

# Bolt for Splunk

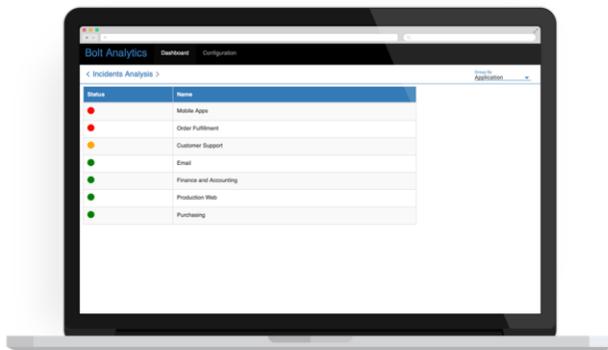
## REAL-TIME INSIGHT

### Intelligent Analysis for IT Incident Management

Bolt is an incident, detection and management solution that uses a combination of unique learning models and existing data to enable IT Operations to reduce the time to detect and resolve IT incidents, ensuring application level KPI's are always met in full operation. Bolt operates on existing data streams to learn from and analyze the data, delivering key insights, recognizing trends and potential faults in the infrastructure, and linking them to application KPI's.

Splunk is a widely used data aggregator in enterprises. With Bolt's module to support Splunk, IT Ops can now leverage the data sent to Splunk to analyze and respond quickly to incidents. Bolt's unique AI models learn quickly and continue to improve over time for greater accuracy, while having less impact on resources. Users can leverage existing Splunk dashboards for rapid deployment, and the solution is extensible to include data sources beyond Splunk for greater insight.

- Analyze in Real-Time
- No delay prior to incident detection
- Results improved with deep learning
- Statistical techniques and neural models provide more accurate results
- Save on expensive compute resources
- No additional load on Splunk servers
- Easily add new data sources for greater insight without ingesting into Splunk

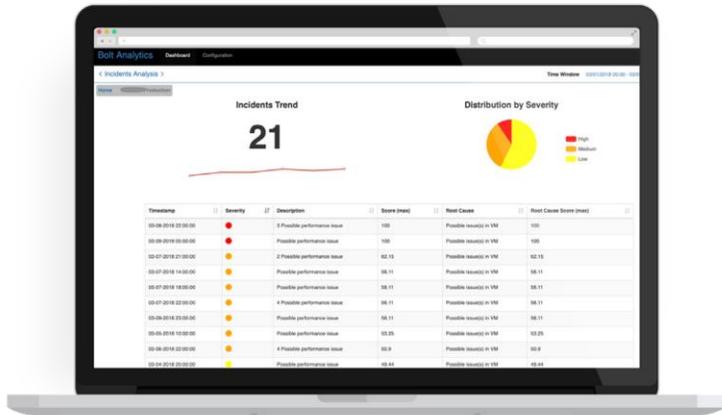


Application Level Dashboard with Color Coded Status

## Use Real-Time Mode for Fastest Response

Waiting for data to be indexed can cause a delay in detecting and responding to critical issues. Bolt's Real-Time Mode infers directly from existing data streams (e.g. Splunk Heavy Forwarder, Logstash) without waiting for data to be indexed, thus reducing detection and response times significantly.

## Incidents Observed for an



## AI for Intelligent Analysis

Bolt combines statistical techniques with neural models to provide a unique solution that is more accurate in determining anomalies with less noise to ensure only real issues are flagged. The combination of statistical techniques with neural models improves the accuracy of models over time.

## Seamlessly Add Analytics to Existing Dashboards

Installation and configuration are typically completed in minutes. Bolt discovers available dashboards and allows the administrator to simply select those to receive the intelligent analysis. Results can be viewed within Splunk or in a separate Bolt UI. The Bolt analysis is done on separate servers so no additional load is placed on the Splunk servers, eliminating the need for expensive system upgrades.

## Add Data Sources Without Ingestion

Bolt is extensible to other data sources that are not being captured by Splunk, such as VMWare vSphere, SQL Server, AWS, Microsoft Azure. By adding more data sources, Bolt can provide a more holistic view of the infrastructure and more effectively detect incidents and provide accurate analysis.

## Root Cause Analysis of

