Darktrace Sensors

Modern organizations require overall visibility of virtual environments in addition to the traditional, physical estate. 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 sometimes unable to capture all the traffic that flows between VMs and inside the cloud.

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 and thus will not pass by the TAP or a physical switch SPAN port. The challenge is to provide a solution that offers visibility of your cloud and virtual infrastructure, including inter-VM traffic, and allows for scalability, without impacting server performance.

Darktrace Sensors seamlessly extend the self-learning, real-time threat detection capability of the Enterprise Immune System into cloud and virtualized environments. They provide organizations with enhanced visibility and insight into all points of the network, however it is configured.

DARKTRACE vSENSORS

Darktrace vSensors are lightweight software components that extend Darktrace's visibility in virtualized environments. They provide the Enterprise Immune System with comprehensive visibility of today's distributed infrastructures.

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 hardware server, allowing for scalability. The vSensor requires bi-directional TCP port 443 and inbound TCP port 22 connectivity to the Darktrace master appliance.

The vSensor will extract only the relevant metadata using the Darkflow system, sending aproximately 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 and any other virtualized environment that supports Open Virtualization Formats (OVF).

DARKTRACE OS-SENSORS

Darktrace OS-Sensors are lightweight, host-based server agents that extend Darktrace's visibility into third-party cloud environments, including AWS, Rackspace, and Microsoft Azure.

OS-Sensors intelligently extract single copies of network traffic for analysis by the master Darktrace appliance. They are easily installed onto virtual machines in the cloud and capable of dynamically configuring themselves to avoid data duplication and streamline bandwidth use. Working in conjunction with vSensors, data is aggregated 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.

Deployment Scenarios

There are several use cases where vSensors and OS-Sensors are particularly valuable to Darktrace customers.

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.

Managed Third-Party Cloud Provider

One of the benefits of using a managed third-party cloud is enabling access from non-corporate sites, such as from home or whilst travelling. However, this environment necessarily creates blind spots from a security point of view. Darktrace is able to address this scenario even if you do not have direct access to the physical cloud 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 vSensor, it gains visibility of lateral information flow within the cloud too. Darktrace is also able to capture virtual network traffic thanks to its OS-Sensors, allowing you to achieve visibility of all cloud activity without requiring access to the hypervisor and with minimal performance impact.

Cloud-Only Environments

If your organization has internal users that access data in the cloud, and does not have on-premise network, Darktrace is able to deliver and manage a cloud-only deployment. In this scenario, Darktrace's Enterprise Immune System technology runs entirely in the cloud, without a physical appliance.

A cloud-only deployment includes the full service offered on the physical appliance, from data collection, mathematics, and detection, through to the Threat Visualizer and our expert cyber-analyst services. Instead of installing a physical appliance, Darktrace runs a dedicated service for your organization, and vSensors and OS-Sensors are installed onto your existing cloud.

Technical Specification

In order to install Darktrace vSensors and OS-Sensors, you will need the ability to either span virtual traffic into a specified VM or to install OS-Sensors onto VMs in a managed hosting service. You will also need connectivity to the Darktrace master appliance and sufficient bandwidth to transfer 1% of original traffic volume spanned to the virtual appliance.

Network Stats	Device Limit	10	100	500
	Traffic	10Mbps	100mbps	400Mbps
	Connections per minute	1000	5000	20000
Approximate vSensor requirements	CPUs	2	4	8
	Ram	3GB	8BG	32GB
	Hard Drive	10GB	30GB	100GB