v3.3.2 Release Notes for Forcepoint Behavioral Analytics

Release Notes | Forcepoint Behavioral Analytics | v3.3.2 | 21-Aug-2020

Use the Release Notes to find information about what's new and improved in Forcepoint Behavioral Analytics version 3.3.2.

Features

Certified DDP Compatibility

As part of the Human Point System, Forcepoint Behavioral Analytics version 3.3 is certified to deliver Dynamic Data Protection (DDP) with the following combinations of Forcepoint DLP:

Forcepoint Behavioral Analytics	Forcepoint DLP	Forcepoint One Endpoint
3.3.2	8.7.1	20

DDP requires the use of the Forcepoint One Endpoint as the Endpoint Security solution. DDP is now supported on macOS 10.15 (Catalina).

Ingest all DLP Incidents in Forcepoint DDP

The system can now ingest incidents without their associated events if they are lost or do not come within 60 seconds of each other. If this happens, a forged event is reconstructed from the incident as well as possible.

The new incidents channel types that will be ingested as Incident mode are:

- "CASB_NEAR_REAL_TIME" (Forcepoint DLP Cloud Applications)
- "EMAIL" (Email Gateway, whether through Protector or Forcepoint Email Gateway)
- "HTTP" (Forcepoint Web Security proxy HTTP channel, or ICAP integration with 3rd party proxy through Protector)

- "HTTPS" (Forcepoint Web Security Proxy HTTPS channel)

MDS endpoint requires credentials/proper authentication

The MDS endpoint /reference/actor/{id}/report/rql has been secured so only users with proper authentication can access the endpoint entity data.

Improved informative messages on the Analytic Dashboard and Entity Timeline

The Analytic Dashboard and Entity Timeline have been updated to provide clear informative messaging when data does not appear. These messages explain why analytic data may not displayed.

Grafana has been enhanced

Grafana has a new metric for the number of merged entities over time. A Graphite metric has been added to monitor the bridged merging of two or more entities into one when aliases overlap.

A Kafka dashboard has also been added to the monitoring stack to show up-to-date information on the Kafka instance.

Error index has been enhanced

Mime4J "warnings" have been removed from the error index. REFC-822 parser debug is now sent to the system logs rather than to an Elasticsearch index.

Known Issues

A list of resolved and known issues in this release is available to Forcepoint Behavioral Analytics customers here.

If you are not currently logged in to the Forcepoint support website, clicking the link brings up a My Account login prompt. Log in to view the list.