Darktrace for Virtualized Environments
Enhanced Visibility for Your Enterprise Immune System
Visibility in Virtualized Environments

Increasingly, organizations are taking advantage of technological advancements to improve their agility and efficiency, opting for virtual servers and virtualization techniques in their data centers. Nearly endless elasticity, expandability with fewer resources, and a reduction in the number of physical servers required are among the benefits that are driving the move from traditional networking to distributed, software-defined networking (SDN). This virtual revolution is not, however, without its drawbacks.

Whereas in traditional, physical networks, traffic can be easily ‘seen’ on the physical wire itself, traffic between virtual machines (VM) residing on the same hypervisor can be difficult to monitor. This is because inter-VM traffic is switched locally on a virtual switch, as opposed to a physical one, and so never makes it down to the network wire where it can be observed. This provides a significant challenge to security; a blind spot in which information flow in and out of the host server can be monitored, but the traffic inside is invisible. With the trend towards increasing virtualization, the number of these blind spots will only increase.

These blind spots can cause operational challenges, particularly in high frequency or tightly regulated environments. Many organizations today require overall visibility of all their data, including the packets passing between VMs, to strengthen their ability to pinpoint early indicators of cyber-threat in real time, and reduce operational risks.

While network tap solutions can be used to mirror and access virtual traffic that leaves the virtual environment and travels over the physical network, they are unable to capture all the traffic that flows between virtual machines (VMs). For example, an application may be distributed across both physical and virtual environments, with the database tier residing on the physical server, while the web and app tiers are virtualized. In this case, the network traffic between the two VMs may never traverse the physical network, so will not pass by the TAP or a physical switch SPAN port.

The challenge is to provide a solution that gives visibility of inter-VM traffic, while not impacting on performance of the server, and allowing for scalability.

Summary

Darktrace vSensors and OS-Sensors seamlessly extend the self-learning, real-time threat detection capability of the Enterprise Immune System into virtualized environments. They provide organizations with enhanced visibility and insight into all points of the network, both on premise and in the cloud.
Darktrace vSensors and OS-Sensors

Darktrace's Enterprise Immune System works by observing all network activity, in order to identify critical anomalies that exist within a company's infrastructure. The core Darktrace appliance is installed at the heart of the physical network, through which the majority of digital communications have to traverse.

To ensure that the Enterprise Immune System has comprehensive visibility of today's distributed infrastructures, including within virtual environments, Darktrace has developed the vSensor.

The vSensor software is installed as a virtual appliance configured to receive a SPAN from the virtual network switch. This allows it to capture all inter-VM traffic, without a single packet being lost or dropped by the system. It stores the packet captures on a rolling basis, optimizing the disk space and I/O performance, and ensuring that there is minimal impact on the performance of the server. Only one vSensor needs to be installed on each of the hardware servers, allowing for scalability.

The vSensor will extract only the relevant metadata using the Darkflow system, sending 1% of the original raw network traffic ingested onto the master appliance efficiently and securely, wherever it is located on the physical network.

Darktrace vSensors are distributed in industry-standard formats, representing a virtual (software) appliance. They have been developed for VMWare, ESXi and any other virtualized environment that supports Open Virtualization Formats (OVF).

For third-party clouds, vSensors are supported by OS-Sensors. These are lightweight, host-based server agents which intelligently extract copies of network traffic for analysis by the master appliance.

Benefits
- Ingests virtual traffic from a limited set of IPs
- Does not ingest physical network traffic
- Sends data efficiently and securely to the master appliance, wherever it is located on the physical network
- Sends approximately 1% of the original raw network data ingested to the master appliance
- Works with third-party clouds
vSensor Use Cases

There are several use cases where the vSensor is particularly valuable to our customers.

1. Multiple VMs within owned hardware servers

A standard deployment of the Darktrace Enterprise Immune System involves the capture of all traffic from a virtual server within one hardware appliance to a virtual server in another hardware appliance. This is because the traffic traverses the physical network connection.

With the vSensor installed into the hardware server, acting as just one more VM, visibility is extended to traffic between the VMs within the same physical appliance.

The vSensor software must be used in conjunction with a master Darktrace (hardware) appliance.

---

**Fig. 2: Visibility of a virtualized hardware server with Darktrace vSensor**
2. Remote Locations

An organization may have remote offices or locations, with several machines at each one. A typical scenario might be a distribution of 300 small sales offices or retail stores, with 5 machines in each. It may not be practical for an organization with this infrastructure to deploy 300 Darktrace appliances into each individual location.

Using the Darktrace vSensor, this is not necessary. If the relevant traffic is spanned into a virtual environment hosting the vSensor, then Darktrace can capture their intercommunications and obtain insights into the data moving within each location. The data is sent back to the master appliance, where the advanced analysis of the Enterprise Immune System is performed.

Fig.3: Visibility of branch servers using Darktrace vSensor
3. Managed Third-Party Cloud Provider

If your organization uses a managed cloud-computing environment, you may want your security monitoring to include the data moving within that cloud environment, even if you do not have direct access to the physical server. The master Darktrace appliance, connected to the physical network, already captures the activity of a user or client accessing data within the cloud data center. Supported by the vSensor, it gains visibility of lateral information flow within the cloud too.

Darktrace is able to capture virtual network traffic thanks to Darktrace’s OS-Sensors. OS-Sensors are lightweight, host-based server agents, that are easily installed onto virtual machines in the cloud. They intelligently create single copies of network traffic, in a non-intrusive manner, and are capable of dynamically configuring themselves to avoid data duplication and streamline bandwidth use. Data is aggregated within the vSensor, and fed back to the master appliance via a secure connection.

Darktrace OS-Sensors are fully configurable, allowing organizations to see all or selected cloud traffic, without requiring access to the hypervisor, and with minimal performance impact. Available for Linux and Windows, Darktrace OS-Sensors are robust and resilient, allowing organizations to enhance visibility and deliver Enterprise Immune System monitoring to cloud environments, wherever they are hosted.

![Diagram of visibility in third-party-hosted servers with Darktrace vSensor](image)

*Fig.4: Visibility in third-party-hosted servers with Darktrace vSensor*
Resources Required:

- Ability to install virtual appliance within virtualized environment
- If you have access to the hardware server you will automatically be able to do this
- Ability to either span virtual traffic into specified VM, or to install OS-Sensors onto VMs in a managed hosting service.
- Connectivity to the Darktrace master appliance
  - Sufficient bandwidth to transfer 1% of original traffic volume spanned to virtual appliance

vSensor technical specification

<table>
<thead>
<tr>
<th></th>
<th>S</th>
<th>M</th>
<th>L</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPUs</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>RAM</td>
<td>3GB</td>
<td>8GB</td>
<td>32GB</td>
</tr>
<tr>
<td>Hard Drive</td>
<td>1GB</td>
<td>4GB</td>
<td>32GB</td>
</tr>
<tr>
<td>Device Limit</td>
<td>10</td>
<td>100</td>
<td>1000</td>
</tr>
<tr>
<td>Traffic</td>
<td>10Mbps</td>
<td>100Mbps</td>
<td>400Mbps</td>
</tr>
<tr>
<td>Connections per minute</td>
<td>1000</td>
<td>5000</td>
<td>20000</td>
</tr>
</tbody>
</table>

About Darktrace

Named ‘Technology Pioneer’ by the World Economic Forum, Darktrace is one of the world’s leading cyber threat defense companies. Its Enterprise Immune System technology detects previously unidentified threats in real time, powered by machine learning and mathematics developed at the University of Cambridge, which analyze the behavior of every device, user and network within an organization. Some of the world’s largest corporations rely on Darktrace’s self-learning appliance in sectors including energy and utilities, financial services, telecommunications, healthcare, manufacturing, retail and transportation. The company was founded in 2013 by leading machine learning specialists and government intelligence experts, and is headquartered in Cambridge, UK and San Francisco, including offices in Auckland, Boston, Chicago, Dallas, London, Los Angeles, Milan, Mumbai, New York, Paris, Seoul, Singapore, Sydney, Tokyo, Toronto and Washington D.C.

info@darktrace.com
tel: +44 (0) 1223 350 653
tel: +1 415 896 7898
www.darktrace.com