GEMINI ENTERPRISE:

Road to Operational Intelligence

For the IT Operations organization, the idea of having operational intelligence (OI) across the enterprise is the right goal. As a big data deployment matures and value is realized, this idea begins to resonate across the team. OI represents a maturity level where an organization sees operational value from the solution and can quantify the investment value across the company. It is the nexus of:

- proper implementation and ease of management for linear scalability of the big data solution,
- mastery of the search language, and
- moving from reactive forensic investigation to continuous monitoring.

However, just like any enterprise software deployment, there are pitfalls along the way to OI that can slow or stop this ambitious journey in its tracks.

THE PROBLEM

In most organizations, deployment typically starts with some commodity hardware and just a few people individually using the solution for investigative purposes. As initial value is demonstrated, use spreads across the operations team, and into the Cloud creating a hybrid deployment. The burden of hardware (and/or virtual machine) management becomes more formalized in the organization. Some individuals become proficient in the search language and proactive monitoring marks the first steps to OI. There are four points at which major barriers to reaching operational intelligence maturity found:

1. commodity hardware and home-grown management no longer scale to meet enterprise and use case demands of continuous and simultaneous searches,
2. the loss of a key employee who had mastered the search syntax,
3. the volume of alerts labeled as critical grows beyond the ability to triage, and
4. the realization that proactive monitoring doesn't obviate the need for scalable analysis of individual alerts, getting to root cause, and addressing business process issues.

Finally, cost can be an issue for management of the big data solution. For example, some managed service providers report that for large deployments, management costs can be 3x the cost of the license.

SOLUTION OVERVIEW

Gemini Enterprise views your entire solution as a single analysis stack (see figure 1) that seamlessly works to address all four of these problems. Deployed on-premises, in the cloud (public or private), or as a hybrid solution.

geminidata.com | contact@geminidata.com | (415) 826 - 7269 | 15 Funston Ave, San Francisco, CA 94129

Gemini Appliance: Physical or Virtual

One of the keys to big data deployment and ongoing management success is making sure your hardware meets big data vendor described hardware specifications. Gemini supports both a physical and software based appliance option. Any node consists of a hardened OS on a physical or software based appliance that meets or exceeds big data vendor specifications. You always have the flexibility to reconfigure cluster topology. Gemini appliances support a hybrid on-prem and cloud-based deployment. For specific use cases, private cloud is also supported.

Gemini Enterprise: Big data management software

In addition to being able to manage machine roles (search head, indexer or forwarder) on-the-fly, Gemini Enterprise provides a single interface for all OS level configurations. deployment in sync. From the management console, access any system with SSH. Configure any or all aspects of a node's operating system without having to directly SSH into the device. In addition, configure log rotation, Syslog NG, NTP, failover, and storage. Network interface configurations are all addressed in the web user interface, including port redirections, network aggregation, and configuration. Reduce the number of tedious tasks and the amount of time it takes to grow you deployment with scheduled job execution and automated provisioning.

Your Big Data Solution:

For your data indexing and Hadoop-based solutions, Gemini Enterprise supports direct web-based editing and version control of configuration files and the ability to start/stop any node, Gemini Enterprise performs node and cluster management, provides visualizations of your deployment, and gives you the tools you need to successfully manage and monitor your deployment in a single user interface. Add more indexers, search heads, and forwarders as fast as data volumes grow

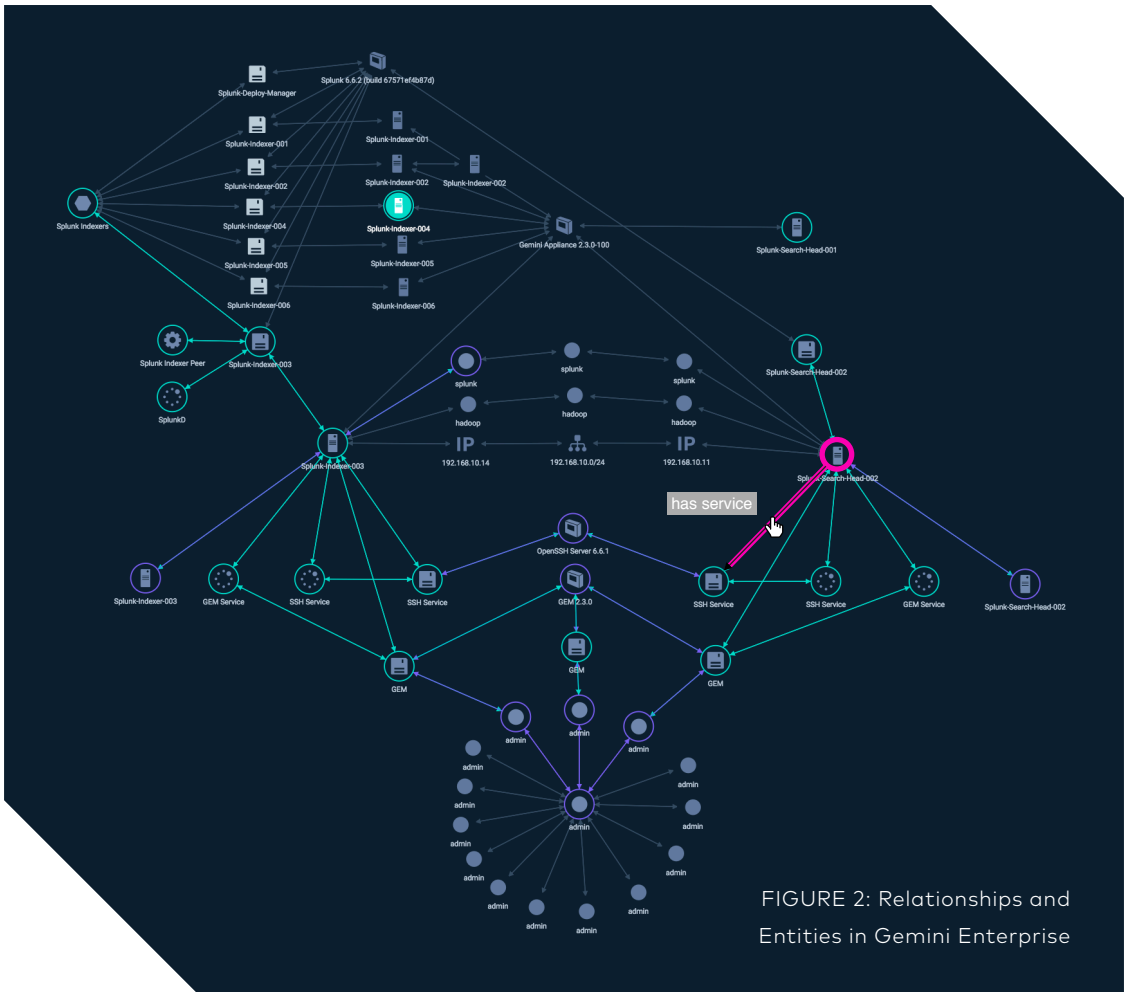


FIGURE 2: Relationships and Entities in Gemini Enterprise

Fast Investigations

Even for the most experienced search language specialist, searching and manually pivoting through data, looking for all connections and relationships to a single IP address, email address, hostname, or URL, is exhausting time- consuming work. Gemini Enterprise uses AI and your Common Information Model (CIM) or Common Event Format (CEF) compliant data to find and classify all related entities and their relationships. This extends operational intelligence to include analysis and accurate storytelling to help you meet and exceed service level agreement (SLA) targets.

Often the direction information travels (to, or from an object, or in both directions) is key to understanding the relationships between objects (see figure 2).

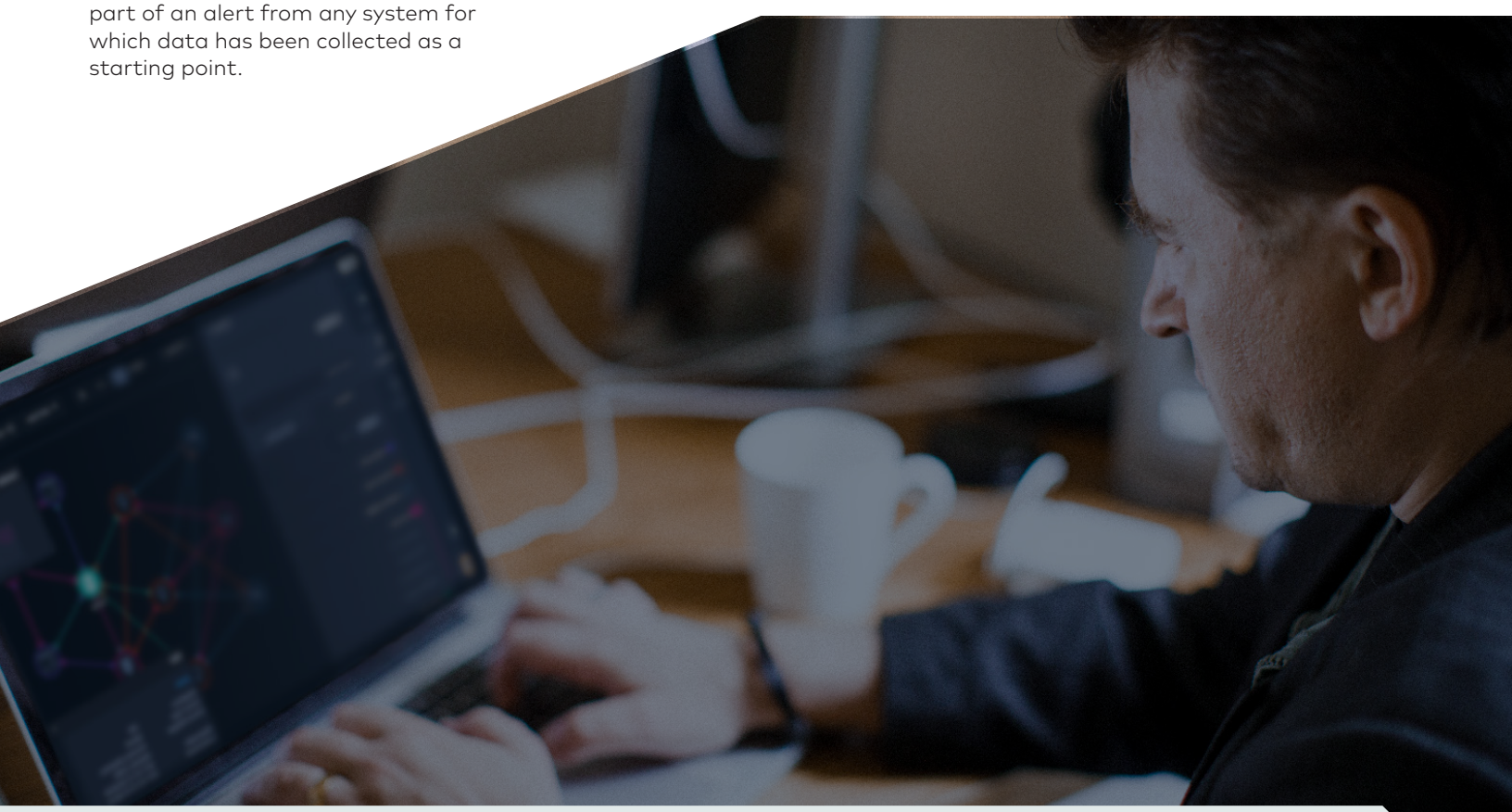
Gemini Enterprise applies inductive and deductive reasoning to intelligently organize your data to visually represents events, entities and the relationships between them. It also will display entities for which you have no data but are inferred by other data sources. Once a story has been created in Gemini Enterprise, you can save it in a library of stories for training purposes to support communication with the C-Suite. Use any part of an alert from any system for which data has been collected as a starting point.

Among the many possible use cases for Gemini Enterprise are:

- transactional analysis and troubleshooting,
- auditing software patch deployments,
- payment processing errors,
- user privilege analysis,
- troubleshooting big data deployments, and
- any other use case where root cause analysis is needed.

SUMMARY

Managing mission critical big data deployments means getting the most value out of the solution with the least possible impact on the IT operations team. Implementing a big data solution as a full analysis stack that scales on-demand dramatically reduces dollar and human costs to the business and can provide internal customers better service level agreements. The analysis stack tells you not only what happened, but also how it happened. The C-suite can get a complete and compelling story for any issue or problem. Gemini Enterprise provides an easy way to accelerate your journey to OI and beyond.



Gemini provides Continuous Data Analysis. We translate data into knowledge using machine reasoning. With Gemini Enterprise, gain enterprise knowledge and awareness, accelerate analysis with AI, and simplify management of big data platforms. Designed for modern architectures, Gemini Enterprise reduces complexity in the cloud or on premises. Gemini Data was founded and built by experts from Splunk, ArcSight, and AppDynamics that understand the importance of building awareness across the enterprise. Find more information at geminidata.com or follow us on Twitter @geminidataco.