



AMEnterprise



Explore Alert Manager Enterprise Features

- Intuitive User Interface
- Notification Schemes (Mail, Slack, and Webhooks)
- Rule Manager for Alert Suppression
- Workflow Action to trigger GET/POST-Requests and Searches
- Alert Aggregation to combine repeating alerts
- Role-Based Access Control
- Multi-Tenancy 💰
- Security Knowledge Pack for Cyber Kill Chain and Mitre Att&ck Framework, NIST, CIS and CVE 💰
- Business hours support available 💰



Download Alert Manager Enterprise from Splunkbase



To try out our premium feature packs, request a free 30-day trial key.

splunk> Partnerverse

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2023 Splunk Inc. All rights reserved.

What is Alert Manager Enterprise?

Datapunctum's Alert Manager Enterprise enables IT Operations and Security teams to manage alerts using Splunk Enterprise and Splunk Cloud.

Add Alert Manager Enterprise's Alert Action to your existing searches and start streamlining your alerts immediately.

Why Alert Manager Enterprise?

Handle the entire lifecycle of an alert, from detection, notification, and initial triage up to root cause analysis and response within a single tool and interface. In addition, AME allows you to go from alert to actionable insight instantly.

Evolve from simple fire-and-forget alerting by leveraging AME's notification schemes to reach important stakeholders using their desired channels.

Implement the need-to-know concept and least privilege principle using role-based access control. AME is built with managed service providers and large enterprises in mind. It allows you to split your alerts into multiple tenants with complete separation.

Use the built-in Security Knowledge Pack to utilize industry-accepted frameworks such as the Unified Cyber Kill Chain, MITRE ATT&CK, CIS Controls, NIST and CVE in your workflow. Enrich your alerts and help your Security specialist classify events more precisely and confidently.

Alert Manager Enterprise supports a wide range of deployment options, from your dockerized development environment to a multi-site search head and indexer cluster.



Reseller:

4Data Solutions
 Zeppelin Building • 3rd Floor • 59-61 Farringdon Road
 London, EC1M 3JB info@4datasolutions.com
 +44 330 128 9180

Datapunctum AG • Badenerstrasse 47 • CH-8004 Zurich info@datapunctum.com
 +41 44 500 73 01

