Deloitte.

ALL THE BENEFITS OF SPLUNK—ACROSS ENVIRONMENTS—THROUGH ONE WINDOWPANE:

# Welcome to Splunk Federated Cloud

> Your business: modernized, containerized, and connected.

## A multicloud solution: Because data should add value, not overhead

Scaling resources and services to grow your business requires operating in a multicloud—or federated cloud—environment. Although moving to the federated cloud should accelerate growth, the complexity of designing, implementing, and managing this transformation threatens to slow operations.

Deloitte can accelerate your possible with Splunk Federated Cloud, a scalable and reliable computing platform that runs Splunk across multiple cloud environments—on-premises, public cloud, private cloud, or third-party data centers—to provide a streamlined view of your applications and microservices through a single portal.

By leveraging the flexibility and scalability of the federated cloud, our offering is built for enterprises who can't miss another threat, problem, insight, or opportunity in this fast-changing IT landscape.

Combining the advantages of Splunk analytics and Deloitte's leading cyber security and operations expertise, Deloitte can create the reference architecture, implement it, and manage the system once installed—pulling Splunk's insights through a single pane-of-glass view. Equipped with real-time observability, application performance management (APM), and AI-driven analytics, your business can easily access information to resolve issues proactively, all while protecting sensitive applications and data.

Spanning on-prem and public cloud environments, Splunk Federated Cloud provides the reliability, availability, stability, and serviceability needed to turn insights into opportunities.

Deloitte is ready to deploy Splunk Federated Cloud to modernize how your business stores and analyzes data today.

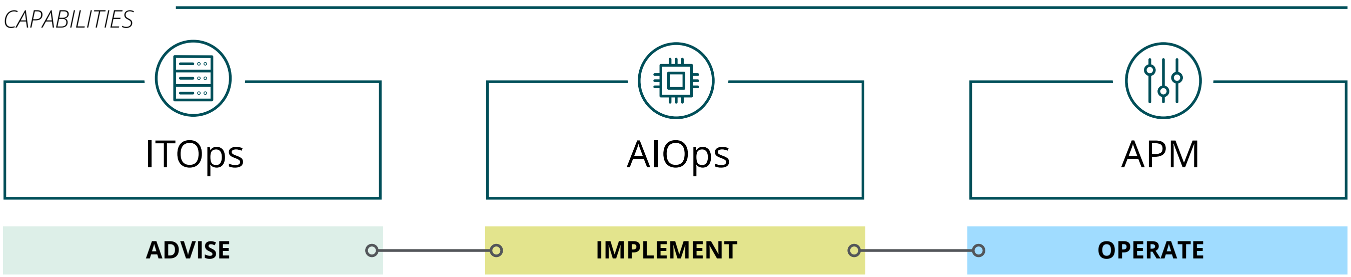
> *Deloitte's Splunk Federated Cloud offering moves your business into a multicloud environment. We manage the complexity, so you can scale and excel.*

# Observability powers continuous business—when you can't miss a minute

Distributed, multicloud systems are expensive to maintain and run, and unwieldy—it's hard to find the information you want when you need it. Despite the cloud's appealing flexibility and growing prevalence, organizations often haven't—or can't—move data to the public cloud because of volume, security concerns or regulations, or both. Meanwhile, for many enterprises, more ingress merely means more to manage: more interfaces, more storage and computing requirements, more security and compliance concerns, and more time, resources, and risk.

Splunk Observability implemented by Deloitte, included as part of our Splunk Federated Cloud offering, delivers reliable, highly available IT and application services at scale. To do this, it optimizes IT environments to collect, analyze, and manage large volumes of machine and application log data—while meeting your business' specific security and governance needs.

## *Deloitte and Splunk Alliance Service Offerings*



*CAPABILITIES*

ITOps

AIOps

APM

**ADVISE**

**IMPLEMENT**

**OPERATE**

*KEY OFFERINGS*

- ITOps and Infrastructure Management Strategy
- AIOps for proactive and predictive monitoring and maintenance strategy
- APM Strategy for Micro Services, API's and Containerized workloads

- ITOps and IM implementation & Configuration
- AIOps Implementation and Configuration
- APM Implementation & Configuration

- Platform migration & consolidation services
- Platform upgrade services
- Observability Process automation & workflow orchestration

- Enterprise Infrastructure Realtime and Proactive Monitoring and Operate
- AIOps Application Monitoring and Operate
- Application Performance Management and Operate

*ENVIRONMENTS*

**On-Premise/CoLo**

**Hybrid Cloud**

**Multi Cloud**

## *Continuous operational improvements, real-time operational responses*

Through **AI-enabled ITOps**, our solution covers all infrastructure components with robust health monitoring that provides insights into performance issues.

This real-time monitoring boosts the ability to identify root causes behind issues much more quickly. With real-time visibility, deep business insights, and automated responses, you can resolve issues before they become incidents.

Faster diagnosis and repair mean more uptime availability, reliability, and time for doing—rather than fixing—business.

## *Spanning any workloads to modernize enterprise IT your way, now*

Deloitte can deploy Splunk regardless of workloads used. It's truly **workload agnostic**. Splunk can monitor the hardware and application landscape, whether they're located in an on-premises, co-located private cloud, or hybrid model, and using cloud platforms including HPE GreenLake, Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), and others.

Splunk Federated Cloud meets your business where its data is—spanning workloads and environments—to modernize how your enterprise manages data without commotion. With this solution, we serve you so you can focus on serving your customers. Business and IT staff can spend more time working productively with applications as tools, instead of problems that need to be solved.

Splunk's anywhere, real-time performance monitoring and data analytics save cost, time, and infrastructure so you can use your resources to scale your possible.

### Workloads Splunk Federated Cloud can integrate into the multicloud

Hewlett Packard Enterprise

aws

Google Cloud

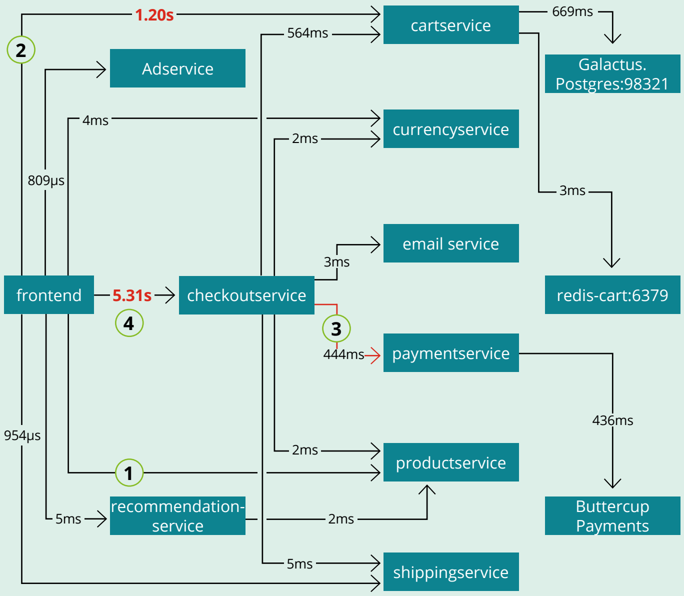
## *Boost application performance and end-user experience—with no business disruption*

**APM.** Identify bottlenecks and root causes quickly with AI-driven analytics. Monitor your APIs and microservices to identify any exceptions across the entire application process for all architecture, plus the performance of every service within a business process in a given lifecycle.

***These insights into exceptions within your APIs and microservices result in:***

- Significantly lower mean time to detect (MTTD) and mean time to restore (MTTR)
- Increased uptime availability, so your system is more fully operational—more of the time—for your end-users

For instance, for an e-commerce company, Splunk can visualize a service map of a sale: A user finds an item, puts it in their cart, goes to cart, adds payment info, and checks out. A kink in this process frustrates potential customers and loses sales. Rather than hunt for an unknown issue, an IT user receives an alert and can see a red arrow within the service map pointing to payment service. Clicking on that, they quickly determine it's an API service token issue, fix it, and avoid an aggravating—and costly—end-user experience.

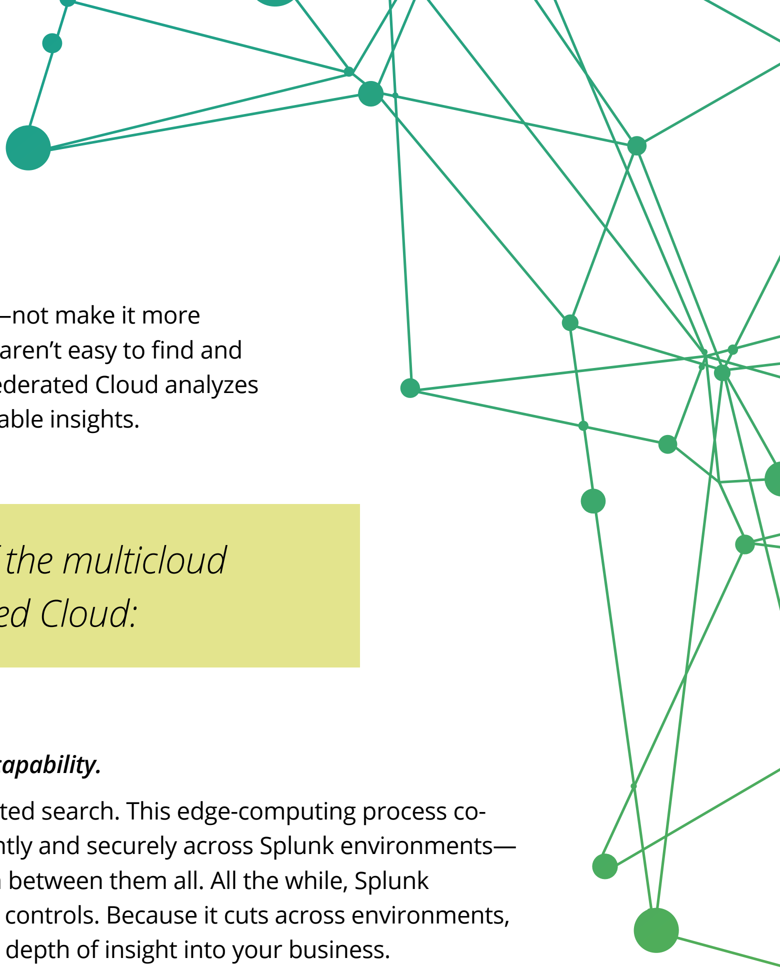


**1.** User finds an item for purchase

**2.** Adds item to the cart

**3.** Adds payment information

**4.** Checks the item out for purchase



# Three ways we make multicloud manageable

Ultimately, a federated cloud model should serve your business—not make it more complicated to run. No matter how detailed the analytics, if they aren't easy to find and understand, the most valuable insights remain hidden. Splunk Federated Cloud analyzes massive amounts of log data in real-time to give enterprises valuable insights.

*To make use of the flexibility and scalability of the multicloud model without the headaches, Splunk Federated Cloud:*

1

***Finds your data—across environments—with Splunk's new capability.***

Our offering relies on a new capability from Splunk: federated search. This edge-computing process co-locates your search head and indexer to scour data efficiently and securely across Splunk environments—on-prem, cloud, or hybrid. Then, it can run a unified search between them all. All the while, Splunk manages security permissions with role-based data access controls. Because it cuts across environments, federated search topples siloed information to offer a new depth of insight into your business.

2

***Shares everything through a single pane of glass.***

Our Splunk Federated Cloud solution runs efficiently to deliver insights extracted from all your data through a single pane of glass. The data from multiple environments—public and private cloud—comes through one open telemetry (OTEL) agent. In other words, DevOps and SecOps users can monitor microservices and glean insights through a single interface. Flexible, customizable dashboarding capabilities let your IT staff peer into infrastructure, data security, performance, and compliance from that interface. With your data streamlined into one easy-to-read source of truth, your business will no longer waste time or expertise on hunting for a needle across workload-haystacks—whether it's the root of a security event or an IT issue. Our user-centered design enables your IT and business resources to spend time scaling. Splunk Federated Cloud offers alerts, visualized data analytics, and service mapping—prompting swift action. Health monitoring and issue identification can be done in one place at one time, increasing operational performance.

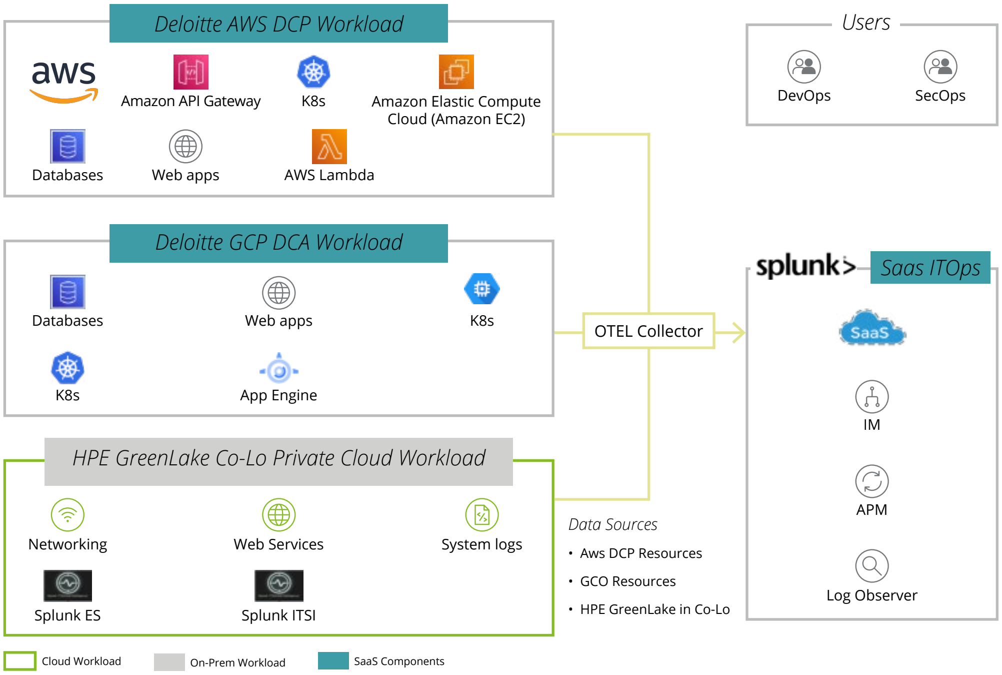
3

***Containerizes Splunk to enhance operational performance at a lower cost.***

To collect and analyze massive quantities of log data, Deloitte implements containers using Kubernetes. Our containerization approach requires less computing power, less storage, and fewer memory resources, saving your business infrastructure and cost. Containerization also limits bugs and errors, freeing developers to build rather than fix.

# *A deeper dive into how containerization can cut infrastructure*

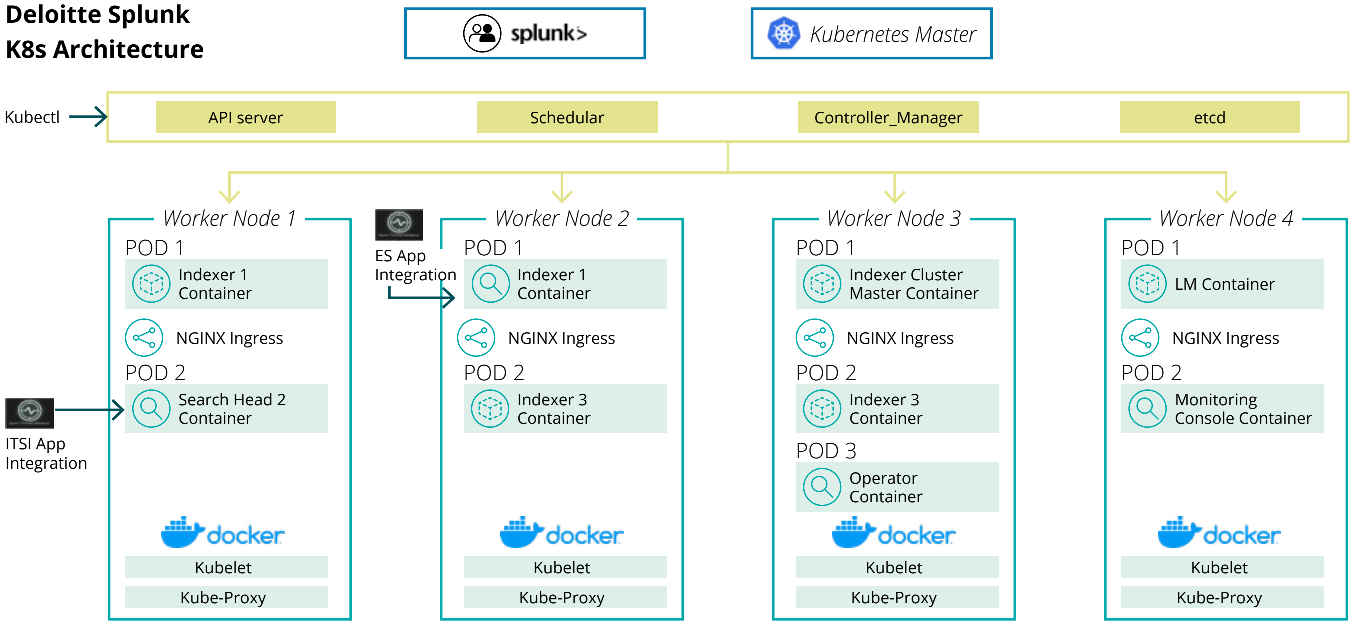
To test containerized Splunk performance, we created the reference architecture mapped below and brought it to life running realistic workloads on an HPE data center at Equinix.



We ran different search types—dense, sparse, and rare—on containerized Splunk successfully, proving out the reference architecture using Splunk Federated Cloud.

To maximize available resources, our offering containerizes multiple instances of Splunk on each server and multiple servers in a Kubernetes cluster. Here, using Kubernetes v. 1.19 and an NGINX ingress, we containerized Splunk indexers, search heads, and heavy forwarders. ***Note how Kubernetes architecture functions down to the IT level—and how much infrastructure it eliminates:***

**Deloitte Splunk K8s Architecture**



### *The HPE Intel server platforms behind our containerized approach*

In the lead-up to validating Containerized Splunk, Deloitte worked with HPE and Intel to identify the right infrastructure based on the workloads planned for testing. Together, we decided on three Intel-based HPE ProLiant DL380 Gen10 Plus servers, each configured with:

- Processors: Two Intel Xeon Gold 6326 (16 cores at 2.9 GHz each)
- Memory: Sixteen 32 GB AM (512GB)
- Solid state drives (SSDs) for data: Four Intel Optane SSD DC P4800X 750GB NVMe
- Solid state drives (SSDs) for boot: Two 480 GB SSDs
- Network index card: One 10/25 GigE
- Operating system: Red Hat Enterprise Linux 8

# In the multicloud, amplify your resources and scale to achieve your possible

***Comprehensive results.*** Retrieve the results you need from all Splunk environments simultaneously with federated search capability.

***Lower costs.*** Deploying Splunk Enterprise on containers can streamline your operational expenses and infrastructure, reducing the amount of CPU, memory, and storage your business needs to run.

***Actionable insights.*** Data analytics, shared through features such as service mapping, prompt action and fixes for immediate impact with minimal effort. Monitor and identify the root cause of issues early on—then resolve without impacting the broader footprint.

***Increased reliability, availability, and stability of applications.*** AI-enabled IT Ops and APM can drive MTTD and MTTR down.

***Workload-agnostic ecosystem.*** Deloitte works across cloud providers and on-prem to move your business to the federated cloud.

***Easy to customize, easy to stand up.*** With Splunk Federated Cloud, Deloitte can move your business to a multicloud environment seamlessly. Then we'll manage the solution to track and analyze your business' data across distributed environments for real-time insights. Meanwhile, you'll see all your enterprise's workloads through a single pane of glass. This applies to any workload, across environments, so your IT staff can turn those insights into actions immediately.

# Key takeaways

As transaction volumes grow rapidly, so does the amount of data that needs to be ingested, monitored, tracked, and reported. More data shouldn't mean more cost, time, and effort. When Deloitte deploys the Splunk Federated Cloud solution, data is liberated from workload and environmental silos to deliver actionable insights.

*Together, we unlock the possible within your enterprise:*

Containerization of components can reduce cost, enhancing operations with decreased CPU, memory, and storage requirements.

Our multicloud approach spans workloads and environments so you modernize quickly while scaling securely—without impacting the entire ecosystem.

Our federated cloud solution is ready to be implemented for your business needs.

Splunk Federated Cloud handles large volumes of unstructured data, and Deloitte mines our leading cyber security expertise to implement and manage it.

# Modernize your business without disrupting operations

*Get*

- ✓ Scalability
- ✓ Flexibility
- ✓ Resiliency
- ✓ Security
- ✓ Federated search
- ✓ Compliance with governance and technical needs

*Without*

- ⊗ Extra infrastructure—and the maintenance that comes with it
- ⊗ Sensitive workloads on insecure environments
- ⊗ Scripts and set-up for your team
- ⊗ Wasted cost and resources

Let's translate Splunk's insights into modern data storage with less infrastructure and lower cost. Together, we'll solve your biggest challenges, accelerate time to value, and deliver outcomes to support your business. We're ready. Are you?

## *Get in touch to achieve your possible.*

**Andy Daecher**
Lead Alliance Partner, HPE
Deloitte Consulting LLP
adaecher@deloitte.com

**Mitch Hall**
VP Alliance Relationship, HPE
Deloitte Consulting LLP
mithall@deloitte.com

**Leslie Turkson**
Managing Director, Cloud
Deloitte Consulting LLP
lturkson@deloitte.com

**Vinay Mahamkali**
Senior Solution Manager,
System Engineering
Deloitte Consulting LLP
vmahamkali@deloitte.com

**Ashish Mujumdar**
Manager, Cloud Engineering
Deloitte Consulting LLP
amujumdar@deloitte.com

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.