Consenso esplicito e abilitazione della ricerca avanzata orbitale nell'AMP per la distribuzione degli endpoint (per i clienti esistenti dall'8 gennaio 2020)

Sommario

Passaggio 1: Consenso esplicito alla ricerca avanzata orbitale
Passaggio 2: Abilita ricerca avanzata orbitale in un criterio esistente
Passaggio 3: Abilita ricerca avanzata orbitale in un nuovo criterio e gruppo di computer (facoltativo)
Passaggio 4: Esplora la Console orbitale

Cisco ha recentemente lanciato due pacchetti per AMP for Endpoints: Caratteristiche e vantaggi. La ricerca avanzata orbitale è una caratteristica chiave del pacchetto Advantage. Tutti i clienti esistenti alla data di lancio (8 gennaio 2020) possono scegliere di utilizzarlo gratuitamente per il resto della durata del contratto. Le domande frequenti (FAQ) contengono ulteriori informazioni sui pacchetti e su come questi influiscono sui clienti esistenti alla data di lancio.

Orbital Advanced Search è una nuova funzionalità avanzata di Cisco AMP for Endpoints progettata per semplificare le indagini di sicurezza e la ricerca di minacce fornendo oltre un centinaio di query di catalogo. In questo modo è possibile eseguire rapidamente query complesse su uno o tutti gli endpoint. In questo modo è possibile ottenere una maggiore visibilità su quanto è accaduto in un endpoint in un determinato momento, eseguendo un'istantanea dello stato corrente.

Con la ricerca avanzata orbitale, è possibile eseguire le seguenti attività importanti in modo migliore e più rapido:

- **Caccia alle minacce**. È possibile cercare in tempo reale artefatti dannosi per accelerare la ricerca di minacce.
- **Indagine sull'incidente**. Individuazione rapida della causa principale dell'incidente, con conseguente riduzione dei tempi di risoluzione.
- **Operazioni IT**. È sufficiente tenere traccia dello spazio su disco, della memoria e di altri elementi relativi alle operazioni IT.
- **Vulnerabilità e conformità**. Verificare rapidamente lo stato dei sistemi operativi per verificare la presenza di versioni e aggiornamenti delle patch, assicurandosi che gli endpoint siano conformi alle policy correnti.

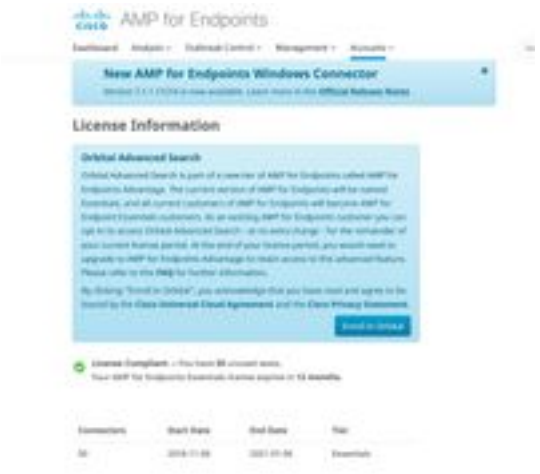
Questo documento è una guida dettagliata per illustrarvi come scegliere la nuova funzionalità e abilitarla sugli endpoint. È disponibile anche una Guida Orbitale. I clienti di AMP for Endpoints possono abilitare la ricerca avanzata Orbital facilmente se sugli endpoint è già installato un connettore (7.1.5 o superiore). Vedere l'argomento della Guida di AMP for Endpoints Console su Orbital per la versione più recente di Connector e altre informazioni. Orbital Advanced Search è attualmente supportato sugli host Windows 10 a 64 bit con versione 1703 (Creators Update) o successiva.

Una volta completati questi passaggi, vedere la guida introduttiva per una descrizione più

dettagliata di come iniziare a utilizzare la funzione di ricerca avanzata Orbital.

Passaggio 1: Consenso esplicito alla ricerca avanzata orbitale

Se non si è precedentemente registrati alla versione beta di Orbital Advanced Search o si è scelto esplicitamente di farlo, è possibile farlo dalla pagina Informazioni sulla licenza nella console di AMP for Endpoints. Per effettuare il consenso esplicito a Orbital Advanced Search, accedere alla console AMP for Endpoints e selezionare l'elenco a discesa **Account > Informazioni licenza**. In questa pagina è possibile fare clic su **Registra in Oracle** per accedere a questa funzionalità.



NOTA: È necessario essere un utente privilegiato (admin) per scegliere di partecipare a Orbital Advanced Search.

Passaggio 2: Abilita ricerca avanzata orbitale in un criterio esistente

Se sugli endpoint è già installato un connettore (versione 7.1.5 o successiva), è possibile abilitare la ricerca avanzata orbitale in un criterio esistente per gli endpoint.

- Accedere alla console AMP for Endpoints. In Gestione > Criteri, selezionare il criterio in cui si desidera abilitare la ricerca avanzata orbitale e fare clic sul pulsante **Modifica** per aprire la **Modifica criterio** in *Impostazioni avanzate* selezionare **Orbitale** e verificare che la ricerca avanzata orbitale sia abilitata. È necessario selezionare la casella **Attiva ricerca orbitale avanzata**. In caso contrario, selezionare la casella per attivarla.

A questo punto tutti i connettori installati con questo criterio attiveranno automaticamente la ricerca avanzata orbitale sull'endpoint.

Passaggio 3: Abilita ricerca avanzata orbitale in un nuovo criterio e gruppo di computer (facoltativo)

Come descritto in precedenza, dopo aver attivato la ricerca avanzata orbitale in un criterio esistente, per tutti i connettori che utilizzano tale criterio verrà attivata la ricerca avanzata orbitale e per tutti i nuovi connettori che utilizzano tale criterio verrà attivata anche la ricerca avanzata orbitale. Ad esempio, se nel gruppo "Proteggi" sono presenti 1000 computer, la semplice attivazione della ricerca avanzata orbitale in tale criterio attiverà automaticamente la ricerca avanzata orbitale su tali endpoint, a condizione che sia distribuito Connector versione 7.1.5 o successive.

La creazione di nuovi criteri e gruppi è facoltativa. Tuttavia, se si desidera utilizzare la ricerca avanzata orbitale su un gruppo specifico di endpoint utilizzando un nuovo criterio e gruppo, è sufficiente seguire la documentazione del prodotto per creare un nuovo criterio e/o gruppo e verificare che la ricerca avanzata orbitale sia abilitata nel criterio come mostrato in precedenza.

Passaggio 4: Esplora la Console orbitale

Dopo aver abilitato la ricerca avanzata orbitale in un criterio con una versione di Connector successiva alla 7.1.5 installata in almeno un endpoint, è ora possibile eseguire query su un endpoint per raccogliere informazioni.

- Andare a **Gestione > Computer** e individuare un computer con Ricerca avanzata orbitale Espandere il riquadro e fare clic su **Query orbitale**. (È possibile accedere alla console Orbital anche selezionando **Analisi > Ricerca avanzata orbital**).
- La console orbitale viene caricata in una nuova scheda del browser. Se necessario, fare clic su **Log in with Cisco Security (Accedi con Cisco Security)** per eseguire l'autenticazione utilizzando le credenziali della console AMP esistente.

NOTA: È inoltre possibile accedere a Orbital Advanced Search direttamente all'indirizzo https://orbital.amp.cisco.com

- Nel campo **Endpoints** vengono visualizzati i computer sui quali verrà eseguita la query. È possibile immettere un GUID specifico o **tutti** in questo campo per eseguire una query su tutti gli endpoint dell'organizzazione per i quali è abilitata la ricerca avanzata orbitale. Se si desidera eseguire un campionamento casuale degli endpoint, fare clic sui puntini di sospensione (...) per aprire la finestra di dialogo **Aggiungi endpoint casuali**.
- Èpossibile immettere istruzioni SELECT personalizzate nel campo **SQL** oppure fare clic su **Sfoglia catalogo query** per aprire il **catalogo query**, che contiene decine di query che è possibile aggiungere alla query. **Non è necessario sapere come scrivere un'istruzione SQL SELECT per utilizzare Orbital.**

- Fare clic su **Query**. La query viene eseguita sugli endpoint specificati e i risultati vengono visualizzati nel riquadro di destra. È possibile modificare la query ed eseguirla nuovamente. Potete scaricare i risultati. È possibile salvare la query come job da eseguire in base a una pianificazione configurabile.
- Per ulteriori informazioni introduttive su Orbital Advanced Search, consultare la Guida introduttiva