Automated Deployment of Guest Introspection & VMware Data Security

With the virtualization layer within the SDDC, organizations can insert security services that inherit the attributes of the Goldilocks zone. There are number of examples of what partners are able to achieve when they have access to host-based context, are effectively isolated from the attack domain, and can be delivered as a distributed service, with the ability to provision, insert and manage security services quickly and easily.

In this article I am going to show you how to transform your automated security solutions for optimal context and isolation while minimizing resource overhead. So in a nutshell in this article we will talk about Guest Introspection and VMware Data Security deployment. However before we go into the code and API side, I would like to put some lights on these two solutions.

Guest Introspection

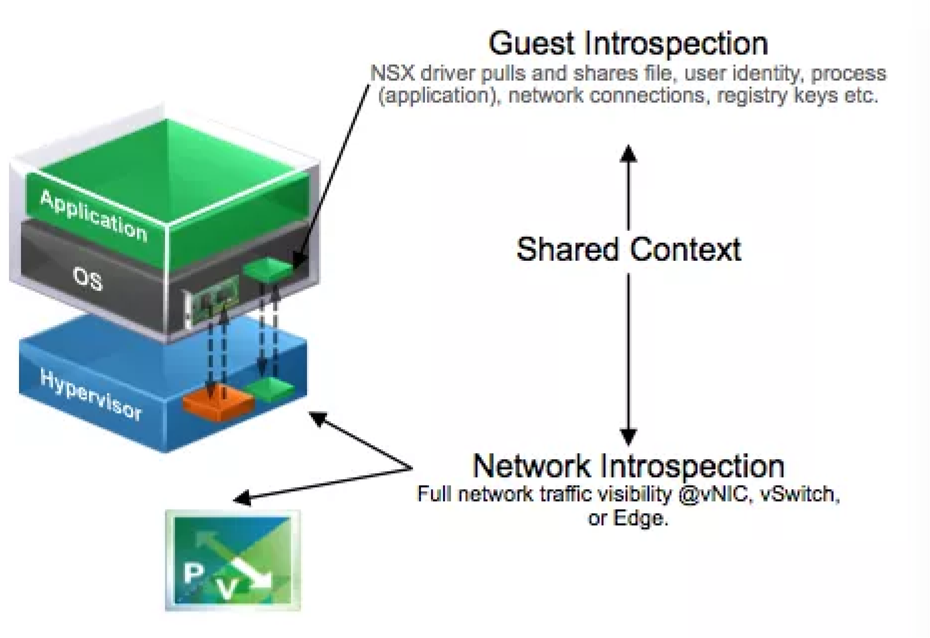
Guest Introspection strengthens security for virtual machines while still improving performance for endpoint protection. This is done by offloading the antivirus and anti-malware agent processing to a dedicated Security Virtual Appliance that is delivered and supported by VMware partners. Guest Introspection or EPSEC in vCNS world is a framework of different elements, including Application Programming Interfaces (APIs) that are developed by VMware Engineering to enable Endpoint security partners to integrate these solutions into the VMware vSphere (SVM) platform. This integration is performed at the hypervisor layer that provides the introspection.

It’s important to note that customers do not consume EPSEC, but they benefit from the integration of EPSEC through Endpoint products and solutions.

Traditional antivirus solutions require an agent in each virtual machine. All of those agents manage an antivirus signature. You can either configure a client-side schedule to do the virus scanning or you can use a centralized schedule running on the master server. In this approach, if you look at the consolidation ration, your memory, CPU, and network overhead may become a significant overkill.

However, there are other solutions as well, which can be configured for a distributed scan over a configurable time interval. It can reduce the resource usage in VMs and in your ESXi as well.

You can still get exposed to a threat in this model if your antivirus signature is not up-to-date. Until the time you update your signature in guest machines, your VM is at risk. Some antivirus software comes with the automated process of pushing the antivirus signature to the guest machines (registered clients). NSX provides built-in services to manage the security posture of workloads at scale.

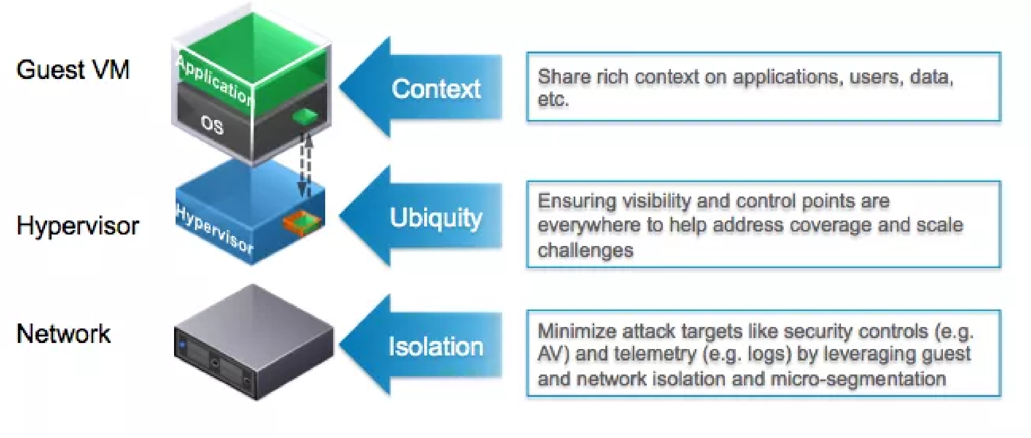

Guest Introspection
NSX driver pulls and shares file, user identity, process (application), network connections, registry keys etc.
Application
OS
Hypervisor
Shared Context
Network Introspection
Full network traffic visibility @vNIC, vSwitch, or Edge.
P
V

Guest Introspection – key benefits

The Guest Introspection service in NSX for vSphere allows you to offload the following security functions from the VM to a dedicated appliance on the host:

- Protection: Virus definitions can be kept up-to-date easily as they are stored on an always-on appliance. So if an attacker is targeting a particular VM, the virus engine is not compromised.
- Efficiency: You don’t need to install an agent on each guest on the host. An agent is provided with a driver, which is included in VMware Tools. You just need one appliance per host. So you need just one scanning engine and one signature database per host. There is also no antivirus storm.
- Assurance: As there is no need to install the software, deployed VMs are protected as soon as they are switched on.
- Centralized management: Using a single management console, vCloud security administrators can manage policies and see if the antivirus is functioning correctly.

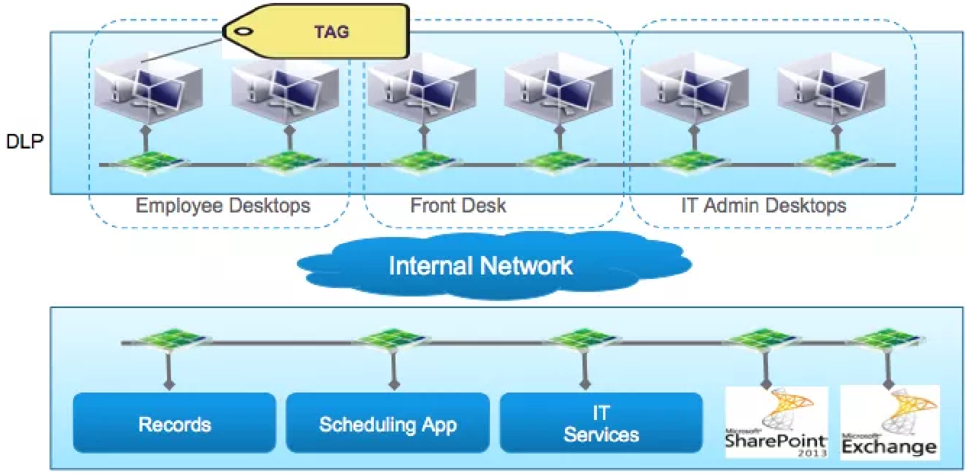
So in a nutshell NSX Guest Introspection transforms security by providing context & minimizing overhead.


Guest VM
Application
OS
Hypervisor
Hypervisor
Network
Context
Share rich context on applications, users, data, etc.
Ubiquity
Ensuring visibility and control points are everywhere to help address coverage and scale challenges
Isolation
Minimize attack targets like security controls (e.g. AV) and telemetry (e.g. logs) by leveraging guest and network isolation and micro-segmentation

VMware Data Security

VMware Data Security for NSX provides visibility into sensitive data stored within your organization’s virtualized environments.

You can ensure that sensitive data in your environment is adequately protected and assess compliance with regulations around the world, and you can do it by using reports from data scans performed by VMware Data Security for NSX.



It enables you to choose from built-in templates for standards and regulations governing the most common types of sensitive data, including PII (Personally Identifiable Information), PCI- DSS (Payment Card Industry Data Security Standard), and PHI (Patient Health information) within your organization’s virtualized and cloud environments. You can use the violation reports and make sure that sensitive data is adequately protected and assess compliance with regulations around the world.

To get Data Security for NSX into action, you should create a policy that defines the regulations that apply to data security in your organization and specifies the areas of your environment and files to be scanned. A regulation is composed of content blades that identify the sensitive content to be detected. Data Security for NSX supports PCI, PHI, and PII related regulations only.

Once you start a Data Security scan, it analyzes the data on the virtual machines in your VMware vSphere inventory that you define as a boundary, and then generates a report that contains the number of violations detected and the files that violated your policy. You can perform all data security tasks using REST APIs and that is something that we will focus on in a minute.

From the deployment perspective of these two services, you need to deploy Guest Introspection first and then Data Security as the later depends on the first.

Excerpts from the NSX API Guide:

The security fabric simplifies and automates deployment of security services and provide a platform for configuration of the elements that are required to provide security to workloads. These elements include:

Internal components:

- USVM
- Endpoint Mux
- Data Security
- Logical Firewall

External components:

- Partner OVFs/Vibs
- Partner vendor policy templates

For partner services, the overall workflow begins with registration of services by partner consoles, followed by deployment of the services by the administrator.

Subsequent workflow is as follows:

1. Select the clusters on which to deploy the security fabric (Mux, Traffic filter, USVM).
2. Specify an IP pool to be used with the SVMs (available only if the partner registration indicates requirement of static IPs)
3. Select portgroup (DVPG) to be used for each cluster (a default is pre-populated for the user).
4. Select datastore to be used for each cluster (a default is pre-populated for the user).
5. NSX Manager deploys the components on all hosts of the selected clusters.

Request

POST **https://<nsxmgr-ip>/api/2.0/si/deploy?startTime=<time>**

Request Body

```
<clusterDeploymentConfigs>
<clusterDeploymentConfig>
<clusterId>cluster-id</clusterId>
<datastore>ds-id</datastore>
<services>
<serviceDeploymentConfig>
<serviceId>service-id</serviceId>
<dvPortGroup>dvpg-id</dvPortGroup>
<ipPool>ipPool</ipPool>
</serviceDeploymentConfig>
</services>
</clusterDeploymentConfig>
</clusterDeploymentConfigs>
```

So you see you need to use this API to deploy these services where Service ID is either Guest Introspection or Data Security. My friend Timo Sugliani has written a cool code in PowerCLI calling this API to deploy both of these services. Click on the link to download the code and re-use it in your environment. This code not only deploys the security solutions but also configures the Data Security policy scan only .sec extension which are less than 5KB in size.