Proof of Value:
Darktrace Cyber AI for Cloud and SaaS

The Immune System Approach

The Darktrace Cyber AI Platform delivers total cloud and SaaS coverage, giving customers an immune system approach to security no matter where their infrastructure extends.

The intricate patchwork of services and platforms that compose the cloud makes security in this area increasingly complex. While the cloud allows for incredible innovation, it has also expanded the attack surface at an alarming rate and rendered the traditional paradigm of the network border obsolete.

Prior tools and practices for cloud security are often too slow, siloed, and static to recognize the subtle signs of a novel or advanced attack. Neither cloud-native nor third-party security controls have the enterprise-wide insight and autonomous adaptability that are necessary to defend hybrid and multi-cloud environments.

It takes the immune system approach offered by the Darktrace Cyber AI Platform to secure digital ecosystems that operate across a wide range of cloud and SaaS services. Darktrace uses self-learning AI to continuously learn what normal 'patterns of life' look like for every user, device, virtual machine, and container across an organization. By actively developing a bespoke understanding of 'self,' Darktrace can identify the subtle anomalies that point to an advanced attack, without any pre-defined assumptions of 'good' or 'bad.' Darktrace Cyber AI is the only security solution that learns 'on the job', continuously adapting as your business evolves - a critical feature given the speed and scale of development in the cloud.

Correlating Across Environments

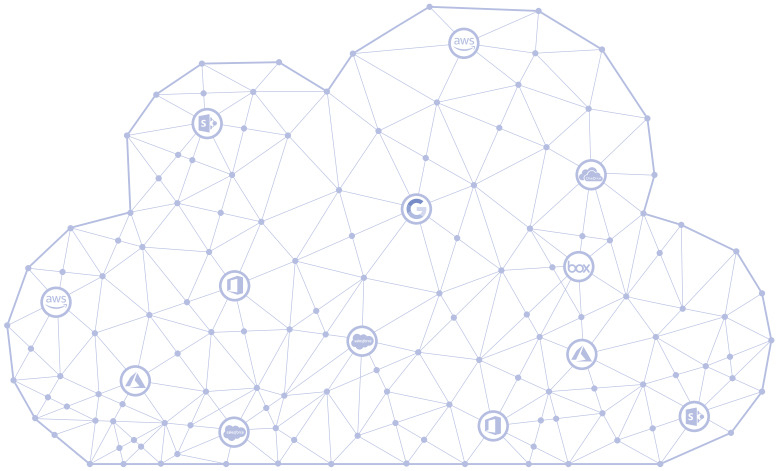
Unified visibility and multi-dimensional insight are the keys to ensuring protection for organizations that leverage the cloud. Darktrace Cyber AI correlates activity across SaaS applications like Salesforce and Microsoft 365, cloud services like AWS and Azure, and all on- and off-premise digital infrastructure. With this wide lens, Darktrace stitches together seemingly disparate events into a cohesive narrative, allowing you to see that unremarkable behavior viewed in isolation may point to a greater picture of malicious activity.

Defense Against Every Threat

While pre-programmed point solutions can complement this approach, Darktrace Cyber AI is the only proven technology to stop the full range of cyber-threats in the cloud, from malicious insiders or attackers with compromised credentials, to critical misconfigurations that expose data and networks.

Just as the sheer scale of cloud and SaaS environments offers us unprecedented efficiency, it also lets threat actors launch machine-speed attacks that inflict damage at a staggering rate. Once an attack in the cloud is ongoing, it might take just a few seconds to infect dozens of cloud-hosted servers, or to inflate an organization's cloud footprint to the point of costing the company millions.

To avoid massive loss of data or damage to critical infrastructure, organizations require the machine-speed security offered by the Darktrace Cyber AI Platform. For truly complete protection, Antigena Autonomous Response gives defenders 24/7 security with the ability to autonomously stop attacks.



The Proof of Value

The Darktrace Proof of Value (POV) is a 30-day, no-fee, no-obligation trial that gives clients the opportunity to see how Darktrace cloud and SaaS coverage works directly for their digital infrastructure. By deploying a Darktrace probe, customers can gain full visibility of their cloud and SaaS environments and leverage enterprise-wide insight to piece together the subtle signs of an advanced attack – no matter where the signs are made manifest.

Darktrace is compatible with all major cloud providers and SaaS applications, and requires no pre-input or configuration. Coverage is extremely flexible, with bespoke deployments available for digital infrastructures of all shapes and sizes. The technology easily integrates with SIEM dashboards and SOC environments, allowing security teams to adopt Darktrace without changing existing business processes.

If desired, organizations can easily extend Darktrace's cloud and SaaS coverage into the on-premise network. Critically, behaviors across your hybrid and multi-cloud environment will be visualized in a unified view and dynamically correlated for comprehensive visibility and detection.

> "Darktrace AI adapts while on the job, illuminating our network and cloud infrastructure in real time, and allowing us to defend the cloud with confidence."
>
> **CISO, Aptean**

POV Benefits

Enterprise-Wide Visibility and Insight

As part of the POV, Darktrace provides unified visibility and insight into the digital environment in which it's deployed. With access to the Cyber AI Platform's Threat Visualizer, customers can view, investigate, and play back security incidents. The Threat Visualizer reveals how Darktrace's self-learning AI applies crucial enterprise-wide context to identify malicious behavior, stitching together a cohesive narrative when it comes to the complex patchwork of cloud and SaaS services.

Machine-Speed Adaptability and Response

The speed and scale of development in cloud environments requires machine-speed security that continuously adapts to your organization. With the POV, defenders can leverage an immune system that evolves with their digital infrastructure, recognizes the subtle anomalies associated with an emerging attack in real time, and stops threats before they escalate into crises.

Threat Intelligence Reports (TIRs)

During the Darktrace Cloud and SaaS deployment POV, clients receive three Threat Intelligence Reports (TIRs). Produced by Darktrace's world-class Cyber Analyst team, the TIRs summarize and assess the discoveries made each week of the POV, helping security teams and executives understand and evaluate their organization's current threat level.

Running a Cloud and SaaS POV

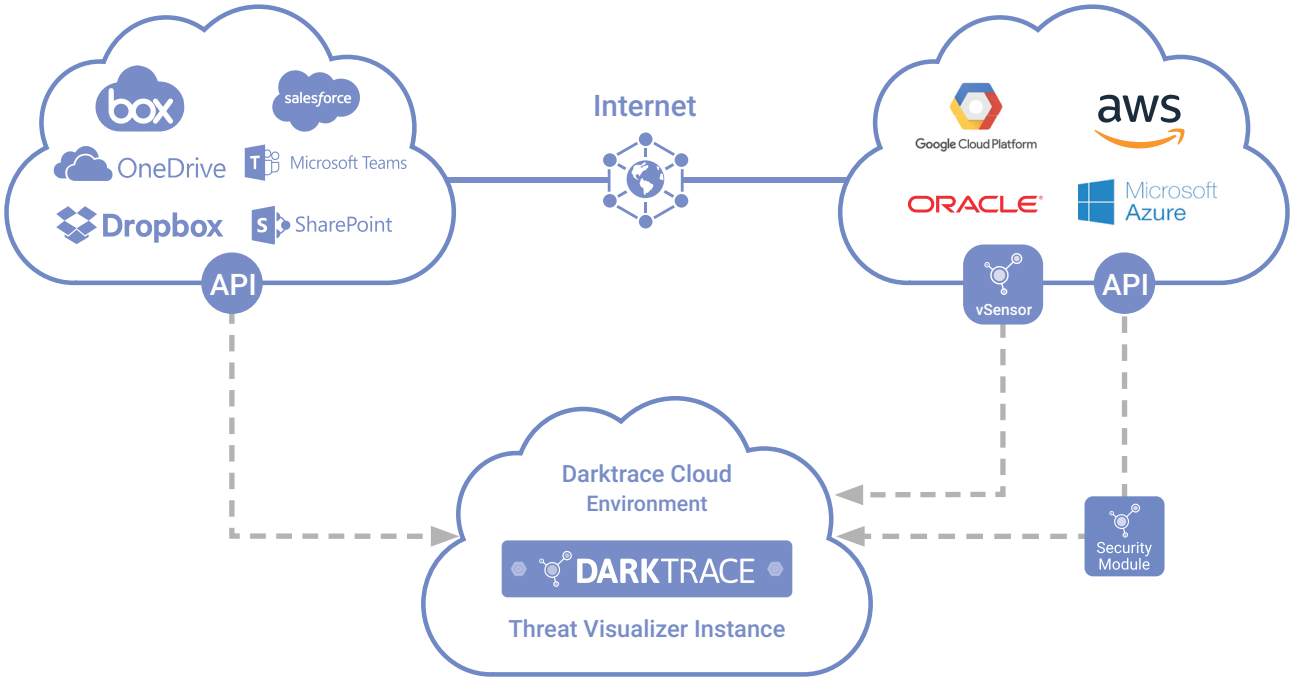
Cloud and SaaS POVs are remarkably straightforward and include a range of deployment scenarios:

Cloud-Only (IaaS and/or SaaS) – For cloud-only deployments, the Darktrace platform manages a cloud-based Darktrace instance, which receives traffic from sensors deployed in the customer's IaaS and/or SaaS environments. The Darktrace cloud instance is hosted in Darktrace's own AWS environment.

For IaaS environments, Darktrace deploys a local 'vSensor' (virtual probe) in each cloud environment. The vSensor captures real-time traffic in AWS, Azure, and GCP, from AWS VPC Traffic Mirroring, the Azure vTAP, and GCP Packet Mirroring, respectively. The receiving vSensor processes the data and feeds it back to the cloud-based Darktrace instance. AWS, GCP, and Azure customers additionally have the option of deploying a 'Darktrace Cloud Module' to monitor IaaS management and data events at the API level, such as logins, editing virtual servers, or creating new access credentials.

To cover other IaaS environments (e.g. Alibaba Cloud, Rackspace, and others), Darktrace's lightweight host-based 'osSensor s' are installed on each cloud endpoint and configured to send intelligent copies of cloud traffic to the local vSensor deployed in the same cloud environment, which then feeds it back to the cloud-based Darktrace instance for analysis. 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. These agents are free to use and can supplement the use of mirroring services that a customer might be paying for.

For SaaS applications, provider-specific Darktrace SaaS Modules are enabled on the Darktrace cloud-based instance and will interrogate the security APIs of the relevant SaaS solutions. SaaS solutions covered include Salesforce, Microsoft 365, OneDrive, SharePoint, Box, Dropbox, G Suite, Jumpcloud, and Egnyte.



Hybrid Cloud (IaaS) – For hybrid IaaS deployments, Darktrace will similarly deploy vSensors and osSensor s as appropriate. Cloud traffic and event data is then fed to a Darktrace probe in the cloud or on-premise network. For the latter scenario, Darktrace will deploy a physical appliance that ingests real-time network traffic via a SPAN port or network tap.

Hybrid Cloud (SaaS) – For hybrid IaaS deployments, Darktrace will similarly deploy vSensors, osSensors, and Cloud Modules as appropriate. SaaS data is then analyzed and correlated with traffic and user behaviors across the corporate network. These Security Modules allow Darktrace Cyber AI to see what remote users do, even when they aren't connected to the corporate network.

Sizing for Darktrace Deployment

In order for a customer with a cloud-only environment to trial Darktrace Cyber AI Cloud and SaaS coverage, customers must participate in a sizing call before the deployment. Darktrace requires details on:

- The number of VPCs and VMs
- Device count/bandwidth estimates
- Type of environment (e.g., production or development)
- SaaS applications to monitor
- Expected install date

The sizing call is a key step in running a POV that requires a cloud-hosted Darktrace instance, as we want to avoid oversizing and appropriately allocate resources within the Darktrace AWS instance. Darktrace requires at least two days' notice to deploy the cloud instance.

box
salesforce
Google Cloud Platform
G Suite
Microsoft Azure
aws
Microsoft 365
Dropbox
EGNYTE
JumpCloud
Directory-as-a-Service

> Darktrace represents a new frontier in AI-based cyber defense. Our team now has complete real-time coverage across our SaaS applications and cloud containers.
>
> **– CIO, City of Las Vegas**

For more information:

Book a demo now

Download Antigena White Paper

Hear from our customers