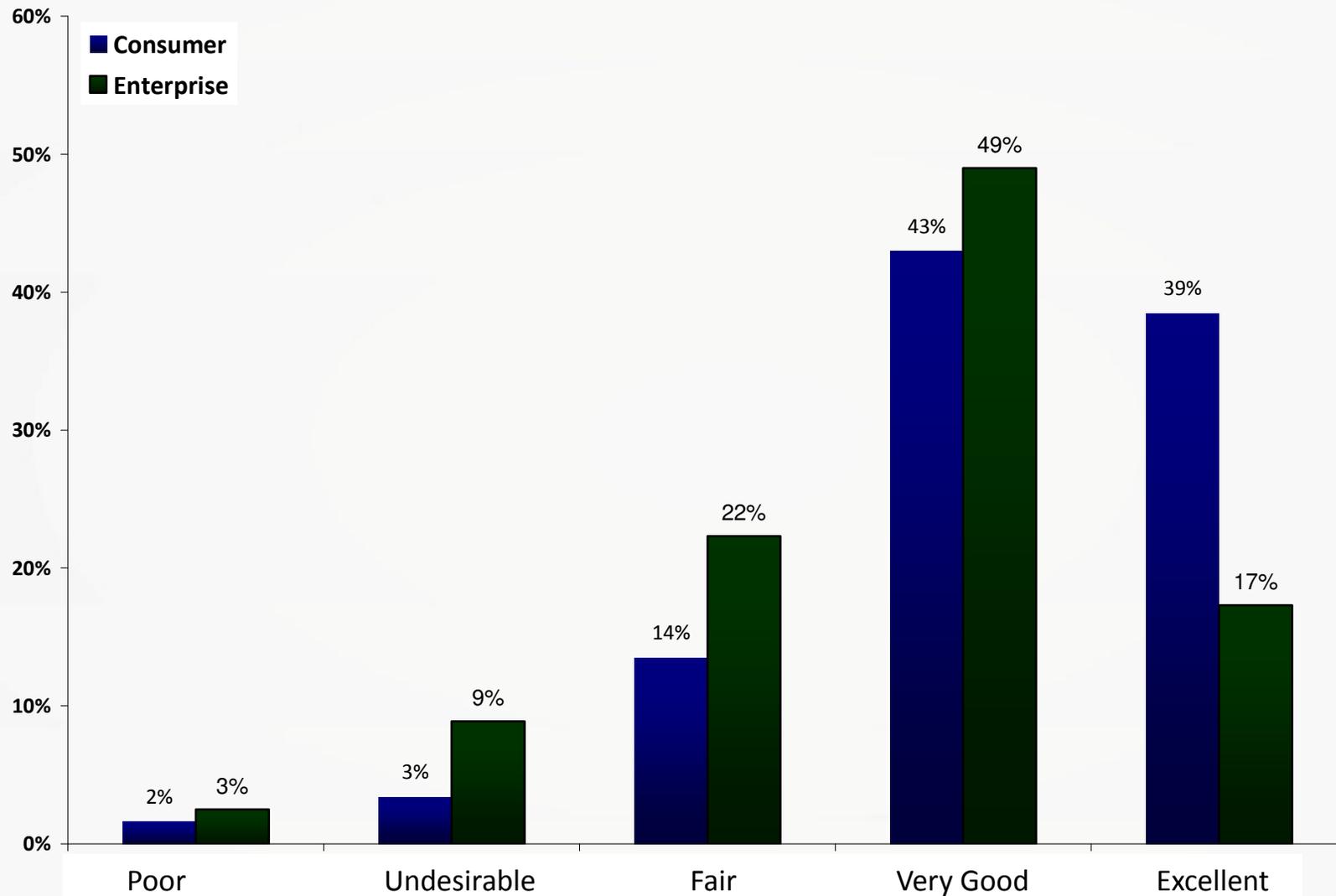
Trustworthiness of vendor: Comparison



Overall opinion of Vendor: Comparison



Overall opinion of AV product: Comparison



Summary of results

- Top issues for consumers:
 - Performance/resource usage.
 - Price.
 - Technical support.
 - Detection/removal.
- Top issues for enterprises:
 - Performance/resource usage.
 - Removal (detection).
 - Price.
 - Support.



Summary of results

- Consumers:
 - 74% rated their AV vendor on a “4” or “5”.
 - Trust their AV company more than enterprise customers.
 - Are more satisfied with their AV product than enterprise customers.
- Enterprises:
 - 56% rated their AV vendor on a “4” or “5”.
 - Are far more concerned with removal of infected systems than almost anything else (save performance).



Review of Technical Support practices



Sunbelt Software

Technical support

	Ease of finding support	Toll free support	Email	Chat	KB
Vendor 1	5	No	No	No	Yes
Vendor 2	5	Per Incident	Yes	Yes	Yes
Vendor 3	3	Yes(1)	Yes	Yes	?
Vendor 4	5	No	Yes	No	Yes
Vendor 5	4	Yes	Yes	No	No
Vendor 6	5	No	Yes	Yes	Yes
Vendor 7	5	No	No	Yes	Yes
Vendor 8	1	No	No	No	No
Vendor 9	3	No	Yes	No	Yes
Vendor 10	3	Yes	Yes	No	No
Vendor 11	5	Yes	Yes	No	Yes
Vendor 12	5	Yes(2)	Yes	Yes	Yes
Vendor 13	5	Yes	Yes	Yes	Yes
Vendor 14	5	Yes	Yes	No	Yes
Vendor 15	2	Per Incident	No	No	Yes

1 = Had to dial local number to get toll-free number

2 = Only for installation and known problems. Otherwise \$9.95 per call.



Sunbelt Software

Technical support

- **Ease of finding support**
 - Average score of 4 (1=low, 5=high)
- **Out of 15 vendors:**
 - 6 offer toll-free support.
 - 6 do not offer toll-free support.
 - 2 (or 3) charge for toll-free.
 - 11 offer email support, 4 do not.
 - 6 offer chat, 9 do not.
 - Most offer KBs.



Technical support

	Length of IVR tree	Length of time waiting for email response	Length of time waiting on phone
Vendor 1	n/a	n/a	n/a
Vendor 2	ddn't call/ pymnt req	~ 17hours	ddn't call/ pymnt req
Vendor 3	2	~17 hours	>15 min
Vendor 4	n/a	~ 10 hours	n/a
Vendor 5	0	24 hours (still waiting)	2min 45sec
Vendor 6	n/a	15 mins	n/a
Vendor 7	ddn't call/ pymnt req	n/a	ddn't call/ pymnt req
Vendor 8	n/a	n/a	n/a
Vendor 9	n/a	no response yet	n/a
Vendor 10	1	1.5 hours	<1 min
Vendor 11	0	30 min	<1min
Vendor 12	2	~9 hours	~1 min
Vendor 13	1	~12 hrs	~1 min
Vendor 14	2	~ 4 days	<15min
Vendor 15	2	n/a	n/a



Technical support

Overall impression (1-5 rating)	
Vendor 1	1
Vendor 2	2
Vendor 3	3
Vendor 4	3
Vendor 5	3
Vendor 6	3
Vendor 7	2
Vendor 8	1
Vendor 9	1
Vendor 10	3
Vendor 11	5
Vendor 12	4
Vendor 13	5
Vendor 14	3
Vendor 15	1

Median rating of 3, Average rating of 2.7



Sunbelt Software

Summary of support findings

- Sometimes difficult to find support.
- Difficulty getting someone on a phone: Out of 15 vendors, only 6 (40%) offer free toll-free support .
- In a number of cases, long wait times for an email response.



Other business issues

- Aggressive marketing practices endanger long-term viability of the business.
- Automatically billing credit cards.
- “Scan and scare” tactics.
- “Alerts” that a version is being discontinued, upsell to a paid version.
- Spamming.
- Relying on poor quality third-party e-commerce providers.
- Bundling in toolbars - Yahoo, Google or Ask.



It's not all bad.
But things could be better.



Sunbelt Software

The solutions

- R&D:
 - Amp-up investment to stay on top of threats.
 - New technologies: Cloud, whitelisting, advanced emulation, etc.
 - Increased QA, evolving dev practices.
 - Reductive, vs. additive philosophy.
- Deliver more for less.
- Optimize organizational lines for the New Malware Order.
- Continue to evolve industry testing strategies to reflect reality.



The solutions

- Enlightened self-interest
 - Furthering the interests of others ultimately serves the interest of yourself.
- Continued community involvement reduces malware threat and eases the strain on researchers
 - Takedowns, anti-phishing workgroups, anti-malware workgroups, ARF, etc.
 - Atrivo/Intercage/Estdomains effort.
- Researchers and technologists have a right to a say in the business practices of their companies.
- Continued industry cooperation



The end

email: alex@sunbeltsoftware.com



Sunbelt Software