Analyst Insight

Aberdeen Group
A Harte Hanks Company

February 2014

The Risk of "Free" Endpoint Security

Every organization has deployed anti-virus / anti-malware solutions, but how much have you have actually reduced your risk? Aberdeen's analysis not only confirms the high risk of unprotected endpoints, but also demonstrates that endpoint protection really does reduce risk. In addition, it confirms that "free" endpoint protection (e.g., Microsoft) is better than no protection at all, but also shows that in fact it is not really free — enterprise-class endpoint protection (e.g., McAfee) actually reduces risk by 60–70% compared to the "free" solution, even net of the incremental licensing cost.

Baseline: The Risk of Leaving Endpoints Unprotected

Making a business case for investments in information security has never been easy. We make these types of investments to protect against bad things from happening, and the results pretty much come in one of two flavors:

- Bad things didn't happen (at least so far as we know), or
- Bad things happened anyway (in spite of our investments)

That's an oversimplification, but it sums up the mental pretzel security professionals typically get themselves into when faced with making a business case. This Analyst Insight demonstrates how security professionals can do a better job at communicating security-related risks to business decision-makers, and at showing how investments in security controls actually reduces those risks.

For illustrative purposes, the focus is on **endpoint protection** — or what we more commonly call **anti-virus** or **anti-malware** solutions. Aberdeen's research on enterprise security has shown that virtually *all* organizations have deployed this basic foundation of endpoint protection.

Establishing a Proper Understanding of Risk

Security professionals have developed a tendency to be sloppy and imprecise in terms of the language we use to communicate about risk — we tend to talk a lot about *threats*, *vulnerabilities*, *exploits*, and the many security *technologies* that can be used to protect against them. But none of that is really talking about **risk**.

When speaking about security risks, we should be speaking about the **probability** of successful exploits, and the **magnitude** of the corresponding business impact. If we aren't talking in these terms, then we aren't actually talking about risk.

Analyst Insight

Aberdeen's Analyst Insights provide the analyst perspective of the research as drawn from an aggregated view of surveys, interviews, analysis, and industry experience.

Definitions

Some essentially equivalent definitions of security **risk**:

√ The likelihood of a threat agent exploiting a vulnerability, and the corresponding business impact.

√ The probability and magnitude of a loss, disaster, or other undesirable event.

√ Something bad could happen.

But how do we estimate the likelihood of endpoints becoming infected? How do we estimate the magnitude of the resulting business impact? The probabilities and magnitudes that we need to speak about are **not certain**, and security professionals tend to be people who place a high value on technical detail and engineering-caliber precision.

Using the specific example of deploying anti-virus / anti-malware solutions, let's begin by establishing a solid baseline: what is the risk of leaving our endpoints *unprotected*?

Probability of Exploit

It's tempting to go on about the high volume of known malware, and the growth and trends in malware over time — this kind of information is widely available from the leading solution providers — but this would just be falling back into old patterns of talking about threats, vulnerabilities, exploits, and technologies. What we need to do is estimate the likelihood that potential exploits will be successful; that is, *what is the probability of infection*?

One useful source for this estimate is provided by Microsoft, which regularly reports a metric called *computers cleaned per mille* (CCM) — that is, for every 1,000 computers scanned by the Microsoft Malicious Software Removal Tool (MSRT), CCM is the number of computers that needed to be cleaned. For the first six months of 2012, the infection rate per 1,000 computers with *no endpoint protection* was between 11.6 and 13.6 per month.

Magnitude of Business Impact

Having established an estimate for the likelihood of an infected endpoint, what can we say about the magnitude of the corresponding business impact? A reasonable, generic list of possibilities could easily include:

- The cost to respond, remediate, and recover from the infection
  - Cost of lost productivity for users
  - Cost of responders
- Other opportunity costs as a result of the infection
  - Loss of current revenue (e.g., business that was lost while work could not be done)
  - Loss of future revenue (e.g., negative impact on brand, reputation, or trust)
  - Loss of carrying out the organization's mission (e.g., for business impact that might be best expressed in non-financial terms)
- Loss or exposure of sensitive data
  - Fines, legal fees, make-good costs

Analyst Insight

Making decisions in the face of *uncertainty* happens in business every single day. To be effective in communicating properly about security-related risks, security professionals need to get comfortable with some key concepts:

- √ Our estimates are never going to be *certain* — after all, if we knew with certainty what was going to happen and how big an impact it would have, it wouldn't be a *risk*!
- √ Reducing the uncertainty even a little bit is better than doing nothing at all — even if we can estimate only a *subset* of the risks, it still contributes to a better-informed business decision.
- √ If your organization has information or estimates that are more specifically suited to your particular computing environment than those Aberdeen has outlined — use them! The point is that we should use the best information available to calibrate our estimates, and ultimately to reduce the uncertainty.

- Compromise of intellectual property (this is another example of loss of future revenue)

For illustrative purposes, let's focus only on the **cost to respond, remediate, and recover** from infected endpoints, and the opportunity cost from **loss of current revenue** — which means that we will be making a *conservative*, *understated* estimate of the total risk. In other words, the actual risk from infected endpoints will be even higher. Keep in mind, however, that if the objective of the analysis is to demonstrate that an investment in endpoint protection is justified by a reduction in risk compared to unprotected endpoints, then meeting that threshold is enough!

To carry out these computations, we need to make a number of estimates:

- For every 1,000 unprotected endpoints, how many endpoints are likely to become infected? (we have this already: the CCM data)
- How many users does this affect? (e.g., we might assume that there is a one-to-one relationship between endpoints and users)
- How many associated servers are there? (e.g., we might assume that there is a ten-to-one relationship between endpoints and servers)
- How long does it take to respond, remediate, and recover from an infection? (Aberdeen's research findings provide insight into this)
- What is the fully loaded cost per user for this unproductive time? (note that most users will be at lower pay grades, but infections could also happen to the most highly-paid executives)
- How much of this time is actually unproductive? (e.g., users may still be able to do other productive work, so not all of their time is lost)
- What is the fully loaded cost per responder for this time?
- For every US$10M in revenue associated with the servers, how much revenue is lost if the servers become infected? (e.g., how much revenue is permanently lost, as opposed to merely delayed or deferred)

Full details on Aberdeen's model assumptions can be provided on request.

Modeling the Risk, Using Probabilities and Magnitudes

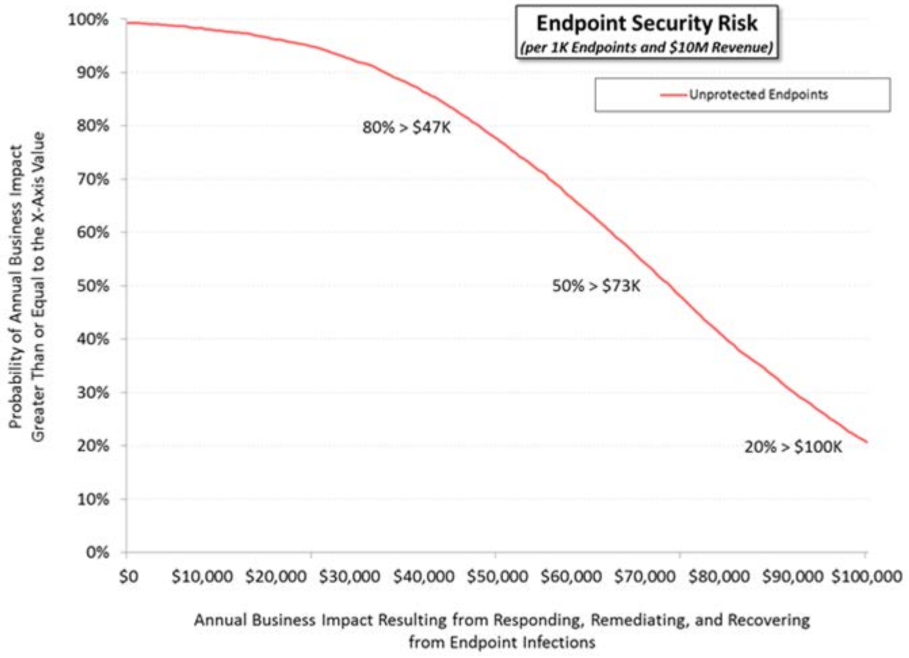
Note that all of these estimates involve *ranges* and *distributions* — i.e., none of them can really be known with precision, so doing computations based on precise, static values would not be doing a very good job at expressing the risk to the business decision-maker.

Instead, we can carry out the computations for many (say, ten thousand) scenarios, each of which uses a random value from our estimated ranges and distributions — a proven, widely-used approach called **Monte Carlo analysis**. The results of these computations are likewise not a single, static number; the output is also a range and distribution, from which we can describe both probabilities and magnitudes: exactly what we are looking for!

The result is presented in Figure 1, which shows the (conservative, understated) risk for 1,000 unprotected endpoints and $10M in revenue from their associated servers. Some of the many statements about risk that can be taken from this chart:

- There is an 80% probability that the annual business impact from unprotected endpoints is greater than $47K
- There is a 50% probability that the annual business impact from unprotected endpoints is greater than $73K
- There is a 20% probability that the annual business impact from unprotected endpoints is greater than $100K

Figure 1: Endpoint Security — The Risk of Unprotected Endpoints



Source: Aberdeen Group, February 2014

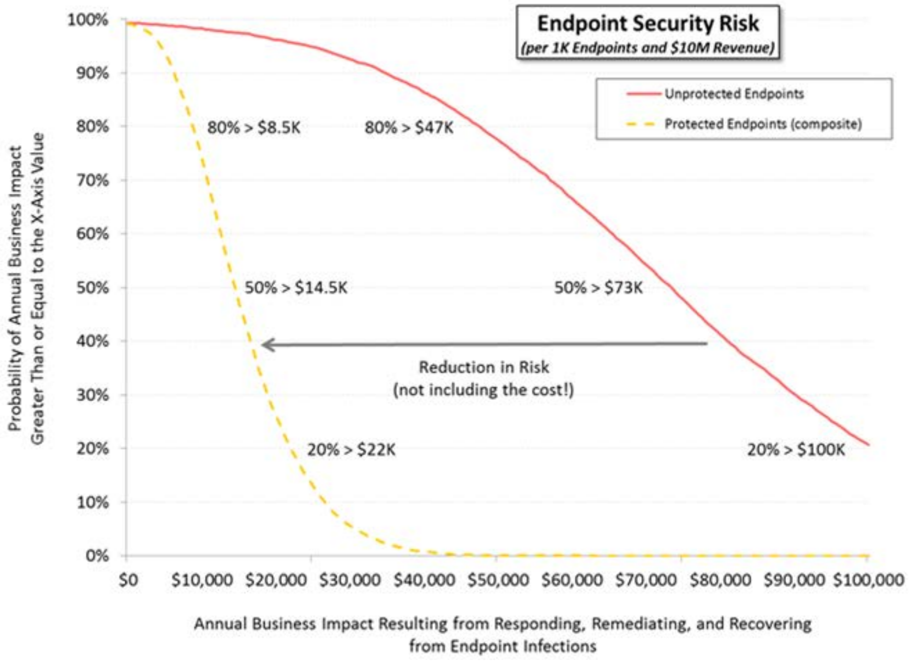
Note that this analysis does *not* tell us what the ultimate business decision will be: one decision-maker might approve an investment in endpoint protection to mitigate the risk, while another might be willing to accept the risk. But that's exactly the point: this type of analysis helps to make better-informed business decisions, within the organization's **appetite for risk**.

Yes, Anti-Virus / Anti-Malware Really Does Reduce Risk

Having established a baseline for the risk of unprotected endpoints, we can now model the risk of *protected* endpoints. In other words, we can compare the "before" with the "after" — where "after" includes the implementation of an anti-virus / anti-malware solution. The Microsoft CCM metrics indicate that for protected systems (i.e., a composite of all systems running any kind of anti-virus software), the infection rate per 1,000 computers was between 1.4 and 3.8 per month. This is a dramatic reduction in the number of infections, which we can use as our estimate for the likelihood that exploits will be successful even after the implementation of an anti-virus / anti-malware solution.

The rest of the model can be carried out exactly as before. By making the computations over ten thousand independent scenarios, each of which uses a random value from our estimated ranges and distributions, we end up as before with a range and distribution for the annual business impact. The results are presented in Figure 2 and in Table 1. This is an improvement of about 80%!

Figure 2: Endpoint Security — Yes, A/V Really Does Reduce Risk



Source: Aberdeen Group, February 2014

Table 1: Risk of Unprotected Endpoints vs. Protected Endpoints, Based on Monte Carlo Analysis

For every 1,000 endpoints and $10M in revenue from associated servers, there is a(n) …	Unprotected Endpoints	Protected Endpoints
… 80% probability of the annual business impact being greater than:	$47K	$8.5K
… 50% probability of the annual business impact being greater than:	$73K	$14.5K
… 20% probability of the annual business impact being greater than:	$100K	$22K

Source: Aberdeen Group, February 2014

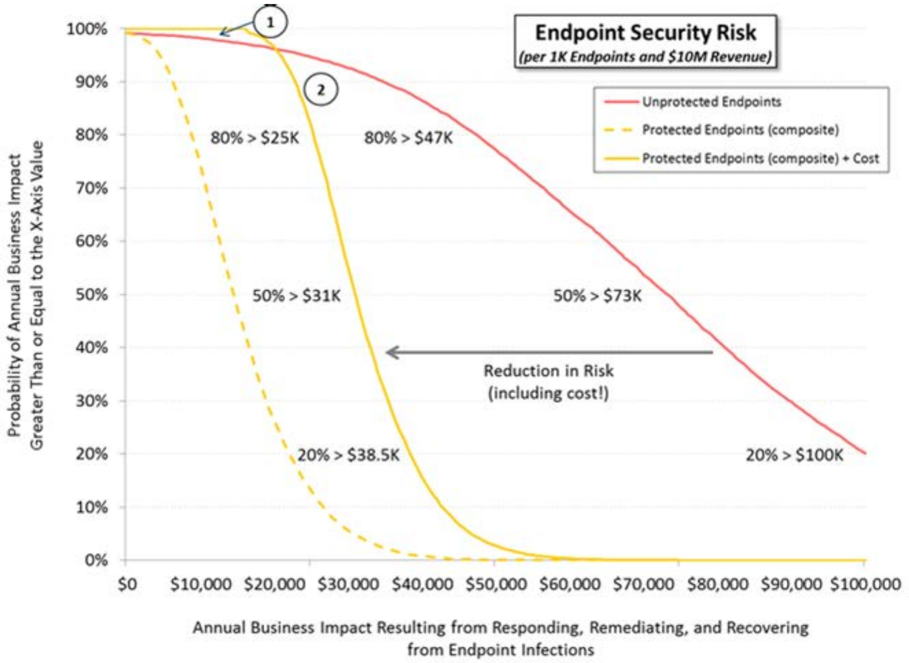
But something important is missing from this analysis: the *cost of implementing and supporting the endpoint protection solution* also needs to be

Analyst Insight

It should go without saying that the purpose of implementing a security solution is to *reduce* the likelihood of a successful exploit, not to *eliminate* it — we can all acknowledge that no security control can be expected to be 100% effective.

accounted for. Because this iteration of our model is based on CCM data for a *composite* of anti-virus software, let’s illustrate the concept by assuming that the annual cost is a fixed $15 per endpoint. After incorporating these costs into the model, we end up with the results in Figure 3.

Figure 3: Endpoint Security — A/V Reduces Risk, Even Net of Cost



Source: Aberdeen Group, February 2014

This update to the model reflects the reality that endpoint protection needs to be implemented on *all* endpoints — i.e., we can’t have foreknowledge about which specific systems will be infected, so we generally have to protect them all. This means that there is a 100% chance that we will spend $16,500: the $15 per year cost of endpoint protection for 1,000 endpoints and 100 associated servers. In addition, we can see that there is about a 3% chance (see area “1” in Figure 3) that the annual business impact would be *lower* with no endpoint protection at all. But the likelihood that we have reduced the organization’s risk, net of the investment in endpoint protection, is about 97% (see area “2”). So we really can say — with near-certain confidence — that *yes, anti-virus really does reduce our risk*, by about 50%–60% for a composite of all anti-virus solutions.

Imagine how refreshing it would be for the business decision-makers we are advising, if we consistently framed security discussions in the context of the organization’s appetite for risk!

“Free” A/V, Part I — Yes, It’s Better Than Nothing!

At this point we can get more specific, and look at the reduction in risk from implementing a particular endpoint protection solution: Microsoft

Security Essentials. The questions on the table: is "free" A/V really better than nothing? And is it really free?

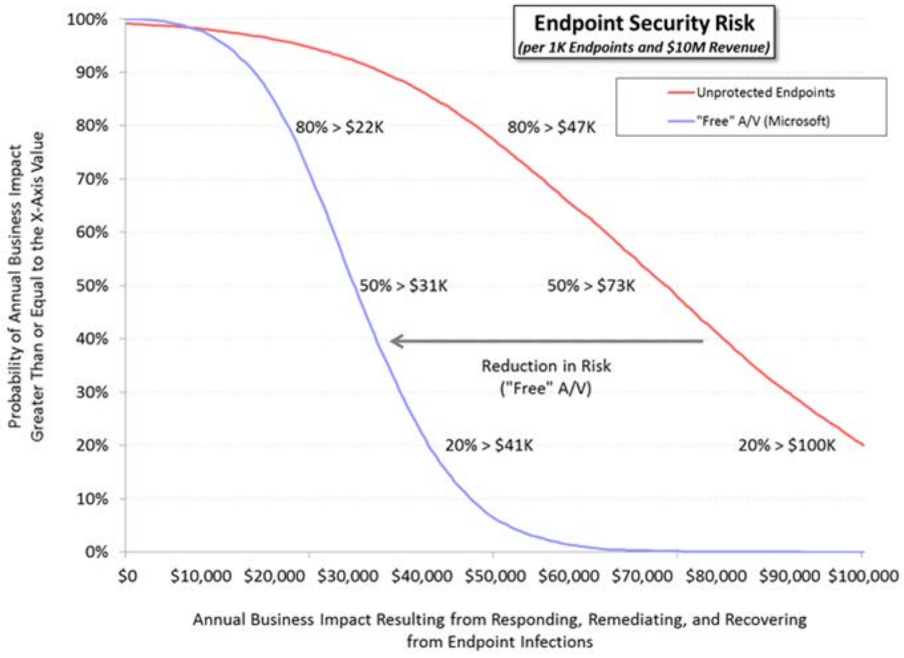
We can continue to use Microsoft's CCM metrics as our estimates for the infection rates for unprotected systems, but we now need to estimate the *exploit block rate* for a specific anti-virus solution. One public source of this kind of data comes from NSS Labs, who conducted testing of multiple endpoint protection solutions against a mix of 41 exploits, more than 200 attack scenarios, and multiple versions of four different web browsers.

For unprotected systems, the block rate is obviously 0%. For systems running Microsoft Security Essentials, NSS Labs found a block rate of 65%. Because a single, static value for the block rate does not reflect reality, Aberdeen incorporated a small range centered around 65% into the Monte Carlo model.

In addition, although there is no incremental license cost for the Microsoft anti-virus solution, there is still an incremental administrative cost — so based on the analyst's estimate, an amount that equates to about two hours per week of a full-time equivalent administrator's time was also incorporated into the model, and calculated over 10,000 iterations.

The results are presented in Figure 4 and in Table 2. This is an improvement of between 50%–60% compared to unprotected endpoints. So *yes, "free" A/V is clearly better than nothing*!

Figure 4: Endpoint Security — Yes, Free A/V Better than Nothing



Source: Aberdeen Group, February 2014

Analyst Insight

√ If your organization has information or estimates that are more specifically suited to your particular computing environment than those Aberdeen has outlined — use them! The point is that we should use the best information available to calibrate our estimates, and ultimately to reduce the uncertainty.

Table 2: Risk of Unprotected Endpoints vs. Free A/V, Based on Monte Carlo Analysis

For every 1,000 endpoints and $10M in revenue from associated servers, there is a(n) …	Unprotected Endpoints	"Free" A/V (Microsoft)
… 80% probability of the annual business impact being greater than:	$47K	$22K
… 50% probability of the annual business impact being greater than:	$73K	$31K
… 20% probability of the annual business impact being greater than:	$100K	$41K

Source: Aberdeen Group, February 2014

"Free" A/V, Part II — Why Free Actually Costs More!

Our insights so far beg the next obvious question: is a "free" endpoint protection solution the best business decision? What is the incremental benefit, if any, of investing in an enterprise-class endpoint protection solution? By now, the approach should seem straightforward: update our Monte Carlo model using the block rate for a specific, commercial endpoint protection solution, along with estimates for its total annual cost — and evaluate the resulting reduction in risk, net of the incremental investment.

For systems running endpoint protection from McAfee, testing by NSS Labs found a block rate of 97%; Aberdeen incorporated a small range centered around this value into the Monte Carlo model. In addition, the annual total cost of the McAfee solution was estimated to be between $5.00 and $12.00 per endpoint per year, based on publicly available pricing data.

The results are presented in Figure 5 and in Table 3. The model shows that the commercial McAfee endpoint protection solution actually reduces the risk by 60%–70% more than the "free" Microsoft solution, even net of the incremental cost of licensing. In other words, *"free" anti-virus actually costs more than an enterprise-class endpoint protection solution.*

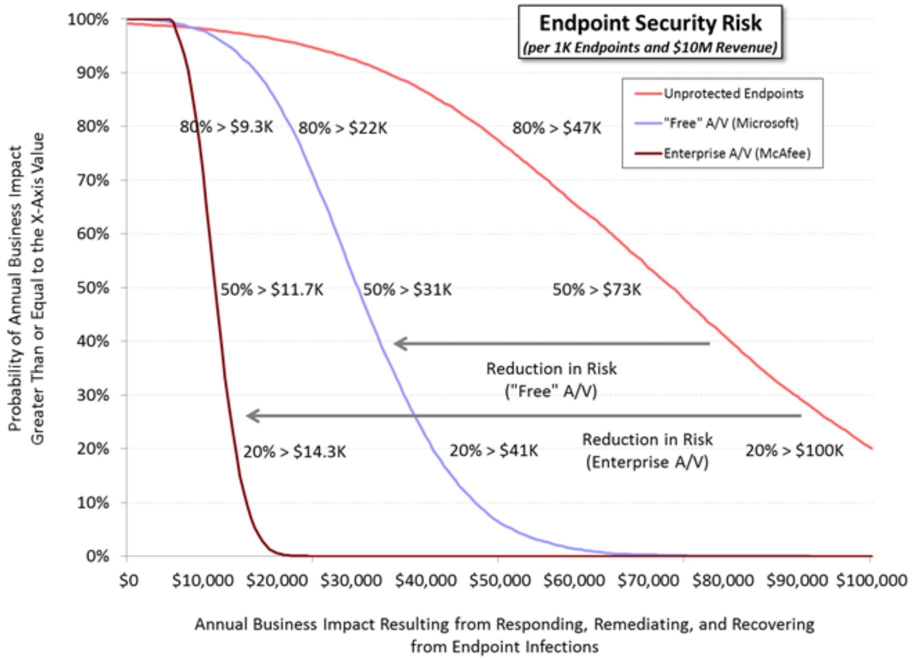
Table 3: Risk of Free A/V (Microsoft) vs. Enterprise A/V (McAfee), Based on Monte Carlo Analysis

For every 1,000 endpoints and $10M in revenue from associated servers, there is a(n) …	"Free" A/V (Microsoft)	Enterprise A/V (McAfee)
… 80% probability of the annual business impact being greater than:	$22K	$9.3K
… 50% probability of the annual business impact being greater than:	$31K	$11.7K
… 20% probability of the annual business impact being greater than:	$41K	$14.3K

Source: Aberdeen Group, February 2014

If we wanted to, we could attempt to model additional differences between enterprise-class and "free" solutions — including the impact of performance (e.g., scan times), the overhead of installing and managing multiple products from multiple solution providers, and other factors known to impact the end-user experience. These differences also favor the enterprise-class solution, but they have a much smaller effect on the aggregate business impact than the information we already have — so in terms of the question at hand, there is relatively low incremental information value to be gained by carrying out this additional work.

Figure 5: Endpoint Security — Free A/V Actually Costs More



Source: Aberdeen Group, February 2014

The Bigger Picture: Anti-Virus Alone is Not Enough

In *Endpoint Security: Anti-Virus Alone is Not Enough* (April 2012), Aberdeen looked at the bigger picture of endpoint security — and found that while 100% of respondents have deployed an anti-virus / anti-malware solution, most organizations have also deployed one or more complementary endpoint security controls as part of a *defense-in-depth* approach to protecting their users, systems, applications, and data. These include:

- Endpoint protection (anti-virus / anti-malware)
- Patch management
- Configuration and change management
- Intrusion prevention
- Email and web security
- Endpoint data encryption
- Browser-based security (e.g., reputation)
- Application whitelisting
- User behavior (e.g., anti-phishing training)

Analyst Insight

The traditional, *signature-based* approaches to protecting against vulnerabilities typified by anti-virus / anti-malware solutions — i.e., determining what is "good" by detecting and subtracting what is known to be "bad" — is increasingly being augmented by complementary endpoint security technologies, as part of a *defense-in-depth* approach.

In an analysis and comparison of companies whose endpoint security is based on anti-virus software alone (the "anti-virus group") with companies whose endpoint security includes anti-virus and a mix of other complementary solutions, the total annual business impact for the anti-virus-only group was actually found to be 1.5-times more. Part of this is due to the anti-virus-only group being *less operationally efficient* — i.e., the top performers generally tend to manage their IT Security initiatives at higher scale and lower cost. Solution providers that integrate multiple endpoint security solutions under a comprehensive, integrated management platform also contribute to such operational efficiencies.

But the biggest difference was a result of the anti-virus-only group being *less effective* — i.e., the anti-virus-only group bore the burden of *higher costs not avoided* in comparison to companies who deployed greater defense-in-depth to reduce their risk.

Incorporating any of these additional controls into our Monte Carlo model would follow the same basic approach that we have been following so far — that is, starting with informed estimates for:

- The likelihood of successful exploits, post-implementation of any additional controls
- Any changes in the business impact as a result of implementation, e.g., a reduction in the time to respond, remediate, and recover from an incident based on improved operational capabilities
- The incremental cost of implementing and supporting the additional controls

These extensions to the model are beyond the scope of this specific Analyst Insight, but Aberdeen plans to continue developing these types of risk-based models in its research publications going forward.

Solutions Landscape (illustrative)

Solution providers for endpoint protection range from smaller anti-virus / anti-malware specialists to larger providers of comprehensive, integrated endpoint security platforms. An illustrative list includes:

- *McAfee (Intel)*
- *Symantec*
- *IBM Tivoli*
- *Check Point*
- *Lumension*
- *Sophos*
- *Trend Micro*
- *Webroot*
- *Microsoft (System Center)*
- *F-Secure*
- *Kaspersky Labs*
- *Total Defense (formerly CA)*
- *ESET*
- *Panda*
- *AVG*
- *Avast*
- *ThreatTrack Security (formerly GFI Software / Sunbelt Software)*

Summary and Key Takeaways

This Analyst Insight demonstrates how security professionals can do a better job at communicating security-related risks to business decision-makers, and at showing how investments in security controls actually reduces those risks.

Using the specific example of deploying **anti-virus / anti-malware solutions**, Aberdeen developed a simple Monte Carlo model to show the risk of infections for every 1,000 endpoints and every $10M in revenue from their associated servers. Key takeaways from this analysis include:

- There is a high risk to unprotected endpoints
  - There is an 80% likelihood of the annual business impact being greater than $47 / endpoint / year
  - There is a 20% likelihood of the total business impact being greater than $100 / endpoint / year
- In general, endpoint protection significantly reduces endpoint security risk
  - The likelihood of reducing the organization's risk, net of the investment in endpoint protection, is virtually 100%
  - Said another way, anti-virus really does reduce risk, by about 50%–60% for a composite of all anti-virus solutions
- Yes, "free" endpoint protection (e.g., Microsoft) is better than no protection at all
- But "free" endpoint protection (e.g., Microsoft) is not really free
  - There is an 80% likelihood of the annual business impact being greater than $22 / endpoint / year
  - There is a 20% likelihood of the annual business impact being greater than $41 / endpoint / year
- Enterprise-class endpoint protection (e.g., McAfee) is actually lower cost than "free" endpoint protection (e.g., Microsoft)
  - The McAfee solution reduced risk by 60–70% compared to the "free" Microsoft solution, even net of the incremental investment in licensing costs
- In the bigger picture of endpoint security, Aberdeen's research has found that 100% of respondents have deployed an anti-virus / anti-malware solution, but a majority of organizations have also deployed one or more complementary endpoint security controls as part of a comprehensive, *defense-in-depth* approach to protecting their users, systems, applications, and data.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research

Crackpot Rigor: When Making a Business Case for Security Goes Too Far; December 2013

Endpoint Security and the DSD Top 4: One Size Does Not Fit All; March 2013

Endpoint Security: Anti-Virus Alone is Not Enough; April 2012

Network Security: Firewalls Alone are Not Enough; March 2012

Endpoint Security and Endpoint Management in the Era of Enterprise Mobility and BYOD: Still Better Together; December 2011

To Patch, or Not to Patch? (Not If, But How); October 2011

Is Your Vulnerability Management Program Leaving You at Risk? (Most Likely, Yes); June 2011

Why Don't More Enterprises Adopt Endpoint Encryption?; March 2011

Managing Vulnerabilities and Threats (No, Anti-Virus is Not Enough); Dec. 2010

The State of IT (In)Security, and How to Avoid Costs by Investing More; November 2010

McAfee Users Have Lower TCO for Endpoint Security, Endpoint Management; October 2009

Endpoint Security, Endpoint Management: The Cost-Cutter's Case for Convergence; March 2009

Making Time for Better IT Security - Sooner, Faster, Later; September 2008

Vulnerability Management: Assess, Prioritize, Remediate, Repeat; July 2008

Author: Derek E. Brink, CISSP, Vice President and Research Fellow, IT Security and IT GRC (Derek.Brink@aberdeen.com)

For more than two decades, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.5 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte Hanks Company, Aberdeen's research provides insight and analysis to the Harte Hanks community of local, regional, national and international marketing executives. Combined, we help our customers leverage the power of insight to deliver innovative multichannel marketing programs that drive business-changing results. For additional information, visit Aberdeen http://www.aberdeen.com or call (617) 854-5200, or to learn more about Harte Hanks, call (800) 456-9748 or go to http://www.hartehanks.com.