

The Virtualization Practice

White Paper:

A Look at Trend Micro Deep Security 7.5

Edward L. Haletky

Analyst

March 2011

© 2011 The Virtualization Practice. All Rights Reserved.
All other marks are property of their respective owners.

Abstract

Trend Micro Deep Security 7.5 has been available since VMworld 2010. The Anti-malware component requires VMware vShield Endpoint and at least VMware vSphere 4.1. Deep Security 7.5 adds quite a bit of functionality to the virtual environment. Being the first product to make use of the Endpoint Security mechanisms within VMware vSphere. Deep Security 7.5 provides a mechanism to move anti-virus out of each VM and into a single Deep Security Virtual Appliance. In addition, Deep Security 7.5 contains a firewall, IDS/IPS, web application protection, integrity monitoring, and log inspection from previous versions.

Table of Contents

Product Overview	3
Ease of Install (Install-ability)	4
Ease of Use (Usability)	5
Functionality	7
Auditability (Continual Auditing)	9
Integration with other Products	9
Conclusion	9

Product Overview

Trend Micro Deep Security 7.5 accomplishes two major goals of interest to virtualization security. Provide defense in depth with the virtual network as well as off load per VM anti-malware detection to a single virtual appliance: a Deep Security Virtual Appliance (DSVA). Making use of Deep Security provides the ability to add host-based security controls without the resource impact of in-guest anti-malware agents. This most likely will increase VM density.

Part of any overview of Deep Security 7.5 is a review of the network stack that makes up the virtual network (vNetwork). Figure 1 shows two network stacks based on using standard VMware vSwitches (left) and VMware vSwitches with the Cisco Nexus 1000V or N1KV (right).

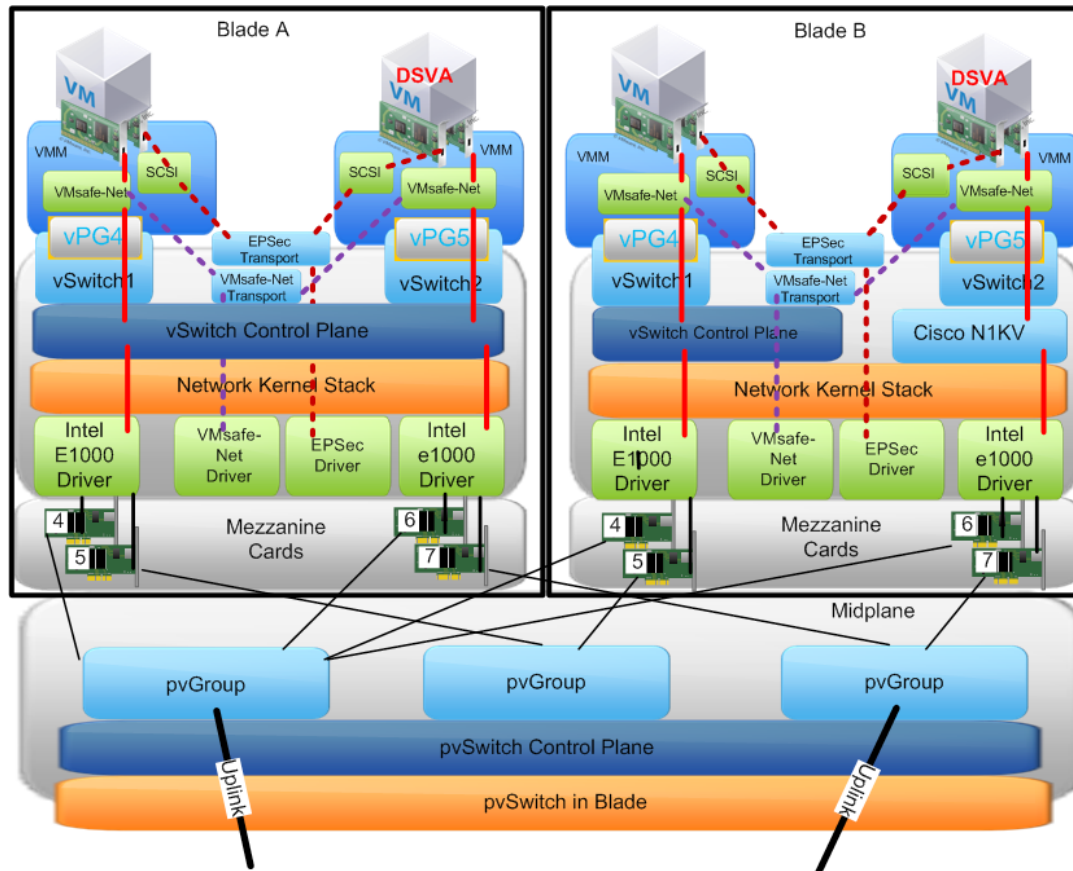


Figure 1: Network Stack

The two stacks are very similar and Trend Micro Deep Security fits into this picture in two locations. However, to understand how the product fits into the stack, it is important to understand how the technology works. Deep Security 7.5 provides several important features. One is a VMsafe-Net per virtual NIC (vNIC) packet filtering firewall and another is VMware vShield Endpoint Security (EPSec).

Each of these technologies makes use of different transport layers. With EPSec (dashed red paths), the EPSec driver is provided by VMware and creates the EPSec transport, which in many cases acts just like a VMware vSwitch. Registered to the driver is the DSWA for the host on which it runs. In this way, EPSec traffic that traverses the virtual SCSi devices knows to which Virtual Appliance to route the traffic via the transport mechanism provided. VMsafe-Net (dashed purple paths) its traffic on the other hand via the VMsafe-Net module that lives between the vSwitch portgroup and the VM's virtual NIC. Network traffic to be inspected is routed through the VMsafe-Net Transport to the DSWA, which is registered with the VMsafe-Net driver provided by Trend Micro.

While VMsafe-Net can operate on all packets passed through the VMsafe-Net components, EPSec only operates on that traffic sent to it via the EPSec Driver within the VM. This driver is required as file open and changes must be sent through the EPSec path to the DSWA. Not all file/block traffic is sent through

the EPsec paths to the per-vSphere host DSVA. On file open the file blocks are sent, and from then on only the changed blocks.

This combination, while currently unique among virtualization security vendors, is not solely what makes the product itself unique. The unique component of Trend Micros Deep Security 7.5 is that it provides fail-safe security. Not only does it make use of the VMware introspection agent-less components (VMsafe-Net and EPsec) but continues to include the agent-based security well known in the physical environment. In this way, if the virtualization components fail, the VM is moved to a host without the introspection components, or, at administrator discretion, the agent-based Trend Micro solutions can be enabled to provide a fail-safe approach to virtualization security as seen in Figure 2.

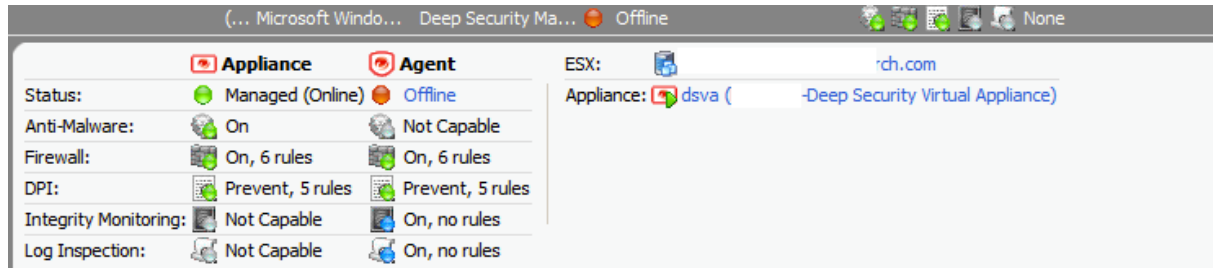


Figure 2: Deep Security Manager: Fail-Safe Security

In emergencies, virtual environment upgrades, and maintenance, this fail-safe approach to security is extremely useful.

Ease of Install (Install-ability)

Trend Micro Deep Security 7.5, if you do not want to make use of its anti-malware integration with vShield Endpoint is fairly simple to install: Install Deep Security Manager (DSM) then deploy DSVA on each host you desire to protect. However, once you desire to turn on the anti-malware functionality, then you also need to install and configure the VMware vShield Manager before installing and configuring DSVA. DSVA also requires your VMware vShield Endpoint License to be entered via the vSphere Client License management screens.

The documentation for Trend Micro Deep Security 7.5 provides a step-by-step approach, with graphics, to installation, configuration, and initial management of your VMware vShield Manager and the subsequent implementation of Deep Security Virtual Appliance. The documentation is excellent, and explains all steps in the process of implementing Deep Security 7.5 with EPsec support. Without this documentation the installation would be difficult at best as there are dependencies on VMware vShield Endpoint that must be addressed in the proper order.

After installation of the DSVA on all hosts to be protected and verification that VMware vShield Endpoint is operational, it takes a bit of time before EPsec can be used. I am not sure if this is due to Deep Security 7.5 or VMware vShield, but there is a delay of up to 30 minutes before everything appears to work. However, during these 30 minutes you can familiarize yourself with the Deep Security Manager user interface and complete the configuration steps outlined within the installation documentation. I found it a clean interface with many useful elements on the dashboard (Figure 4).

The documentation, however, does not go into where to place Deep Security Manager within your virtual network. Specifically the documentation does not outline that the best practice for virtualization security is the implementation of a segregated management network such as outlined within Figure 3.

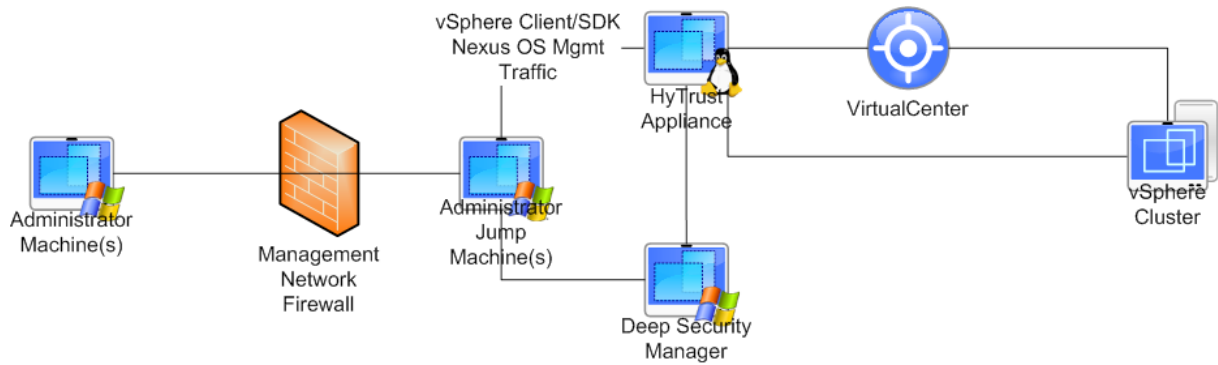


Figure 3: Deep Security Manager as a Component of the Virtualization Management Network

Such a management network, as shown in Figure 3, would move all management of the virtualization environment to within a bastioned and protected area. Deep Security 7.5 could provide the firewall for such a network but since you need an Edge firewall and not a zone-to-zone firewall, it is best to use VMware vShield Edge or some other form of virtual firewall. Deep Security 7.5, however, would provide defense-in-depth once you enter the firewall ensuring that vSphere Client/SDK traffic would only be sent to Virtual Center and/or to the vSphere ESX or ESXi hosts themselves. For example, if a HyTrust Appliance was also part of the mix you could use Deep Security 7.5 to ensure the proper packets went first through HyTrust before hitting VMware vCenter or the ESX or ESXi hosts.

Deep Security 7.5 not only provides a fail-safe approach it also provides the ability to create network and Guest OS defense-in-depth mechanisms, but is not an Edge Firewall.

The implementation of a management network using Deep Security 7.5 is missing from the installation documentation. It should be there, with the steps necessary to implement such a security policy. However, even with this lacking, the installation goes smoothly as the documentation is well written and if followed will provide the necessary steps to get Deep Security 7.5 working in short order. In addition, the installation guide contains well written uninstall instructions.

Ease of Use (Usability)

Deep Security Manager provides an easy to use dashboard, as seen by Figure 4, that shows the current status of the Deep Security implementation. However, unlike other tools, once integrated into VMware vCenter, Deep Security only shows the Folders of the virtual environment in the left hand pane of the interface and the dashboard in the right. At first glance, the VMs seem to be missing.

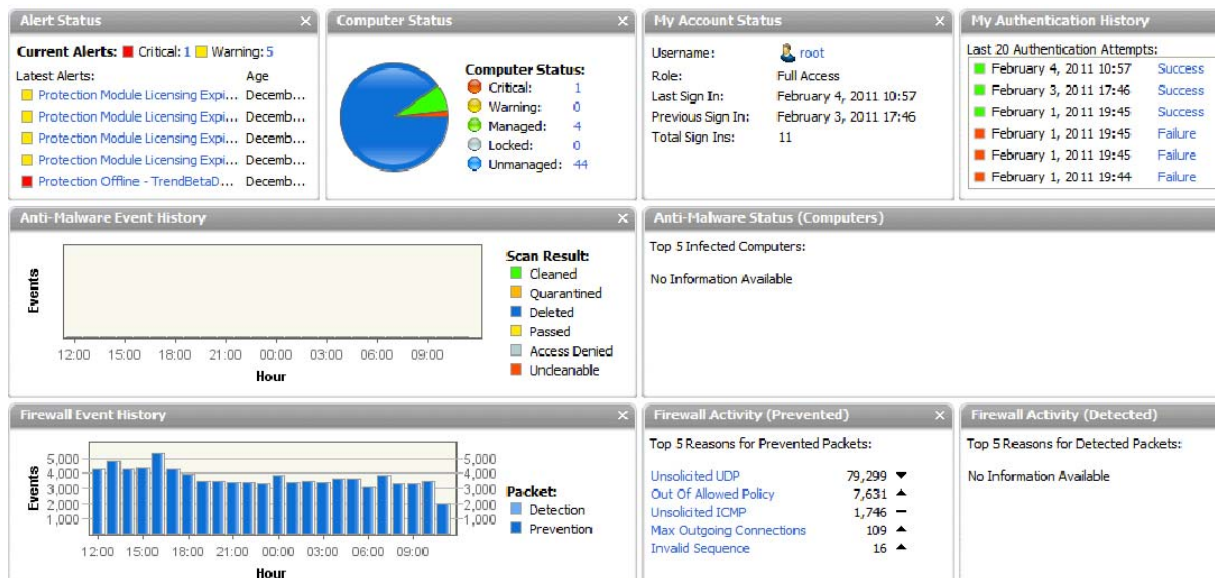


Figure 4: Deep Security Manager Dashboard

Yet, they are not missing. You are required to click on the Folder in the left hand pane to get a list of VMs and their current status. Some issues show up in the Dashboard but not the current status of the virtual machines. That requires access to the Folders as depicted in Figure 5. The status pane shows the current state of the VMs within the Folder including whether the VM is managed or unmanaged and the options that are enabled for the tool that is in use. If the Appliance (DSVA) is in use then you have Anti-Malware, Firewall, and Deep Packet Inspection (DPI) enabled. If the Agent is in use, then you also gain Integrity Monitoring and Log Inspection from within the VM. Only one option is available at a time. Generally, when Appliance Status is Managed (Online) the Agent will be Managed (Standby) or Offline.

The only aspect of Deep Security 7.5 that is not available within the Agent is the Anti-Malware component. Yet, it does appear that both the Agent and the Appliance can be on simultaneously to get all the features of Deep Security 7.5: Offline Anti-Malware as well as Log Inspection and Integrity Monitoring. This last option is shown in Figure 6.

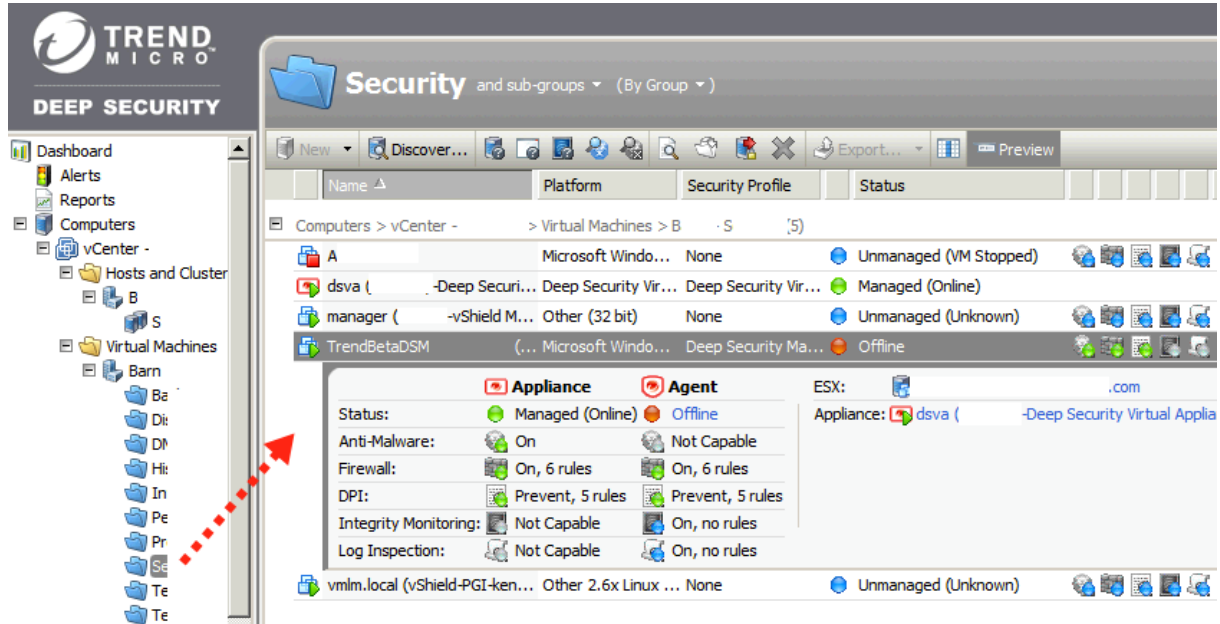


Figure 5: Folder Pane plus VM Status Pane

With a large number of VMs, the VM status window could become a bit crowded and confusing. That is when the Search functionality will become quite important as well as an appropriate naming convention to your VMs. This issue with usability, when you have 1000s of VMs, is a common issue amongst all management tools.

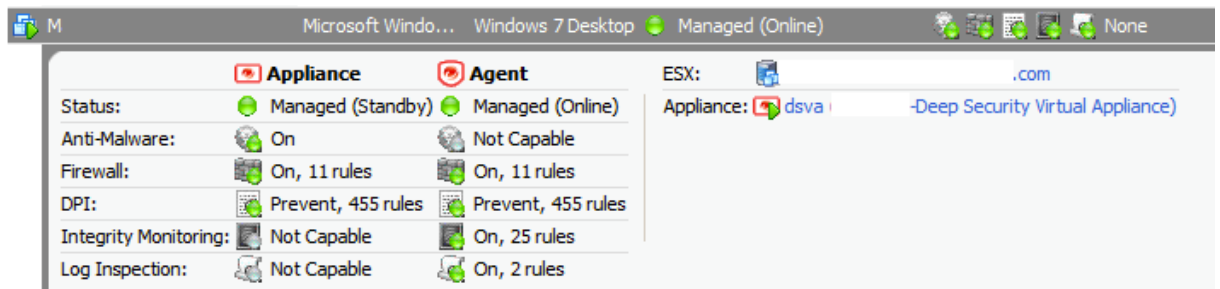


Figure 6: All Capabilities Enabled

The search function allows you to look for those VMs in incorrect state, such as Offline. While complex elements cannot be easily searched, machine names, and status can be, which is important in trying to monitor your Deep Security 7.5 implementation.

Functionality

Deep Security 7.5 contains several features that will improve the overall security of your environment by providing defense in depth even if without Edge firewall capability. Keep in mind that this represents part of your solution and not the complete set of required virtualization security functionality. Deep Security 7.5 provides:

- Packet Filtering Firewall via Trend Micro's VMsafe-Net implementation (not using the VMware vShield App/Zones APIs)
- Endpoint Anti-Malware Support via the VMware vShield Endpoint APIs
- Deep Packet Inspection that makes use of Trend Micro's VMsafe-Net implementation making use of Trend Micro's own Intrusion Detection, Prevention, and Web Application Protection rules.
- Integrity Monitoring if the Deep Security 7.5 Agent is also in use, which allows the agent to scan for changes to oft-attacked system files.
- Log Inspection that allows the agent to search the logs for the virtual machine for any security related issues. This functionality does not include a remote log server.

With the Trend Micro per VM agent installed, Deep Security 7.5 can offer all these functions but without the agent, Integrity Monitoring and Log Inspection of select operating systems are not available for use. With only the agent, Anti-Malware Support is not available yet the firewall is.

Trend Micro's firewall has the unique ability to Fail-Safe if for some reason the VMsafe-Net drivers and virtual appliance are not available. In this case the agents are then enabled to act as a per VM firewall.

In the following diagram of a segregated virtual network, DSM and DSVAs slot into very specific locations and require unique interactions for each running mode within your environment. Specifically, DSVAs combine a VMsafe-Net Virtual Appliance with an EPSec Virtual Appliance so that here is only one virtual appliance. However, if this appliance is not available, the agents within the VMs must be able to talk to the DSM in order to handle deep packet inspection. All agents must also be able to receive rule updates direct from DSM, which implies that DSM should be within the Administrative network. So placement of DSM will be very important within the physical and virtual network.

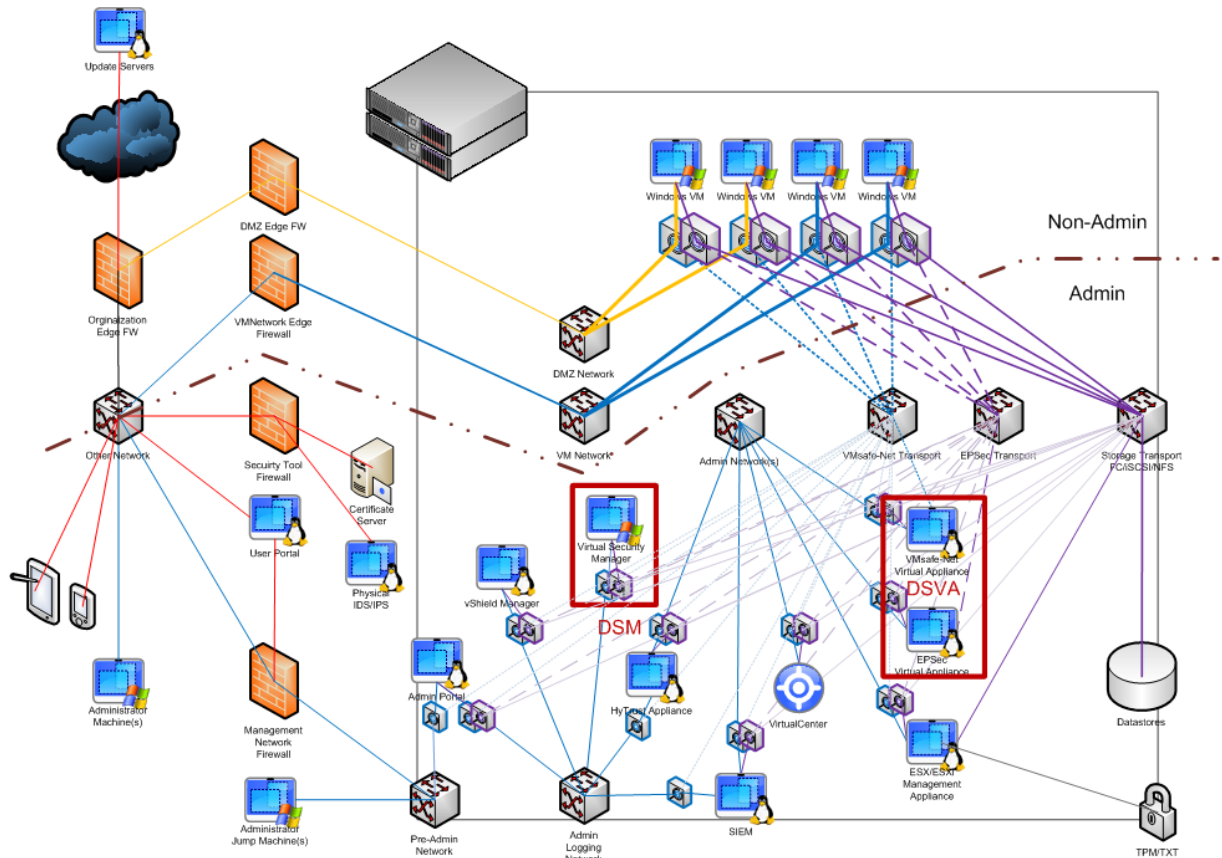


Figure 7: Basic Network/Virtualization Security Diagram

Figure 7 shows how Deep Security 7.5 would fit into a possible virtual network configuration. Coming out of each VM are two distinct control paths, the first is the probe (dotted-blue) used for VMsafe-Net which in turn talks to a VMsafe-Net appliance over a well defined and hidden transport. The second probe (dashed purple) is for the vSCSI device that has attached to it a Filter that communicates using the EPsec Transport to the virtual appliance that will handle endpoint security. The Deep Security Virtual Appliance or DSVA is a single device that handles both these tasks, providing a per-virtual NIC firewall and anti-malware scanning of blocks within the VM.

A second virtual appliance is also required, Deep Security Manager or DSM. As we stated earlier, DSM and DSVA must live within the administrative component of any virtual network. This administrative network is depicted in Figure 7 as everything below the dash-dot-dot dark-red line. The intersection is usually an external network switch through different edge firewalls (which could be done using vShield Edge or some other edge firewall). While inside the virtual network VMsafe-Net packet filtering provided by Deep Security 7.5 could be used standalone (or used in conjunction with vShield App).

Figure 7 is fairly busy, but the key is to note that all the 'administrative' tools are within an administrative network, which is split between a pre-admin network and a logging network and finally the real administrative network. These network splits are important because no one should directly access vCenter or the ESX hosts unless they are virtualization administrators and it is either a required action (such as adding licensing) or a break glass situation (as in fixing a problem). All else should be proxied via portals and all data used should be logged from the portals through the administrative networks.

Additional logging will be required to maintain GRC requirements going forward. DSM provides some of these for End point security, but more is required for the actual virtualization hosts. Auditing must increase within the virtual environment to aid in forensics analysis of security breaches.

Auditability (Continual Auditing)

Deep Security Manager (DSM) contains a single pane of glass approach to determine if there are issues with the virtual machines protected by Deep Security. DSM contains a robust notification system as well as a single dashboard that could be running at all times. Notifications can be made via email and as such via SMS.

With five specific functions that cover quite a bit of the virtualization space, the single DSM dashboard could notify of many issues, but not all of them. As such, its auditing capabilities are limited to its own functions. However, via its notification capabilities, auditing could be expanded within other tools to include Deep Security.

Deep Security 7.5 does send data to syslog servers as well as Arcsight CEF legacy and 1.0 formats. This is configurable under System Settings -> Notifications. The use of these services allows other tools to correlate security events as well as archiving events for future auditing needs.

There are three components of Deep Security that help with auditing. The first is Deep Packet Inspection (DPI) VMsafe-Net component of its packet filtering firewall. DPI acts as an IDS or IPS and therefore has auditing capabilities for virtual networks. The second component only works if the Deep Security Agent is installed within a VM and that is the Log Inspection component. However, this is limited to the guest operating systems and is looking for specific Endpoint security issues. The last is Integrity Monitoring, which is also only available if the Agent is installed.

All three report up to DSM and could be used to increase overall auditing, but only for the Endpoint environment or the virtual networks protected by Deep Security 7.5.

Integration with other Products

Trend Micro Deep Security 7.5 integrates with VMware vShield Endpoint and includes support for Arcsight CEF legacy and 1.0 format as well as the ability to send data to syslog servers. Trend Micro Officescan is the basis for the Anti-Malware product that makes use of VMware vShield Endpoint. The rule derivations are from the same source as the rules for the VMsafe-Net deep packet inspection: Trend Micro's own rules derived from their security center. Both Officescan and Deep Security 7.5 share the same rule sets, albeit in different forms.

There is no integration with other third-party tools such as any of the current SIEMs on the market or other servers. This could cause issues with unified auditing. Deep Security 7.5, however, offers a pretty robust set of tools that target Endpoint Security and components can be applied to the entire virtual environment with some success. However, it is recommended that other tools also be used in conjunction with Deep Security 7.5 such as HyTrust, Administrative portals, SIEM servers, and user portals.

Deep Security's Anti-Malware component is dependent on vShield Endpoint and as such has all the limitations of vShield Endpoint. For best integration, ensure ALL nodes to which a VM can be vMotioned or run has vShield Endpoint enabled. If you do not, there could be some very interesting issues with VMs not being able to be booted, etc. These are unrelated to Deep Security 7.5, but are vShield issues being addressed by VMware.

Conclusion

Deep Security 7.5 provides a robust set of tools to add to your toolbox. Trend Micro is the only vendor currently shipping a product that works with VMware vShield Endpoint to provide offline Anti-Malware scanning. This functionality combined with Deep Security's existing packet-filtering per virtual NIC firewall provides increased security within the virtual environment. The performance increases by offloading malware detection as outlined in a Tolly Report (<http://www.tolly.com/DocDetail.aspx?DocNumber=211101>) are significant. I saw this within my own environment. The perceived performance improvement is visible to the naked eye.

While Deep Security 7.5 does not provide security for the entire virtual environment it covers the necessary security measures for within the virtual environment. The other aspects to consider are limiting access to the administrative components and proper placement of Deep Security Manager so that Trend Micro Deep Security 7.5 fail-safe modes all work as expected.

Fail-safe is a key component of Deep Security 7.5, and as such is a clear winner in functionality. While this does require an agent installed within each VM, this agent is mainly there as a fail-safe precaution. Failing-safe is a requirement for security within the virtual environment and Trend Micro is on the proper path.