DARKTRACE VIRTUAL SENSORS AND AGENTS

Introduction

Enterprise networks are no longer confined to a local, physical network - distributed environments and virtualized infrastructure are frequent and increasingly large components of an organization's network. While network tap solutions can be used to access virtual traffic that leaves the virtual environment and travels over the physical network, they are not sufficient to cover the wide and complex range of network scenarios that now comprise the new enterprise network.

Key network traffic may never traverse the physical network. For example, systems may be distributed across both physical and virtual environments, with a database tier residing on a physical server while the web and app tiers are virtualized. In this case, the virtual-tier traffic will not pass by the tap or a physical switch SPAN port. Even where physical traffic is to be monitored, it may not be feasible to alter the configuration of the network to deploy a tap solution. Many organizations also maintain limited or no physical network, with day-to-day operations taking place in a third-party managed Cloud.

Darktrace provides a suite of virtual sensors and agents ideal for deployment in these network scenarios, extending visibility and response into the virtualized parts of your infrastructure. Sensors are compatible with packet mirroring and automation methods in all major private cloud providers.

Darktrace Sensors seamlessly expand self-learning, real-time Darktrace DETECT and Darktrace RESPOND capability to provide organizations with enhanced visibility and insight into all points of the network, whether physical or virtualized.

Autonomous Response

Virtualized deployments support Darktrace RESPOND autonomous response applied via vSensors, osSensor and cSensor agents. vSensors can perform Darktrace RESPOND/Network actions directly or instruct their associated osSensors - agent or containerized - to respond. Darktrace RESPOND/Network is enabled by default on both vSensors and osSensors - where a valid license key is present on the associated Darktrace master, no additional configuration is required to begin taking actions. cSensor agents support specialized Darktrace RESPOND/Endpoint response through Darktrace DETECT & RESPOND/ Endpoint coverage.

vSensor

Darktrace vSensors are lightweight components intended for deployment in virtualized networks or where on-premises traffic cannot be routed through a physical probe. vSensors support Darktrace RESPOND and can perform network actions directly or instruct their associated osSensors - agent or containerized - to respond.

vSensors can be deployed as a standalone virtual machine receiving inter-VM traffic from a virtual switch, in a VPC traffic-mirroring scenario, or by collecting packets from osSensor agents deployed on hosts to be monitored. vSensors can ingest and process physical network traffic in addition to virtualized, ideal for scenarios where altering the physical network is not possible. Traffic ingestion via AWS VPC Traffic Mirroring and Google Cloud Platform (GCP) Packet Mirroring is also supported for both ingestion and autonomous response.

The vSensor will extract only the relevant metadata, sending on approximately ~2-4% of the original raw network traffic ingested to the Darktrace deployment efficiently and securely.

The vSensor supports VXLAN and ERSPAN type I and type II, as well as GRE with transparent ethernet bridging. In addition to processing network traffic, vSensors can ingest and forward syslog-format logs to the Threat Visualizer.

Multiple communication modes are available between the Darktrace platform and the vSensor - the most suitable mode is dependent on the location of the vSensor, the availability of the master, and whether communication must occur over an untrusted network.

Standalone Darktrace vSensors are distributed in industry-standard formats including VMWare and platforms that support Open Virtualization Format (OVF). Deployment is also compatible with autoscaling, automated resource creation such as AWS QuickStart; automation templates are available for AWS, Google Cloud Platform and Microsoft Azure.

osSensor

Darktrace osSensors are lightweight, host-based agents that extend Darktrace's visibility into third-party cloud environments including AWS, Google Cloud Platform, and Microsoft Azure. The osSensor software is installed on each customer device where visibility is desired and monitors all of the network traffic to/from that device; the monitored traffic is then sent to the vSensor for analysis. For containerized environments, the osSensor is also available as a Docker container.

Darktrace osSensors are easily installed onto virtual resources 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 Darktrace deployment via a secure connection.

The agent works with Windows, select Linux distributions and any Linux environment running the Docker engine. Third-party containerized platforms such as Azure AKS, Amazon EKS, Google GKE and AWS ECS Fargate are supported.

osSensors are autonomous response enabled and can take Darktrace RESPOND actions directly on their host device when instructed by a connected vSensor. osSensors require a vSensor connection and cannot be deployed standalone.

containerSensor (Technical Preview)

The Darktrace containerSensor is a tracking sensor which enhances Darktrace DETECT pattern of life analysis in Kubernetes and other containerized environments (*support for ECS coming soon*). The containerSensor retrieves metadata about workloads, allowing traffic observed within the cluster to be assigned to consistent, recognizable entities. This approach allows dynamic workloads to be modelled as a group according to the task they are performing, significantly enhancing Darktrace's understanding of operations within clusters. Examples of these might include cronjobs which run periodically, horizontally scaling services which change over time, or even static groups of containers which rarely change but should be modelled as a single entity.

The containerSensor does not ingest network traffic within Kubernetes environments and is designed to be paired with a Darktrace sensor performing Deep Packet Inspection; a connected Darktrace vSensor (6.1+) is required at a minimum to communicate metadata back to the Darktrace platform.

For ease of deployment, Darktrace provides a Helm Chart to deploy the containerSensor and optionally an osSensor daemonset.

cSensor (Darktrace DETECT & RESPOND/Endpoint)

Darktrace DETECT & RESPOND/Endpoint extends the visibility of the Darktrace Cyber AI Platform and the reach of Darktrace RESPOND autonomous response to remote devices. Coverage is provided via Darktrace Client Sensor ("cSensor") agents installed directly on the endpoint to monitor and control network activity. Unlike the osSensor, it requires no connected vSensor and performs data analysis on-agent.

The cSensor is designed to extend coverage, visibility and Darktrace RESPOND autonomous response over a dynamic workforce.

Deployment in virtualized networks is not the primary deployment scenario. It is ideally used in combination with other Darktrace virtual sensors and deployment options to achieve a combination of greater and simpler visibility.

If you are interested in deploying Darktrace DETECT & RESPOND/Endpoint coverage, please reach out to your Darktrace representative or review the Darktrace DETECT & RESPOND/Endpoint (Customer Portal) introduction.

Specialized Agents

Terminal Services Agent

The Darktrace Terminal Services Agent (TSA) is a lightweight agent which obtains enrichment data for Windows Terminal Services environments such as Citrix Xen App and Microsoft RDSH. Windows Terminal Services environments allow centrally hosted Windows applications to be launched and accessed by remote users. For these environments it is not possible to resolve connections initiated from a centrally-hosted application to a specific end user or IP address from raw network traffic. When installed on the Windows Terminal Server host, the TSA enables Darktrace to identify the user accounts initiating connections.

Please discuss the deployment of the TSA with your Darktrace representative or review the Darktrace Terminal Service Agent (Customer Portal) deployment guide.

Direct Access Agent

The Darktrace DirectAccess Agent (DAA) is installed on Windows servers running DirectAccess. DirectAccess allows users to access internal network resources from external locations; access is provided via a tunnel from the client, through the server to the required resources. In passive network traffic ingestion, these connections originate from the DirectAccess server and not the client devices, providing a challenge for accurate pattern of life modeling. When installed on the Windows DirectAccess server, the agent enables Darktrace to identify the user accounts initiating the connections and model each device accordingly.

Please discuss the deployment of the DAA with your Darktrace representative or review the Darktrace DirectAccess Agent (Customer Portal) deployment guide.

Example Deployment Scenarios

Digital environments encompass a wide and varied range of “networks”: dynamic remote workers, virtualized networks in a public cloud, on-premises datacentres, and ephemeral and containerized workloads. Darktrace virtual sensors can ensure full visibility and ‘pattern of life’ monitoring regardless of network composition and location.

The following example scenarios illustrate how Darktrace agents and sensors can work with your existing infrastructure to extend award winning self-learning Cyber AI across the full range of network environments.

Managed Third-Party Cloud Provider

Darktrace offers a number of deployment options for virtual sensors in a third-party cloud platform, ensuring full visibility over cloud-hosted networks and allowing the security team to review all traffic - physical and virtualized - in a single user interface.

vSensors can be deployed to ingest traffic directly from a virtual switch, via a packet mirroring policy such as GCP Packet Mirroring or from containerized or device-hosted osSensors. Deployment is also compatible with automated resource creation such as AWS QuickStart; templates are available for GCP, AWS and Microsoft Azure.

Deployment scenarios are not mutually exclusive; for example, a vSensor deployed in AWS receiving traffic via VPC mirroring may also have connected osSensors to ensure coverage over pre-nitro instances or AWS EKS containerized infrastructure. Similarly, Darktrace containerSensors deployed across EKS can work with multiple traffic ingestion scenarios.

Virtualized Darktrace deployments

Darktrace offers virtualized Darktrace environments hosted and managed within Darktrace cloud environments (AWS and Azure). Deployment is simple and coverage can be quickly achieved with Darktrace DETECT & RESPOND/Endpoint agents - cSensors - installed on remote endpoint devices.

In this scenario, vSensors and osSensors are vital to expand visibility over on-premises and virtualized resources. vSensors located within the local network can ingest mirrored physical traffic and syslog input from datacenters for encrypted transmission to the virtual Darktrace instance. A combination of vSensors, osSensors and packet mirroring policies deployed through automation templates can then be used to cover cloud-based infrastructure.

Technical Specification

The following refers to Darktrace osSensors, containerSensors and vSensors only; other agents and deployment options such as the Darktrace cSensor are addressed in the relevant documentation.

To deploy Darktrace vSensors and osSensors, the ability to mirror traffic (via a SPAN or a packet mirroring policy) into a specified VM is required. Alternatively, osSensors can be installed directly onto VMs or container hosts in a managed hosting service and communicate traffic to the parent vSensor.

Connectivity is required between the Darktrace master and the vSensor; specific network requirements will differ between communication modes. Sufficient bandwidth is required to transfer approximately 1-4% of the traffic ingested by the vSensor. For osSensor deployments, connectivity is also required between the vSensor and osSensor and sufficient bandwidth is needed to transfer all (deduplicated) ingested traffic to the vSensor for processing. containerSensors require connectivity to the vSensor only.

STATISTIC / REQUIREMENT					
Estimated Devices	50	100	200	400	800
Traffic (Mbps)	100	250	500	1000	2000
CPUs	2	4	8	16	32
RAM (GB)	8	16	32	64	128
Hard Drive (GB)	50	100	200	400	800
Example AWS Instance	m5.large	m5.xlarge	m5.2xlarge	m5.4xlarge	m5.8xlarge
Example Azure Instance	Standard_D2_v3	Standard_D4_v3	Standard_D8_v3	Standard_D16_v3	Standard_D32_v3
Example GCP Instance	n2-standard-2	n2-standard-4	n2-standard-8	n2-standard-16	n2-standard-32

vSensor performance will vary by CPU speed and the nature of the traffic - estimated sizings are provided for guidance only.

If your estimated traffic ingestion is larger than the maximum example above, we recommend using multiple vSensors instead of further scaling a single vSensor. In cloud environments, consider using Darktrace Quick Start templates for AWS, Azure and GCP to benefit from autoscaling to reduce costs with traffic sources which vary over time.