Darktrace Sensors & Modules: Protecting the Dynamic Workforce

Darktrace's Enterprise Immune System can be deployed in a variety of form factors to provide unified and bespoke protection of your dynamic workforce and diverse digital infrastructure. By deploying Darktrace Sensors and Modules, the Enterprise Immune System can scale linearly to consume traffic at relevant choke points and analyze behavior across cloud and SaaS services, remote offices, and core locations both on and off the VPN.

When deployed in real-world environments, Darktrace's Cyber AI is not only self-learning, but also agnostic to diverse data sources. This unique design principle enables the system to continuously analyze raw traffic from across the digital business to learn a joined up, multi-dimensional understanding of the normal 'patterns of life' of your entire organization. To capture this traffic, the following Darktrace Sensors and Modules operate in a decentralized fleet and feed data to a central Darktrace cloud or on-premise instance for analysis.

Sensor & Module Types

Network Coverage – To cover IT, OT, and IoT environments, Darktrace can deploy Physical or Virtual Sensors to ingest raw traffic via a SPAN port or network tap. The number and size of sensors required depends on the peak volume of traffic in that part of the organization. In industrial environments, Darktrace's self-learning AI allows it to learn 'normal' for radically different technologies and deployment types, from decades-old PLCs to distributed sensors and industrial IoT.

Client Coverage – Darktrace Client Sensors can be deployed on the endpoint to extend visibility to branch offices and remote workers off the VPN. This allows the system to analyze real-time traffic of remote workers in the same way it analyzes full traffic in the corporate network, correlating a web of connections to learn an evolving understanding of workforce behavior.

Cloud & SaaS Coverage – Darktrace also provides native coverage of cloud and SaaS services from Salesforce and Dropbox, to AWS and Azure.

Software-as-a-Service (SaaS) – Provider-specific Darktrace SaaS Modules deliver unified visibility across cloud-based collaboration and workforce platforms. SaaS Modules can be deployed remotely and work by interacting with the security APIs of the relevant SaaS solutions, ingesting login and data access events and correlating them with 'patterns of life' in the rest of the organization. Popular deployment scenarios include SaaS Modules for Microsoft 365 (SharePoint, Exchange, etc.), Salesforce, Box, Dropbox, and G Suite.

Infrastructure-as-a-Service (IaaS) – Depending on the deployment scenario and CSP, Darktrace coverage in IaaS environments can include 'vSensors' and 'osSensors' that ingest real-time cloud traffic, as well as 'Security Modules' that ingest event logs highlighting admin activity, such as logins and resource creations.

In AWS, Azure, and GCP, vSensors capture real-time traffic directly from AWS VPC Traffic Mirroring, the Azure vTAP, and GCP Packet Mirroring, respectively. The receiving vSensor processes the data and feeds it back to a central Darktrace instance for analysis. To cover other IaaS environments (e.g. Alibaba Cloud, Rackspace, and others), osSensors are installed on each cloud endpoint and configured to send intelligent copies of cloud traffic to a local vSensor, and in turn, to a central Darktrace instance. Darktrace can also capture container traffic in Docker and Kubernetes via a specialized osSensor, which similarly feeds data to a local vSensor and Darktrace instance for analysis.