Anmeldung und Aktivierung der erweiterten Orbital-Suche bei der Bereitstellung von AMP für Endgeräte (für bestehende Kunden, gültig ab 8. Januar 2020)

Inhalt

Cisco hat kürzlich zwei Pakete für AMP für Endgeräte vorgestellt: Grundlagen und Vorteile. Orbital Advanced Search ist eine Schlüsselfunktion im Advantage-Paket. Alle bestehenden Kunden können ab dem Datum der Markteinführung (8. Januar 2020) die kostenlose Nutzung für die restliche Vertragslaufzeit abwählen. Diese FAQ enthält weitere Informationen zu den Paketen und deren Auswirkungen auf bestehende Kunden zum Zeitpunkt der Markteinführung.

Orbital Advanced Search ist eine neue erweiterte Funktion in Cisco AMP für Endgeräte, die Sicherheitsanalysen und die Nachverfolgung von Bedrohungen durch die Bereitstellung von mehr als hundert Katalogabfragen vereinfacht. So können Sie komplexe Abfragen schnell für alle oder alle Endpunkte ausführen. Dadurch können Sie jederzeit einen detaillierten Überblick über die Ereignisse an jedem Endpunkt erhalten, indem Sie einen Snapshot des aktuellen Status erstellen.

Mit Orbital Advanced Search können Sie die folgenden wichtigen Aufgaben schneller und besser erledigen:

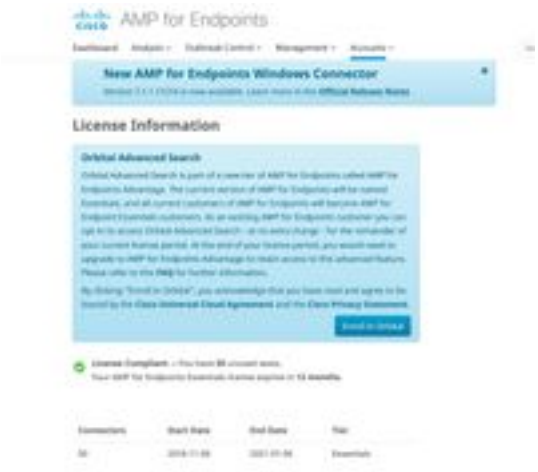
- **Nachverfolgung von Bedrohungen**. Suchen Sie nach schädlichen Artefakten nahezu in Echtzeit, um Ihre Suche nach Bedrohungen zu beschleunigen.
- **Incident Investigation**. Schnelle Behebung der Ursache des Vorfalls
- **IT-Betrieb**. Verfolgen Sie einfach den Speicherplatz, den Arbeitsspeicher und andere IT-Betriebsartefakte.
- **Schwachstellen und Compliance**: Prüfen Sie schnell den Status von Betriebssystemen auf Versionen und Patch-Updates, um sicherzustellen, dass Ihre Endgeräte die aktuellen Richtlinien einhalten.

Dieses Dokument enthält eine schrittweise Anleitung, wie Sie sich für das neue Feature anmelden und es auf Ihren Endgeräten aktivieren können. Ein vollständiges Benutzerhandbuch ist ebenfalls erhältlich. AMP für Endgeräte-Kunden können die erweiterte Orbital-Suche ganz einfach aktivieren, wenn auf Ihren Endgeräten bereits Connector (7.1.5 oder höher) installiert ist. Die aktuellste Connector-Version und weitere Informationen finden Sie im Hilfethema zu AMP für Endgeräte-Konsolen im Orbital. Orbital Advanced Search wird derzeit auf 64-Bit-Windows 10-Hosts unterstützt, auf denen Version 1703 (Creators Update) oder höher ausgeführt wird.

Sobald Sie diese Schritte abgeschlossen haben, finden Sie eine ausführlichere Beschreibung der ersten Schritte mit der Schnellstartanleitung Orbital Advanced Search.

Schritt 1: Erweiterte Suche im Orbital-Modus

Wenn Sie sich noch nicht für die Beta-Version der orbitalen erweiterten Suche angemeldet oder sich ausdrücklich dafür entschieden haben, können Sie dies auf der Seite mit den Lizenzinformationen in der AMP-Konsole für Endgeräte tun. Melden Sie sich bei der AMP für Endpoints-Konsole für die erweiterte Orbital-Suche an, und wählen Sie das Dropdown-Menü **Accounts > License Information (Konten > Lizenzinformationen)** aus. Auf dieser Seite können Sie auf **In Orbital anmelden** klicken, um Zugriff auf diese Funktion zu erhalten.



HINWEIS: Sie müssen ein privilegierter (Administrator-)Benutzer sein, um sich bei der Orbital Advanced Search anzumelden.

Schritt 2: Aktivieren der digitalen erweiterten Suche in einer bestehenden Richtlinie

Wenn auf Ihren Endpunkten bereits Connector (Version 7.1.5 oder höher) installiert ist, können Sie die Orbital Advanced Search in einer vorhandenen Richtlinie für Ihre Endpunkte aktivieren.

- Rufen Sie die AMP für Endpoints-Konsole auf. Wählen Sie unter **Management > Policies** (Verwaltung > Richtlinien) die Richtlinie aus, in der die erweiterte Orbital-Suche aktiviert werden soll, und klicken Sie auf die Schaltfläche **Bearbeiten**, um die **Richtlinie** unter *Erweiterte Einstellungen* zu öffnen**, wählen Sie Orbital aus, und überprüfen Sie, ob die orale erweiterte Suche aktiviert ist.** Das Kontrollkästchen **Enable Orbital Advanced Search** (Erweiterte Suche aktivieren) sollte aktiviert sein. Ist dies nicht der Fall, aktivieren Sie das Kontrollkästchen.

An diesem Punkt werden alle Connectors, die mit dieser Richtlinie installiert sind, automatisch die Orbital Advanced Search für diesen Endpunkt aktivieren.

Schritt 3: Aktivieren der digitalen erweiterten Suche in einer neuen Richtlinie und Gruppe von Computern (optional)

Wie oben beschrieben, wird bei allen Connectors, die diese Richtlinie verwenden, nach Aktivierung der Orbital Advanced Search-Funktion in einer vorhandenen Richtlinie die Funktion "Orbital Advanced Search" aktiviert. Bei allen neuen Connectors, die Sie installieren, die diese Richtlinie verwenden, ist die Funktion "Orbital Advanced Search" ebenfalls aktiviert. Wenn Sie z. B. 1000 Computer in Ihrer "Protect"-Gruppe haben, wird die automatische Suche nach Orbital Advanced Search auf diesen Endpunkten aktiviert, solange Connector 7.1.5 oder höher bereitgestellt wird.

Das Erstellen neuer Richtlinien und Gruppen ist optional. Wenn Sie jedoch Orbital Advanced Search für eine bestimmte Gruppe von Endpunkten unter Verwendung einer neuen Richtlinie und Gruppe verwenden möchten, folgen Sie einfach der Produktdokumentation, um eine neue Richtlinie und/oder Gruppe zu erstellen und sicherzustellen, dass Orbital Advanced Search in der oben gezeigten Richtlinie aktiviert ist.

Schritt 4: Entdecken Sie die Orbital Console

Wenn Sie Orbital Advanced Search in einer Richtlinie aktiviert haben, deren Connector-Version höher als 7.1.5 auf mindestens einem Endpunkt installiert ist, können Sie jetzt Abfragen auf einem Endpunkt ausführen, um Informationen daraus zu sammeln.

- Gehen Sie zu **Management > Computers**, und suchen Sie einen Computer mit der Orbital Advanced Search Erweitern Sie den Bereich, und klicken Sie auf **Orbitale Abfrage**. (Sie können auch auf die Konsole Orbital zugreifen, indem Sie **Analysis > Orbital Advanced Search** (**Analyse > Erweiterte Orbital-Suche**) wählen.
- Die Orbital-Konsole wird in eine neue Browserregisterkarte geladen. Klicken Sie ggf. auf **Bei Cisco Security anmelden**, um die Authentifizierung mithilfe der vorhandenen AMP Console-Anmeldeinformationen durchzuführen.

HINWEIS: Sie können auch direkt auf die Orbital Advanced Search zugreifen unter https://orbital.amp.cisco.com

- Das Feld **Endpunkte** zeigt die Computer an, die abgefragt werden. Sie können eine bestimmte GUID eingeben oder **alle** in dieses Feld eingeben, um alle Endpunkte in Ihrer Organisation abzufragen, für die die Orbital Advanced Search aktiviert ist. Wenn Sie eine zufällige Auswahl an Endpunkten erstellen möchten, klicken Sie auf die Auslassungszeichen (...), um das Dialogfeld **Zufällige Endpunkte hinzufügen** zu öffnen.
- Sie können benutzerdefinierte SELECT-Anweisungen im **SQL-**Feld eingeben oder auf **Abfrage-Katalog durchsuchen klicken**, um den **Abfragekatalog** zu öffnen, der Dutzende von Abfragen enthält, die Sie der Abfrage hinzufügen können. **Sie müssen nicht wissen, wie Sie eine SQL-SELECT-Anweisung schreiben, um Orbital zu verwenden.**

- Klicken Sie auf **Abfrage**. Die Abfrage wird für die angegebenen Endpunkte ausgeführt, und die Ergebnisse werden im rechten Bereich angezeigt. Sie können die Abfrage bearbeiten und erneut ausführen. Sie können die Ergebnisse herunterladen. Sie können die Abfrage als Auftrag speichern, der auf einer festgelegten Basis ausgeführt werden soll, die Sie konfigurieren können.
- Weitere Informationen zu den ersten Schritten mit der Orbital Advanced Search finden Sie im Quick Start