

Puppet and Splunk

Action and analysis in one place

Many enterprise IT organizations rely on Puppet and Splunk to operate their essential applications. Puppet provides key operational data that enterprises depend on to improve decision making and take immediate, automated action. Splunk enables IT, DevOps, and Security teams to investigate, monitor, and analyze data within infrastructure and applications in their environments. Together, Puppet and Splunk help teams build a foundation of continuous analysis and automation across their entire organization.

Through a series of apps and modules, Puppet and Splunk have integrated our unique, complementary solutions to address multiple enterprise challenges – giving organizations an effective way to discover insights, analyze data intelligently, and act quickly.

Prioritize alerts and take corrective action

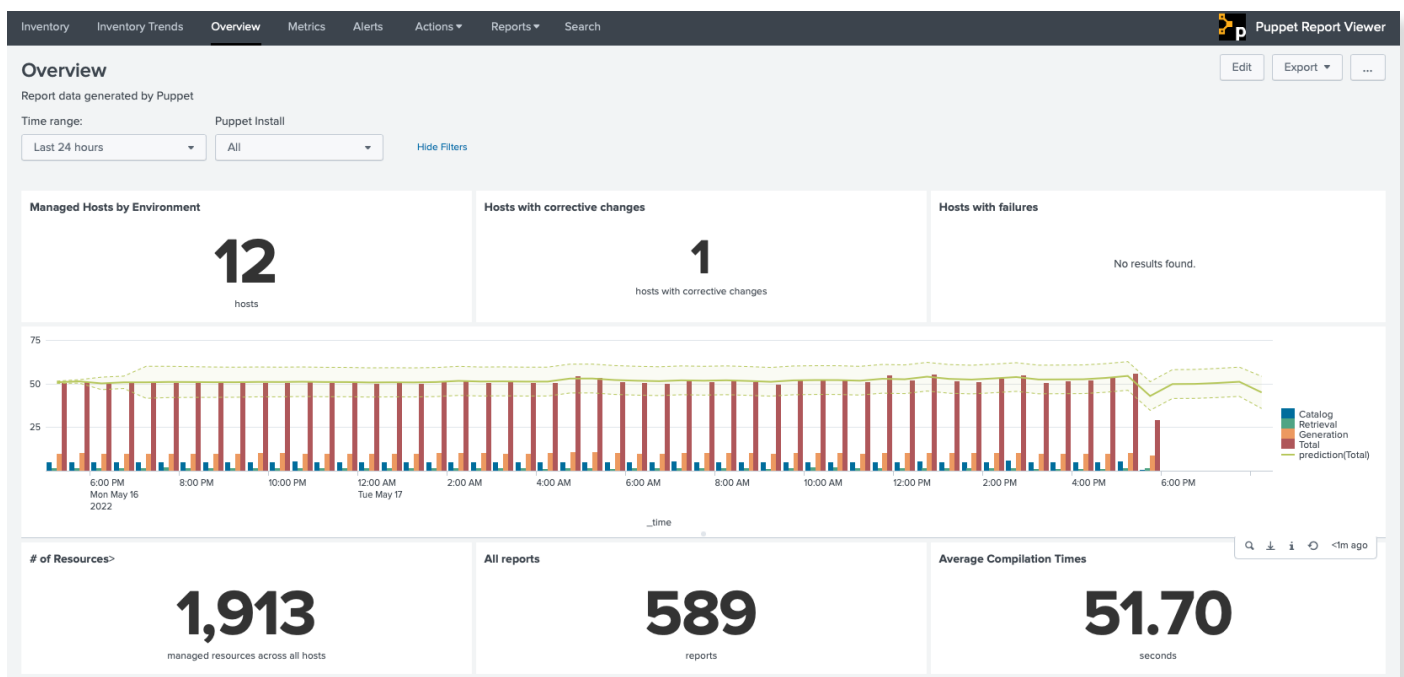
- Trigger corrective or investigatory actions in Splunk based on context-rich data from Puppet
- Save time on manual processes and ticket passing by automating repetitive tasks

Enrich data with context

- Receive real-time insights from infrastructure changes
- Detect issues quickly and spot abnormal trends and patterns

Add uniformity to your IT infrastructure

- Avoid one-off scripts that are difficult to scale and share
- Keep a comprehensive and dense audit trail of events to ensure compliance



Automate actions on Splunk alerts

Acting on Splunk alerts manually can be time-consuming, making it difficult to prioritize what's important and ultimately slowing down mean time to repair (MTTR). Puppet and Splunk dramatically improve MTTR for critical incidents. Puppet shares real-time, context-rich data with Splunk about how infrastructure is changing and provides users with the ability to trigger corrective or investigatory action right from within Splunk.

Determine compliance and standardize security

Scanning infrastructure to determine compliance in organizations with sensitive or highly regulated environments is cumbersome and remediation or enforcement is typically done separately. Puppet Enterprise enables teams to efficiently test for compliance and automate systems into a compliant state while leveraging Splunk for reporting, insights, and analysis.

Deploy and manage Splunk enterprise

Keeping critical data flowing to Splunk can be a challenge, especially in large enterprise environments. Puppet Enterprise provides enterprise-grade automation for Splunk and can ensure that the Splunk Forwarder is always available, running, and configured properly. Puppet Enterprise can even automate the installation and management of your Splunk server.

Visualize data with dashboards

Gathering the right Puppet metrics that enable actionable insights is often left to the operator, which can limit the capacity to troubleshoot issues. Out-of-the-box dashboards provide meaningful insights into company data and allow users to take quick action to remediate issues.

Manage custom reporting

Maintaining a holistic and historic view of your organization's infrastructure can be challenging. Puppet Enterprise provides detailed inventory and change data, which can be sent to Splunk to create custom reports and dashboards that allow teams to gain detailed insights and track data trends over time.

Getting started

To get started, download the Puppet and Splunk apps from Puppet Forge and Splunkbase.

- [Splunk Module for Puppet Enterprise](#) - Puppet Forge [↗](#)
- [Puppet Enterprise Status Check](#) - Puppet Forge [↗](#)
- [Puppet Report Viewer](#) - Splunkbase [↗](#)
- [Puppet Alert Actions](#) - Splunkbase [↗](#)

Puppet by Perforce gives IT operations teams back their time and offers peace of mind with infrastructure automation that enables security and compliance. More than 40,000 organizations — including more than 80 percent of the Global 5000 — rely on Puppet's open source and commercial solutions. In 2022, Puppet was acquired by Perforce Software, backed by Francisco Partners and Clearlake Capital Group. Puppet's brand and software suite work standalone within Perforce. [Learn more at puppet.com/integrations/splunk](https://puppet.com/integrations/splunk)