Endpoint Security: Anti-Virus Alone is Not Enough

For many organizations, endpoint security consists of anti-virus software and network security consists of a firewall. What can Aberdeen’s research tell us about these minimalist approaches, in comparison to organizations that have deployed additional security defense-in-depth? This Analyst Insight confirms – and quantifies – the prevailing wisdom that enterprise security based on anti-virus software alone is not enough.

Business Context: Greater Complexity, Greater Risk

The IT computing infrastructure for many organizations has gotten considerably more powerful – and considerably more complex – over just the past couple of years. Back-end systems refers not only to the hosts, storage and applications within the enterprise datacenter – but also to virtualized resources in the datacenter or in the cloud. Endpoints refers not only to traditional enterprise-provisioned devices – but also to highly mobile devices that are increasingly owned and managed directly by enterprise end-users. Networks refers not only to electronic interconnections and protocols between systems – but also to social connections and collaboration between people, both within and across organizational boundaries. Aberdeen has recently begun referring to the transformations being made possible by these converging trends using the term SoMoClo™.

Figure 1: Public Vulnerability Disclosures, 1996-2011


This document is the result of primary research performed by Aberdeen Group. Aberdeen Group’s methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc.
As organizations seek the compelling benefits – and struggle at times with the additional complexities – of these transformations in their IT computing infrastructure, they must also deal with the corresponding vulnerabilities, threats and risks. Industry sources such as IBM X-Force report that although the number of public vulnerability disclosures varies from year to year (Figure 1), increasingly savvy attackers are adapting their techniques, and emerging technologies such as social, mobile and cloud are creating new avenues for attack. Perhaps more disturbing is that the industry in general is consistently unable to keep pace with the number of vulnerabilities and threats: 58% of vulnerabilities disclosed in 2011 had vendor patches available on the same day, but 38% still have no patch available. The fact that this is a slight improvement (over the past 5 years, 44% or higher of publicly disclosed vulnerabilities have had no patch available) does not change the perception that enterprises are running faster and falling further behind.

**Aberdeen’s Research Findings: Endpoint Security**

What endpoint security solutions are companies deploying to cope with the ever-evolving security threat landscape? Aberdeen routinely asks respondents about their current use, planned use and current evaluations of a wide range of IT Security technologies; the results for selected endpoint security technologies from a 2011 study of more than 160 organizations are shown in Figure 2. As indicated by the light blue bars, all (100%) respondents have deployed anti-virus / anti-malware; more than 4 out of 5 have also deployed technologies such as email (86%) and web (82%) monitoring and filtering; 75% have deployed patch management; 48% have deployed host-based intrusion detection and prevention (HIPS); and so on.

**Figure 2: All Organizations Have Deployed Anti-Virus Software**

![Graph showing deployment of anti-virus and other technologies](image)

Source: Aberdeen Group, April 2012

Meanwhile, the blue and red lines which are superimposed on the light blue bars in Figure 2 indicate the percentage of the leaders and laggards from.

**Analyst Insight**

One growing problem is that the traditional, signature-based approach to protecting against the vulnerabilities shown in Figure 1 is under significant stress. Most new malware represents slight variations of previously identified malware, a malevolent engineering process which is repeated continuously by attackers. The traditional approach of determining what is “good” by detecting and subtracting what is known to be “bad” is not being discarded, but increasingly it must be augmented by complementary endpoint security technologies and a defense-in-depth approach (Figure 2).

**Defining Maturity Classes**

To distinguish Leading or Best-in-Class companies (top 20%) from Industry Average (middle 50%) and Laggard organizations (bottom 30%) among IT Security-related survey respondents, Aberdeen generally uses the following performance criteria:

- Number of actual security-related incidents
- Number of audit deficiencies (incidents of non-compliance)
- Operational costs

Companies with top performance based on these criteria earn Best-in-Class status.

Full details are available in each respective benchmark report (see Related Research).
the study (see the sidebar on the previous page) that have deployed these selected endpoint security technologies. In general, the leaders have consistently deployed these technologies to a higher degree than have the laggards – and by inspection, one can easily see by the gap between the two lines which technologies have the strongest correlation with top performance (e.g., patch management, host-based intrusion detection and prevention).

Is Anti-Virus Alone Good Enough?

But what about those organizations for which endpoint security consists solely of anti-virus – is this an effective strategy? Can the differences, if any, be quantified? These questions were the motivation for this Analyst Insight.

For this analysis, Aberdeen compared 37 companies whose endpoint security is based on anti-virus software alone, e.g., no patch management, etc. (the "anti-virus group") – with 119 companies whose endpoint security includes anti-virus and a range of other endpoint security solutions (the "defense-in-depth group"). The leading performers (top 20%) from Aberdeen’s benchmark study are also included for reference.

Based on their survey responses, Table 1 summarizes the following averages for these three groups:

- Number of IT Security-related incidents experience in the last year (see the sidebar at right for the types of incidents experienced)
- Total cost of IT Security-related incidents – i.e., costs not avoided – calculated based on an average cost per incident of $120,000
- Total cost of IT Security initiatives (includes estimates for all related costs for people, process and technologies)

### Table 1: IT Security-related Costs Invested, Costs Not Avoided (Not Normalized)

<table>
<thead>
<tr>
<th>Averages per Group (last 12 months)</th>
<th>Anti-Virus Group</th>
<th>Defense-in-Depth Group</th>
<th>Leaders (Top 20%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of IT Security-related incidents experienced</td>
<td>9.0</td>
<td>11.0</td>
<td>9.1</td>
</tr>
<tr>
<td>Total cost of IT Security-related incidents (costs not avoided) (Note 1)</td>
<td>$1,080,000</td>
<td>$1,320,000</td>
<td>$1,090,000</td>
</tr>
<tr>
<td>Total annual cost of IT Security-related initiatives (Note 2)</td>
<td>$520,000</td>
<td>$960,000</td>
<td>$790,000</td>
</tr>
<tr>
<td>Total annual investment in IT Security</td>
<td>$1,600,000</td>
<td>$2,280,000</td>
<td>$1,880,000</td>
</tr>
</tbody>
</table>

Note 1: based on an average cost per security incident for this study of $120,000. Industry estimates for these figures can vary dramatically; Aberdeen strongly encourages readers to substitute values which are deemed reasonable for their own organization.

Note 2: includes estimates for all related costs for people, process and technologies

Source: Aberdeen Group, April 2012

Definitions

In Aberdeen’s study, IT Security-related incidents experienced in the last 12 months included (in order of decreasing frequency):

- Malware
- Non-criminal misuse
- Loss or theft of IT assets
- Misuse of access privileges
- Targeted phishing
- Network / system intrusion
- Data loss or exposure
- Denial of Service attacks
- Social engineering
- Malicious hacking
- Loss or theft of IP
- Employee sabotage
- Cyber-terrorism

Note carefully that the figures in Table 1 are not normalized, so comparisons between groups at this point are apples-to-oranges; a normalized comparison (based on the percentage of annual revenue for each group) is provided in Table 2.
A Simple Framework for Evaluating Business Value for Investments in IT Security, and Acceptance of Risk

For the purposes of evaluating and comparing the business value of enterprise investments in IT Security initiatives, Aberdeen frequently uses the following simple equation:

\[
\frac{\text{Efficiency}}{\text{Effectiveness}} = \frac{\text{(Total Annual Cost of IT Security-related Incidents Avoided)}}{\text{(Total Annual Cost of IT Security Initiatives)}} + \frac{\text{(Total Cost of IT Security-related Incidents Not Avoided)}}{\text{(Total Cost of IT Security-related Incidents Not Avoided)}}
\]

The denominator includes the total annual cost for the organization's IT Security initiatives (in yellow); also in the denominator, however, are the total costs from IT Security-related incidents that were not avoided in the last 12 months (in red), in spite of the investments that have been made. The sum of these two values is a measure of the total annual investment an organization makes in IT Security.

In the numerator, ideally, are the best estimates for the total costs of IT security-related incidents that were avoided in the last 12 months as a result of the organization's investments (in green) – these may be difficult to come by, however, and imprecise at best.

For this reason, the most general way to think about this simple framework is that any investments in technologies and services that lower the total annual cost of the initiative (efficiency) and cause a greater shift from the denominator to the numerator in terms of incidents avoided (effectiveness) will have a strongly positive impact on the overall return on annual investment.

Table 2: Costs Invested, Costs Not Avoided (Normalized as a Percentage of Annual Revenue)

<table>
<thead>
<tr>
<th>Averages per Group (last 12 months), normalized as a percentage of annual revenue</th>
<th>Anti-Virus Group</th>
<th>Defense-in-Depth Group</th>
<th>Leaders (Top 20%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total cost of IT Security incidents (costs not avoided) (Note 1)</td>
<td>0.12%</td>
<td>0.09%</td>
<td>0.07%</td>
</tr>
<tr>
<td>Total annual cost of IT Security-related initiatives (Note 2)</td>
<td>0.06%</td>
<td>0.06%</td>
<td>0.05%</td>
</tr>
<tr>
<td>Total annual investment in IT Security</td>
<td>0.18%</td>
<td>0.15%</td>
<td>0.12%</td>
</tr>
<tr>
<td>1.5-times higher</td>
<td>1.3-times higher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Percentage of IT Security-related risk effectively accepted (Note 3)</td>
<td>68%</td>
<td>58%</td>
<td>58%</td>
</tr>
</tbody>
</table>

Note 1: based on an average cost per security incident for this study of $120,000. Industry estimates for these figures can vary dramatically; Aberdeen strongly encourages readers to substitute values which are deemed reasonable for their own organization.

Note 2: includes estimates for all related costs for people, process and technologies

Note 3: calculated as (Costs Not Avoided) / (Costs of Initiatives + Costs Not Avoided)

Source: Aberdeen Group, April 2012

In Table 2, the figures for each group presented in Table 1 have been normalized as a percentage of annual revenue. Compared to the leading performers, for example, we can now see that the anti-virus-only group...
actually spent 1.5-times more in total. Part of this is due to the anti-virus-only group being less efficient – i.e., the leaders generally tend to manage their IT Security initiatives at higher scale and lower cost. But the biggest difference is due to 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.

A second insight that can be gleaned from this simple analysis is the percentage of IT Security-related risk that is effectively accepted (either deliberately, or by virtue of ignoring – which is the equivalent of accepting). That is, the ratio of (red) / (yellow + red) in our simple equation indicates the percentage of total annual costs that are the result of incidents not avoided, in spite of the investments that have been made – a rough indicator of accepted risk. As shown in Table 2, the anti-virus-only group effectively accepted 68% of its IT Security-related risk, compared to just 58% by the leading performers.

Solutions Landscape (illustrative)
Solution providers for endpoint security range from smaller specialists (e.g., vulnerability- and patch management specialist Secunia) to larger providers of comprehensive, integrated endpoint security platforms. An illustrative list of the leading solution providers in the latter category includes:

- McAfee (Intel)
- Symantec
- IBM Tivoli
- Check Point Software Technologies
- Lumension
- Sophos

Summary and Key Takeaways
Aberdeen’s analysis confirms the prevailing wisdom that endpoint security based on anti-virus software alone is not enough. This is an important point to emphasize, particularly given the technology mega-trends (e.g., social, mobile, cloud) that are dramatically transforming our IT computing infrastructure, and the corresponding changes in the security threat landscape. In addition, the inclusion of anti-virus solutions such as Microsoft’s Forefront Endpoint Protection as part of the underlying endpoint platform may mislead some organizations to make an erroneous conclusion – i.e., that "free A/V" is "good enough for me".

On the contrary, compared to the top 20% of all respondents the anti-virus-only group actually spent 1.5-times more per year in total cost related to IT Security. Not investing in additional endpoint security solutions is shown to be a false economy – in reality, the anti-virus-only
group is ignoring (and therefore effectively accepting) 68% of the risk and the associated costs of security-related incidents.

Endpoint security initiatives for all organizations should adopt a more comprehensive, defense-in-depth approach to protecting their platforms, networks, applications and data. The Solutions Landscape provides an illustrative list of leading solution providers for such comprehensive, vendor-integrated endpoint security solutions.

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

Related Research

<table>
<thead>
<tr>
<th>Network Security: Firewalls Alone are Not Enough; March 2012</th>
<th>The State of IT (In)Security, and How to Avoid Costs by Investing More; November 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Security and Endpoint Management in the Era of Enterprise Mobility and BYOD: Still Better Together; December 2011</td>
<td>McAfee Users Have Lower TCO for Endpoint Security, Endpoint Management; October 2009</td>
</tr>
<tr>
<td>To Patch, or Not to Patch? (Not If, But How); October 2011</td>
<td>Endpoint Security, Endpoint Management: The Cost-Cutter’s Case for Convergence; March 2009</td>
</tr>
<tr>
<td>Is Your Vulnerability Management Program Leaving You at Risk? (Most Likely, Yes); June 2011</td>
<td>Making Time for Better IT Security - Sooner, Faster, Later; September 2008</td>
</tr>
<tr>
<td>Managing Vulnerabilities and Threats (No Anti-Virus is Not Enough); Dec. 2010</td>
<td></td>
</tr>
</tbody>
</table>

Author: Derek E. Brink, Vice President and Research Fellow for IT Security (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.harte-hanks.com.

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc. (2012a)