

# DARKTRACE/CLOUD AWS MODULE

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How It Works

The Darktrace/Cloud AWS module monitors management and administration activity via interaction with AWS CloudTrail. AWS CloudTrail audits Management Events and Data Events (S3/Lambda) which are compiled into logfiles and stored in the AWS S3 bucket created during the configuration process. Data is processed directly from the CloudTrail logfiles, returned information is therefore limited to the events that AWS chooses to audit for each service via CloudTrail and the data recorded as part of each entry. The module can monitor AWS services including:

- EC2
- IAM
- S3
- VPC
- Lambda

Full information about AWS services which support CloudTrail monitoring can be found in the relevant AWS documentation. The AWS module does not currently support the monitoring of CloudTrails created via AWS ControlTower.

AWS CloudTrail events are produced up to 15 minutes after activity occurs. In high-traffic environments, the volume of events that must be retrieved in each polling cycle may result in latency between CloudTrail log production and appearance in the Threat Visualizer.

The diverse event types produced by AWS are organized by Darktrace into categories based on the action type and the AWS service that generates it. These categories then appear as metrics in the Darktrace Threat Visualizer which can be used for modeling.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.



## Considerations

AWS works on a 'pay-as-you-go' policy for event logging and API calls. Hence there are small charges involved in CloudTrail detecting events, the API request performed by the Darktrace appliance to get these events and storage costs for the event logs. Costs are dependent upon the amount of activity within AWS, the interval between Darktrace polls and any additional configuration settings applied.

Darktrace/Cloud AWS module also automatically removes associated log files from S3 a day after they are generated, thereby preventing significant data build up. This setting can be disabled via the System Config page and is not available in **Restricted Mode**.

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

## Write-Only Mode

**Write-Only Mode** filters CloudTrail to only record AWS "Write" events, significantly decreasing processing time in busy environments and reducing costs for log storage, API requests made, and number of events recorded. The filter utilizes the "read-only" and "write-only" settings available in AWS CloudTrail - more information can be found in the AWS documentation.

To use this mode, "Automatically Configure CloudTrail" and "CloudTrail Write Event Filter" must be enabled on the Darktrace System Config page. The events logged can also be customized during the creation of the CloudTrail.

## Permissions

Darktrace/Cloud AWS module requires the linked IAM user to have permission to see and modify AWS CloudTrails and have full access to the S3 bucket associated with monitoring. These permissions allow the module to access AWS CloudTrail logfiles, reconfigure the CloudTrail if a misconfiguration is detected, and modify the bucket containing logfiles to ensure there is not an increasing buildup of old logs. Detailed example policy statements are provided in the configuration guide.

*Programmatic MFA is also supported on the linked IAM user from Darktrace Threat Visualizer v5.2.*

## Restricted Mode

The module can also be deployed in a restricted mode where the linked IAM user is solely granted "read" and "list" permissions to the S3 bucket containing the monitoring logs, but is not granted access to CloudTrail.

## Automatic Account Retrieval

Account IDs are used to retrieve logs from CloudTrail; the module will only retrieve logs for accounts it is aware of. The module can automatically retrieve an up-to-date list of all accounts under the organization if provided an IAM user with the **organizations:ListAccounts** permission. This list can also be provided manually on the Darktrace System Config page.

## Deployment Process

The deployment process for Darktrace/Cloud AWS module is relatively straightforward and is described in more detail in Deploying Darktrace/Cloud AWS module. For deployments in **Restricted Mode** or with alternative configuration settings, these steps may differ.

For default configuration, the process outline is:

1. Create a new Trail (in AWS CloudTrail); by default the Trail applies to all regions and outputs all logfiles into an S3 bucket.
2. Create an IAM user that has permission to access and modify the CloudTrail and associated S3 bucket.
3. Input configuration details, such as the new IAM user access keys, into the Darktrace Threat Visualizer configuration page.

**After performing these steps, your Darktrace/Cloud AWS module will be authorized and begin monitoring events immediately.**