Darktrace for Cloud & SaaS

As organizations increasingly rely on cloud services and SaaS applications to streamline business practices and increase flexibility, the challenge of securing critical data has taken on a new dimension.

These distributed infrastructures can introduce new attack vectors and create dangerous blind spots. Indeed, fear of security breaches can be a significant factor holding back cloud adoption.

It is critical to have visibility of all cloud and SaaS services, in order to reduce risk and identify atypical or suspicious behavior that may indicate a security breach or cyber-attack.

Darktrace's technology covers cloud environments and SaaS, protecting critical data and users far beyond the boundaries of the traditional network perimeter. What is more, all activity is visualized through a single interface, the Threat Visualizer, allowing security teams to see and manage their entire digital estate holistically

Darktrace Cloud

Darktrace Cloud delivers Darktrace's world-leading cyber-threat detection and real-time visibility to the cloud, and is compatible with all major cloud providers, including AWS, Google Cloud Platform, and Microsoft Azure.

Seamlessly integrating with Darktrace Enterprise, Darktrace Cloud extends visibility into otherwise unseen parts of your network, giving security professionals rich insights and a real-time overview of activity in the cloud. Whether faced with an insider threat, an attacker targeting data in the cloud, or a significant misconfiguration that could be exploited in the future, Darktrace Cloud helps eliminate blind spots and protect your data, wherever it resides.

Darktrace Cloud is 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 Cloud is robust and resilient, providing end-to-end coverage across the digital business.

Key Benefits

Removes Blind Spots

Provides complete visibility of third-party cloud environments and SaaS applications, detecting threats at an early stage and putting security back into the hands of the user.

Installed in Minutes

Easy to deploy with minimal performance impact, delivering end-to-end coverage in a single pane of glass.

Google Cloud Platform

Microsoft Azure

rackspace the open cloud company

amazon web services EC2

Real-World Threat Discovery

At a financial services company, Darktrace Cloud detected a brute-force attack against a server within the cloud infrastructure, which was accidentally exposed to the Internet.

The connection between the cloud and physical network segments meant that the network as a whole would have been compromised had the attack succeeded. Not only did the activity pose a significant security risk, but with so many connection attempts being received continuously, there was also the real possibility of a denial of service affecting the server.

Darktrace SaaS

Darktrace SaaS leverages Darktrace's self-learning technology to detect developing threats and anomalous behavior in SaaS applications, such as Salesforce, Dropbox, and Office 365.

By accessing log information and rich security insights via APIs, Darktrace SaaS spots genuine anomalies and subtle threats, including highly unusual file changes, user logins, and data transfers.

For example, if an employee starts downloading abnormally large volumes of data or transferring unusual file types, Darktrace SaaS would analyze the behavior against a range of weak indicators and determine whether the activity is anomalous and potentially threatening. Darktrace SaaS interacts seamlessly with SaaS applications via HTTPS requests, allowing user interactions to be processed and monitored in real time, whether they originate inside the network or from remote locations.

Darktrace SaaS covers all major SaaS providers, including Salesforce, Box, G Suite, AWS, Dropbox, and Microsoft Office 365.

box

salesforce

Dropbox

Office 365

G Suite

Darktrace as a Service

If your organization has internal users that access data in the cloud, and does not have an 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.

> When we activated Darktrace Cloud, it was like flipping on a switch in a dark room.
>
> **- TRJ Telecom**

Real-World Threat Discovery

A disgruntled employee decided to spend their last day with a company attempting to steal a large volume of customer data by uploading it to Dropbox. Dropbox was widely used at the company, so the employee believed that their activity would go unnoticed.

While legacy tools would not have recognized the behavior as threatening, Darktrace SaaS accurately detects even the slightest deviations from normal. As a result, the illegitimate transfers were identified before the employee could successfully steal the information.

Contact Us

North America: +1 (415) 229 9100

Latin America: +55 (11) 97242 2011

Europe: +44 (0) 1223 394 100

Asia Pacific: +65 6804 5010

info@darktrace.com