

Splunk IT Essentials Work

Speed up troubleshooting by bringing all IT data into one view

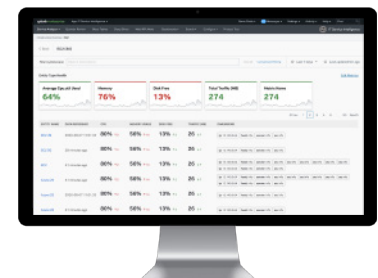
- **Fast time to value** with out-of-the-box dashboards, automatically populated once data is in (using existing Splunk add-ons)
- **Correlated logs and metrics** for quick entity context
- **Accurate review of alert events** for faster mean-time-to-resolve (MTTR)
- **Unified view** for all infrastructure data allows for fast investigations

Entity types supported and monitored

- *nix
- Kubernetes Node
- Kubernetes Pod
- Unix/Linux Hosts
- VMware Cluster
- VMware Datastore
- VMware ESXi Host
- VMWare vCenter
- VMware VM
- Windows Hosts
- And more!

Today's IT teams are challenged with wrangling data stuck in multiple, disparate tools and apps. The lack of holistic visibility into all components of the IT environment leads to incomplete insights, long investigation times and difficulty pinpointing root causes. Logging into individual entities of a production environment is both insecure and inefficient. Conducting "room by room" investigations after sharing all necessary credentials costs valuable time and energy, and if investigations don't begin in a timely manner, logs may 'roll off' point monitoring solutions, making it more difficult to do analysis with incomplete data. IT teams may be forced to perform potentially unnecessary reboots, further extending MTTR and resulting in frustrated users, employees and customers.

IT Essentials Work reduces context switching by consolidating Splunk apps and third-party point solutions into a single, centralized view



IT Essentials Work

Splunk IT Essentials Work (ITE Work) expedites alerting, streamlines investigative workflows, and accelerates troubleshooting, helping IT teams easily get started with simplifying advanced IT management. By consolidating tools, reducing cost and complexity, and correlating all IT data into a single view, Splunk offers a better understanding of the performance and health of your entire environment.

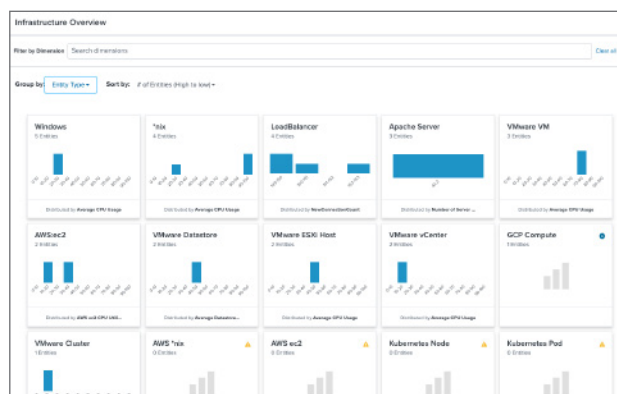
With prescriptive, curated content that reduces the learning curve, you get step-by-step guidance to expand and accelerate adoption of Splunk for common IT tasks and use cases. With ITE Work, you can expedite alerting with metrics and quickly transition to streamlined investigative workflows and troubleshooting with your logs — all in the same workspace. **This is the foundation for any IT team's modernization journey.**

Key Capabilities

An entity represents an IT component that requires management in order to deliver a service. Entities are usually hosts, but can also be cloud or virtual resources, network devices or applications. IT Essentials Work correlates logs and metrics for each entity, and uses log-based analysis to observe and understand the performance of all your entities. This prevents siloes and wasted time trying to onboard data and build custom dashboards.

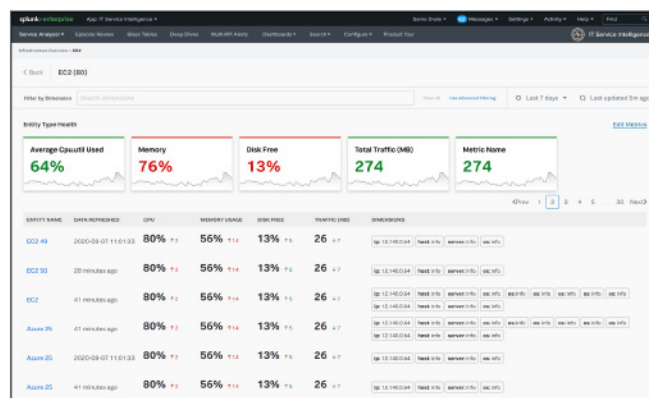
Infrastructure Overview to keep tabs on entity health

Out-of-the-box dashboards provide a quick view of the status of key KPIs for different entity types. You can understand what's going on at an entity-level, as well as across your entire infrastructure with Infrastructure Overview. Visualizations let you see which specific entities have high CPU usage and drill down into that specific entity to see what's causing it. The ability to group by entity type, apply filters and see logs associated with specific metric data enables log-based analysis for speedy and seamless troubleshooting.



Holistic view of all active entities to reduce context switching

From a single view, you can see all your data — whether metric or log event data — and correlate key dimensions for context and performance. You can define groups to easily group and filter infrastructure metrics, status, alerts and investigations. This holistic view allows for a better understanding of infrastructure health so you can observe and understand the performance of your entities. Having one workspace with high-level visualizations makes it easier to determine trends, conduct immediate investigations and reduce context switching.



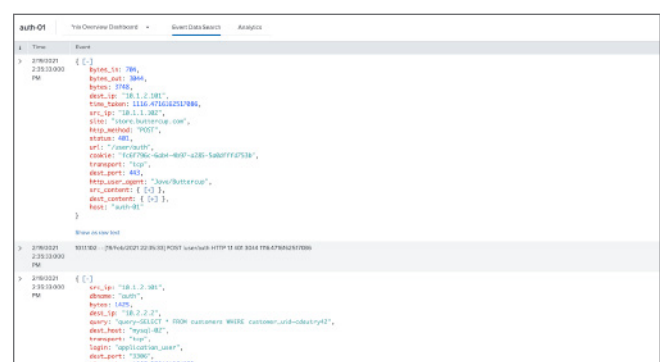
Drill deeper into data to streamline investigative workflows

IT Essentials Work lets you use out-of-the-box dashboards to get up and running immediately and see the status of key KPIs over time. You can quickly identify trends or specific points in time where KPI status changed, and drill down into the entity health page where you can monitor metrics like average CPU usage, average memory usage, average datastore latency and average network traffic across all hosts. With IT Essential Work, you can see what's happening, troubleshoot faults and get a specific, entity-level view of the issue — without writing queries or code or building custom dashboards.



Event Data Search shows relevant logs from last 60 minutes

IT Essentials Work includes a feature called Event Data Search, that lets you quickly analyze the health of your infrastructure. Event Data Search looks at entity status across different infrastructure types and identifies inactive entities that could be causing issues in the production environment. With this capability, you can track the status of entities based on variation in data ingestion rate, drill down into individual entities to analyze log data to track performance entities and speed up troubleshooting using the infrastructure data from application logs.



Alerting for faster triage

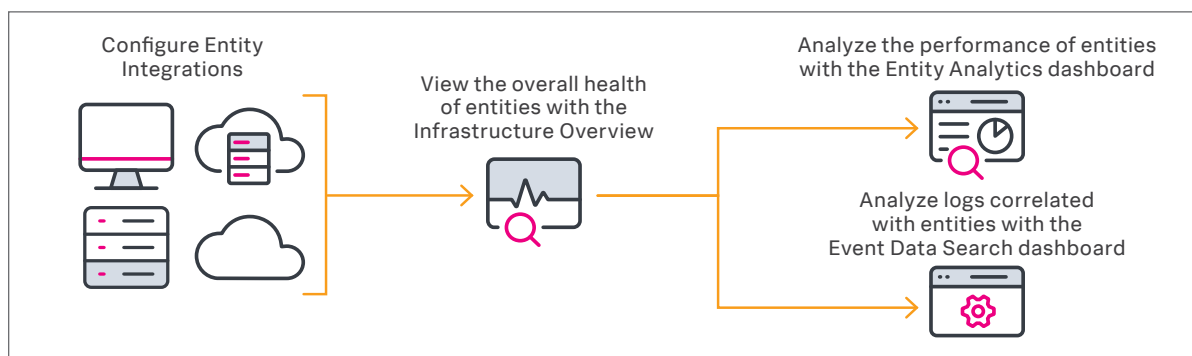
Custom-triggered alerting at a group or entity level lets you perform root cause analysis faster. You can also triage alerts more effectively by understanding which conditions triggered the alert, assessing the severity of the alert and viewing all triggered alerts to decide what actions to take. By setting up thresholds and generating alerts at a specific infrastructure level and being able to analyze alerts across different infrastructure types, you can get alerted on your most vital metrics.

Severity	Title	Incident Path	Time	Description	Status
Normal	Average CPU Usage metrics alert for 'Yes entity type'	yesentity.com	2018-03-27 15:53:00+0000	Average CPU Usage current value is 95.94765538824932	View Details
Normal	Average CPU Usage metrics alert for 'Yes entity type'	yesentity.com	2018-03-27 15:53:00+0000	Average CPU Usage current value is 95.94765538824932	View Details
Normal	Average CPU Usage metrics alert for 'Yes entity type'	yesentity.com	2018-03-27 15:53:00+0000	Average CPU Usage current value is 95.94765538824932	View Details
Normal	Average CPU Usage metrics alert for 'Yes entity type'	yesentity.com	2018-03-27 15:53:00+0000	Average CPU Usage current value is 95.94765538824932	View Details
Normal	Average CPU Usage metrics alert for 'Yes entity type'	yesentity.com	2018-03-27 15:53:00+0000	Average CPU Usage current value is 95.94765538824932	View Details
Critical	Average CPU Usage metrics alert for 'Yes entity type'	yesentity.com	2018-03-27 15:53:00+0000	Average CPU Usage current value is 95.94765538824932	View Details
Critical	Average CPU Usage metrics alert for 'Yes entity type'	yesentity.com	2018-03-27 15:53:00+0000	Average CPU Usage current value is 95.94765538824932	View Details
Normal	Average CPU Usage metrics alert for 'Yes entity type'	yesentity.com	2018-03-27 15:53:00+0000	Average CPU Usage current value is 95.94765538824932	View Details
Normal	Average CPU Usage metrics alert for 'Yes entity type'	yesentity.com	2018-03-27 15:53:00+0000	Average CPU Usage current value is 95.94765538824932	View Details
Normal	Average CPU Usage metrics alert for 'Yes entity type'	yesentity.com	2018-03-27 15:53:00+0000	Average CPU Usage current value is 95.94765538824932	View Details

How it Works

IT Essentials Work gives you access to all the default entity integrations, including *nix, Windows and VMware. After you import your entities, you can view and monitor your entity types in the Infrastructure Overview and drill down further into individual entities to analyze associated log data and track performance metrics.

This diagram shows a basic entity integration workflow, configured to monitor hosts, containers and virtual infrastructures as entities.



Benefits

Enjoy a simple, easy approach to leveraging pre-built content built on industry best practices. IT teams can confidently work together to perform safe, secure and rapid investigations, identifying root causes without the hassle of logging into production environments or switching between apps and point solutions.

- **Ease of use** – no Search Processing Language (SPL) required
- **Fast time to value** – prescriptive data collection allows out-of-the-box dashboards to be populated immediately
- **Intuitive interface** – easy user experience with insight into on-prem/hybrid/cloud environments
- **Single experience, multiple activities** – monitor, alert, troubleshoot and investigate all from a single UI
- **Quick root cause analysis** – get alerted on issues that matter and find the root cause of an issue fast

ITE Work offers an easy first step on your journey towards IT modernization. When your organization is ready, ITE Work integrates with [Splunk Infrastructure Monitoring](#) and offers seamless adoption of advanced use cases in [Splunk IT Service Intelligence \(ITSI\)](#), such as service insights and event analytics.

Get up and running in minutes

Splunk IT Essentials Work is available as a [free app on Splunkbase](#), download it to get an easy start with log-based analysis and faster troubleshooting. ITE Work can be used in tandem with [IT Essentials Learn](#), both of which are included with Splunk Cloud as part of [IT Cloud Foundations](#). Try a free trial of [Splunk Cloud](#) today!



Learn more: www.splunk.com/asksales

www.splunk.com