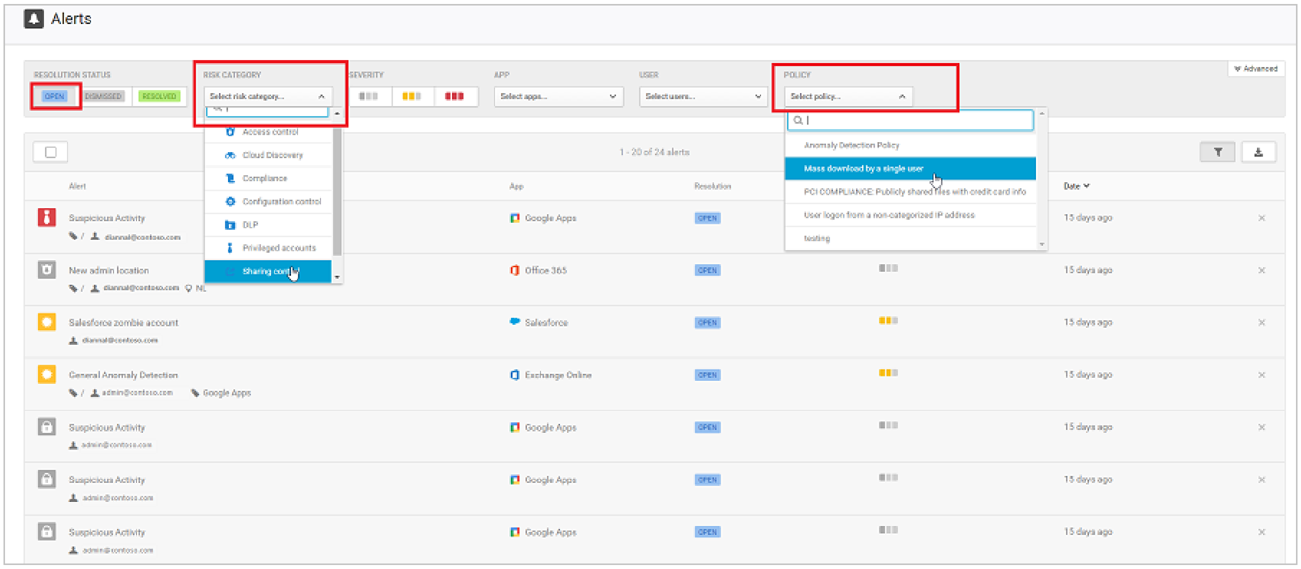
Manage Alerts

Alerts are the entry points to understanding your cloud environment more deeply. You might want to create new policies based on what you find. For example, you might see an administrator signing in from Greenland, and no one in your organization ever signed in from Greenland before. You can create a policy that automatically suspends an admin account when it is used to sign in from that location.

It is a good idea to review all of your alerts and to use them as tools for modifying your policies. If harmless events are being considered violations to existing policies, refine your policies so that you receive fewer unnecessary alerts.

1. Under **Open alerts**, click **View all alerts**. This section of the dashboard provides full visibility into any suspicious activity or violation of your established policies. It then helps you safeguard the security posture you defined for your cloud environment.



Alert	App	Resolution		Date
Suspicious Activity / dlannal@contoso.com	Google Apps	OPEN		15 days ago
New admin location / dlannal@contoso.com NL	Office 365	OPEN	▮▯▯	15 days ago
Salesforce zombie account dlannal@contoso.com	Salesforce	OPEN	▮▮▯	15 days ago
General Anomaly Detection / admin@contoso.com Google Apps	Exchange Online	OPEN	▮▮▯	15 days ago
Suspicious Activity admin@contoso.com	Google Apps	OPEN	▮▯▯	15 days ago
Suspicious Activity admin@contoso.com	Google Apps	OPEN	▮▯▯	15 days ago
Suspicious Activity admin@contoso.com	Google Apps	OPEN	▮▯▯	15 days ago

2. For each alert, you need to investigate and determine the nature of the violation and the required response.

3. When you finish this process, mark the alert as resolved.

There are three types of violations you will need to deal with when investigating alerts:

- **Serious violations**: Serious violations require immediate response.Examples:For a suspicious activity alert, you might want to suspend the account until the user changes their password.For a data leak you might want to restrict permissions or quarantine the file.If a new app is discovered, you might want to block access to the service on your proxy or firewall.
- **Questionable violations**: Questionable violations require further investigation. You can contact the user or the user's manager about the nature of the activity.Leave the activity open until you have more information.
- **Authorized violations or anomalous behavior**: Authorized violations or anomalous behavior can result from legitimate use.Dismiss the alert.

Guided Demonstration - Protect sensitive files in 3rd party cloud services

A guided demonstration is a recorded click-through simulation. You do not use your lab tenant for this demonstration. Instead simply click the link here to launch this demonstration. A focus will appear in the demonstration showing you the next place to click to advance the demonstration.

Scenario:

Contoso wants to use a classification label to ensure confidential documents in Box are protected.

Time required: 4 minutes