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?

Sunbelt Software

Myths and facts about the AV industry

"The end is nigh upon us! REPENT!"

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

Sunbelt Software

Myths and facts about the AV industry

Sunbelt Software

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

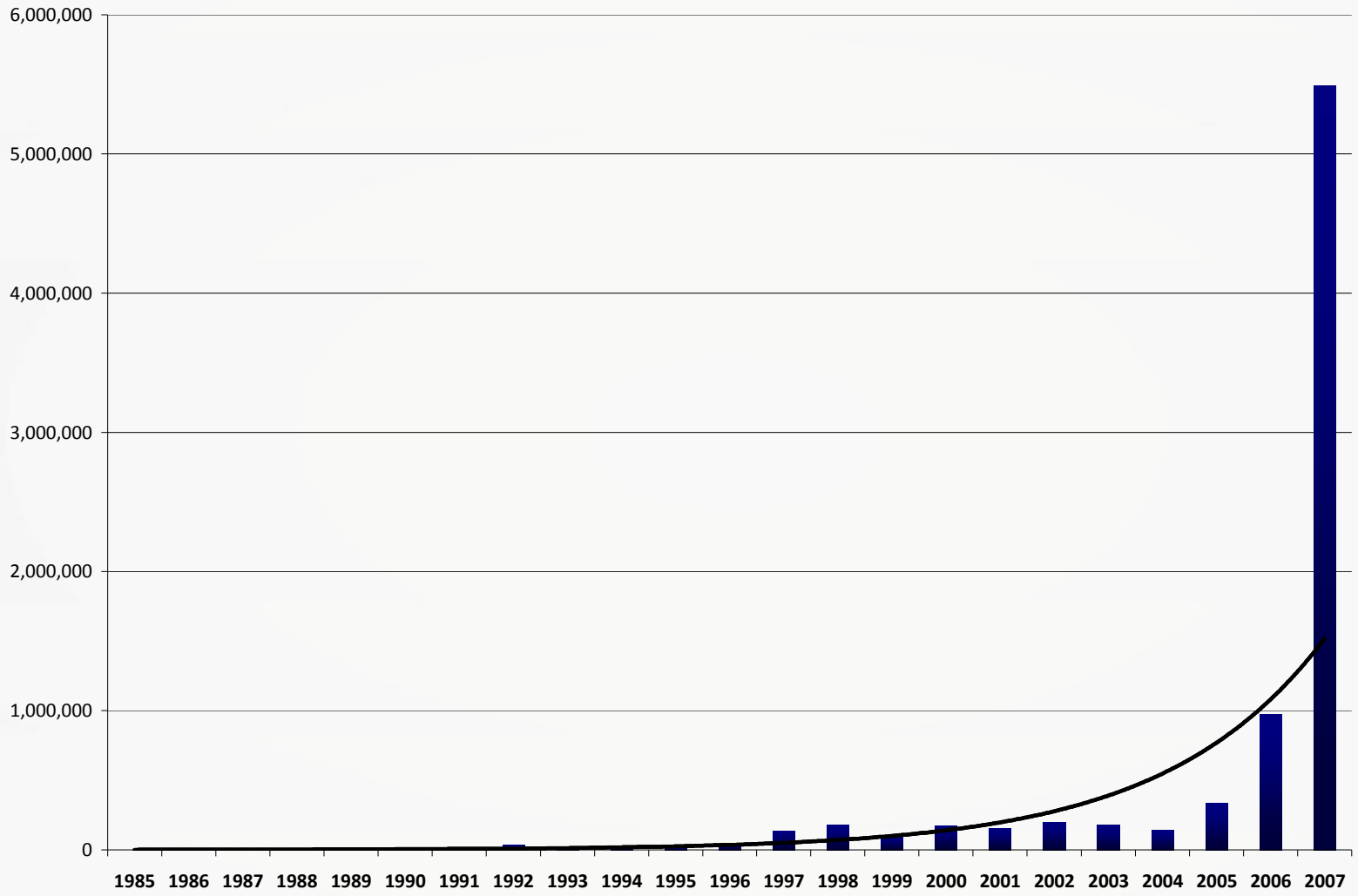
The antivirus industry…and now

Sunbelt Software

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

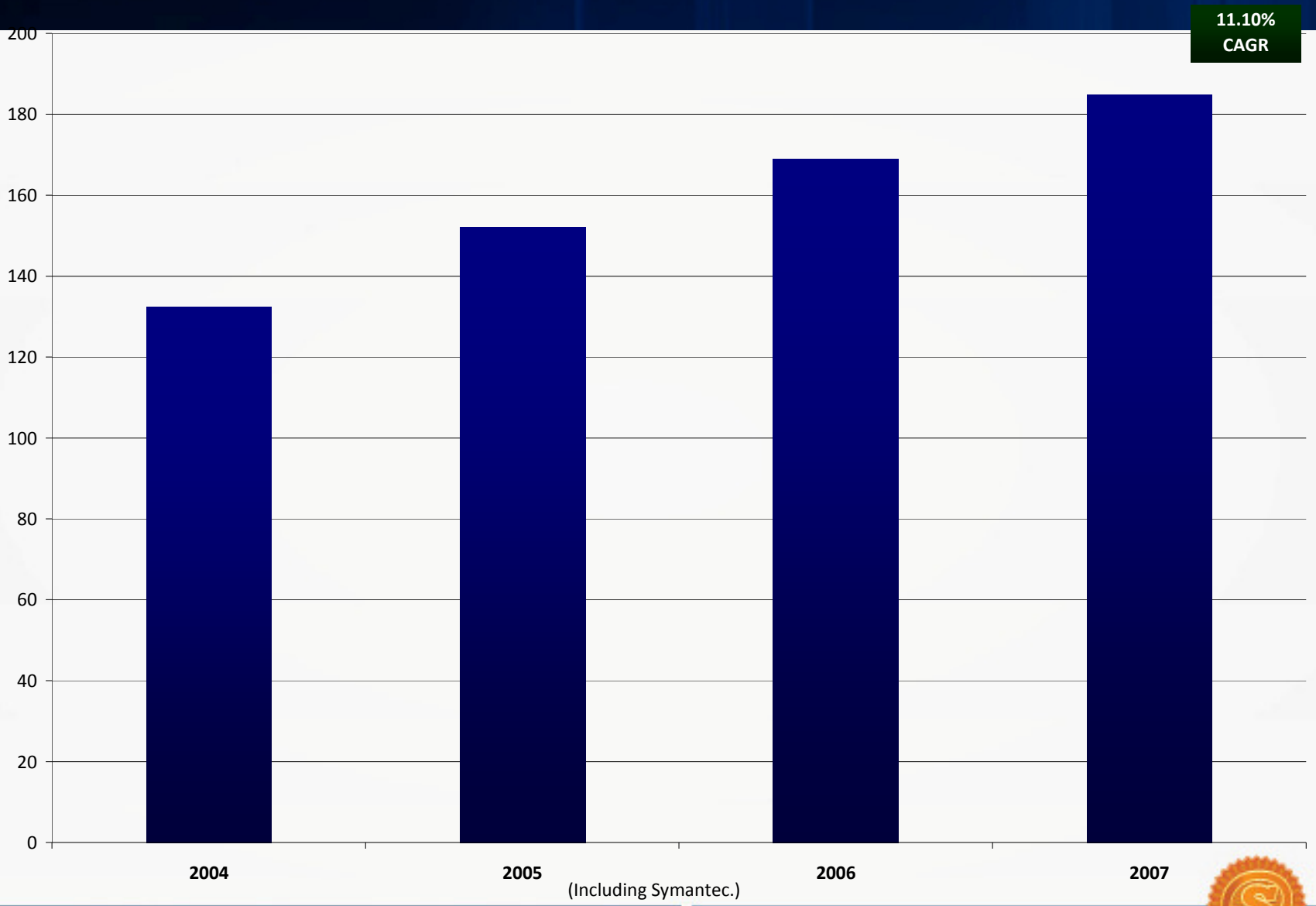
- Growth is slowing, but still there:
  - Gartner: Worldwide security software revenue will increase from more than $10.5 billion in 2008 to more than $13 billion in 2012, a CAGR of 6.8% from 2007 through 2012.

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.

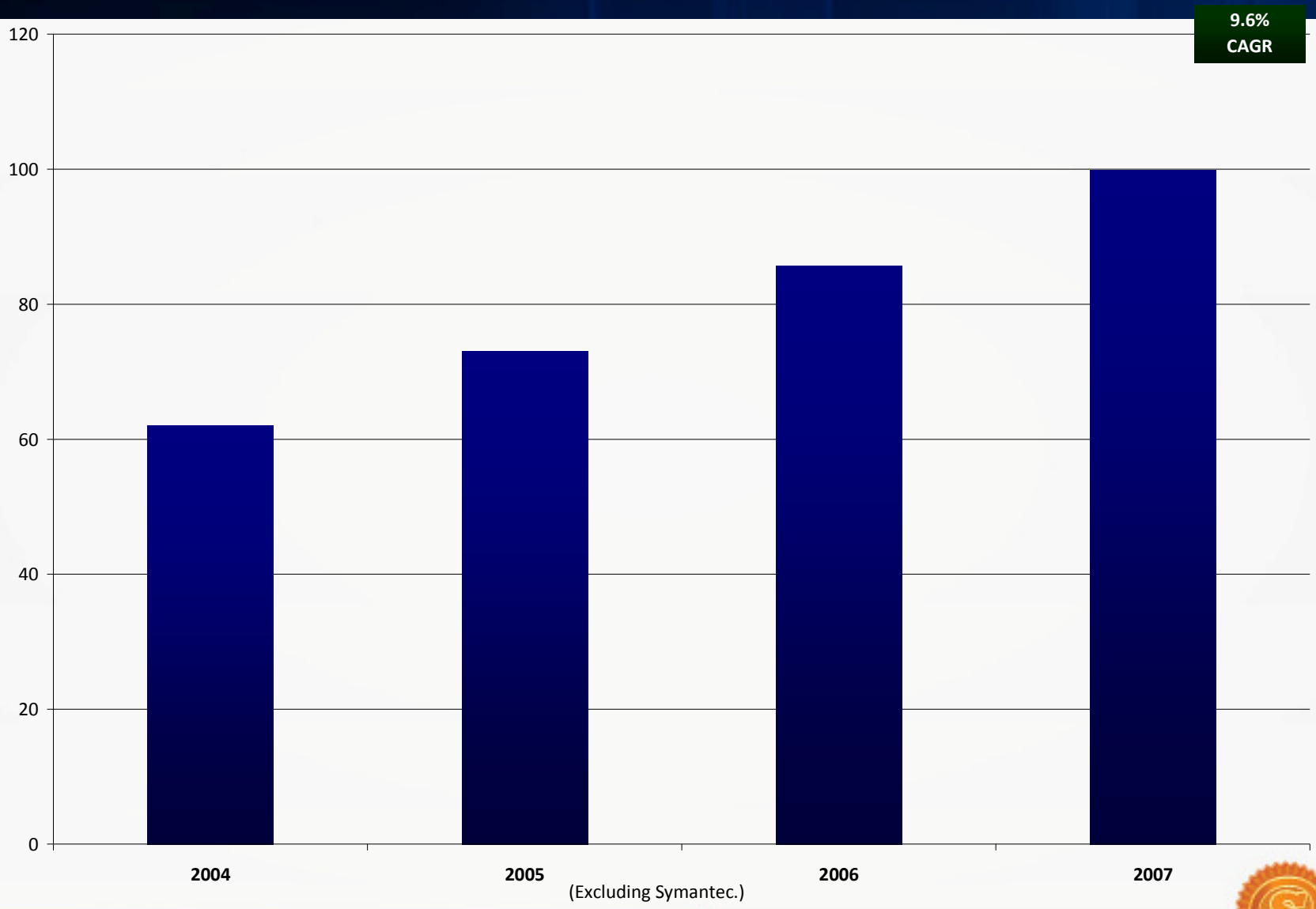
* Never Trust a Software Executive with Numbers

Revenues



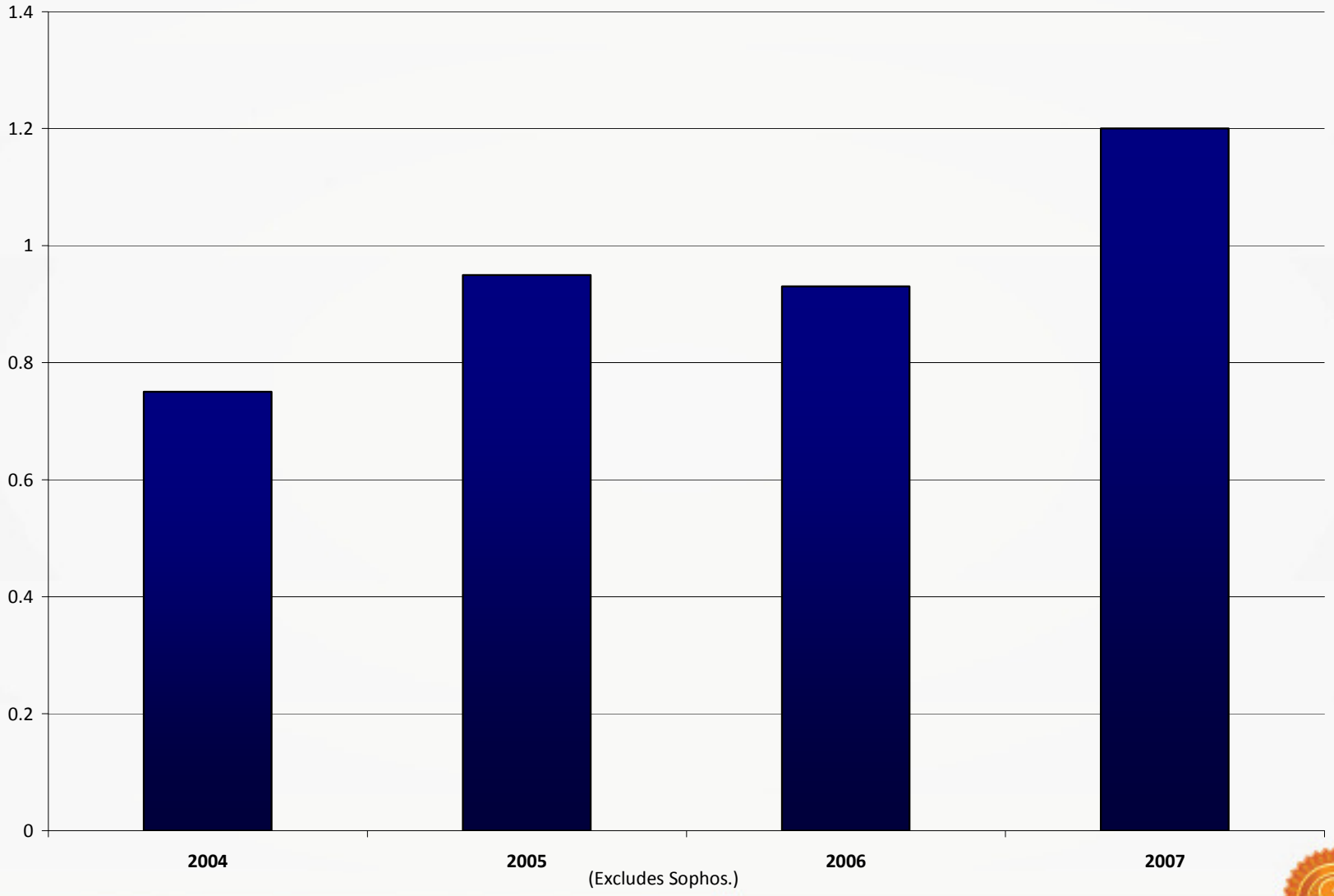
Sunbelt Software

Revenues



Sunbelt Software

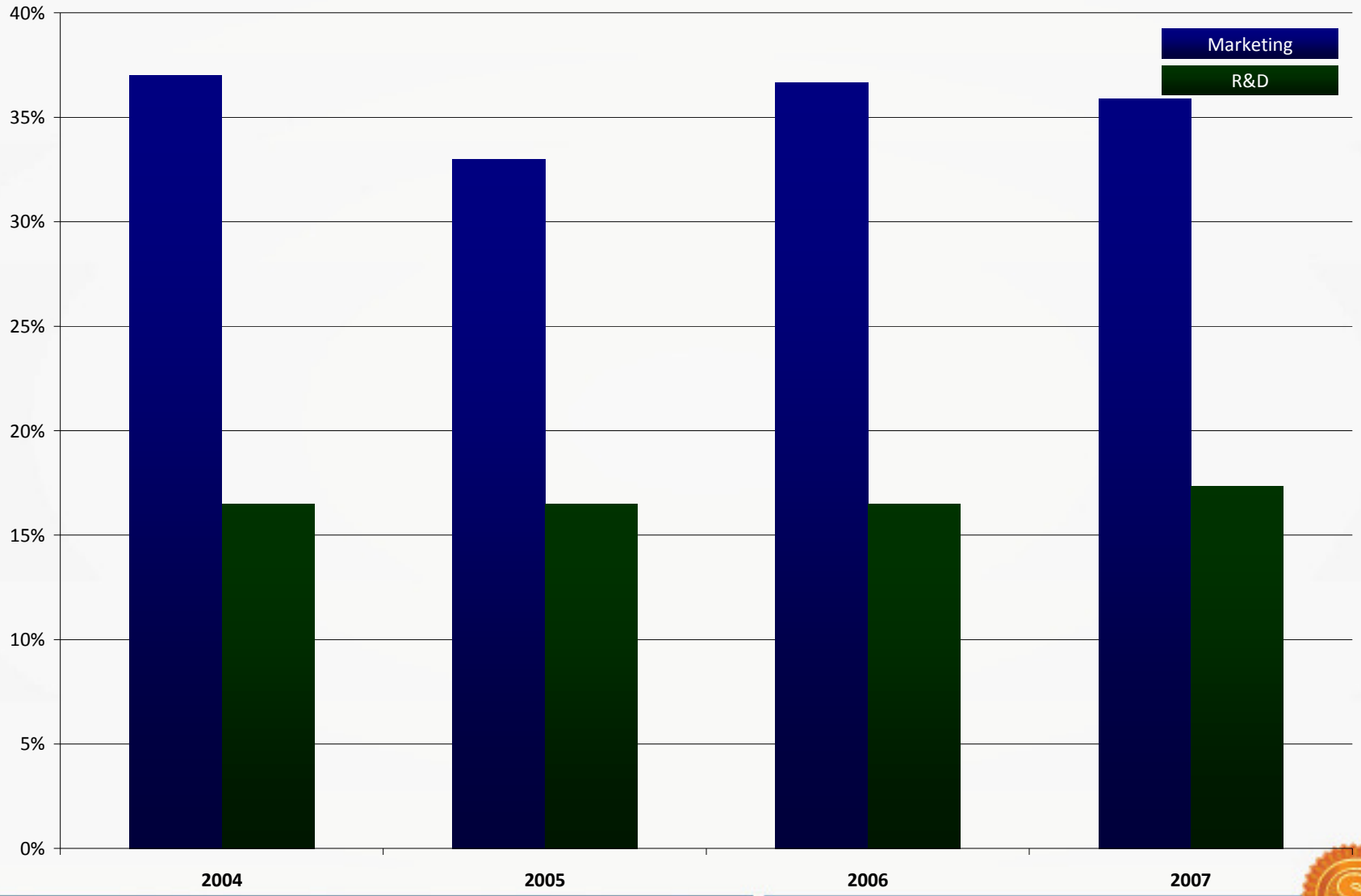
Earnings Per Share Growth



(Excludes Sophos.)

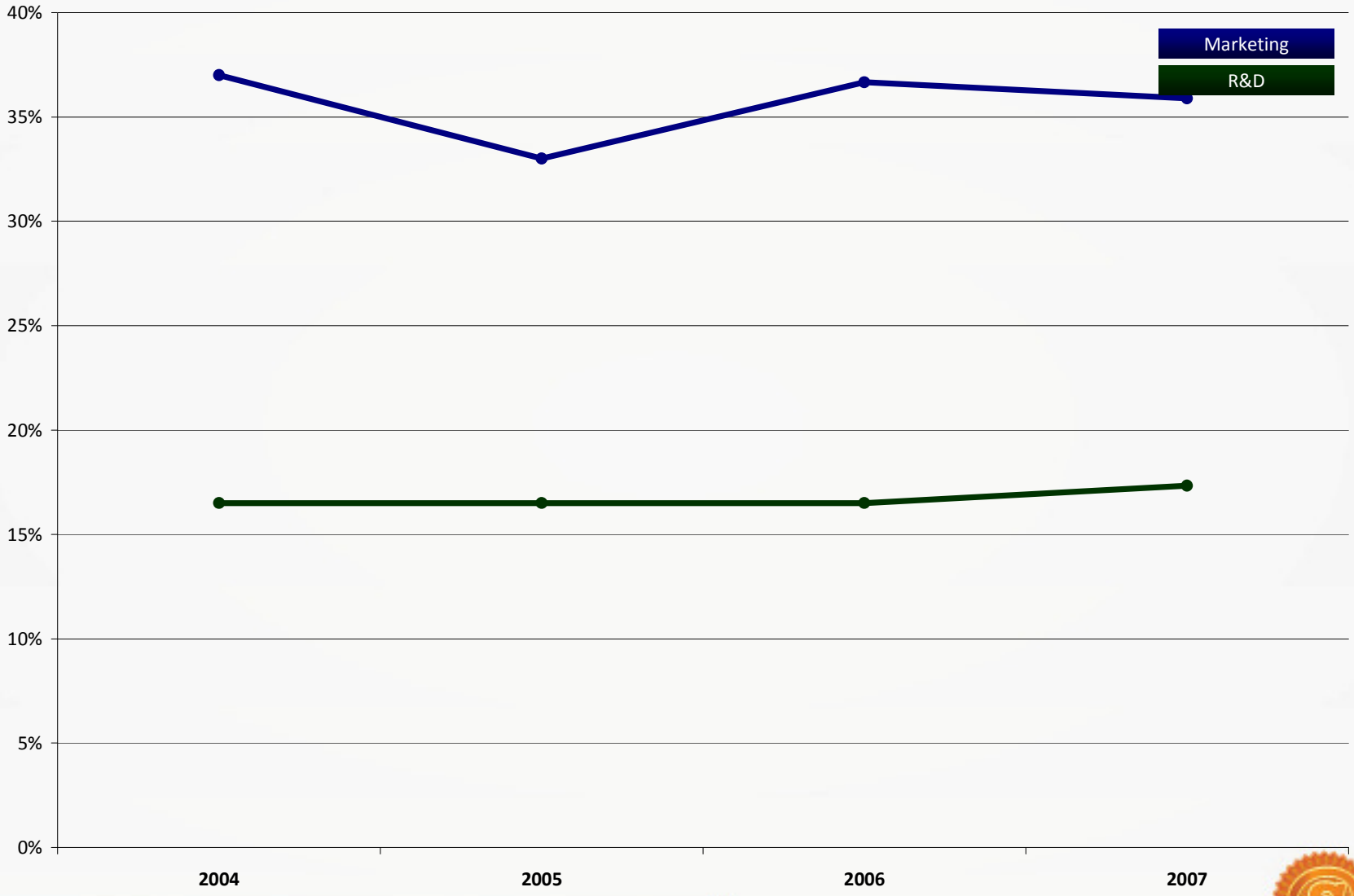
Sunbelt Software

Median expenditures as a percentage of revenue



Sunbelt Software

Median expenditures as a percentage of revenue



Sunbelt Software

What do customers think?

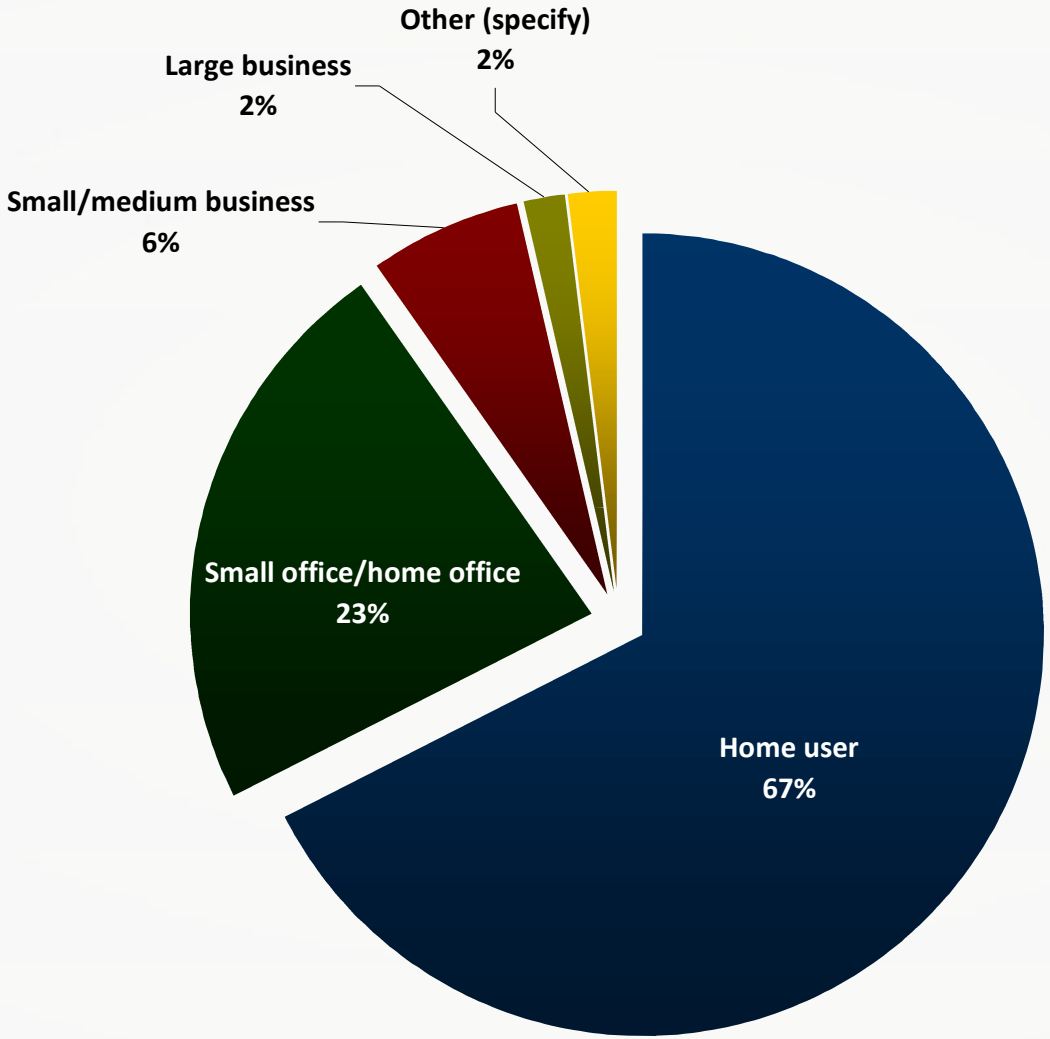
Consumer antivirus user survey

754 surveys taken in September, 2008.

Public was readers of Wxpnews and VistaNews.

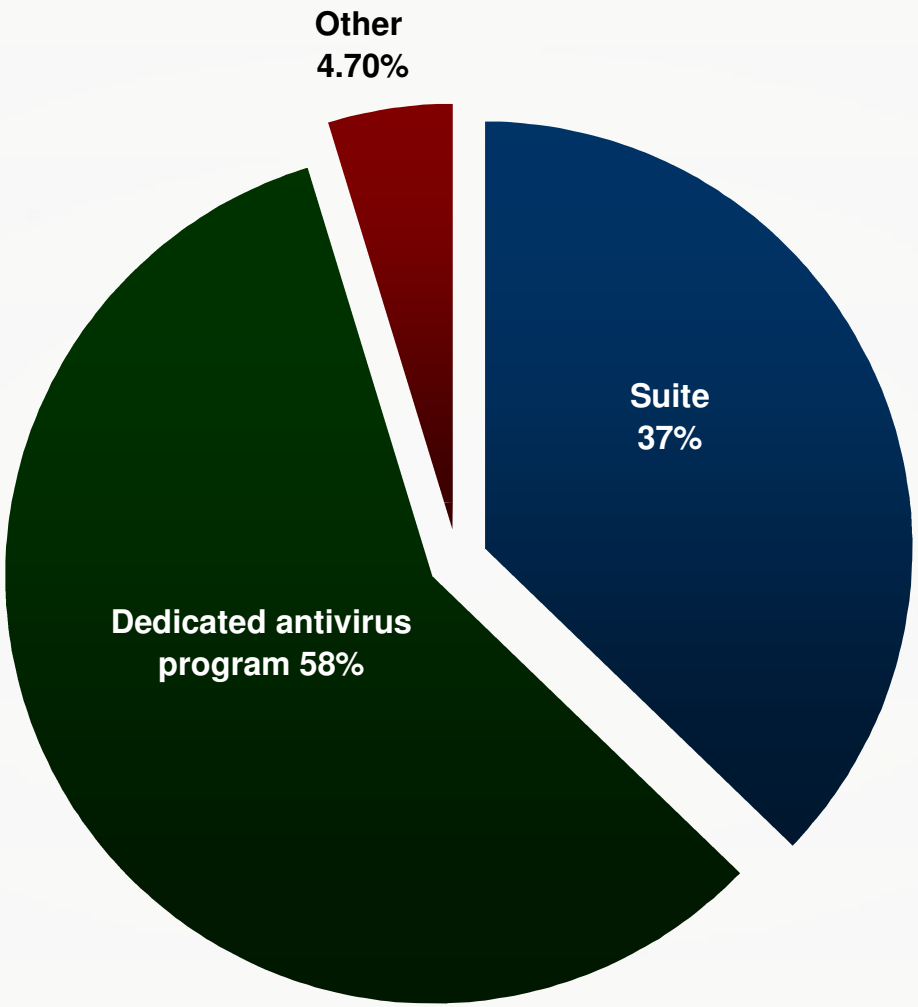
Sampling error of 3.6% (95% confidence interval).

Type of customer



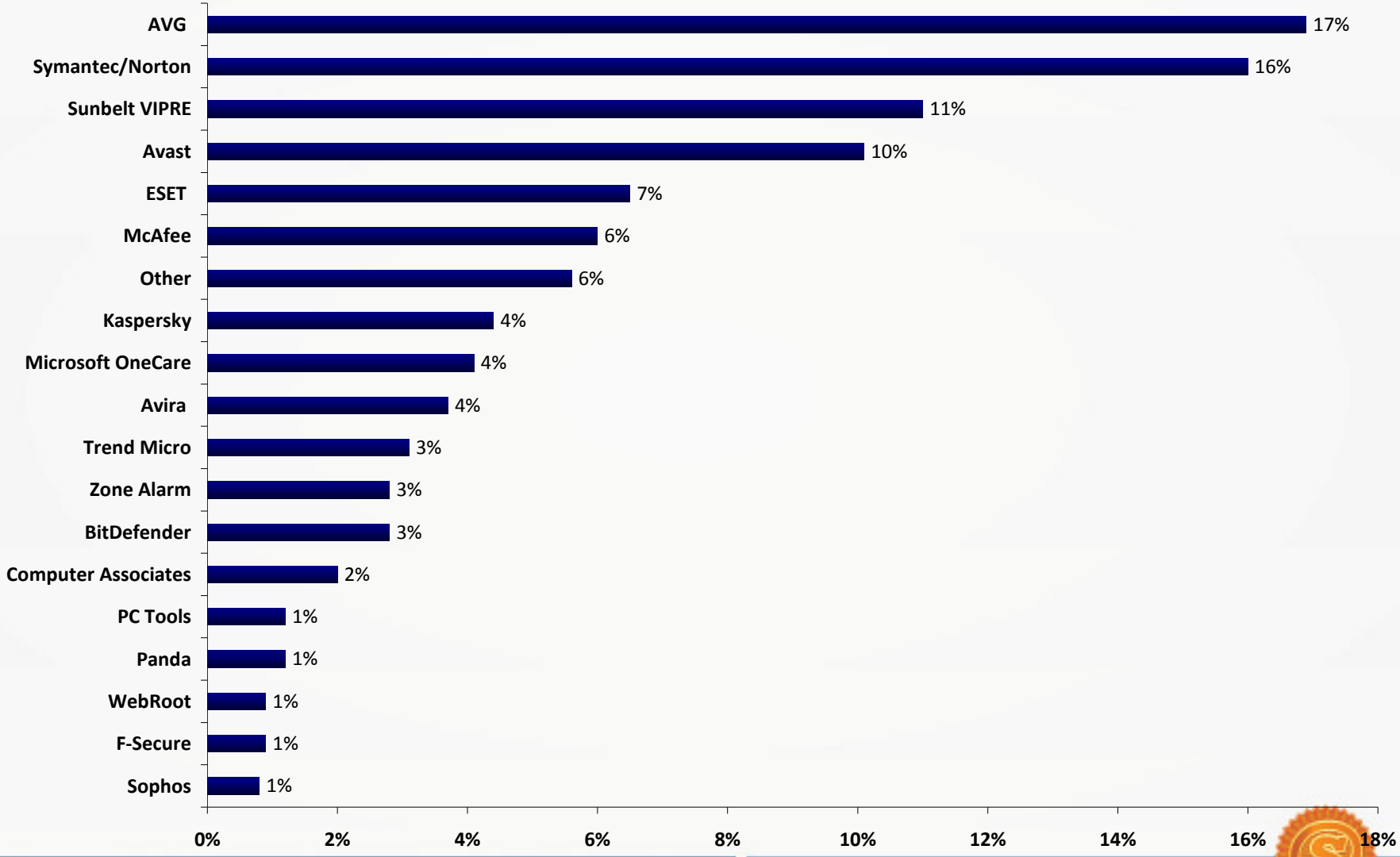
Sunbelt Software

Type of product used



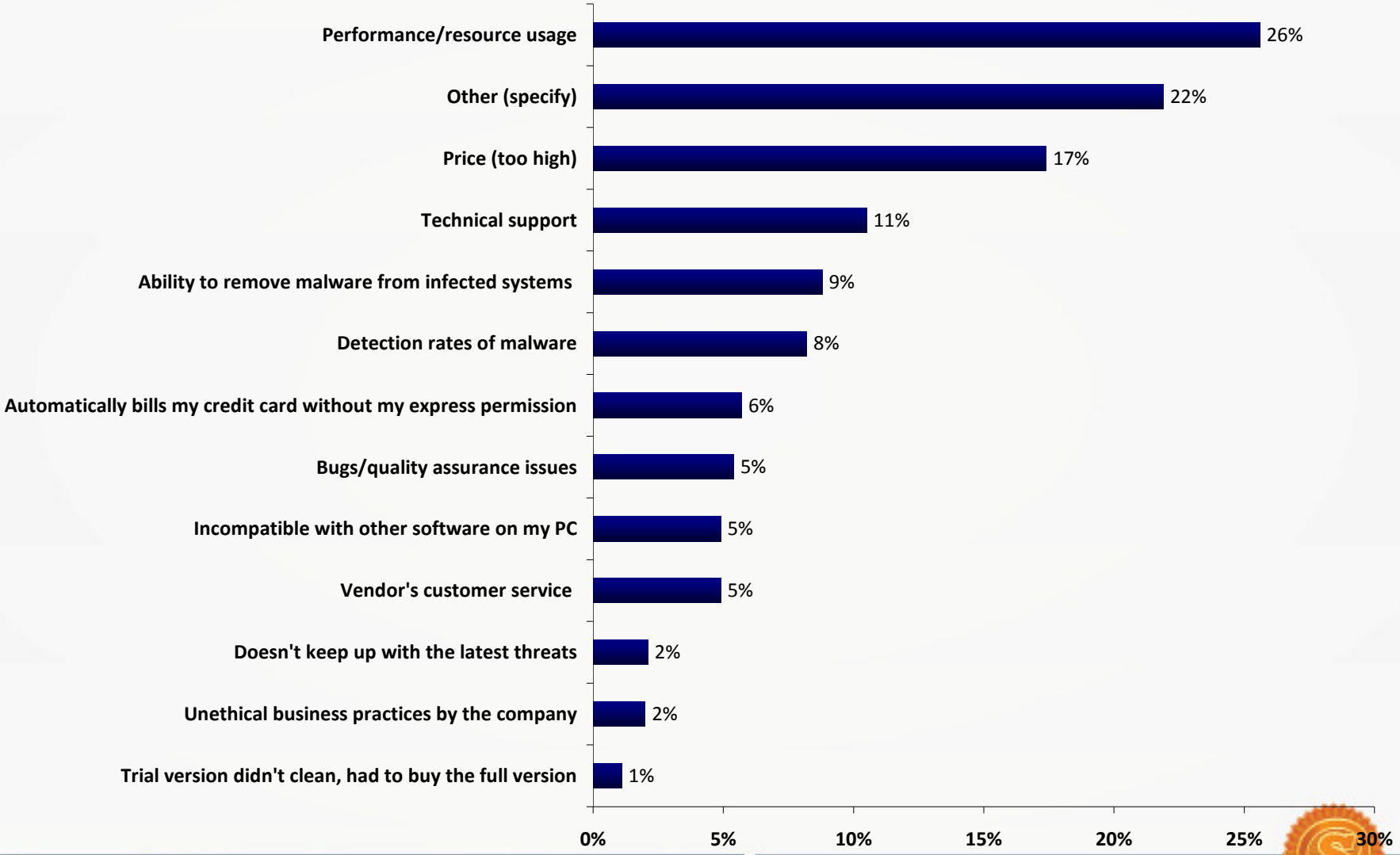
Sunbelt Software

What brand is primarily used



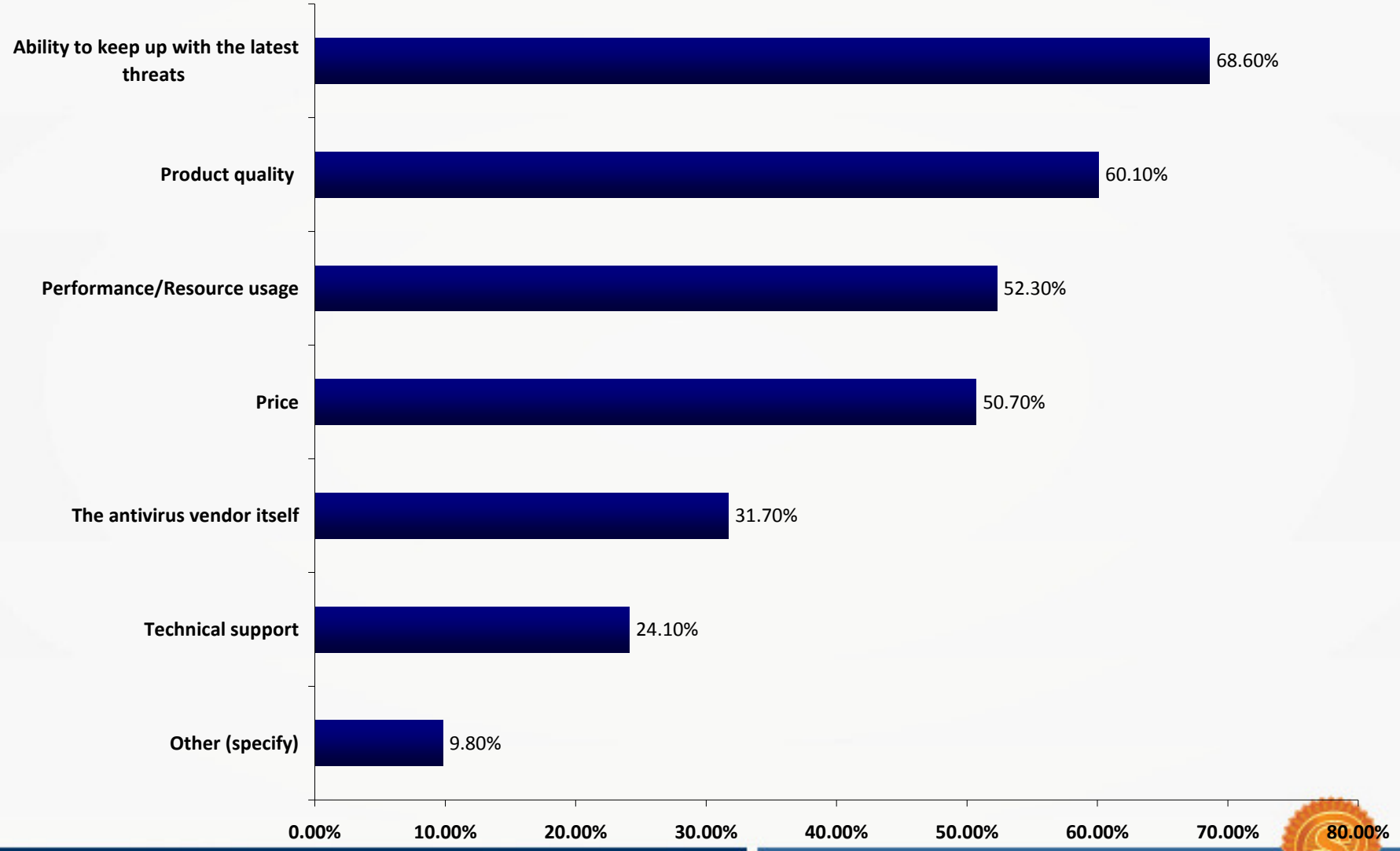
Sunbelt Software

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



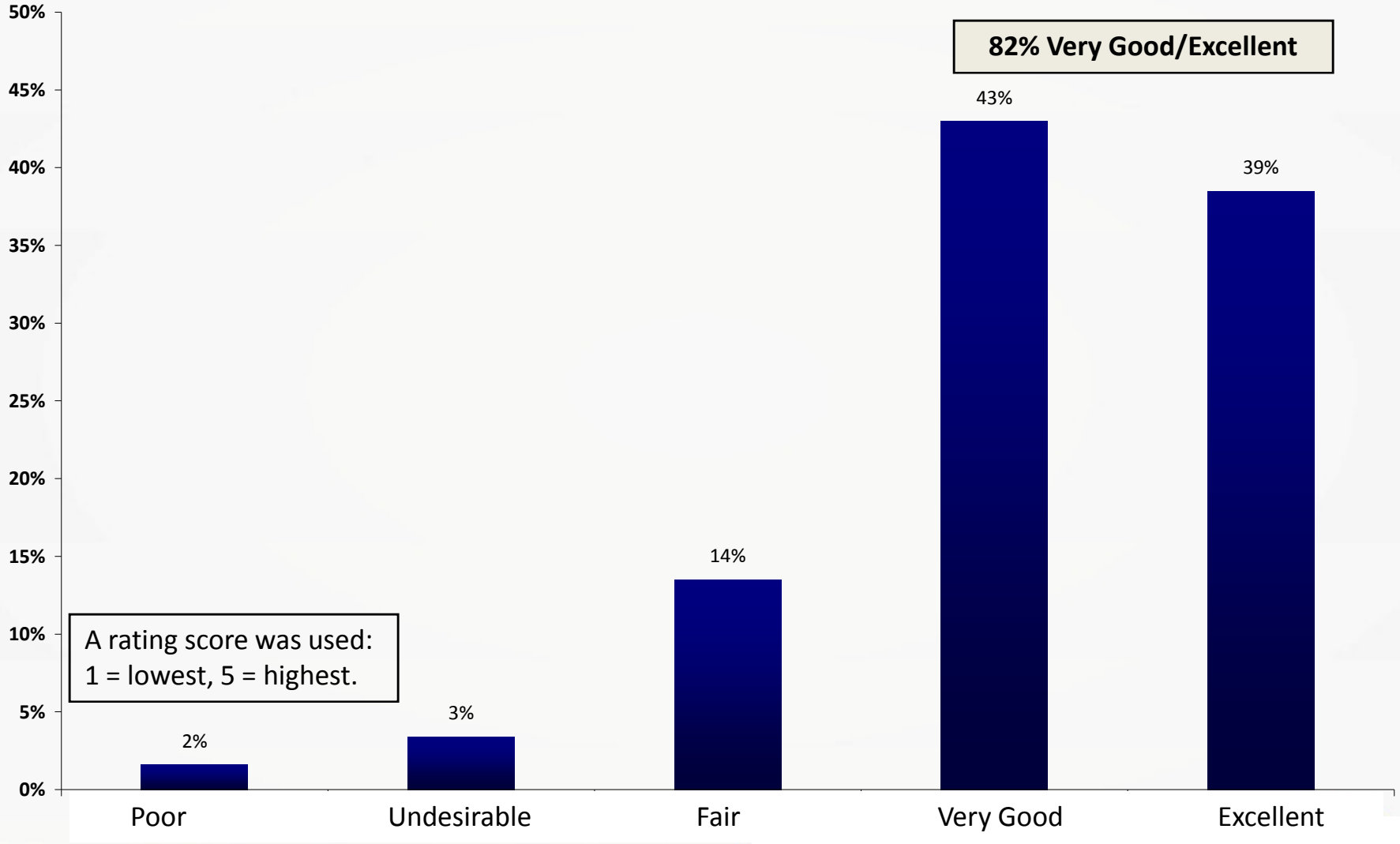
Sunbelt Software

What do you *like*?

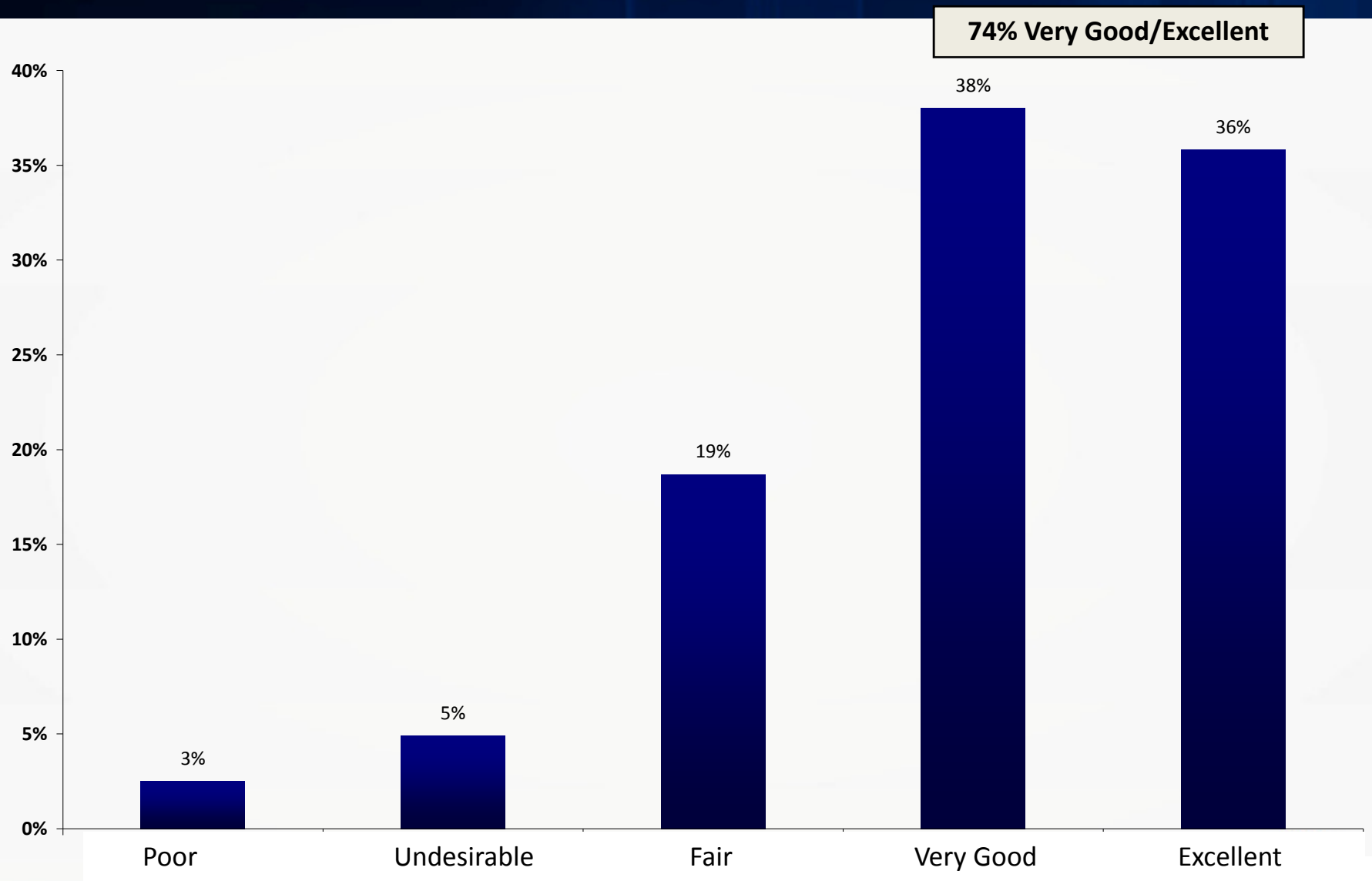


Sunbelt Software

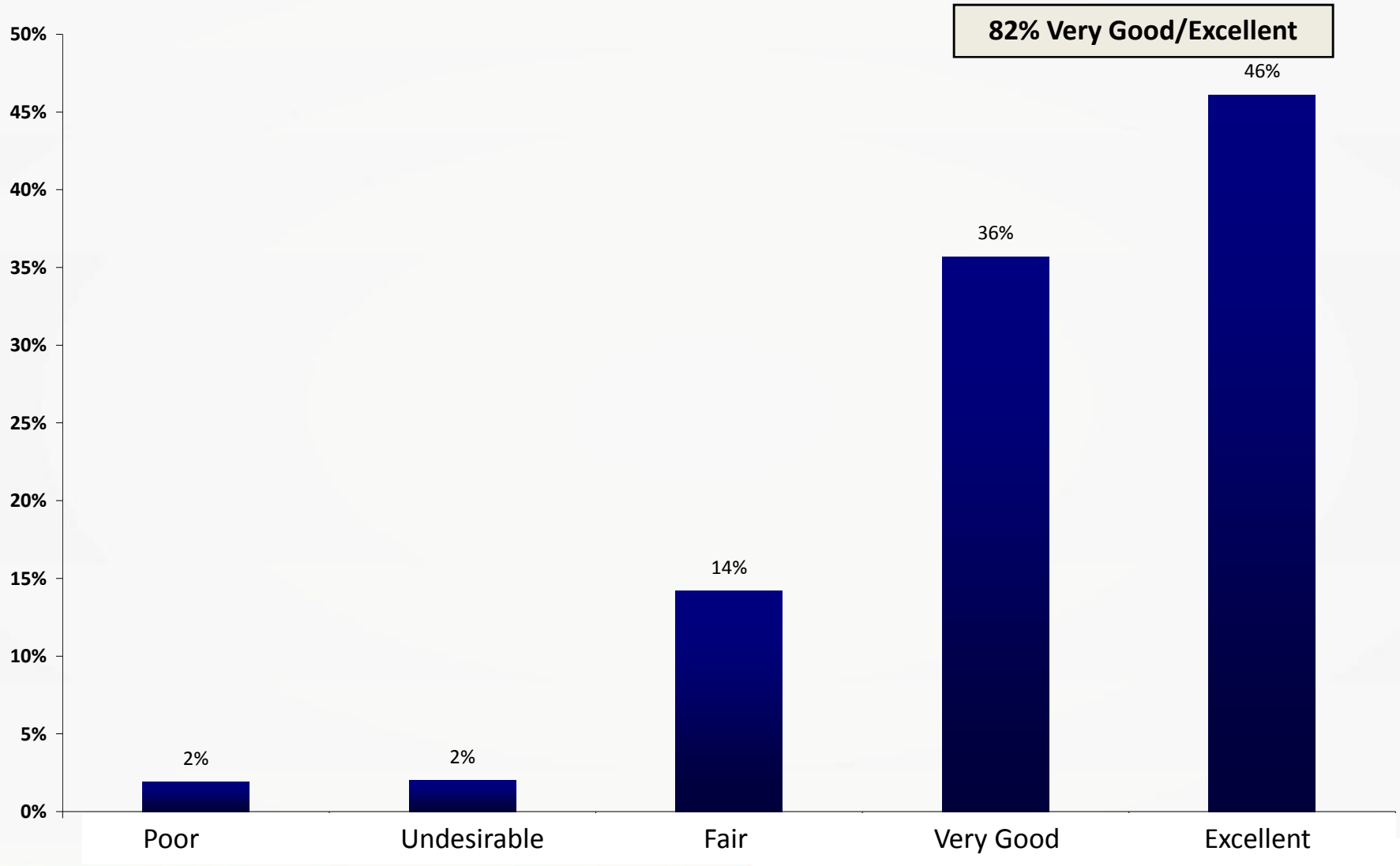
Your overall opinion of your antivirus product?



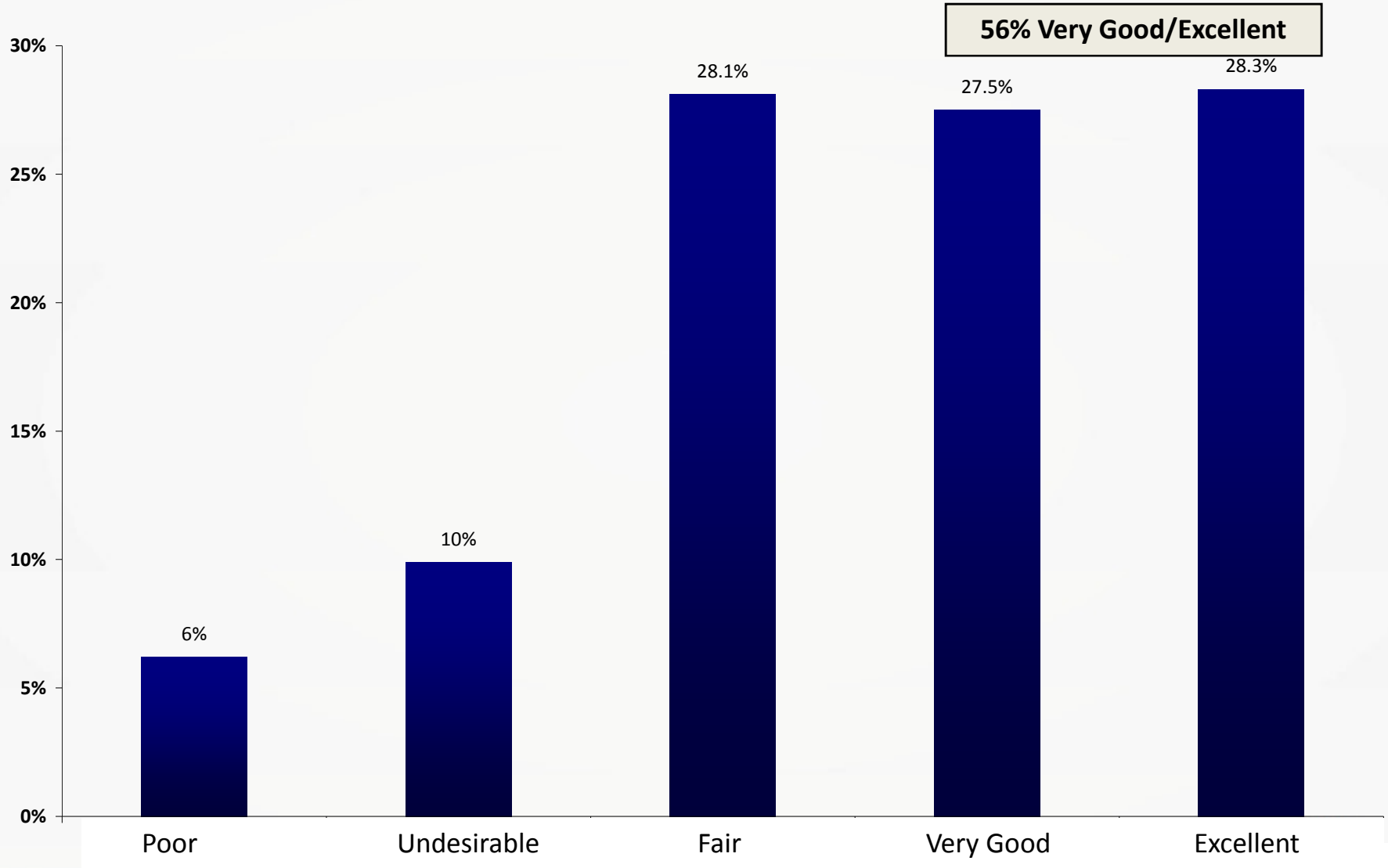
Overall opinion of your antivirus vendor?



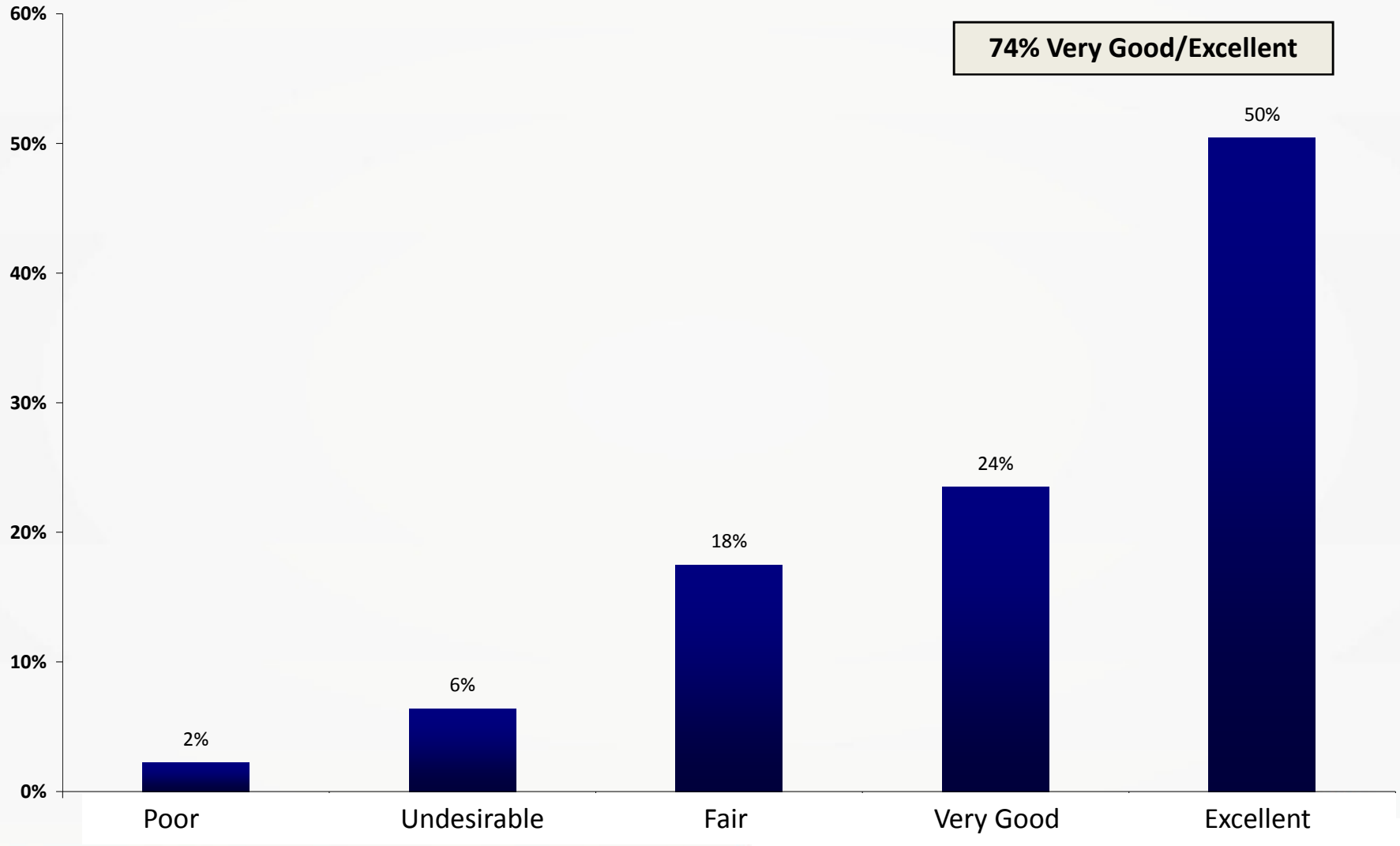
Trustworthiness of your antivirus vendor?



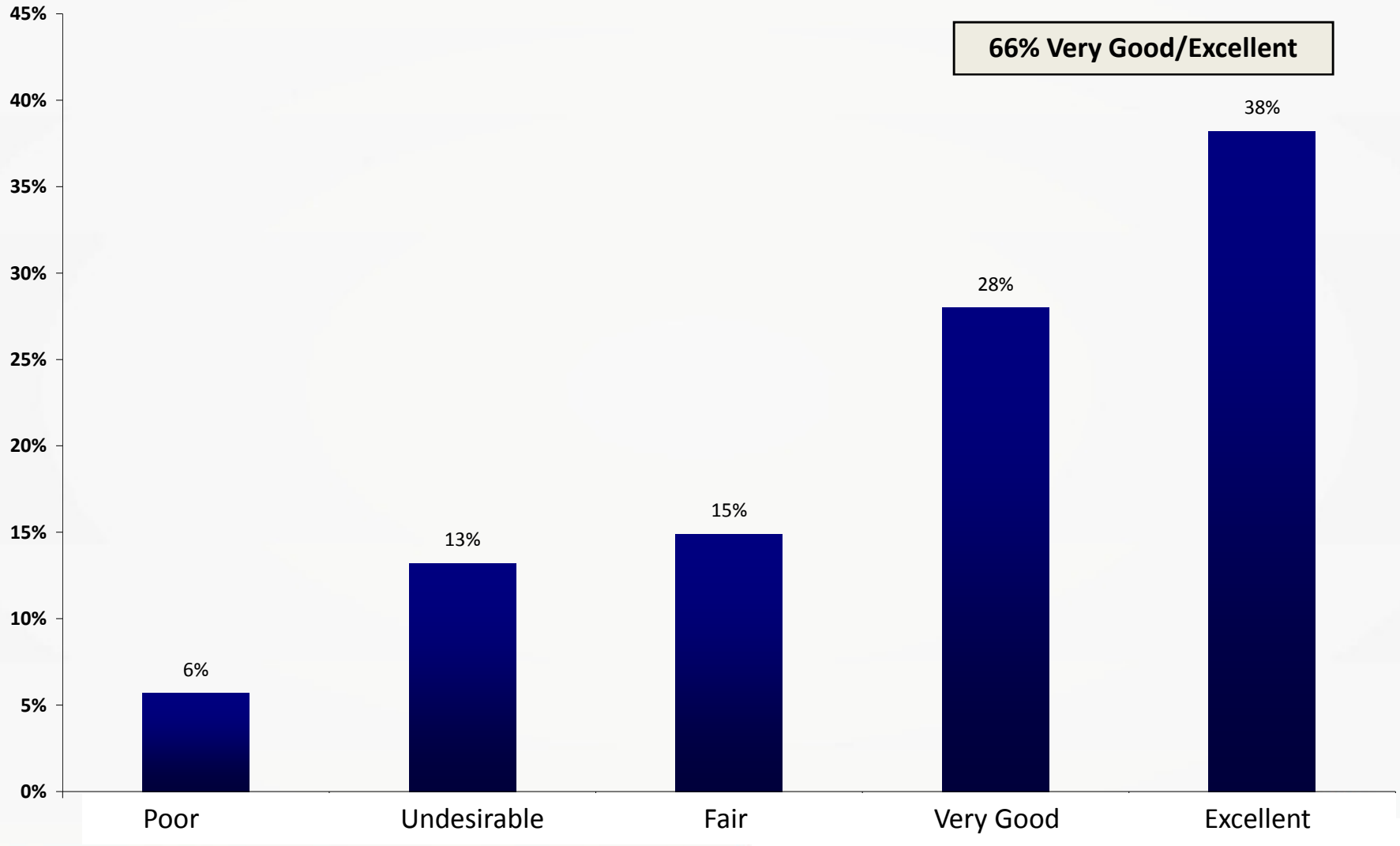
How would you rate the technical support?



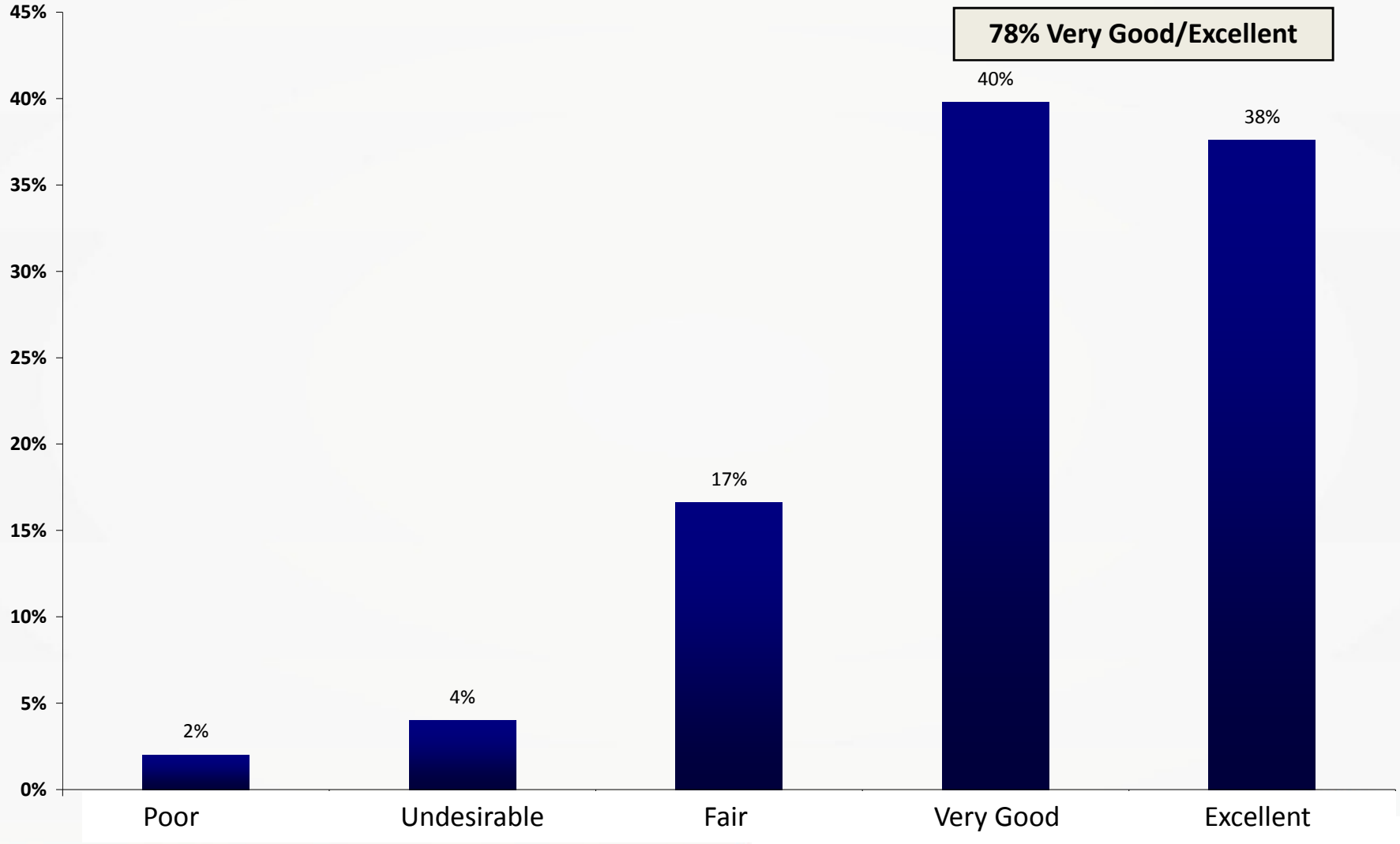
The value for your money of your antivirus product?



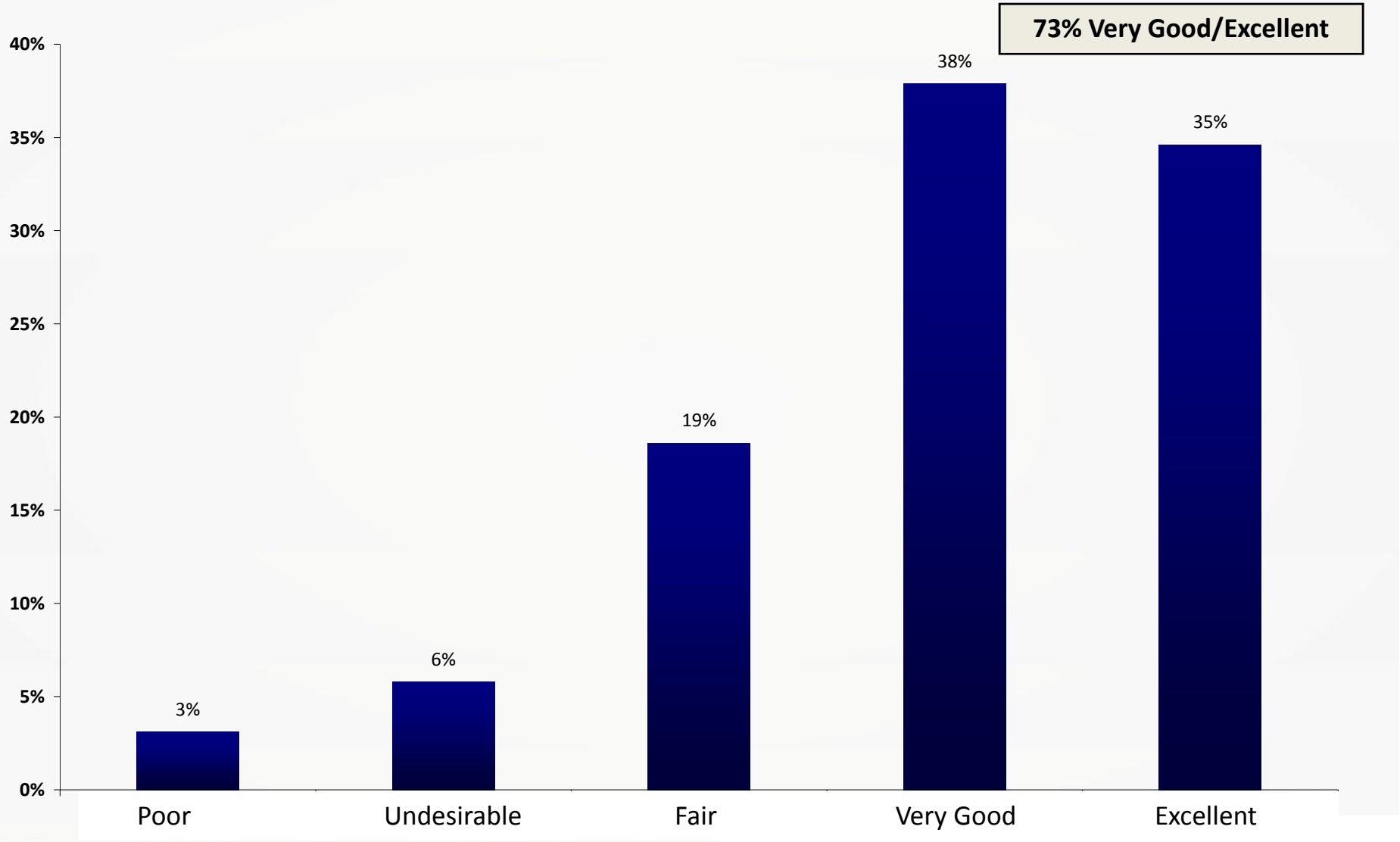
The performance and resource usage?



Ability to protect you against malware?



How well does it clean up malware infections?



Enterprise antivirus user survey

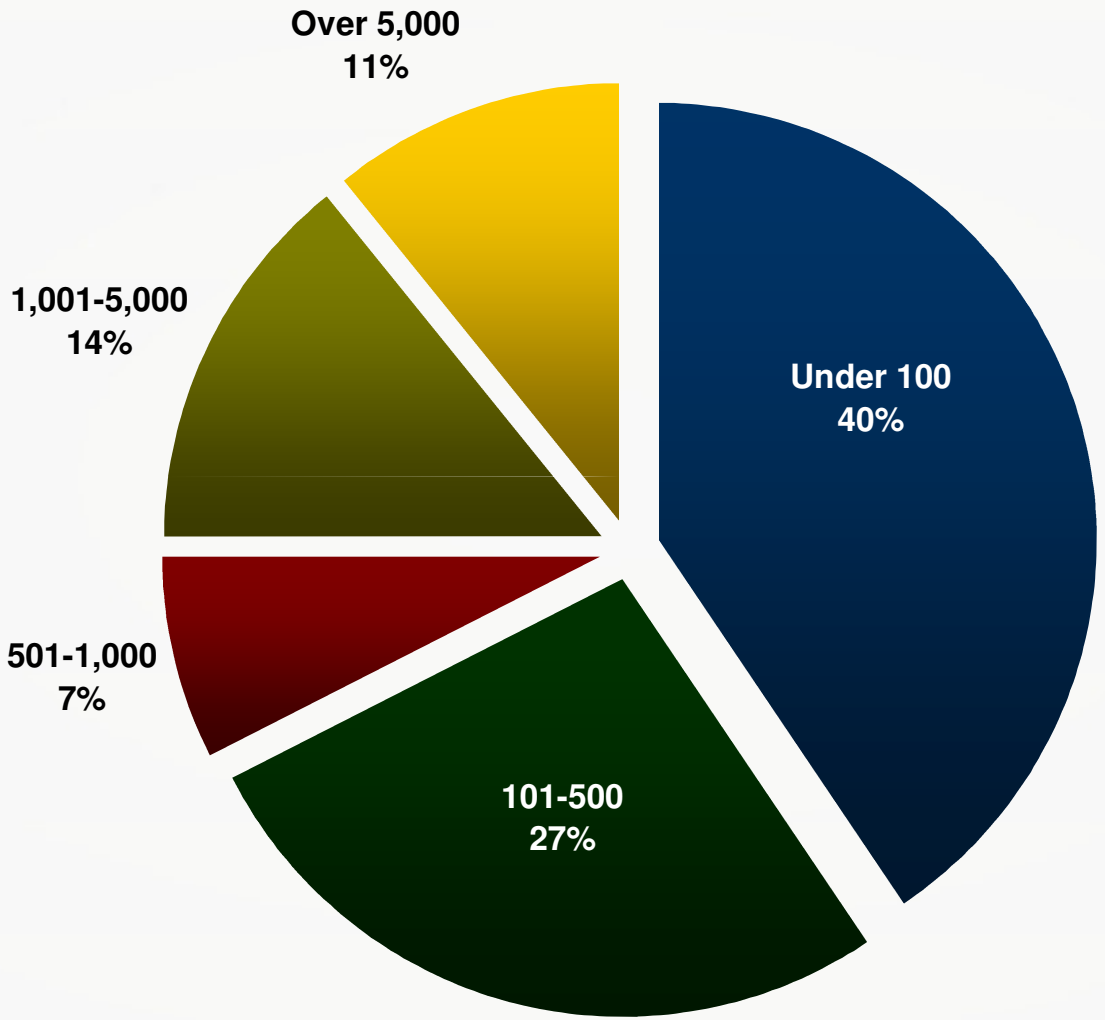
207 surveys taken in September, 2008.

Public was readers of WServerNews and NT SysAdmin forum.

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

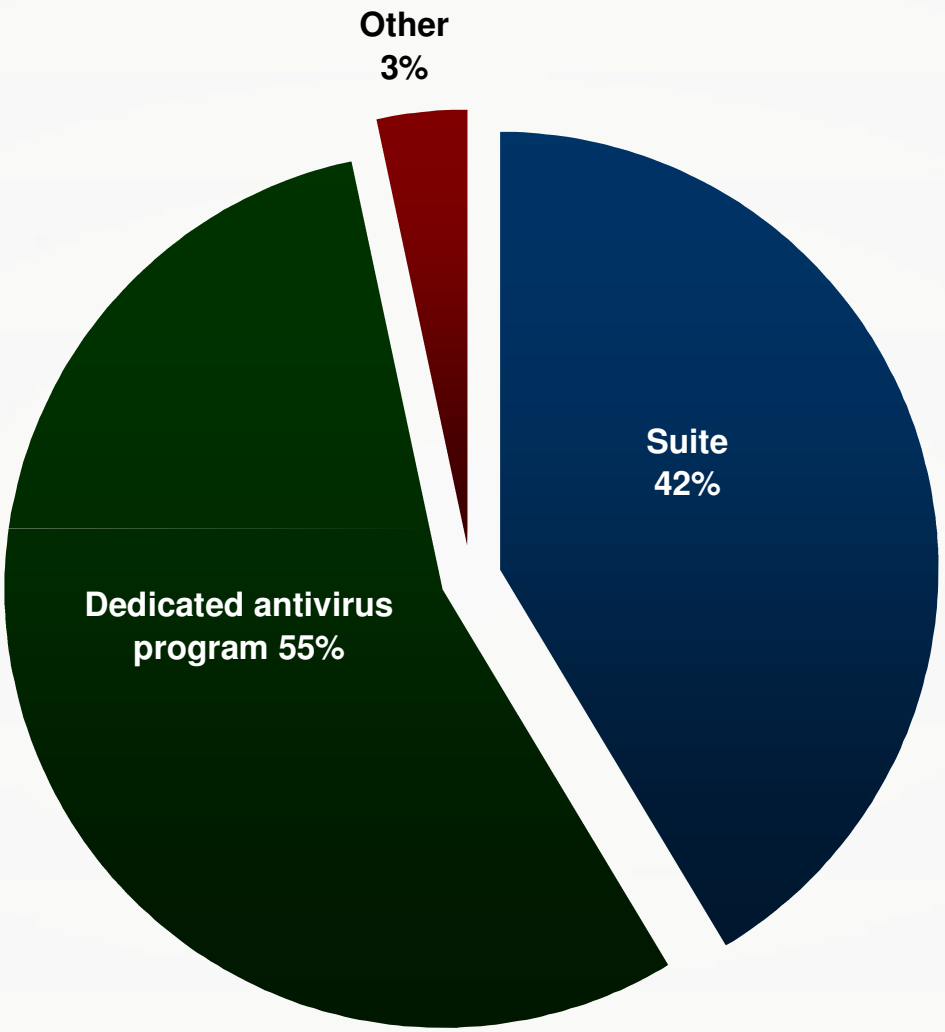
Sunbelt Software

How many seats are there in your enterprise?



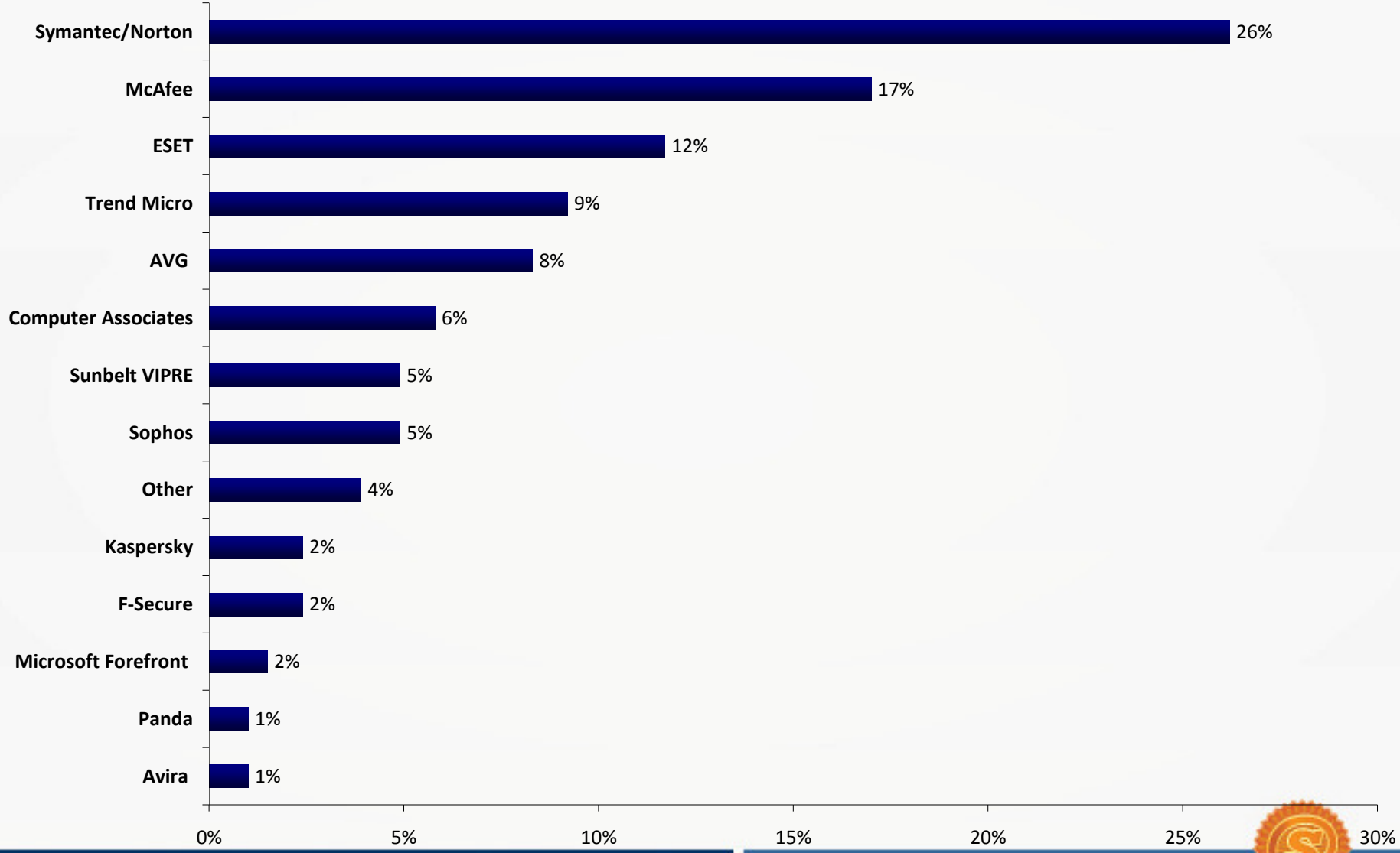
Sunbelt Software

Are you running a suite or a dedicated antivirus program?



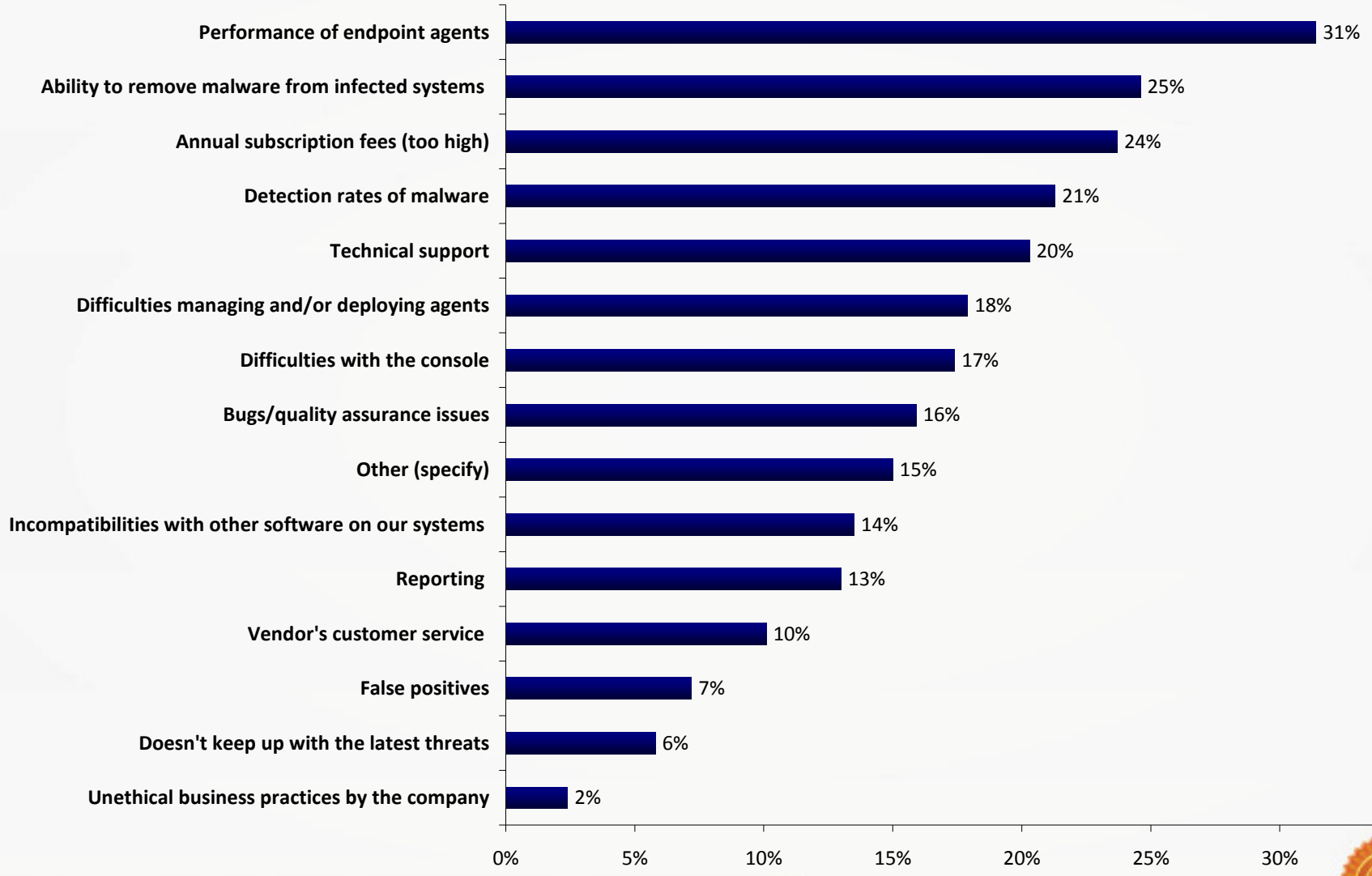
Sunbelt Software

What is your primary antivirus product for endpoints?



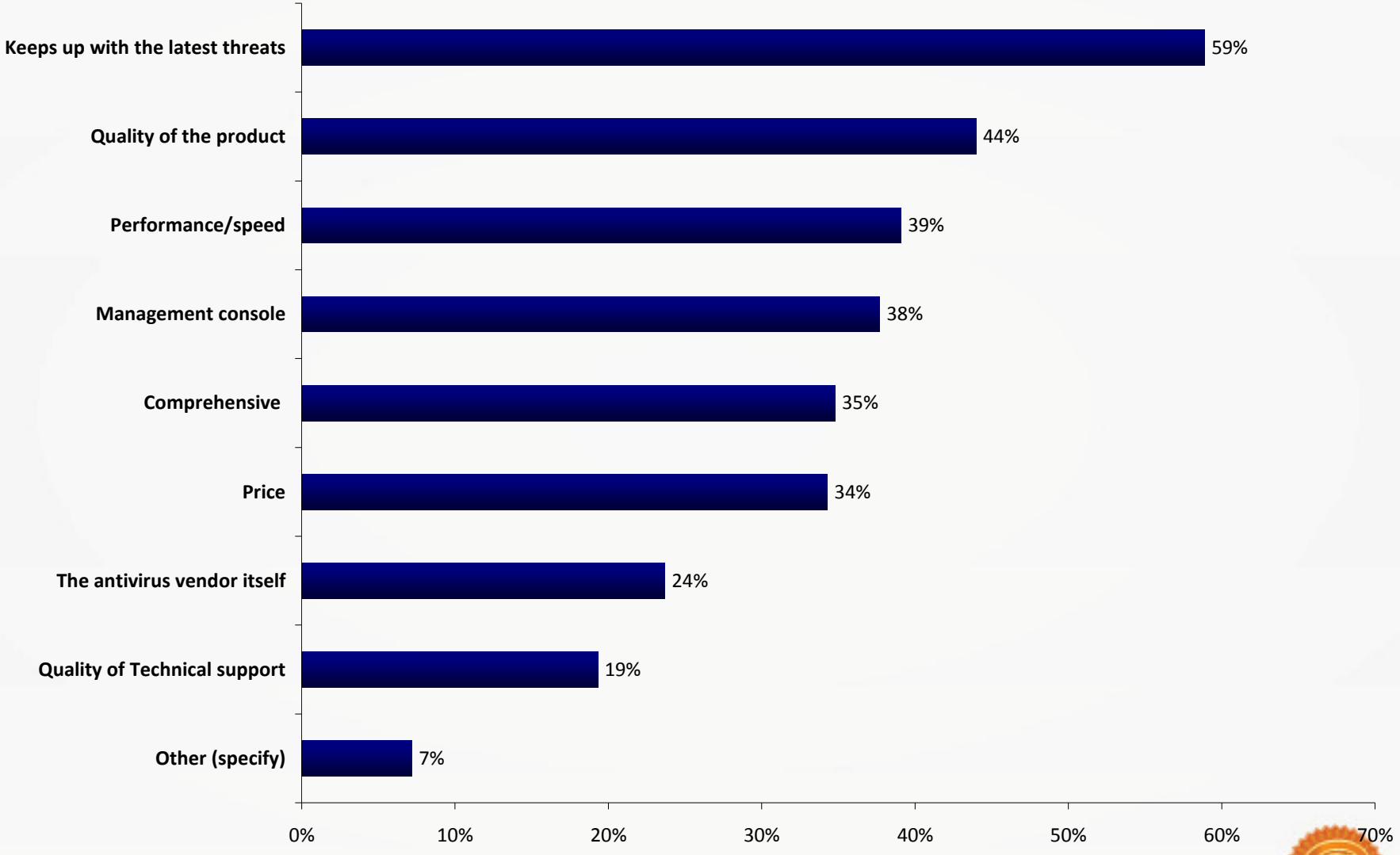
Sunbelt Software

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



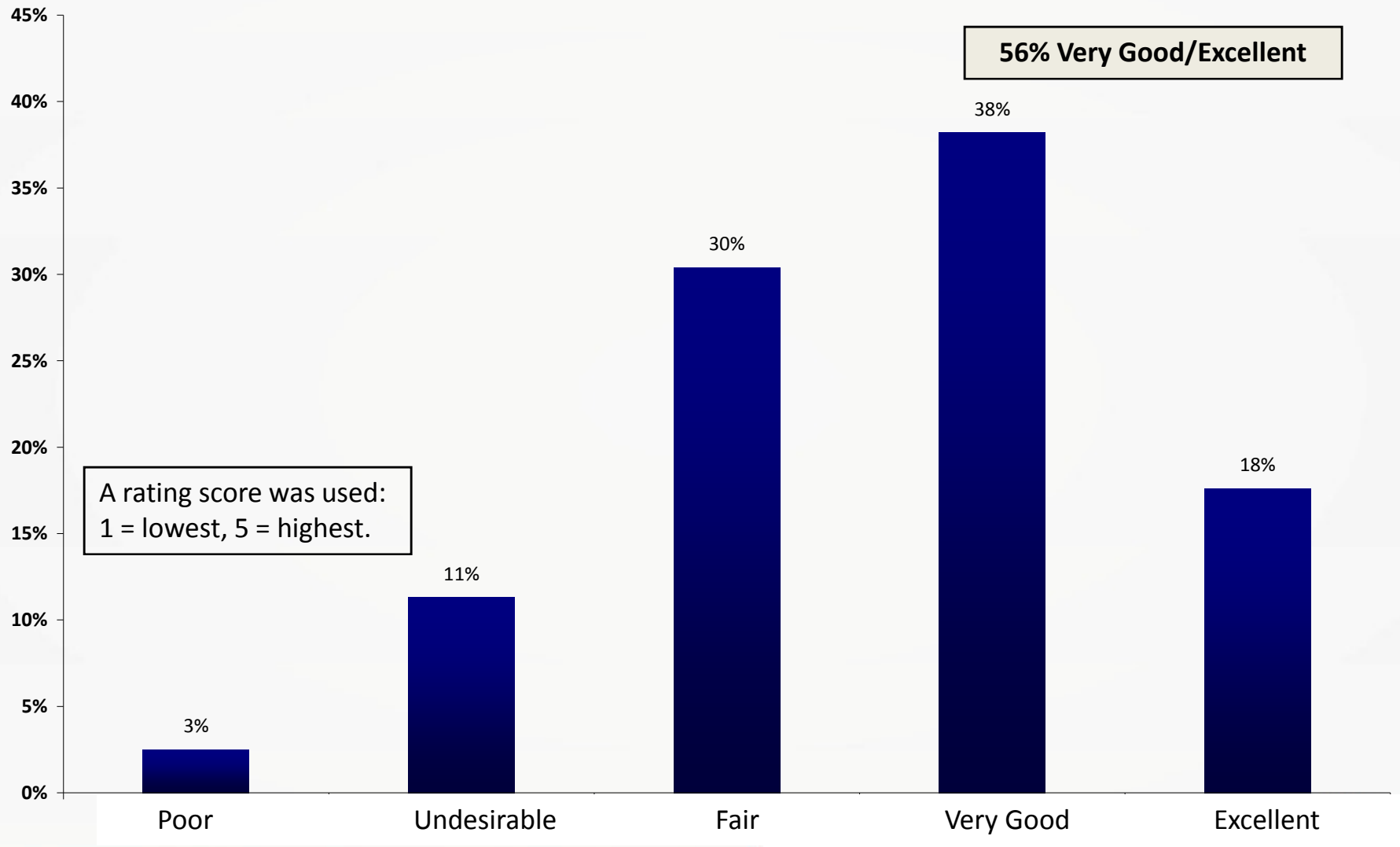
Sunbelt Software

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

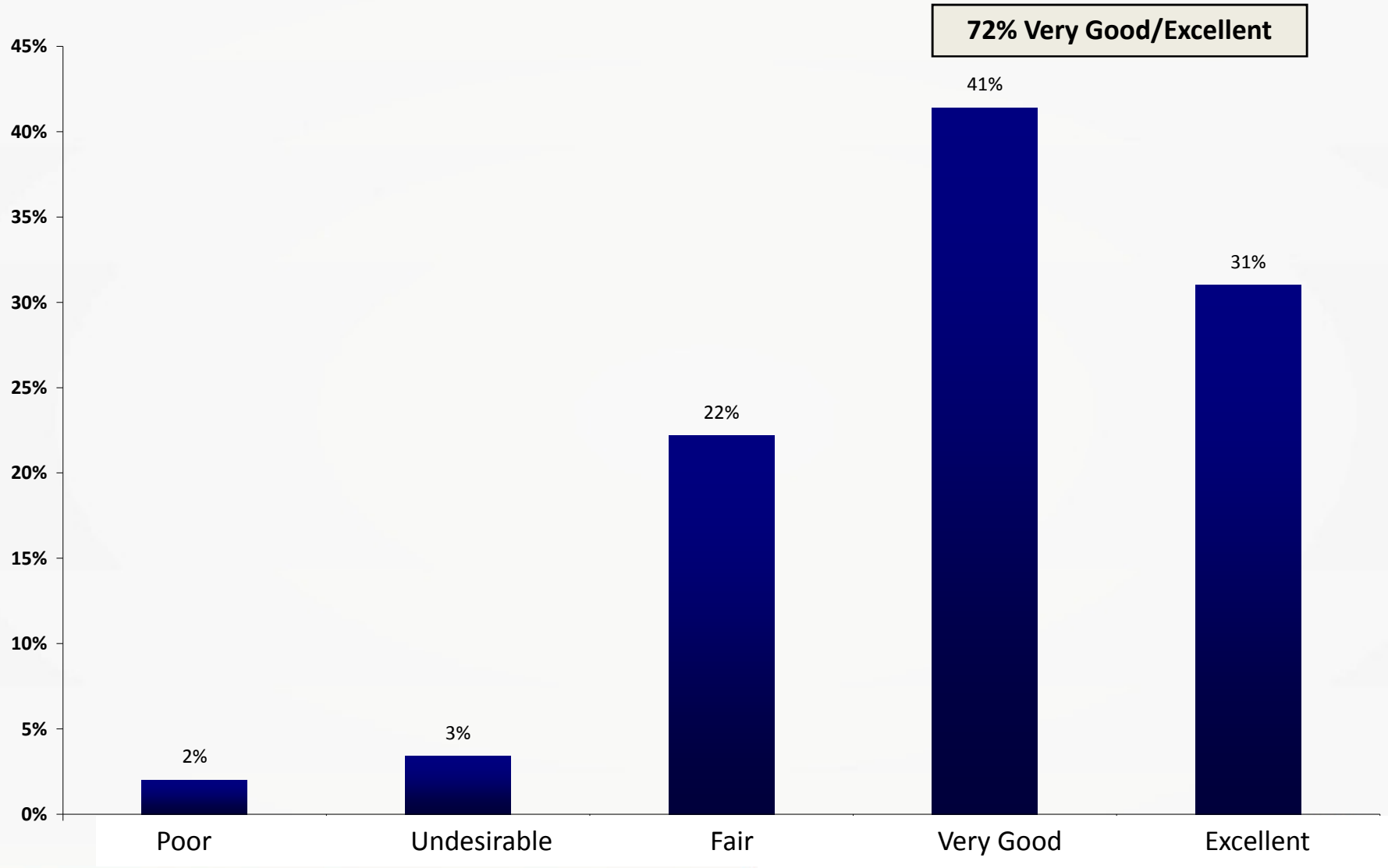


Sunbelt Software

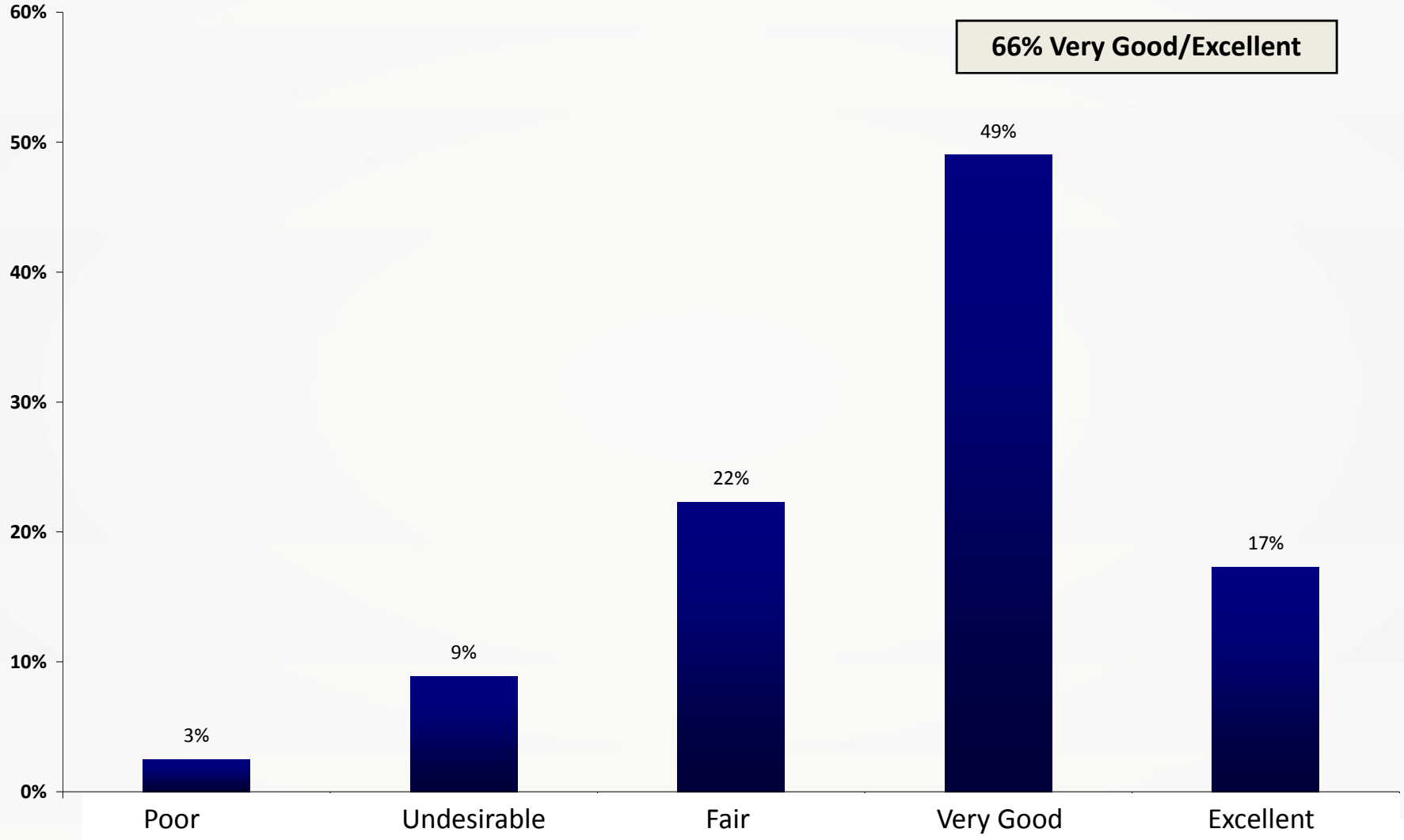
Overall opinion of your antivirus vendor?



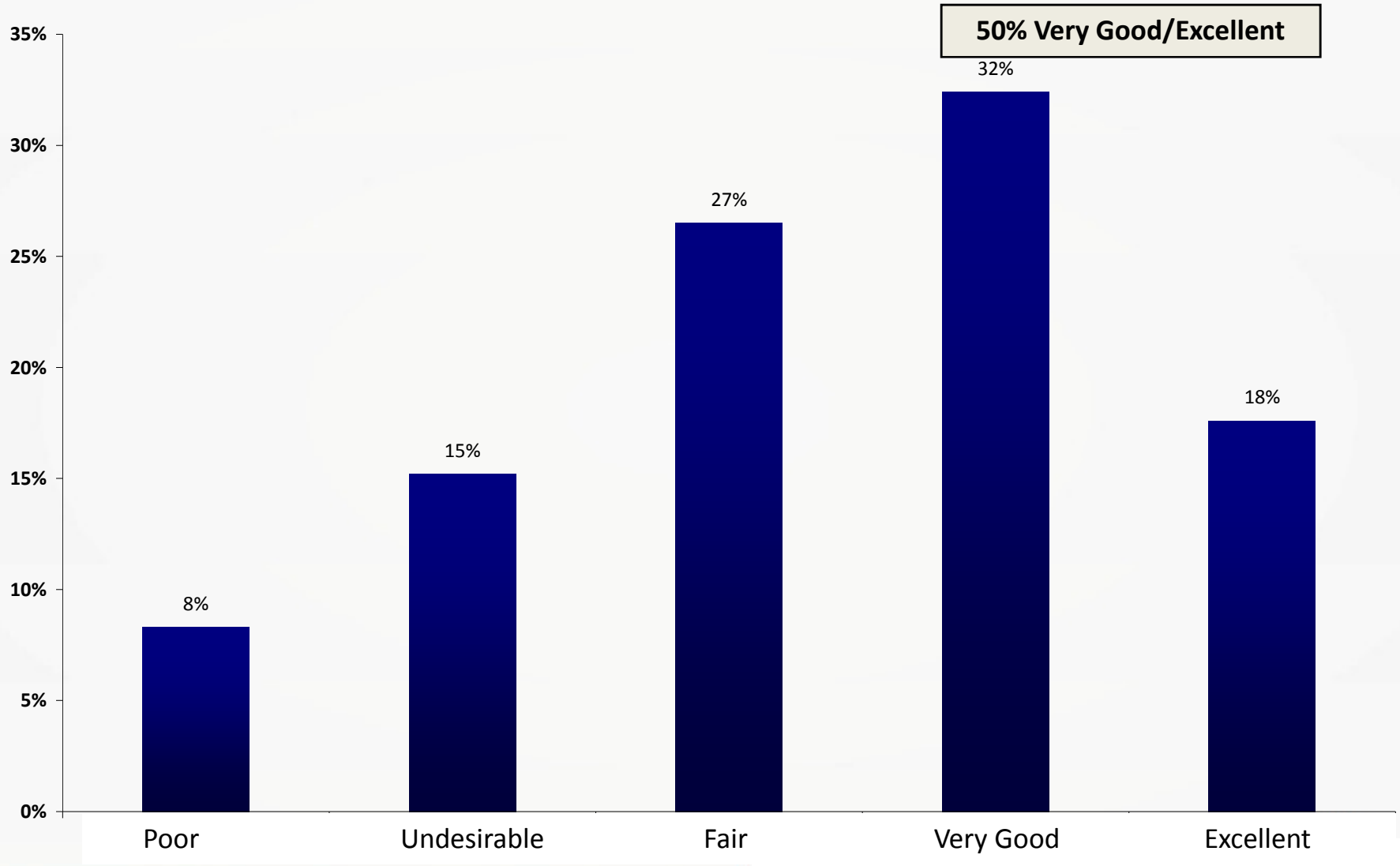
The trustworthiness of your antivirus vendor?



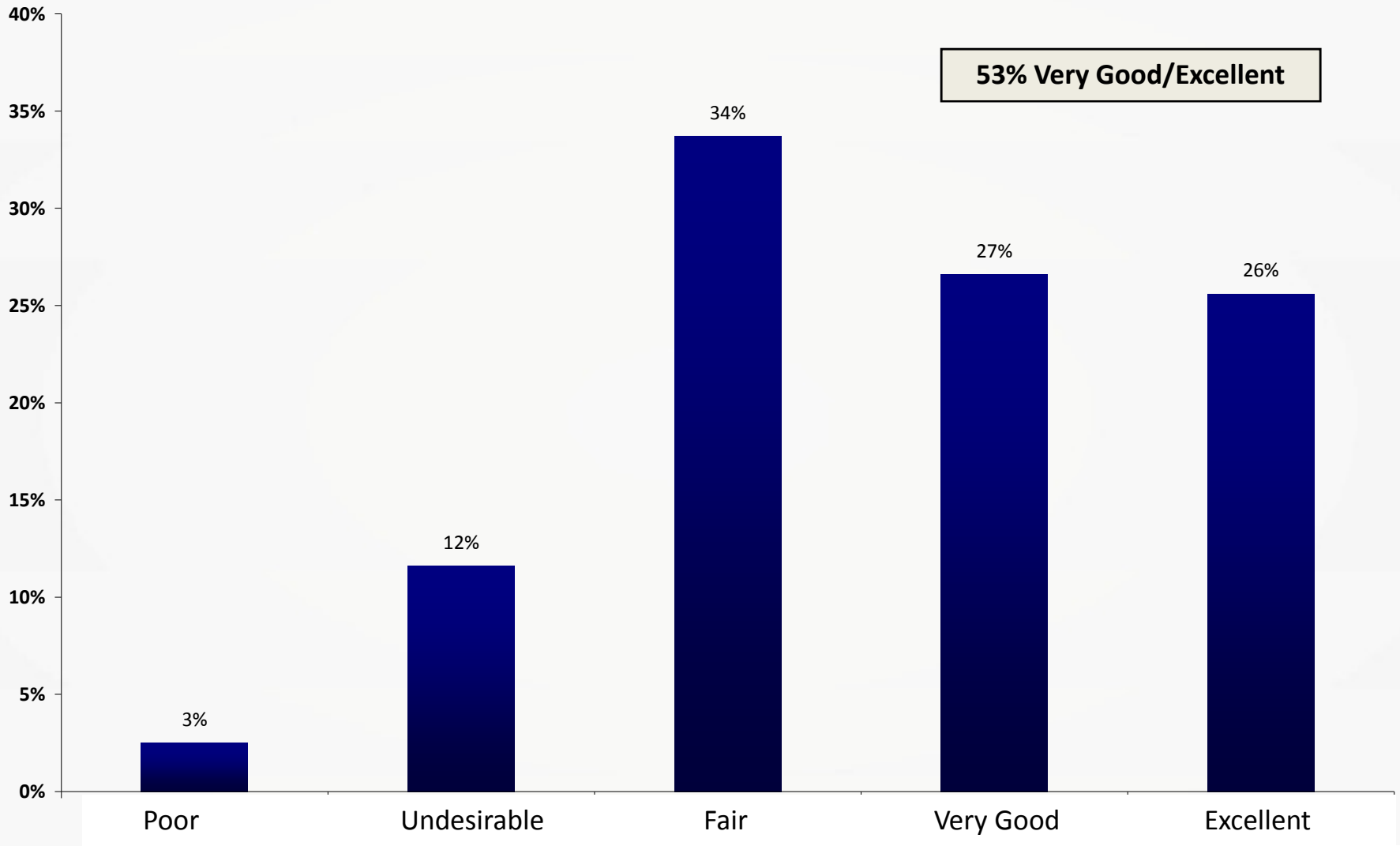
Your overall opinion of your antivirus product?



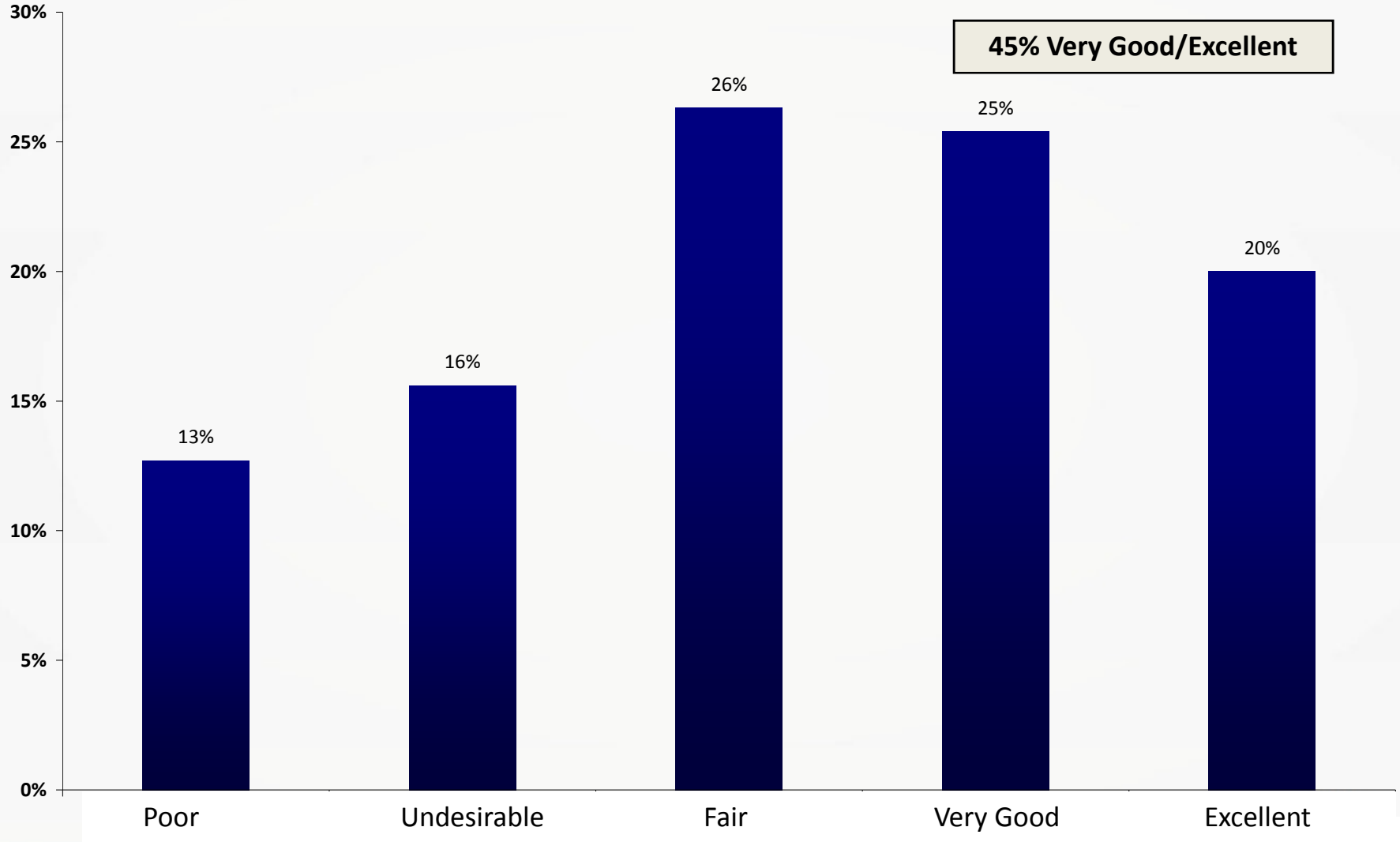
How would you rate the support of your antivirus vendor?



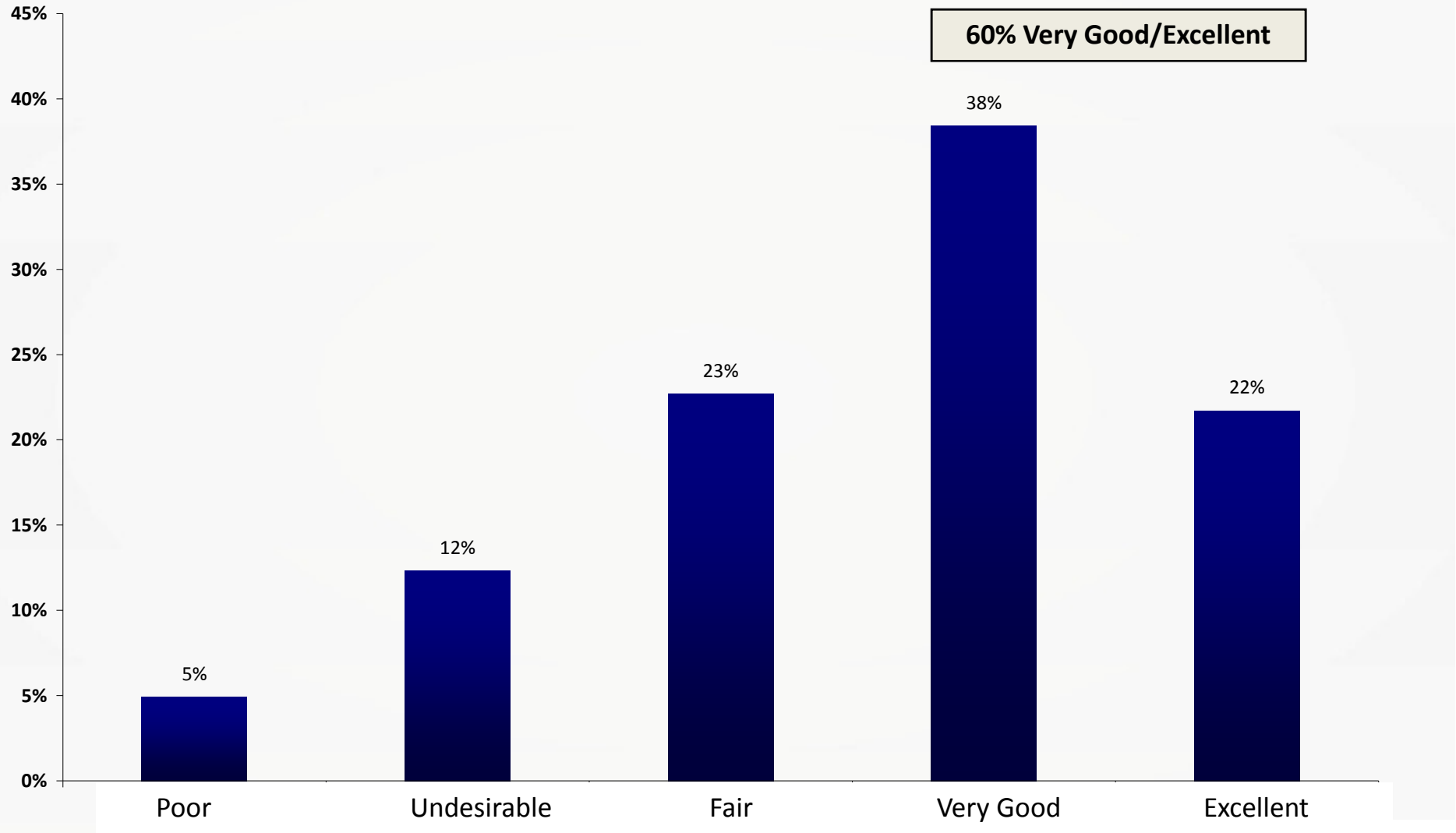
The value for your money of your antivirus product?



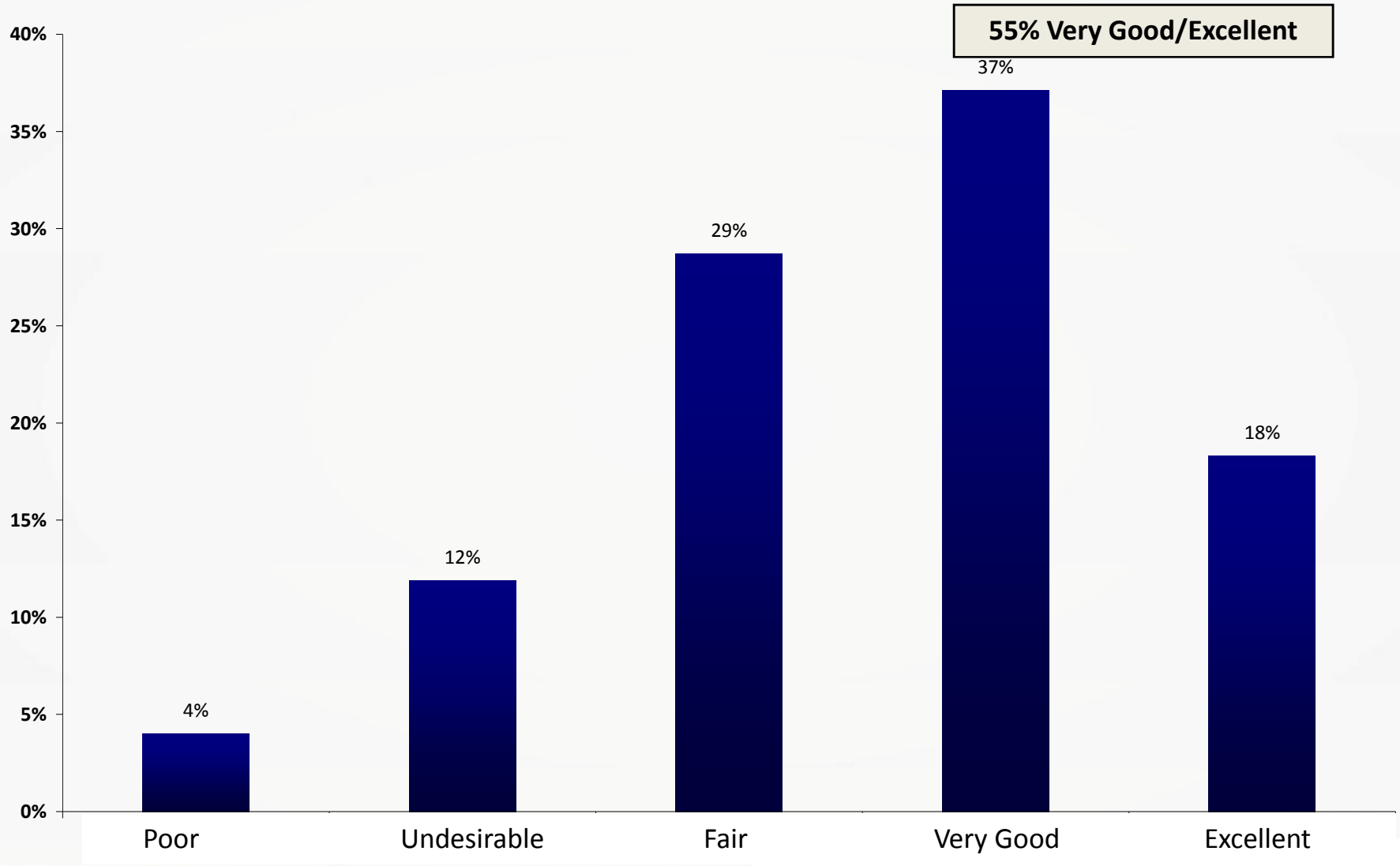
The performance/resource usage of your antivirus product?



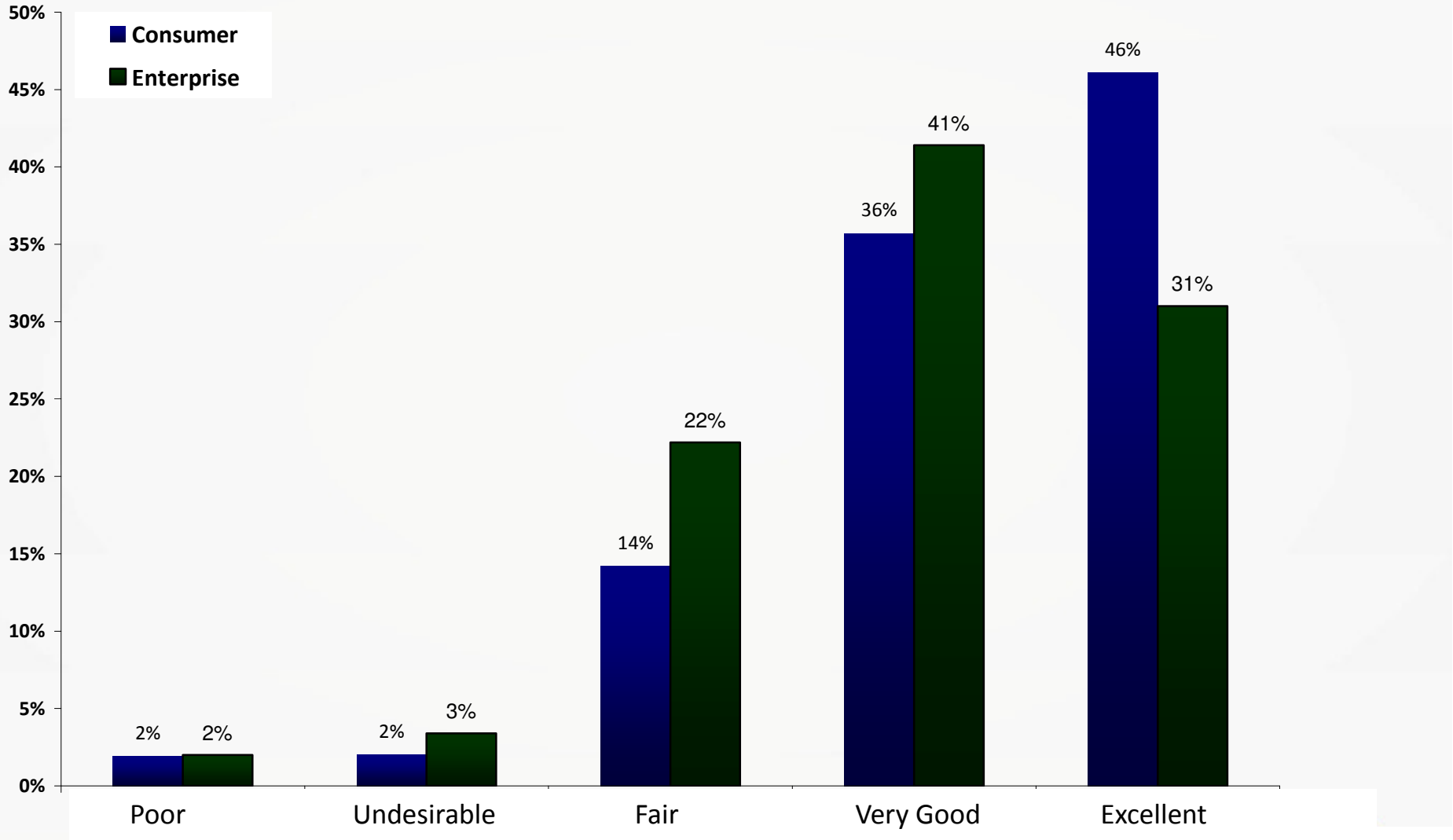
Ability to protect against malware?



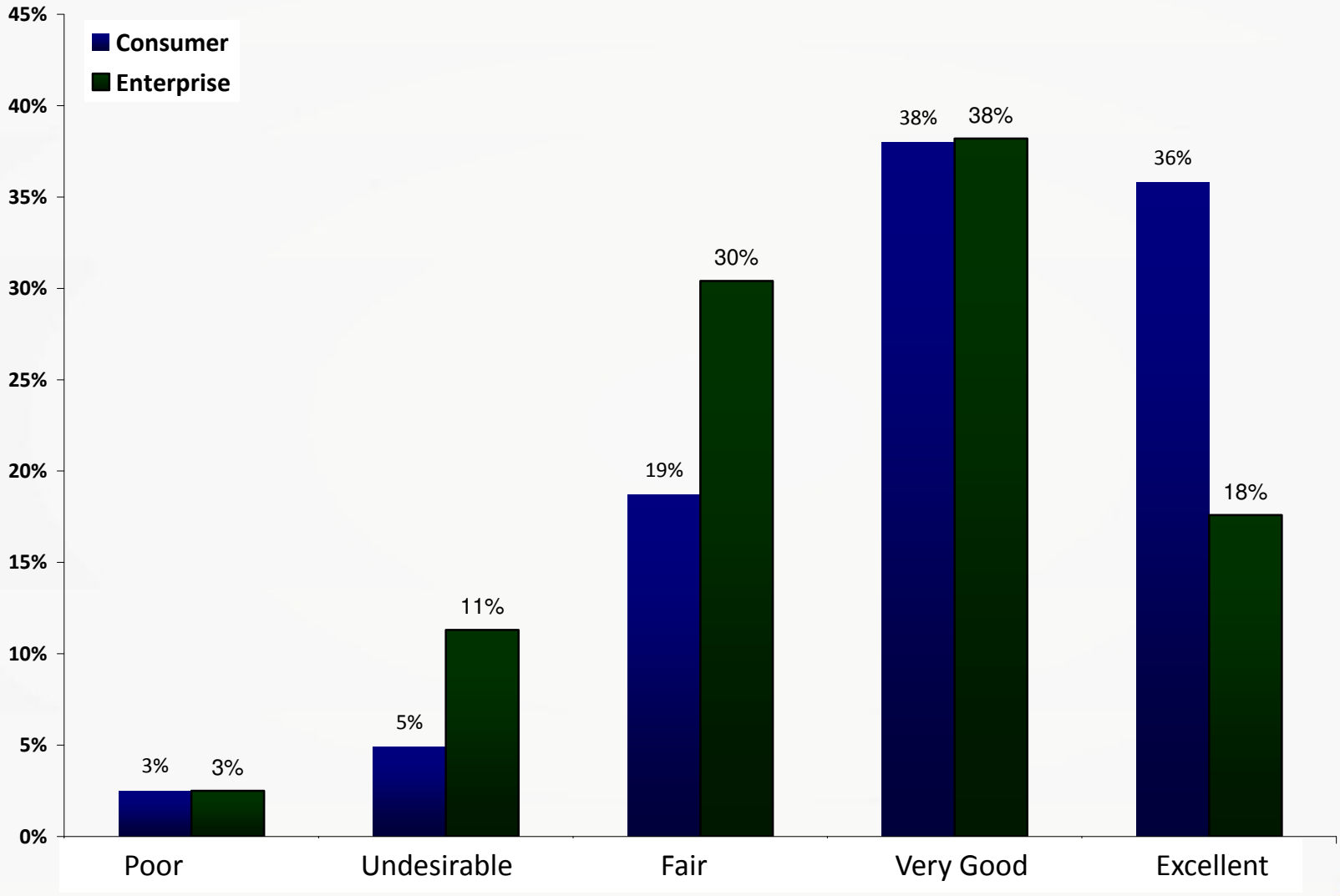
Cleans up infected systems?



Trustworthiness of vendor: Comparison

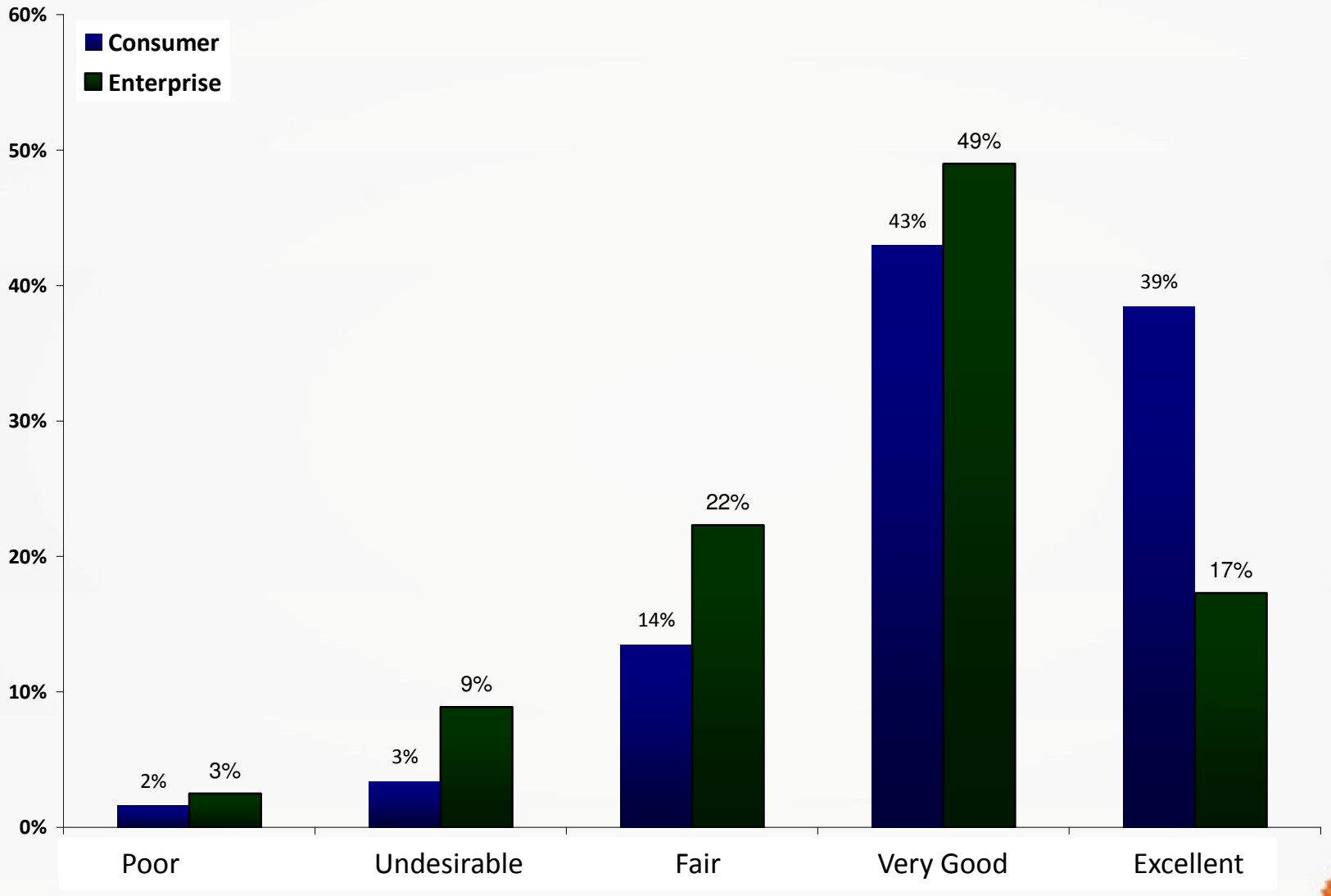


Overall opinion of Vendor: Comparison



Sunbelt Software

Overall opinion of AV product: Comparison



Sunbelt Software

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.

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

	Overalll 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

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