Malwarebytes™

SMB Cybersecurity Trust & Confidence Report 2021

Just how much do organizations trust their cybersecurity?

Contents

We had questions

Foreword

This report began with a few simple questions we were asking ourselves at Malwarebytes HQ. Simple questions with answers that had tricky implications.

Questions like,

> ***"How confident are organizations in cybersecurity to tackle new threats?"***
>
> ***"Just how confident are IT Directors in their endpoint cybersecurity?"***
>
> ***"How do they know if it's working?"***
>
> ***"And what happens to the organization if it's not working but they think it is?"***

(The answers, as they turned out: Not much. Fairly. A couple ways that are problematic. Bad, terrible, not-good things.)

In sum, what is the current state of trust and confidence when it comes to IT security professionals and their corporate endpoint protection?

The results painted a complicated picture, far more M.C. Escher than Andy Warhol.

Read on for our insights and dig into the data that support them.

Methodology

Research findings are based on a survey conducted by Savanta Inc. across the US in January 2021. 704 respondents were asked general questions around efficacy and trust of cybersecurity providers. The study targeted IT decision makers and heads of cybersecurity working at organizations sized between 50–999 employees. Respondents are recruited through a number of different mechanisms, via different sources to join the panels and participate in market research surveys. They are invited to take part via email and are provided with a small monetary incentive for doing so.

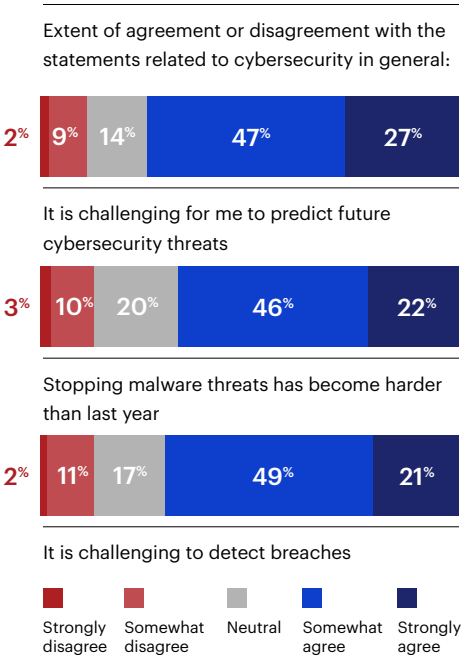
Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. In this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 3.7 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

All gas, no brakes

Navigating today's cybersecurity landscape

As SMBs (small- and medium-sized businesses) put 2020 in the rearview mirror and look towards the future, it's becoming apparent that threats are evolving in ways that make them harder to predict and harder to stop. It's like a car with its brake lines cut and the steering wheel replaced with a frozen pizza.

A significant majority of SMBs, 74%, agreed it's challenging to predict future cybersecurity threats, while some 68% agreed that stopping threats has become harder than last year. Another 70% agreed that it's challenging to detect breaches after they've already happened.



Hackers change gears on the information super highway

Case in point: Remote Desktop Protocol (RDP) attacks. Few could have predicted the surge in remote desktop protocol attacks we witnessed in 2020. According to the Malwarebytes State of Malware 2021 report, many of the major breaches in 2020 were due to cybercriminals attacking vulnerable systems manually using RDP attacks, as opposed to using more traditional malware, like Trojans. As you might've guessed, attacks attributed to the Emotet and TrickBot Trojans fell 89% and 68%, respectively.

95%
Trust their security provider

91%
Are confident their provider will protect them

83%
Said cybersecurity threats have become more complex

Letting go of the wheel

We asked SMBs "How much do you trust your primary endpoint protection in providing effective cybersecurity to endpoints in your organization?" A solid 95% of SMBs say they trust their security provider and 91% are confident their endpoint protection can protect systems against dangerous cybersecurity threats. So far so good, but let's muddy the waters a bit.

We then asked SMBs, agree or disagree? "Cybersecurity threats have become more complex over the last year." Some 83% of our SMBs agree.

It would seem that given a long enough timeline and a persistent threat, the majority of SMBs believe a successful cyberattack is inevitable. Only a third, 36%, expect their endpoint security product to detect every threat.

Putting it bluntly, one respondent said "A provider is very unlikely to detect every threat because a new, never seen before threat would be unlikely to trigger a response."

Another said simply "Hackers are always trying harder."

If we can take anything away from this data it's that most SMBs are circumspect about the threats they're facing. Most understand that the idea of achieving "100% protection" is a myth, regardless of how much faith they put in their security.

36%

Expect their primary endpoint protection provider to detect EVERY threat

45%

Expect their primary endpoint protection provider to detect the MAJORITY of threats

19%

Expect their primary endpoint protection provider to detect a FAIR AMOUNT of threats

"A provider is very unlikely to detect every threat because a new, never seen before threat would be unlikely to trigger a response." Survey respondent

Trust but verify

The status of today's complex relationship between SMBs and cybersecurity providers

Like any budding relationship, it's complicated. It usually is. But If you're looking to sum-up the status between SMBs and their cybersecurity vendors, "Trust but verify" hits close to the heart.

Popularized by Ronald Reagan during the 1987 INF Treaty negotiations, this catchphrase has important meaning for IT security teams as well. Namely, that while trust is a lovely foundation for catching malware, blind trust can also have dire consequences.

Needless to say, the ramifications of this delicate and finicky relationship became evident as we began poring over the results of our SMB Cybersecurity Trust & Confidence Report 2021.

The disconnect between SMB sentiments and expectations

At first glance, we notice that SMBs are gushing over their endpoint protection vendor. Almost to a fault, you might argue. In fact, 91% of respondents report that they're either satisfied or completely satisfied with the solution provided by their primary provider. Their over-the-moon sentiment is obvious and heart-warming.

> ***"It's a trustworthy brand and I love it."*** Survey respondent

Yet when pressed for actual expectations, the honeymoon is over quickly. Only 36% expect their provider to detect every threat, while 45% expect to detect only a majority of threats. Not exactly a ringing endorsement on their part. And to add heartbreak to misery, 56% of SMBs either strongly agree or somewhat agree that "it's not a matter of if but when my organization suffers a successful attack or breach."

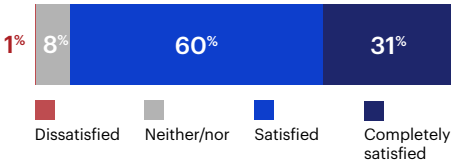
So, if SMBs love their cybersecurity providers so much, why do they expect so little in return? If this was the parachute industry, and 56% of customers fully expected their ripcord to eventually fail mid-fall, there would be trouble in paradise.

Enter the all-forgiving hall pass: SMBs know how tricky malware can be

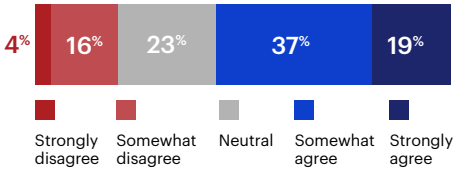
Why then are SMBs so quick to let their cybersecurity providers off the hook?

Despite their concerns over being hacked (and the inevitable mayhem that will ensue), the SMB Cybersecurity Trust & Confidence Report 2021 clearly shows that respondents are willing to cut their vendor some slack. The simple explanation appears to lay in the fact that SMBs realize that cyberthreats are a tremendously thorny issue.

How satisfied or dissatisfied are you with the solution/product provided by your endpoint protection provider?



I believe it's not a matter of if but when my organization suffers a successful attack or breach



"There will always be new threats that are impossible to detect without hindsight, and heuristics are not advanced enough to detect all threats."

Survey respondent

A full 68% either strongly agree or somewhat agree that "stopping malware threats has become harder than last year." The point is further supported by a 70% response that they either strongly agree or somewhat agree that "it's challenging to detect breaches." And as our separate Enduring from Home report clearly shows, this challenge is now being made even more difficult with the COVID-19 pandemic and increasing move to remote work.

68%

Said stopping malware threats has become harder than last year

70%

Agreed that it's challenging to detect breaches

In a nutshell, the majority of SMBs agree that cyberthreats are becoming more complex, more challenging, and harder to predict. It's no wonder that more than half of respondents report it's inevitable they'll suffer the consequences of a malware attack.

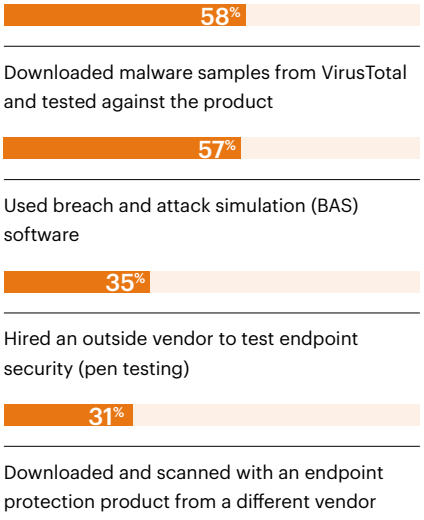
Hence the "Trust but verify" pre-nuptial

Now we get back to the heart of the matter. While SMBs certainly have positive feelings for their cybersecurity providers, as we've noted, their confidence in the relationship's ultimate success is uncertain at best.

That's why SMBs rely on testing to find any weaknesses.

A whopping 78% of companies with 50-999 employees report that they've tested their endpoint protection in the past 12 months, to "see if it is detecting cyberthreats." Clearly, they're looking for verification that the provider is more than just a pretty face. (On the other hand, only 65% of companies with 50-99 employees tested their endpoint protection).

This testing is happening on a variety of fronts. This includes downloading manual samples via VirusTotal (58%), breach and attack simulation (BAS) software (57%), hiring an outside pen testing vendor (35%), and the "wingman" approach of downloading a different endpoint protection for a supplemental scan (31%).



78%

Have tested their endpoint protection in the past 12 months to see if it's detecting cyberthreats

The curious love affair with VirusTotal

Each of these testing methods can be problematic, particularly downloading/uploading samples to-and-from VirusTotal. At 73%, this was the top response among SMBs in business fewer than five years. While these SMBs specifically referred to downloading malware from VirusTotal to test against their primary endpoint protection, our guess is that many respondents were also referring to uploading files from their network to be tested by the 70+ cybersecurity scanners and URL/domain blacklisting services on VirusTotal.

> ***"I believe it is working and will continue to work. I have to trust the vendor to some extent."*** Survey respondent

Either way, there are concerns for SMBs, including when downloading files.

1. It's sometimes difficult to trigger an infection in a sandbox, as threat actors have gotten wise and write their malware so it won't detonate (or will limit its behavior) until it's outside of the sandbox.
2. Malware can break out of containment when being tested and infect your network, including in a virtual machine via hypervisor breakout capability, which allows malware to climb the walls of a sandbox.
3. Files others have uploaded to VirusTotal are often not the latest threats, which could lead to false negatives.

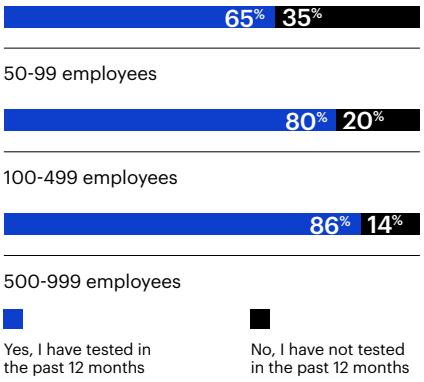
As well as these concerns, are additional issues when uploading files to VirusTotal to be scanned by multiple cybersecurity vendors.

1. VirusTotal may be running outdated software from the participating cybersecurity vendors, which may not detect newer threats.
2. VirusTotal can have privacy issues, as unsuspecting SMBs may accidentally share code that contains sensitive information that can be leaked.

Using the surveys findings, we can break down this "Trust but verify" dance even further to explore other interesting diamonds in the rough.

For example, while previously noted that 83% of companies with 50-999 employees are now testing the effectiveness of their protection, conversely only 65% of companies with 50-99 employees are testing theirs. One could reasonably deduce from this finding that smaller companies have fewer IT resources at their disposal, and can't go the extra step to test.

The relationship between number of employees and testing of endpoint protection in the past 12 months to see if it's detecting cyberthreats

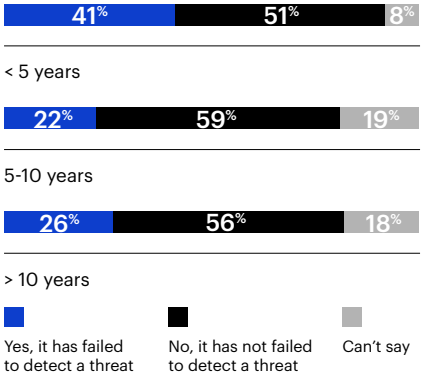


"In the current cybersecurity landscape, it's essential that enterprises implement a layered approach to endpoint security."

Survey respondent

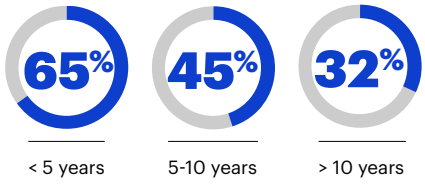
Here's another nugget discovered when digging a little deeper. We found that 26% of SMBs overall responded yes when asked "Has your endpoint protection product ever failed to detect a threat?" Yet for companies that have been in business for fewer than five years, that figure skyrockets to 41%.

The relationship between age of company and whether endpoint protection product has ever failed to detect a threat



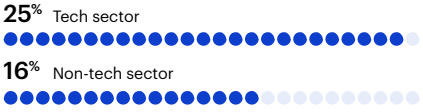
Similarly, younger SMBs are more likely than their more established counterparts to believe that hackers only attack larger organizations. While 65% of companies with fewer than five years under their belt strongly agree or somewhat agree, only 32% of SMBs with 10+ years of experience concur. Again, this suggests small SMBs are less likely to test and are therefore more susceptible to breaches.

Agreement that hackers do not target small- and medium-sized organizations and attack only bigger organizations by company age



Slicing the data even further, by specific industries, we notice some additional trends that are eye-opening. For example, organizations in the tech sector are significantly more likely to strongly agree that it's not a matter of if, but when, their organization suffers a successful attack or breach (25% versus 16%). Organizations in tech are also significantly more likely to strongly agree that stopping malware threats has become harder than last year (26% versus 20%).

Agreement that it's not a matter of if, but when, their organization suffers a successful attack



Agreement that stopping malware threats has become harder than last year

Beware wedding crashers

Separate research by Malwarebytes backs up the fact that it's a good idea SMBs regularly test their cybersecurity protection for holes or weaknesses.

In January of 2021 alone, on 5,021,761 devices on corporate domains that already had another endpoint protection product registered (although it's not certain the software was active), Malwarebytes (a trial version) caught infections that got through on 512,781 of those devices.

That's over 10% of the devices in question, which is alarming. If 10% of endpoints are allowing malware attacks to sneak in despite having an endpoint protection product present, SMBs are certainly wise to double-check (or even triple-check) their cybersecurity protection.

If you're interested, additional insights on SMBs (and companies of all sizes for that matter) can be found in our State of Malware 2021 report.

Bottom line: It's not exactly a marriage made in heaven

As pointed out above, there's a clear disconnect between how SMBs feel about their cybersecurity provider in general, and what expectations they actually have of their protection. While 94% of SMBs report that their primary endpoint protection is very effective or effective, 47% also report that they strongly agree or somewhat agree that their cybersecurity is not up to the task of stopping new threats. This feels like trouble in paradise.

94%

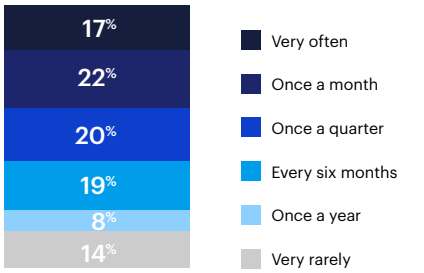
Said their primary endpoint protection is very effective

47%

Agreed cybersecurity is not up to the task of stopping new threats

It's no wonder SMBs are adopting a "Trust but verify" philosophy for their relationship with cybersecurity providers, and for getting a second opinion to help ease their worries (and quite possibly save them from a costly fracas that's either private or public).

Frequency of registering a cybersecurity threat



With 59% of SMBs reporting that they register a cybersecurity threat at least once every three months, the likelihood of trouble in the near future is evident. This disconnect will only shrink when cybersecurity providers find ways to better combat the new, more sophisticated threats that continue to emerge. This includes vendor's advancements in threat hunting, behavioral analysis, machine learning, and other next-generation solutions.

Looking for a sign

How SMBs know their endpoint protection is working

Most protection products make it easy to know when they're working. The signs are obvious.

Apply sunscreen by the swimming pool at noon, and if you're not a lobster by happy hour, bingo. Wear a seat belt while driving to the hardware store, and if you walk away from a fender-bender safely, voila!

But how do SMBs know if their cybersecurity protection is working? Not so simple, as the guiding lights are few and far between.

We asked SMBs for tell-tale signs that their protection is working

The biggest shock of our survey was how unscientific the majority of SMBs are in testing their endpoint protection.

The #1 response when asked "How do you know if your endpoint protection is currently working to protect your organization?" was... My endpoints and network are running normally.

Hmmm, considering the abundance of resources and cash that SMBs are throwing at cybersecurity (not to mention the tremendous consequences that are at stake here), this seems a little flippant. One would reason that companies would use their vast technological might to more closely monitor and evaluate every little nuance of their protection.

But for most SMBs, that's not the case.

Here's the complete breakdown of how SMBs reported knowing if their cybersecurity is working:

1. Their endpoints and network are running normally — 50%
2. They get threat alerts from their endpoint protection product — 47%
3. They look at their product's reporting dashboard — 40%
4. Their product is detecting/ quarantining threats — 39%
5. There are no known breaches reported — 33%
6. No complaints are being reported from users — 31%
7. They still have a job — 20%
8. There's nothing in the newspapers yet — 9%

As a side note, judging from the final two responses, it appears that a sense of humor isn't affected by the age of your SMB either. Given the level of stress, these CISOs and cybersecurity professionals are under, apparently gallows humor comes with the job.

> ***"Even a combination of solutions can't catch every threat, just like a flu shot cannot prevent every strain of flu."***
>
> Survey respondent

Is watching endpoints/network performance really a dead giveaway?

Logic would say no. Here's why.

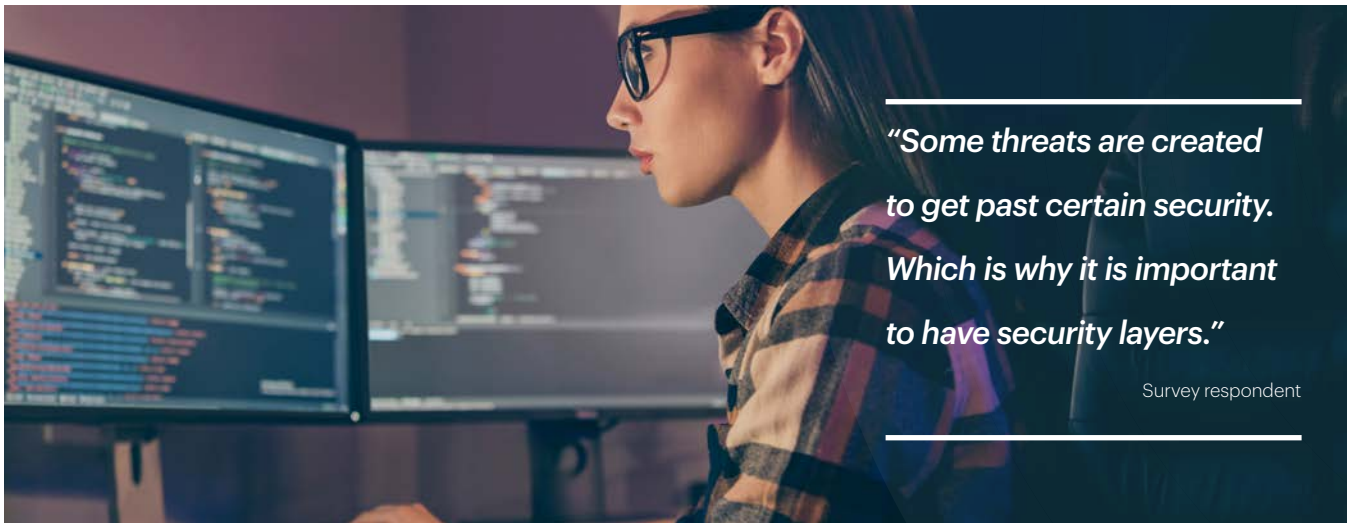
As threat actors become more sophisticated, they're getting even better at covering their tracks. Unlike ransomware, which announces itself boldly, most cyberthreats are designed to evade detection and run silently in the background. This means that a cybersecurity team wouldn't notice a lag in either their endpoints or the network until it's too late.

A case in point is the SolarWinds attack. It went undetected for months and was only discovered by accident. This sophisticated supply-chain attack was embedded in trusted software and escaped detection even by multi-layered defenses.

A few other examples of attacks that wouldn't necessarily show a drop in endpoint or network performance include 1. Living-off-the-land (LOL) assaults that use native tools already on a system to blend in, 2. Advanced Persistent Threats (APTs) that can also remain undetected for a great length of time, and 3. Multi-platform attacks on Macs, Linux, and mobile devices, plus 4. Social media strikes via LinkedIn, Twitter, and other apps. If you want to learn more about the vast variety of attacks out there, browse the Malwarebytes State of Malware 2021 report.

For these and many other similar attacks, looking at endpoint or network performance alone isn't going to cut the Dijon.

As a side note, research shows that a best practice for helping prevent these types of silent killers is to closely monitor all assets and data pathways into the network. SMBs should also consider having a test phase for all new updates before deployment. And naturally, they should keep their endpoint protection updated and third-party software patched. Educating employees on what not to click on never hurts either. With remote work increasing, this becomes especially critical. More info can be gleaned from our separate Enduring from Home report.



"Because there are flaws in every system, in order to stay truly protected we need to manually check our systems for any attempted secret attacks that can bypass the endpoint protection provider."

Survey respondent

Depending on an SMB's age, the writing is on the wall

The whole age issue suggests that SMBs that have been around longer are more apt to use their own cybersecurity protection features to let them know it's working. We can assume that younger companies have less time and fewer resources to invest in their antivirus solution. Given their situation, it's easier to simply look at indicators in their business environment—not signs from their endpoint protection dashboard.

This assumption generally carries over to the revenue size of a company. We see that 56% of SMBs reporting revenues of $100 million or more said "I look at the product's reporting dashboard regularly." Yet only 33% of SMBs reporting revenues of less than $5 million respond the same.

There are also minor similarities among the "non-technical" responses (watching endpoint/network performance, no complaints, still have a job, etc.), concerning the different revenue size of an SMB.

But, it's important to point out, the discrepancies are less extreme here. A case in point is the response to "My endpoints and network are running normally." The data shows that 55% of SMBs reporting revenues of $100 million or more selected this option, while a similar 48% of SMBs reporting revenues of less than $5 million responded the same. This suggests that no matter how large or small your SMB is, you're equally apt to report that you watch your endpoint/network performance to alert you of possible malware.

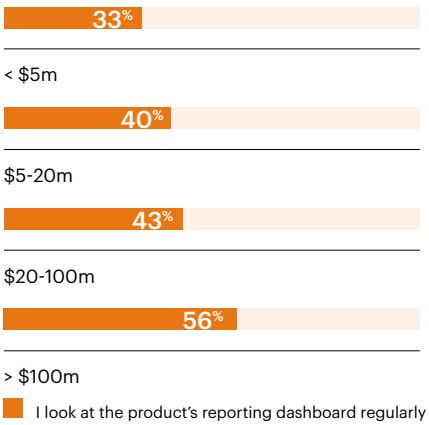
The warning signs are everywhere

To summarize, there's a dangerous lack of testing among SMBs. Our research suggests that a majority of SMBs rely on a surprisingly low-tech method of checking to see if their cybersecurity protection is working. However, the longer SMBs have been in business and the higher their revenues they have, the more likely they are to seek verification through the technical features of their endpoint protection.

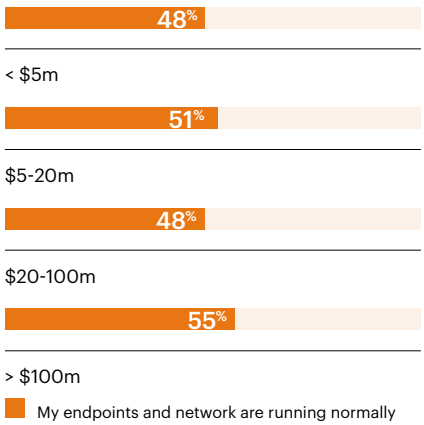
"With so many new threats it is hard for any company to keep up."

Survey respondent

The relationship between revenue and whether a business looks at their endpoint protection product's reporting dashboard regularly



The relationship between revenue and whether an organization knows that its endpoints and network are running normally



A high stakes game

Examining what's at risk in a cyberattack

The IBM Security Cost of a Data Breach Report 2020 puts the global average cost of a data breach at $3.86 million. Looking specifically at SMBs with 500 to 999 employees, the average cost of a data breach was $2.65 million or $3,533 per employee—smaller organizations actually shoulder a larger cost in the event of a data breach. But where are these costs coming from? What's really at stake in the aftermath of a cyberattack?

If we believe the headlines, it would seem the biggest cost after a cyberattack is ransomware pay-outs. The criminal gang behind the REvil (aka Sodinokibi) ransomware claimed $100 million in total ransomware fees extorted from their victims in 2020. Of course, readers should view that number with some skepticism. It's not like cybercriminals are reporting their "revenue" on their taxes.

Ransomware going bust?

To get some perspective, we asked SMBs "If your organization comes under any cyberattack, what do you think would be at stake?" Choosing from the available answers, only 27% of respondents said ransomware pay-out. The top answer among our respondents was a tie between theft or loss of organization's data/files and unauthorized access to system resources with 45% apiece. Rounding at the top three were significant network downtime with 43%, and theft of an organization's customers' personal information/identity theft with 38%.

These answers suggest our respondents have a good instinctive grasp on the current threat landscape. Referring again to the Malwarebytes State of Malware 2021 report, ransomware didn't even crack the top ten business detections for 2020.

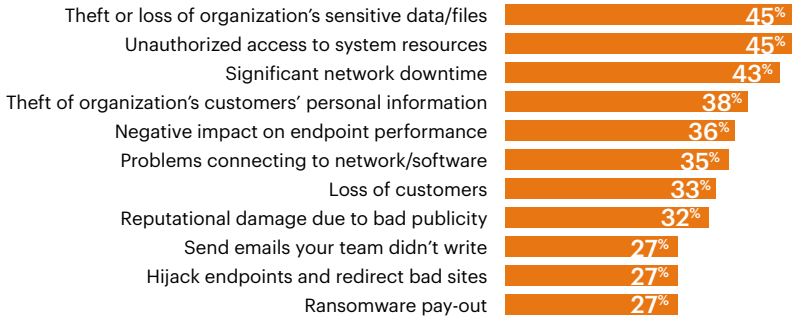
That said, companies with more than $100 million in revenue were significantly more worried about ransomware with 39% citing ransomware pay-out as most at stake when an organization comes under attack.

SMBs who say ransomware pay-out would be most at stake if their organization came under any cyberattack, split by company revenue

Top business detections for 2020:

1. **Trojan**
2. **Adware**
3. **HackTool**
4. **Riskware Tool**
5. **Backdoor**
6. **Spyware**
7. **Worm**

What SMBs think would be at stake if their organization came under attack



"Impacted organizations stand to lose sensitive data and face fines and reputational damage."

Survey respondent

Table stakes

Downplaying the concerns over ransomware, one respondent said "Impacted organizations stand to lose sensitive data and face fines and reputational damage."

It's true—especially for larger organizations with more "skin in the game." These organizations, have massive troves of personally identifiable information (PII) on their servers; e.g., credit card and social security numbers. And they have every reason to be concerned about the bad publicity, legal woes, fines, and loss of business that can result from a data breach.

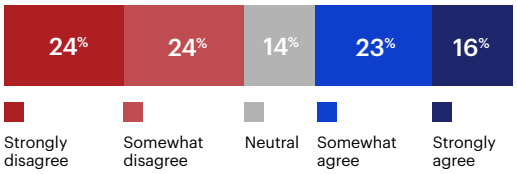
Nearly half, 45%, of companies with more than $100 million in revenue said "reputational damage due to bad publicity" was most at stake in a cyberattack. This is understandable—breaches at larger organizations are more likely to earn unwanted headlines.

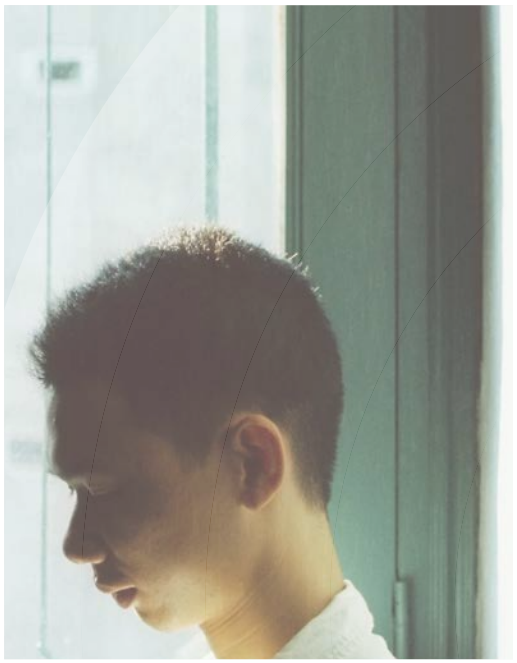
On a related note, there was no clear consensus among our respondents on whether or not hackers preferred to target larger businesses over SMBs.

We asked SMBs, agree or disagree? "Hackers do not target small- and medium-sized organizations and attack only bigger organizations." Some 48% said they disagree, hackers did not discriminate when choosing targets, while 39% agreed that hackers preferred to go after bigger businesses.

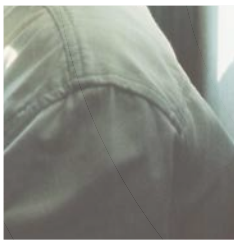
That's well and good, but the numbers don't lie. According to the Verizon Data Breach Investigations Report 2020, security incidences and data breaches are much more common at larger organizations. Clearly there's some cognitive dissonance happening between what SMBs are experiencing in the wild and what they believe to be true.

Hackers do not target small- and medium-sized organizations and attack only bigger organizations





SMBs who say reputational damage due to bad publicity would be most at stake if their organization came under any cyberattack, split by company revenue



Security is easy—until it's not

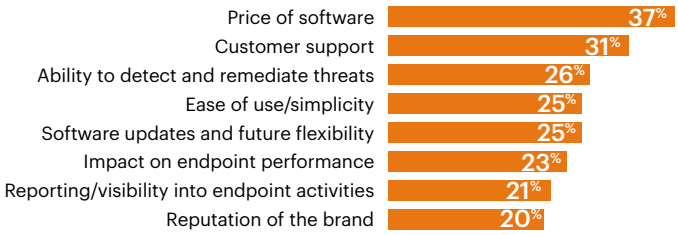
The complexities of modern endpoint protection

Earlier in this report we covered how SMBs believe threats are becoming more complex. By that same token, we wanted to know if SMBs believe endpoint security products are also becoming complex. In the fight against cyberthreats, could it be that our security is becoming unwieldy? As it happens, almost half of SMBs, 46%, agree that endpoint security products are very complex and hard to manage.

On a related note, we asked "If you are dissatisfied with your current endpoint protection product, in which of the following areas does it fall short?"

Given a list of various gripes to choose from, 25% of SMBs cited "ease of use/simplicity"—or the lack thereof. Coming in at number one, 37% of our SMBs, picked price of the software as one area where their endpoint protection falls short. Makes sense. Most respondents appear to appreciate the value of their endpoint protection product.

For those that are disappointed with their current endpoint protection product, these are the areas it falls short:



Mo' endpoints, mo' problems

Ease of use/simplicity and its importance varies depending on the size of the organization. Looking at the cross-section, 20% of organizations from 50 to 99 employees cited "ease of use/simplicity" but that number jumped to 27% for organizations 500 to 999 employees. It seems complexity goes up as organizations grow larger—more endpoints, more problems.

Ease of use/simplicity and its importance varies depending on the size of the organization

And problems that complexity may cause are many. It can start the very first day with difficulties merely deploying new protection products to the endpoints. This can lead to gaps in coverage as some endpoints are missed altogether.

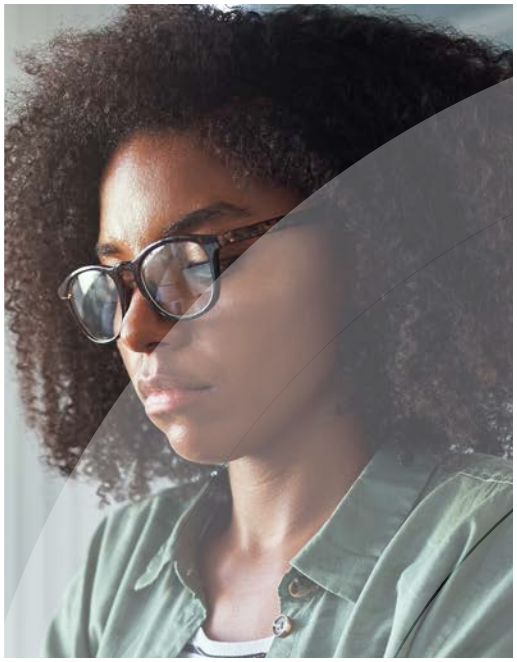
Even more concerning are the issues that arise with a poorly designed endpoint protection management console and reporting. IT security teams scrambling to respond to a threat moving laterally through a network like a California wildfire need real-time visibility at their fingertips. Drilling down through confusing sub-menus to isolate an infected endpoint is a losing game, as many of our respondents realize.

46%

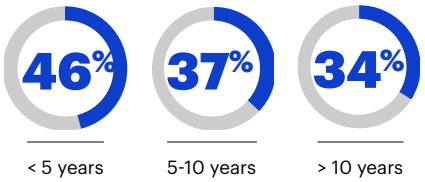
Find endpoint security products very complex/ hard to manage

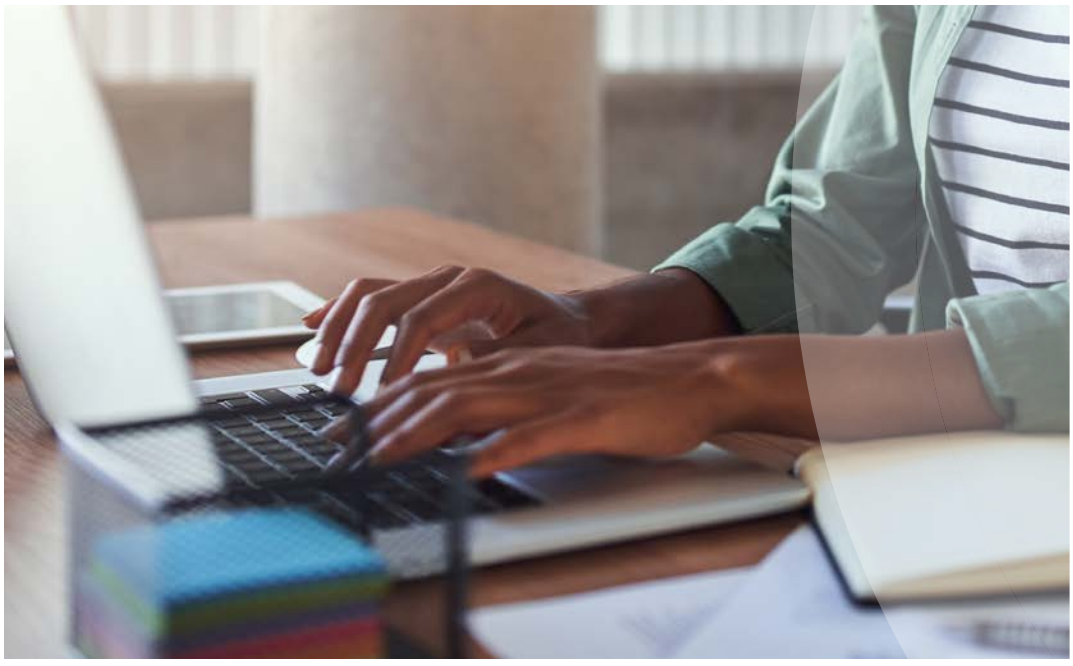
Keeping the faith

When we asked our SMBs "When is the last time you switched from one endpoint protection product vendor to another?", a full 60% said they had been with their provider fewer than three years. For organizations fewer than five years old, 46% said they switched vendors within the past one to three years. That's a lot of software turnover for our younger businesses—at least two vendors since inception. Is it because the technology they're settling on is hard to use? We can't say for sure, but it's a good possibility considering how many of our SMBs, in general, are frustrated with complex and confounding security technology.



Organizations that switched endpoint protection product vendor in the past 1-3 years, split by company age





60%

Have been with their endpoint protection vendor for fewer than 3 years

The verdict is in

Why SMBs buy one cybersecurity provider over another

Although price is arguably the unanimous decision you might expect to be reached by a pool of SMB peers, let's start by pointing to an unexpected finding from our SMB Cybersecurity Trust & Confidence Report 2021.

Cost is not the top answer as to why SMBs choose one cybersecurity solution over another. In fact, "price of the software" ranks well down the list at #7.

37%

Of SMBs say price is the main cause of dissatisfaction with their endpoint protection product

But it's not an open-and-shut case if you look at all of the evidence, as there are some disconnects here and there regarding price. For example, what makes this judgment somewhat perplexing is that when SMBs were asked to comment in their own words about their major challenges, the most common response in our survey centered around "budgets."

Yet price fell to the middle of the pack? Similarly, a majority of SMBs report that when they're "dissatisfied" with their endpoint protection product, the reason is price (37%).

So there seems to be some soul-searching going on among SMBs regarding the price of their endpoint protection.

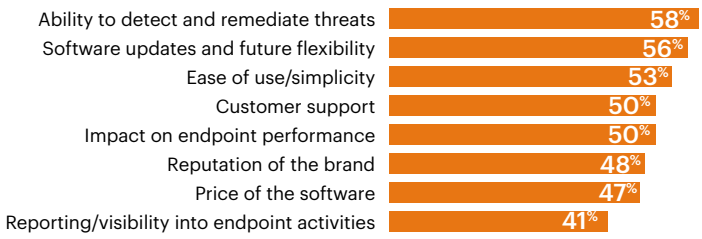
Polling the jury on their buying criteria

As we all know, there are many cybersecurity providers out there. Some are large, well-established, and offer multiple solutions. Others are smaller and more specialized. Prices are across the board, as are approaches to protection and service and support packages.

So, to better understand what goes into the decision-making process, we simply asked SMBs. Surprisingly, the responses were spread out across multiple factors. There was no single clear-cut winner in the bunch. Be sure to keep in mind when looking at the numbers, that respondents were able to select more than one factor.

> ***"Sadly, the upper leadership team does not understand the stakes and why an investment is necessary to protect assets and tomorrow's productivity."***
>
> Survey respondent

Reasons why SMBs choose one cybersecurity solution over another



"We have some problems in choosing the right company to work with. We have had many disappointments with previous companies."

Survey respondent

Evidence points to effectiveness as the top answer

Although not too terribly surprising when you think about it, "Ability to detect and remediate threats" is the #1 response at 58%. After all, that's what SMBs are paying for. If you asked this same question of folks who buy dish soap, you would expect a 99% response rate for "get my dishes clean."

But if this response was such a no-brainer, then you might also expect that it would jump off the page as a clear winner. Then bingo, we're done! We have our verdict. Case closed. But that's not the case here, as effectiveness won by only the slimmest of margin.

Digging deeper, there is another interesting nugget among the responses to "Ability to detect and remediate threats." This centers around the company's length of time in business. This effectiveness-related answer received 63% of responses from those with 10+ years under their belt, while only 35% of SMBs under five years of age said the same.

This discrepancy may be that older companies are more likely to have suffered a breach than younger companies. Therefore, they're less likely to put such a premium on detection, as they figure infections are just part of the game. For more information on the uptick of success in various attacks, see our 2021 State of Malware report.

A surprising verdict for case #2

Unexpectedly, a close runner-up at 56% was the #2 response for what SMBs look for when evaluating cybersecurity: "Software updates and future flexibility of the solution."

This seems to suggest that people have an eye towards the future, and they want to ensure their product will continue to evolve as the threat landscape changes and their organization scales.

Again, this response skews higher with maturity. This response was selected by 58% of SMBs with 10+ years of experience, but by only 45% of those with less than five years of experience. Evidence points to effectiveness as the top answer

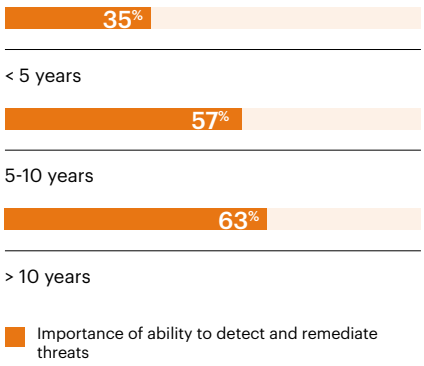
58%

Ability to detect and remediate threats is the top consideration point when evaluating endpoint protection products

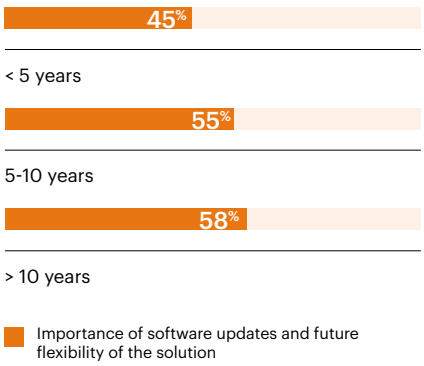
56%

Of SMBs say software updates and future flexibility are an important consideration when evaluating endpoint protection products

The relationship between the importance of the ability of an endpoint protection product to detect and remediate threats and the age of the organization



The relationship between the importance of software updates and future flexibility of an endpoint protection products and the age of the organization



53%

Say ease of use/simplicity is an important consideration when evaluating endpoint protection

Exhibit A: "Ease of use and simplicity"

Third-most-popular among SMBs (at 53%) was "Ease of use/simplicity." Again, not to sound like a broken record, but the leaning towards a no-fuss solution also skewed higher with maturity: 10+ years (55%) versus fewer than five years (39%).

This makes complete sense, as younger SMBs probably dig into the product features less. They're more than likely to turn it on and use default settings. So, complexity is not such a big issue. Conversely, more mature companies may personalize their policies and settings, and they may want a simple dashboard that lets them fine-tune protection. That explains why they put higher relevance on ease-of-use.

There's also a significant difference here in company revenue. The results skew higher among SMBs with revenues above $100 million (77%) versus those below $5 million (49%).

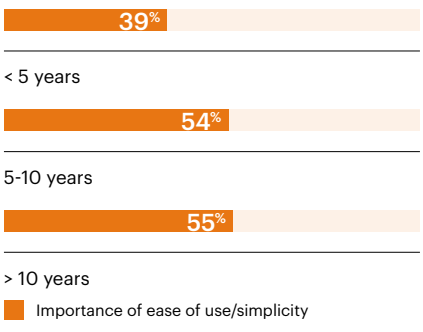
Similarly, you can deduce that SMBs with fewer resources to throw at protection are more likely to put it on auto-pilot. There's also a point to be made here that SMBs in the "tech" sector are significantly more likely to agree + strongly agree that endpoint security products are very complex/hard to manage (52% versus 42%). Another factor that may be influencing this is SMBs increasing complexity with an increasingly remote workforce. For additional insights explore our separate Enduring from Home report.

"Customer support" is on trial as well

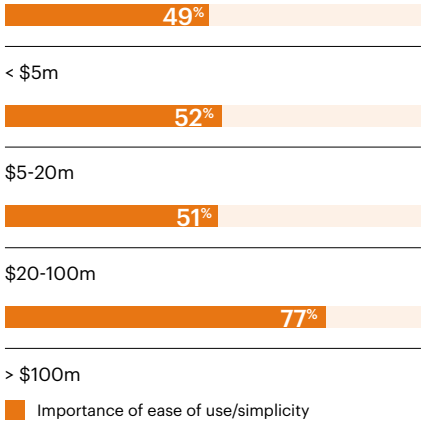
A quick glance shows that "Customer support" is the fourth-most important factor for SMBs when evaluating cybersecurity providers, coming in at 50%.

This is no real surprise that it's in the upper echelon. But as previously discussed, the same patterns continue. This response again skews somewhat higher among mature SMBs and SMBs that have higher revenues—though not quite as much as for the responses discussed above. True, if you're getting your hands less dirty, it's less important to have a support team standing by to answer your questions. But possibly the reason why there's less of a difference is that these less experienced SMBs are using fewer features, so they're less likely to need customer support.

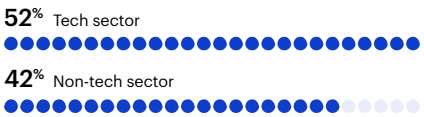
The relationship between the age of the organization and importance of ease of use/simplicity when evaluating an endpoint protection product



The relationship between revenue and importance of ease of use/simplicity when evaluating an endpoint protection product



Agreement that endpoint security products are very complex/hard to manage

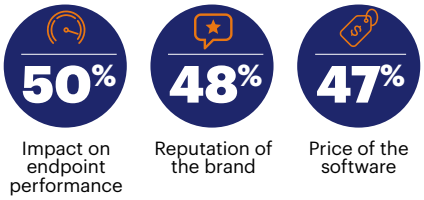


"I imagine that you get what you pay for—we don't buy the most expensive services, so I don't expect them to be top notch."

Survey respondent

The panel is deadlocked on the rest

Rounding out the middle is "Impact on endpoint performance" at 50%, "Reputation of the brand" at 48%, "Price of the software" at 47%.



Similarly, all three of these again skew higher with more mature SMBs. But not so much with SMBs earning higher revenue.

As discussed earlier, it's somewhat surprising that price fell to the bottom of the pack. But then again, when asked specifically about price in greater detail, 79% of SMBs report that they're either completely satisfied or satisfied with the cost of their endpoint protection. Although surprisingly, more mature companies are more satisfied with the cost than younger SMBs, with 77% (10+ years) versus 73% (< 5 years).

79%

Of SMBs are satisfied with the cost of their endpoint security

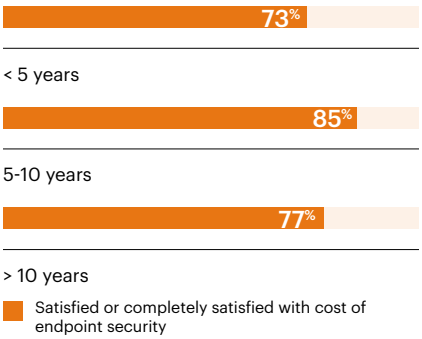
It's also a little surprising that "reputation" received such a high response rate. Perhaps it's the "no one ever got fired for buying IBM" phenomenon?

The factor most likely to be ruled inadmissible

The response that got the least nods was "Reporting/visibility into endpoint activity," at just 41%. Once more, this skews higher by both maturity and revenue. Why? One might deduce that smaller SMBs again aren't digging into the dashboard to see what's happening.

The survey also shows that established SMBs are more subject to regulatory compliance than less established companies. A full 45% of SMBs with 10+ years report that data security is "mandatory/regulated," while only 7% of those with less than five years in business responded the same.

The relationship between endpoint protection cost of ownership and company age



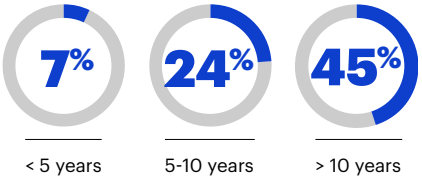
Final verdict? There appears to be a hung jury

In summary, there's surprisingly no clear evidence to support why SMBs purchase a particular cybersecurity product over another. In fact, there are a variety of factors that all come into play—from the effectiveness of detection and remediation to availability of software updates and ease of use.

But surprisingly, when asked directly, price is not among the top responses. However, price seems to be lurking in the jury room. So, it may be more important than SMBs are suggesting.

Perhaps the most convincing result of the survey is that more mature, and more financially successful SMBs, do think differently than smaller and younger companies. Given the preponderance of evidence in this area, one can safely say that we have a split jury here.

Data security is mandatory/regulated within organization



The big picture comes in... and out of focus

Conclusion

2020 was a long slog for SMBs. They had to face a radical adjustment in the way they did business. Many went belly-up. Some thrived. More than a few went remote.

That last bit is important.

Last year SMB IT security teams had to rely on their endpoint protection more than ever. Now their workers were on their home networks, and free to engage in all sorts of risky behavior. Every IT team's waking nightmare. Of course, cybercriminals took advantage (RDP attacks, anyone?).

Given the unusual circumstances, it isn't surprising that the overwhelming number of respondents said they trust their endpoint protection and are confident in its abilities to crush threats.

Perhaps that's because now they have to.

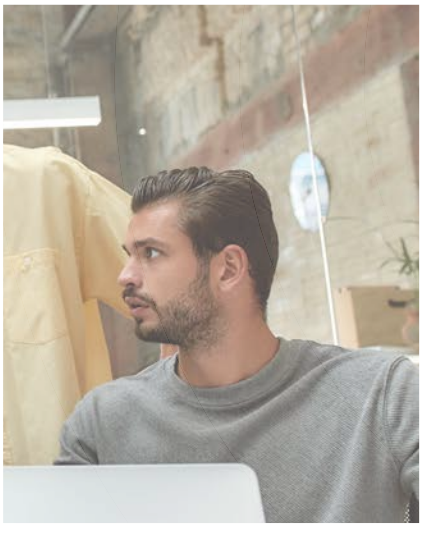
But SMBs also expect to be breached. And they test their endpoint protection regularly because they trust it, but they don't trust it *that* much.

SMBs are conflicted when it comes to the cost of their protection. Price is the number one reason they are dissatisfied with their current endpoint protection product. Conversely, price falls far down the list of the factors they consider when evaluating a new endpoint protection vendor.

And if author F. Scott Fitzgerald was right when he said, "The test of a first-rate intelligence is the ability to hold two opposed ideas in mind at the same time and still retain the ability to function," then the relationship between SMBs and their cybersecurity is sheer genius.

We'll see what they have to say next year.

"The test of a first-rate intelligence is the ability to hold two opposed ideas in mind at the same time and still retain the ability to function." F. Scott Fitzgerald



Contributors

Eric Fairbanks
Director of Content

Darrell Jones
Senior Copywriter

Philip Christian
Content Writer

Troy Kitch
Vice President, Enterprise Solutions

Mark Strassman
Chief Product Officer

Malwarebytes

Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware and exploits that escape detection by traditional antivirus solutions. Malwarebytes completely replaces antivirus with artificial intelligence-powered technology that stops cyberattacks before they can compromise home computers and business endpoints. Learn more at www.malwarebytes.com.