Economic Value Validation

Trend Micro Deep Security

By Jon Oltsik, Senior Principal Analyst with Adam DeMattia, Market Research Analyst and Kyle Prigmore, Associate Analyst

May 2015
Contents

Executive Summary ........................................................................................................................................... 3
Market Overview .................................................................................................................................................. 3
How Trend Micro Addresses Market Needs ........................................................................................................ 4
Multiple Tools in a Single Management Console for Physical, Virtual, and Cloud Increase Ease of Use ........... 5
Automation and Security Management Features like Virtual Patching Drive Operational Efficiency .............. 6
Optimized Modern Data Center Architecture Increases VM Density and Application Performance ..................... 6
Improved Security and Performance Drive Down-stream User Productivity ......................................................... 7
Best of Breed Protection ..................................................................................................................................... 7
Economic Value Model Overview ....................................................................................................................... 9
Cost Categories .................................................................................................................................................. 10
Benefit Categories ............................................................................................................................................ 10
Economic Value Validation Results ..................................................................................................................... 11
Example Enterprise Scenarios ........................................................................................................................... 11
Summary of Results ............................................................................................................................................ 11
Quantifying Relevant Cost and Benefit Differences ............................................................................................ 12
The Bigger Truth ................................................................................................................................................ 16

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.
Executive Summary

ESG was engaged by Trend Micro to develop a detailed Economic Value Validation (EVV) model to quantify and communicate the value of its Deep Security cloud and data center security offering. The EVV analysis is designed to help organizations determine the relative costs and benefits of leveraging Deep Security for their virtual and cloud-based security needs compared with a “present mode of operation” (PMO) that reflects the suite of point security solutions many organizations leverage today, including antimalware protection, which is agent-based; a discrete integrity monitoring solution; specialized cloud-security services for cloud-based servers; and standalone IPS/IDS and firewall solutions. This EVV analysis builds upon eleven in-depth interviews with Deep Security customers and technical stakeholders, relevant product demos, additional ESG market research related to enterprise security requirements, and ESG’s general familiarity with the myriad of security solutions available in the market today. The goal of the EVV analysis is to provide potential customers with a comprehensive picture of the direct and indirect costs they should consider when evaluating investment in a solution to meet all of their security needs.

As discussed in the following pages, Trend Micro Deep Security’s platform approach and differentiated, optimized architecture offers customers the opportunity to reap significant net economic benefit across a broad selection of use cases—often times both in terms of decreased direct costs like hardware and software required, and indirect benefits like IT staff efficiency and end-user productivity. In fact, ESG’s analysis of typical enterprise use cases for Deep Security—including a VDI-centric use case, a cloud-centric use case, and a non-VDI virtualization-centric use case—results in estimated ROIs of 44%, 181%, and 163% respectively. Moreover, when comparing Trend Micro with the generic PMO, Deep Security is estimated to hold a net economic advantage (i.e., sum of TCO and benefit differentials) in excess of $1M across this spectrum of use cases over a three-year time horizon. For organizations taking a holistic view of their data center and cloud security requirements, Trend Micro Deep Security offers an extremely compelling value proposition. The remainder of this report summarizes the rigorous research ESG conducted to quantify the economic profile of both Deep Security and the PMO, and communicates the results of this analysis.

Market Overview

Trend Micro is a global leader in IT security with over 5,000 employees, 26 years of experience, and over $1 billion in revenue. Best known for its antimalware software, Trend Micro provides a comprehensive portfolio of security products and services for both consumer and business users around the world.

Trend Micro Deep Security is designed to help businesses protect physical, virtual, and cloud-based servers against malware, data breaches, and service disruptions. Aside from protection, Deep Security is designed for ease of operations, offering consolidated administration and automated management across any server, in any form factor, deployed in any location.

Many security technology vendors offer specific product suites for server protection, Trend Micro among them. While server security is essential, most enterprise organizations have moved beyond physical servers alone. For example, ESG research indicates that—on average—approximately 60% of x86 server workloads run as virtual machines. Additionally, many firms are moving internal workloads to infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) data centers in the cloud. According to ESG research, 41% of organizations currently

use IaaS services, while others have used IaaS in the past or plan to do so in the future. Similarly, 35% of organizations currently leverage PaaS services while another 32% have used PaaS services in the last two years or plan to do so in the future (see Figure 1).

Figure 1. Use of IaaS and PaaS

Please indicate your organization’s usage of or plans for each of the following cloud computing services. (Percent of respondents, N=601)

- Currently use
- Do not currently use, but we have done so within the past two years
- Do not currently use but we plan to
- No use or plans at this time but we are interested
- No use, plans, or interest at this time
- Don’t know

<table>
<thead>
<tr>
<th></th>
<th>Currently use</th>
<th>Do not currently use, but we have done so within the past two years</th>
<th>Do not currently use but we plan to</th>
<th>No use or plans at this time but we are interested</th>
<th>No use, plans, or interest at this time</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure-as-a-service (IaaS)</td>
<td>41%</td>
<td>13%</td>
<td>16%</td>
<td>11%</td>
<td>16%</td>
<td>2%</td>
</tr>
<tr>
<td>Platform-as-a-service (PaaS)</td>
<td>35%</td>
<td>12%</td>
<td>20%</td>
<td>14%</td>
<td>18%</td>
<td>1%</td>
</tr>
</tbody>
</table>


A typical enterprise organization likely has a variety of server workloads running on a mix of physical servers, virtual servers, IaaS, and PaaS. Furthermore, workloads often migrate from one form factor to another depending upon considerations like performance needs, cost, geographic location, and data center capacity. While this strategy offers financial and operational advantages for IT, it can also introduce numerous security challenges. Security managers want consistent security controls and reporting across all server workloads, but many are forced to deploy different security products for physical servers, virtual servers, and cloud-based workloads. This creates inconsistencies in capabilities around security controls, policy enforcement, and reporting; constrains regulatory compliance processes; and makes server security operations extremely complex.

How Trend Micro Addresses Market Needs

CISOs realize that this is an untenable situation because it increases risk. Additionally, many security departments are under-staffed and under-skilled due to the global cybersecurity skills shortage. In fact, ESG research indicates that 28% of organizations claim to have a problematic shortage of IT security skills. This means that operational overhead caused by complex server workload security will place further burdens on an already overworked security team. Trend Micro Deep Security is designed to alleviate these problems as it offers:

- **Support for multiple form factors.** Deep Security supports physical, virtual, and cloud-based form factors through a consolidated management platform.
- **Web application security.** Deep Security includes protection for common web application attacks to protect business-critical applications and sensitive data.
- **Layered server defenses.** Deep Security includes antimalware with web reputation for malware protection; file and system integrity monitoring for system protection; and log inspection to identify security events or share this data with security analytics and SIEM platforms.

---

3 Ibid.
Active protection. Deep Security provides host-based IDS/IPS protection to shield unpatched or vulnerable servers, including servers with out-of-date operating systems like Windows 2000 and 2003 Server. It also includes a stateful firewall for network protection.

In addition to these server security controls, Deep Security aggregates all management and reporting activities into a single console. This can help ease the deployment, configuration, and policy management challenges associated with managing multiple security products. For Trend Micro customers with multiple enterprise security products, Deep Security integrates with the company’s central management offering, Trend Micro Control Manager. Trend Micro also supports operations-focused applications like vCenter Operations Manager and Splunk, enabling full visibility into security events from those dashboards.

Trend Micro Deep Security: Qualitative Examples of Customer Benefits

As outlined, Trend Micro has taken a platform approach to delivering security for virtual resources and cloud-based services. The goal is to allow organizations to take advantage of the operational and economic benefits of both private- and public-cloud consumption models while at the same time ensuring there are no security gaps and allowing for demonstrable regulatory compliance. Trend Micro Deep Security’s broad feature set, unified management console, and optimized security architecture all contribute significantly to customers’ ability to deliver secured services to end-users in an operationally efficient manner. However, to accurately and defensibly quantify the benefit customers derive from Deep Security, real-world experiences must be gathered, vetted, and interpreted. To accomplish this goal, ESG interviewed current Trend Micro customers to better understand their usage of, and the benefits associated with, Deep Security in order to inform and validate the assumptions used in ESG’s EVV modeling. Based on these interviews, ESG concludes that the benefits of deploying Deep Security are numerous and diverse. ESG’s findings with respect to customer benefits are presented quantitatively in the EVV scenario analysis discussed in this report; they are also summarized qualitatively—in the customers’ own words—in this section.

Multiple Tools in a Single Management Console for Physical, Virtual, and Cloud Increase Ease of Use

One of the key benefits of Deep Security that customers related to ESG is the platform approach of the solution. The ability to quickly deploy tightly integrated modules, expand capabilities as required by the environment (physical, virtual, and cloud), and then manage those controls from a common console is a differentiator from other approaches in the market. Indeed, to get all the capabilities present in Deep Security, it is likely that an organization would need to engage a multitude of vendors, which could lead to ballooning costs. Additionally, administrators would then be required to manage multiple solutions, which could sap both operational efficiency and proficiency.

Qualitative Customer Insights:

“Having a single interface for multiple tools within Deep Security helps a lot. If I had to do Tripwire for file integrity monitoring, and then had other IDS/IPS products as well, all on top of my antivirus, my team couldn’t be as efficient.”

“The fact that all the modules are integrated with Deep Security makes it significantly easier to use than alternatives.”
“We need to be PCI compliant, so we have to have file integrity monitoring. Other vendors are extremely costly, it could be as much as another six-figure cost item. With Deep Security, this is a simple plug-in, not only is it less expensive, it’s easy to turn on.”

Automation and Security Management Features like Virtual Patching Drive Operational Efficiency

Maintaining information security is critical for organizations today. A single breach can be financially catastrophic: The 2013 Target data breach carried with it a $148M price tag and estimates for the recent Sony Pictures hack are currently in the neighborhood of $100M. Despite these incredibly high stakes, the Trend Micro customers with whom ESG spoke still articulate the pressure to do more with less when it comes to security. This is a mandate Deep Security is helping achieve. First, the optimized nature of the solution means that security administrators are freed from continually configuring, updating, and patching agents. Next, Deep Security’s integration with VMware means that the solution is able to automatically detect VMs as they are spun up and apply context-based policies to those VMs. Additionally, those security policies will automatically follow VMs as they move within the data center and even to the public cloud. And host-based IPS enables organizations to virtually patch vulnerable servers, which, in the face of vulnerabilities like Shellshock and Heartbleed, can save organizations significant amounts of time and effort. Finally, integrated audit capabilities help automate the reporting needed to prove compliance with many common standards including PCI, HIPAA, NIST, and SSAE 16. As articulated in the qualitative customer insights, Trend Micro customers are clearly seeing a benefit in the time and effort needed to maintain and report on the security of their environments.

Qualitative Customer Insights:

“What we’ve found since we moved to Deep Security is that now security professionals can actually work on security issues, rather than just updating clients all the time they can focus on strategic issues.”

“We run a lean IT shop. Now we can devote more time on strategic initiatives versus security. Our previous solution was much more administrator intensive. Even though the main driver for Deep Security was improved VM performance, we think we are getting 20-25% savings in administration time.”

“When it comes to updates, we run 2 processes: quarterly for firmware and monthly for software patching. We have several staff devoted to just upgrading but we would probably need two to four more people if we didn’t have Trend Micro.”

“From an update and patching perspective, we had to update each server individually. This was typically spread over two weeks. Now that it is automated we’ve gone from two weeks to one hour to do updates.”

“We’ve been able to significantly compress the time to generate audit reports—for many it’s a one-click operation. This type of reporting used to take a lot of time.”

“It used to be that we would leverage tools for internal auditing and have an external firm to do reporting on our logs. This used to take in the ballpark of about two weeks, today with Deep Security and the Log Inspection module audit prep is done in a day or so.”

Optimized Modern Data Center Architecture Increases VM Density and Application Performance

In the traditional physical-resource world, having an antimalware agent deployed on each physical server makes a lot of sense to ensure comprehensive protection. Likewise, in the cloud world, it is appropriate to deploy an agent on each server, especially if it can be completely automated. However, in a virtual data center where numerous virtual servers all share the same physical server hardware, installing agents at the VM level has serious implications on operational and server performance. With each VM retaining a separate signature library and running an individual detection engine, network usage; host-level CPU and memory usage; and storage I/O and capacity requirements are all increased. This inefficient consumption of resources both limits VM density and hinders the performance of VMs. In contrast to this traditional approach to securing virtual resources, Trend Micro Deep Security utilizes an optimized architecture for VMware environments and is deployed at the hypervisor layer—
which means that one instance of Deep Security protects all the VMs residing on the host in question. Customers are seeing significant gains in both VM performance and density after deploying Deep Security:

**Qualitative Customer Insights:**

“We’ve seen a 30% improvement in VM density with Trend Micro. We’re actually able to get to what Cisco, VMware, and EMC say we should be able to get to in terms of VM density. Without Trend Micro we would have spent more on hardware.”

“We were not getting the VM density we were expecting based on guidance from VMware. Before we had Deep Security we were looking at ordering new hosts—we were able to avoid this big hardware expense after we got Trend Micro in place. We used to get ten to 11 VMs per host, now we usually have around 20 and could probably do more.”

“We’ve saved lots because we can get much more out of our hardware due to the density enabled by the lack of agents with Trend Micro. Moreover, the optimized nature of Trend allowed us to implement the solution in five to ten days. This could have taken as much as six months with other solutions.”

“As a result of using Deep Security we’ve realized that the help desk was being used a lot due to performance issues, scan time, time to reboot, and things of that nature. Now we see almost no calls tied to the performance of servers due to the fact that agents are no longer using up system resources.”

**Improved Security and Performance Drive Down-stream User Productivity**

While this report has already discussed the impact of Deep Security on customer environments in the areas of hardware procurement, security automation, and administrator efficiency, another important area of value lies with application and VDI end-users. Many of the customers ESG spoke with ascribed significant value to the ability of Trend Micro to increase end-user productivity either by improving the performance of virtual and cloud-based applications or simply by allowing the organization to more aggressively promote the usage of disruptive cloud-based services. A sampling of the benefits reported to ESG by Trend Micro customers follows:

**Qualitative Customer Insights:**

“We’ve seen a measurable drop off in the help desk e-mails from disgruntled users due to app performance. We see on average about four tickets per employee per quarter, before Trend Micro that may have been as high as a dozen.”

“Our end-users need tools like box.com or other public cloud utilities for some things. The question is do we try to lock users down so they have to work around us, or can you work with them in some way to make it okay? Deep Security is helping us do the latter.”

**Best of Breed Protection**

While ESG anticipated Trend Micro customers to report parity in the area of server protection of security solutions, a number of customers actually reported a measurable increase in their level of protection after the deployment of Deep Security. ESG considered this potential improvement in its economic model and quantified the impact both on the information security team—which would need to less frequently react to vulnerabilities and malware infections—and the user community—which would gain increased levels of productive uptime.

**Qualitative Customer Insights:**

“We’ve had a significant reduction in the amount of times we need to make major client changes. We no longer have to frequently uninstall, reboot, and reinstall things on our clients.”

“We’ve seen significant productivity improvements for end-users because our manufacturing systems don’t have downtime anymore due to AV. We have 10,000 employees in the U.S., even small increases in availability can have a huge value in terms of productivity.”
“We have never had to reimger a server due to malware with Deep Security. With our previous solution we had to do this a couple of times because the malware would hit the VM before getting blocked.”

“With Trend Micro Deep Security AV is more about preventing initial infection rather than quarantine, the analogy would be vaccinating versus taking an antibiotic. This is a more proactive and better position to be in.”

“When we implemented Trend Micro Deep Security we thought we were clean because we had AV before. What we saw was that Trend was catching viruses that were already there, we feel like we are getting better security results now that we have more visibility and spend less time analyzing.”

These insights are just a subset of the benefits Trend Micro Deep Security customers reported to ESG. The remainder of this paper discusses the process of quantifying these benefits in ESG’s Economic Value Model and discusses the model outputs for a number hypothetical use cases.
Trend Micro Deep Security: An EVV Analysis

For this project, ESG followed its standard, four-phase EVV methodology, depicted in Figure 2.

Please note that the data and conclusions presented in this report regarding the costs and benefits associated with implementing Trend Micro Deep Security, compared with a generic security PMO, reflect the output of ESG’s EVV analysis based on the specific use case and example scenario assumptions modeled for this report. ESG acknowledges that changes to these assumptions will lead to a different set of results and, as such, advises IT professionals to use this report as one validation point in a comprehensive financial analysis process prior to making a purchase decision. Pricing assumptions for Deep Security were provided to ESG by Trend Micro. Other IT equipment and labor cost assumptions were obtained from publicly available sources such as IT vendor websites and published price lists. ESG acknowledges that list prices, configuration details, or other data used as inputs may vary depending on the source of this information.

Economic Value Model Overview

As previously noted, ESG’s EVV methodology compares two scenarios: The first is an organization that elects to leverage Trend Micro Deep Security to secure a variety of cloud-based servers, virtual servers, and VDI instances. The second scenario is an alternative method of securing the virtual and cloud-based environment through the use of a collection of point solutions. The basic profiles for each security solution scenario are:

- **Trend Micro Deep Security scenario:** In this scenario, the customer is using the Deep Security platform including antimalware for VMs; integrity monitoring to detect and report malicious file changes in real time; IDS/IPS and firewall capabilities to shield against vulnerabilities; and log inspection capabilities to increase visibility into events and ease reporting and audit preparation. The model takes into account all Deep Security
solution components including software, support and maintenance, and hardware and IT infrastructure, plus related IT security labor costs for planning, implementation, ongoing administration, and training.

- **PMO consisting of traditional AV and server security tools**: In this scenario, the customer is using a collection of server security point tools including antimalware protection, which is agent-based; a discrete integrity monitoring solution; specialized cloud security services for cloud-based servers; and standalone IPS/IDS and firewall solutions. As with the Trend Micro scenario, the model takes into account all security component costs including software, support and maintenance, and hardware and IT infrastructure, plus, related IT security labor costs for planning, implementation, ongoing administration, and training.

The tasks, processes, and investments used as the basis of comparison between both scenarios fall into three core categories including IT efficiency savings, user productivity improvements, and capital expense savings.

IT efficiency operations included in this economic value model include:

- Initial security system setup activities as well as periodic upgrade activities.
- Antimalware agent updates and patches.
- Monitoring and controlling access to applications.
- Administration and monitoring of antimalware scanning.
- Application administration tasks including adding new virtual servers to the environment, patching servers, and installing and patching applications on virtual servers.

Factors and operations that contribute to user productivity costs and improvements include:

- Application installation and patch delays.
- Virtual server boot and patch delays.
- Antimalware scan interruptions and antimalware database update interruptions.
- Application user downtime tied to threats and security events.

Finally, capital expense savings are estimated based on the ability to reduce hardware, software, and infrastructure purchases due to lower system resource requirements with Deep Security via increased VM density.

Simply put, ESG’s model estimates the likely cost and potential benefits—according to the factors outlined—of deploying either Trend Micro Deep Security or an alternative collection of point security products into a virtual and cloud-based server environment. Data sources used by ESG to derive the assumptions behind the tasks used in the model include in-depth interviews with current Deep Security customers, product demos of the Deep Security platform, and supplementary ESG market research data.

**Cost Categories**

This ESG EVV considers five cost categories: software, maintenance and support, hardware and infrastructure, professional services, and staff personnel. The sum of these categories equals the total cost of ownership (TCO) of each solution.

**Benefit Categories**

This ESG EVV considers three primary benefit categories: IT efficiency savings, user productivity improvements, and savings from avoided capital expenses. The sum of these categories equals the total benefit of each solution.
Economic Value Validation Results

Example Enterprise Scenarios

To illustrate the relative costs and benefits of leveraging Trend Micro Deep Security and the PMO discussed, ESG developed a set of model inputs representative of a range of potential enterprise and large enterprise use cases for a virtual and cloud server security solution. Key environmental characteristics that drive economic outcomes based on ESG’s analysis include: the size and type of the server footprint; density of VMs and VDI instances on physical hardware; size of the user community supported by virtualized and cloud-based applications; size of the user community supported by the VDI implementation; and the value of IT and end-user labor—using salary as a proxy. For the purposes of the analysis presented in this report, ESG has tuned its model assumptions as shown in Table 1.

Table 1. Key Assumptions in Example Scenarios

<table>
<thead>
<tr>
<th>Input</th>
<th>Cloud-centric enterprise use case</th>
<th>VDI-centric enterprise use case</th>
<th>Large enterprise virtualization-centric use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many servers are initially secured and how many will be added over three years?</td>
<td>100 / 400</td>
<td>25 / 15</td>
<td>2,500 / 2,500</td>
</tr>
<tr>
<td>What is the ratio of physical / virtual / cloud servers?</td>
<td>0% / 0% / 100%</td>
<td>100% / 0% / 0%</td>
<td>0% / 95% / 5%</td>
</tr>
<tr>
<td>How many VDI instances will you be securing now and how many will be added over three years?</td>
<td>0 / 0</td>
<td>2,500 / 1,500</td>
<td>0 / 0</td>
</tr>
<tr>
<td>What is the average number of active application users per server?</td>
<td>50</td>
<td>N/A</td>
<td>50</td>
</tr>
<tr>
<td>What is the average number of virtual servers per physical host server?</td>
<td>N/A</td>
<td>N/A</td>
<td>10</td>
</tr>
<tr>
<td>What is the average number of VDI instances per physical server?</td>
<td>N/A</td>
<td>100</td>
<td>N/A</td>
</tr>
<tr>
<td>What percentage of employee time saved should translate into direct productivity gains?</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>What is the average annual salary for an IT administrator?</td>
<td>$80,000</td>
<td>$80,000</td>
<td>$80,000</td>
</tr>
<tr>
<td>What is the average annual salary for an application end-user?</td>
<td>$65,000</td>
<td>$65,000</td>
<td>$65,000</td>
</tr>
<tr>
<td>What is the time horizon of this analysis?</td>
<td>Three years</td>
<td>Three years</td>
<td>Three years</td>
</tr>
</tbody>
</table>


Summary of Results

With the model parameters tuned to the default assumptions in Table 1, ESG’s EVV analysis concludes that the net benefits of implementing Deep Security greatly outweigh the associated costs. Table 2 shows the annual return on investment (ROI), payback period, annual total cost of ownership (TCO), and annual benefit for Deep Security compared against the modeled PMO. The following sections detail the most compelling findings from this analysis as they relate to both the costs and benefits associated with these solutions.
Table 2. Economic Value Summary, Deep Security versus PMO

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Solution</th>
<th>ROI</th>
<th>Payback Period (years)</th>
<th>Annual TCO</th>
<th>Annual Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud-centric enterprise use case</td>
<td>Trend Micro Deep Security</td>
<td>181%</td>
<td>.56</td>
<td>$140,973</td>
<td>$396,571</td>
</tr>
<tr>
<td>PMO</td>
<td></td>
<td>-76%</td>
<td>&gt;5</td>
<td>$497,552</td>
<td>$117,183</td>
</tr>
<tr>
<td>VDI-centric enterprise use case</td>
<td>Trend Micro Deep Security</td>
<td>44%</td>
<td>1.37</td>
<td>$306,708</td>
<td>$440,826</td>
</tr>
<tr>
<td>PMO</td>
<td></td>
<td>-57%</td>
<td>&gt;5</td>
<td>$370,673</td>
<td>$160,183</td>
</tr>
<tr>
<td>Large enterprise virtualization-centric use case</td>
<td>Trend Micro Deep Security</td>
<td>163%</td>
<td>.40</td>
<td>$1,799,577</td>
<td>$4,729,939</td>
</tr>
<tr>
<td>PMO</td>
<td></td>
<td>-65%</td>
<td>&gt;5</td>
<td>$4,120,689</td>
<td>$1,447,204</td>
</tr>
</tbody>
</table>


Annual Benefit

Annual benefit is the sum of all the benefit categories included in this analysis averaged over the time horizon of three years. As displayed in Table 2, while the annual benefit for Trend Micro Deep Security is significant and exceeds its TCO across a variety of use cases, the traditional point solution approach to enterprise security ESG modeled in the PMO is very costly and difficult to derive maximum benefit from.

Annual TCO

Annual TCO is the sum of all the cost categories included in the analysis averaged over the time horizon of three years. As displayed in Table 2, a transition from the PMO to Trend Micro Deep Security should result in a decrease in the annual TCO of the solution between 17% and 72%. This difference is driven in large part by Deep Security’s all-in-one approach to delivering security capabilities.

ROI

ROI is a financial ratio that compares net benefits against total costs and helps makes sense of the cost and benefit numbers estimated by the model. As displayed in Table 2, the ROI for Deep Security in ESG’s default scenarios ranges from 44% to 181%. Based on ESG’s research, the benefits discussed in the qualitative research results section of this paper should significantly outstrip the costs associated with Deep Security by increasing user productivity (by supplying exceptional application performance and availability) and IT efficiency (by eliminating superfluous hardware expenditures and increasing the ease and automation of maintaining the security solution). The results are modeled ROIs that are positive, and significantly so.

Payback Period

Another important metric is the payback period, which is an estimate of when customers will start to see a positive return from the security solution they select. As displayed in Table 2, the payback period as modeled in our default scenarios ranges from as little as ~5 months to as much as ~16 months, depending on the use case.

Quantifying Relevant Cost and Benefit Differences

Economic models are, by definition, abstractions from reality. In any model, numerous estimates and assumptions must be made. ESG’s EVV methodology leverages rigorous market research and in-depth interviews to estimate material differences between two methods of securing virtual and cloud-based server environments, both in terms of how the solutions would be configured and how the solutions impact organizational efficiencies from an IT and end-user perspective. This section discusses important estimates incorporated into ESG’s EVV model.
**Comparative Cost Analysis**

For the hypothetical customer scenarios described, the annualized, subcategorized TCO for Trend Micro Deep Security is displayed in Table 3.

**Table 3. Annualized, Subcategorized TCO, Deep Security**

<table>
<thead>
<tr>
<th>Cost Category</th>
<th>Cloud-centric enterprise use case</th>
<th>VDI-centric enterprise use case</th>
<th>Large enterprise virtualization-centric use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware and IT Infrastructure</td>
<td>$5,033</td>
<td>$5,033</td>
<td>$26,033</td>
</tr>
<tr>
<td>Software</td>
<td>$91,483</td>
<td>$146,666</td>
<td>$1,091,200</td>
</tr>
<tr>
<td>Maintenance and Support</td>
<td>$34,173</td>
<td>$74,800</td>
<td>$582,560</td>
</tr>
<tr>
<td>Professional Services</td>
<td>$1,333</td>
<td>$1,333</td>
<td>$1,333</td>
</tr>
<tr>
<td>Staff</td>
<td>$8,950</td>
<td>$78,875</td>
<td>$98,450</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$140,973</strong></td>
<td><strong>$306,708</strong></td>
<td><strong>$1,799,577</strong></td>
</tr>
</tbody>
</table>

*Source: Enterprise Strategy Group, 2015.*

Key TCO estimates and assumptions, which drive economic differences between Deep Security and the PMO in ESG’s model, are:

- **Software:** For both security solutions and all of the scenarios modeled, software makes up the lion’s share of the TCO in ESG’s EVV model. In the scenarios ESG modeled for this report, Trend Micro Deep Security is assumed to be licensed based on the number of host CPUs in the environment. Additionally, the pricing is impacted by the capabilities required, which include IPS/IDS, firewall, file integrity monitoring, and log inspection. Based on these assumptions and volume-based discounts, ESG’s model estimates that Deep Security will be licensed for between $4,400 and $3,300 per host.

In contrast to Trend Micro’s bundled pricing, ESG estimates individual component pricing for the PMO. For example, ESG estimates each antimalware server agent in the PMO solution is licensed at a capital cost of $597, while each desktop agent is licensed at a capital cost of $57. Additionally, antimalware management console licensing is included at a unit price of $1,197 and it is assumed one license is required for every 250 servers or every 2,000 desktops. In addition to antimalware software costs, ESG assumes that file integrity monitoring will be licensed at a cost of $499 per server. Finally, for cloud-based servers in the environment, specialized cloud security software is assumed to be procured at a cost of $3,600 per license, which is assumed to cover 25 cloud instances. In ESG’s model, and based on ESG’s research into available security offerings, there is significant software cost advantage to taking a platform approach to security.

- **Hardware:** For both security solutions and all of the scenarios modeled, hardware and IT infrastructure makes up a relatively small percentage of the overall solution TCO. At a high level, ESG’s model estimates parity between the two solutions in terms of management server hardware dedicated to security administration, which is assumed to be in the range of $3,500. Additionally, parity is also assumed for the incremental data center and network overhead as the solution scales. These incremental costs are modeled at the rate of $3,500 for every 250 servers and/or 2,000 desktops in the environment. The only hardware cost item where parity does not exist is the physical IPS/IDS appliance assumed to be deployed in the PMO scenario. This appliance is modeled at a capital cost of $40,000 (if fewer than 500 servers are in the environment), $70,000 (if between 500 and 1,500 servers are in the environment), or $130,000 (if more than 1,500 servers are in the environment).

- **Maintenance and support:** Regardless of the security solution modeled, ESG’s model assumes that cumulative hardware and software capital expenditures carry with them an annual maintenance and support cost. For all use cases modeled in this report, this fact drives a significant cost advantage for Trend Micro Deep Security versus the PMO. More specifically, since combined cumulative software and hardware
costs are lower in the Deep Security scenario, modeled maintenance and support costs also tend to be lower for Deep Security—generally in the range of 25-35% lower than the PMO.

- **Staff labor**: Differences in IT security labor costs for planning, implementation, ongoing administration, and training have been alluded to in this report. First, Deep Security’s ability to manage multiple security capabilities in a common user interface shortens the learning curve for the solution. Next, the ability to interact and transact with a single vendor versus a combination of vendors allows IT and security administrators to dedicate more of their time to actual security-related activities. Finally, major architectural differences between Deep Security (highly optimized) and the PMO (traditional architectures) eliminate many one-time and recurring staff activities like agent installation and patching. Across the use cases ESG modeled, staff labor costs in the Deep Security scenario are estimated to be between 45% and 90% less than those in the PMO scenario.

**Comparative Benefit Analysis**

For the hypothetical customer scenarios described, the annualized, subcategorized benefits estimated to be delivered by Trend Micro Deep Security are displayed in Table 4.

**Table 4. Annualized, Subcategorized Benefit, Deep Security**

<table>
<thead>
<tr>
<th>Benefit Category</th>
<th>Cloud-centric enterprise use case</th>
<th>VDI-centric enterprise use case</th>
<th>Large enterprise virtualization-centric use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Efficiency Savings</td>
<td>$55,153</td>
<td>$320,158</td>
<td>$730,912</td>
</tr>
<tr>
<td>User Productivity Improvements</td>
<td>$267,136</td>
<td>$25,235</td>
<td>$2,828,207</td>
</tr>
<tr>
<td>Capital Expense Savings</td>
<td>$74,280</td>
<td>$95,431</td>
<td>$1,170,819</td>
</tr>
<tr>
<td>Total</td>
<td>$396,571</td>
<td>$440,826</td>
<td>$4,729,938</td>
</tr>
</tbody>
</table>

*Source: Enterprise Strategy Group, 2015.*

Most benefits included in the model are characterized as time saved for either the info security team members or application users within the organization. Additionally, it is critical to note that ESG does not assume every saved hour of employee time is productive. Rather, ESG uses the assumption that only 50% of saved staff time to either constituency will be productive. A more detailed breakdown of benefit estimates includes:

- **Avoided capital expenses**: One of the most straightforward benefits quantified in ESG’s model is the fact that, server for server, an optimized server security solution will be able to secure more VMs than traditional solutions. In the scenarios ESG examined for this report, ESG assumes an average 30% reduction in the number of physical hosts and assumes that the average host carries with it a cost of $5,500. Thus, while this benefit is highly dependent on the size of the physical host environment, in the scenarios ESG examined, Deep Security is modeled to provide between $120,000 and nearly $2,000,000 in benefit over and above the PMO. It should also be noted that a customer can, in many cases, use these saved capital expenditures to accelerate other IT initiatives like expanding the VDI footprint or cloud sourcing applications. This type of reinvestment can garner an organization additional benefits, which are not explicitly quantified in the ESG model, but can be significant.

- **IT efficiency savings**: Core workflows impacting the information security administration constituency, which ESG has quantified as materially different between Trend Micro Deep Security and the PMO, include initial security system setup activities as well as periodic upgrade activities; antimalware agent updates and patches; monitoring application control activities; administration and monitoring of antimalware scanning; and application administration tasks including adding new virtual servers to the environment, patching servers, and installing and patching applications on virtual servers. Based on ESG’s research with Deep Security customers, ESG’s model estimates that solution setup and periodic upgrades require three times less IT staff time and effort compared with the PMO due to the platform approach to security enabled by
Trend Micro. Agent updates and patches are eliminated or automated in the Deep Security scenario, creating significant efficiencies. Based on the best-of-breed nature of Deep Security, ESG estimates that the burden of whitelisting activities and monitoring application control activities could be reduced by 40% or more. Finally, the automated and integrated nature of Deep Security is estimated to improve antimalware scan scheduling, monitoring, and reporting significantly.

- **End-user productivity improvements:** Core workflows impacting the application user community, which ESG has quantified as materially different between Trend Micro Deep Security, include application installation and patch delays, virtual server boot and patch delays, antimalware scan interruptions, antimalware database update interruptions, the frequency of malware events impacting users, and recovery times for those end-users. Due to the fact that Deep Security enables higher levels of application performance, ESG has modeled the impact of application install and patch events to result in half the application unavailability experienced in the PMO scenario. Even though these events are modeled to take only a few minutes—three in the Trend Micro scenario versus seven in the PMO scenario—they can impact the entirety of the application user community multiple times per year, leading to a potentially significant number of hours saved with Deep Security. Similarly, server boot and patch times are also estimated to be significantly reduced in a Deep Security environment compared with the PMO. Another end-user impact quantified by ESG’s model is periods of degraded performance occurring during malware scans and malware database updates. ESG anticipates these regular performance degradation occurrences to last significantly longer in an agent-based VMware environment. Finally, as Deep Security end-users attested, the ability of Trend Micro to deliver a more secure, more comprehensive solution optimized for modern computing environments leads to fewer end-user infections and faster resolutions—saving end-users and security professionals from losing time to recovery and rebuild activities.
The Bigger Truth

CISOs have a unique set of objectives in that they must strive for IT security effectiveness along with operational efficiency, all while ensuring that security operations enable high levels of user productivity. Unfortunately, server security can present a challenge in these areas as many organizations secure server workloads using an assortment of disparate security tools. This strategy can impact security efficacy due to variations in security capabilities across products. Additionally, operational efficiency is bound to grow more complex when security staff is forced to develop expertise and operate multiple server security products. By providing a common solution for physical, virtual, and cloud-based server workloads, Trend Micro Deep Security helps to alleviate these problems and helps CISOs maximize security capabilities without causing server security costs to spiral out of control.

Proof matters when it comes to economic value, and who is better to supply validation for a product’s value than its user. Indeed, Trend Micro users confirm that Deep Security is effective in its capabilities, is easy to use and manage for security staff, keeps end-users up and running, and does so with the minimum hardware footprint possible. It is an impressive value proposition and in ESG’s estimation, Deep Security warrants consideration among organizations looking for a pragmatic, easy, and effective way to secure their next-generation IT environment.