Introduction to Rules

F5 Distributed Cloud App Infrastructure Protection (AIP) takes a behavior-based approach to security alerting, governed by rules that focus on events that you consider important. A rule is a statement that tells software what data to look for and how to react to that data. Distributed Cloud AIP uses the rules enabled in your infrastructure to continuously compare event data to alert criteria. When a rule matches alert criteria, then an alert triggers for the event.

To learn more about the different types of rules in Distributed Cloud AIP, see Rule Creation Overview.

> **Important**
>
> The following information is for Distributed Cloud AIP organizations that have migrated to the new Managed Rules functionality. For more information, see Managed Rules: More Details.

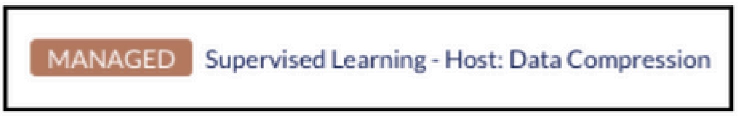
Managed and Unmanaged Rules

Managed Rules

In addition to your existing, custom (unmanaged) rules, Distributed Cloud AIP's new rule functionality includes **managed rules.** Distributed Cloud AIP internally coordinates and monitors these managed rules, which you can leverage in your environment to help you save time on rule creation and management.

Distributed Cloud AIP controls specific fields for managed rules, including the title, description, filter, managed suppressions, and managed classifiers. For more information about which rule fields are fixed and which you can customize, see Anatomy of a Managed Rule.

Managed rules display with the **MANAGED** label in the rules list:



MANAGED Supervised Learning - Host: Data Compression

For more information, see Configure Managed Rules in Your Distributed Cloud AIP Organization.

> **Note**
>
> Managed rules will periodically update to ensure that your organization's rules contain the most accurate and up-to-date information. See Rule Release and Changelog for information about recent changes.

Unmanaged Rules

Unmanaged, or custom, rules are not managed by Distributed Cloud AIP. You can fully customize unmanaged rule titles, descriptions, classifiers, filters, and suppressions to fit your infrastructure's unique needs.

These rules can help you elevate the visibility of security data that matters to you, such as specific user behaviors, container behavior, and/or compliance alignment. Unmanaged rules can also help you to exclude or suppress unactionable or unnecessary data from your environment. For more information about the types of custom rules you can create, see Rule Creation Overview.