IBM DataPower Gateways

Ozair Sheikh
Program Director of Offering Management
API Connect & Gateways

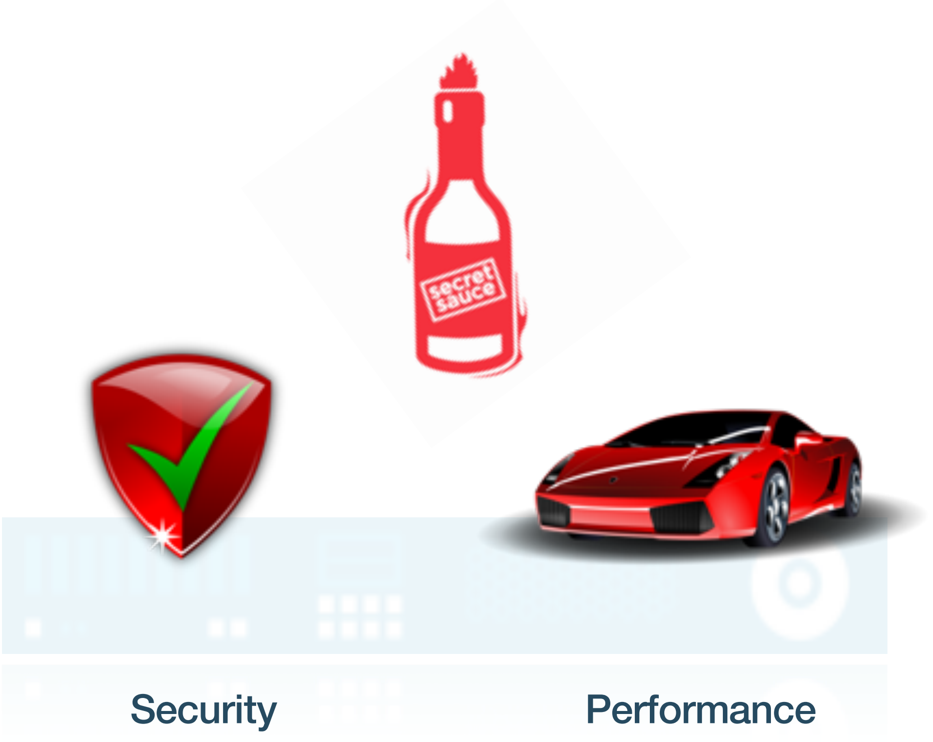
DataPower Secret Sauce

Security: Secure to the core with secure platform & self-contained signed & encrypted firmware image to *minimize risk of security exposures*

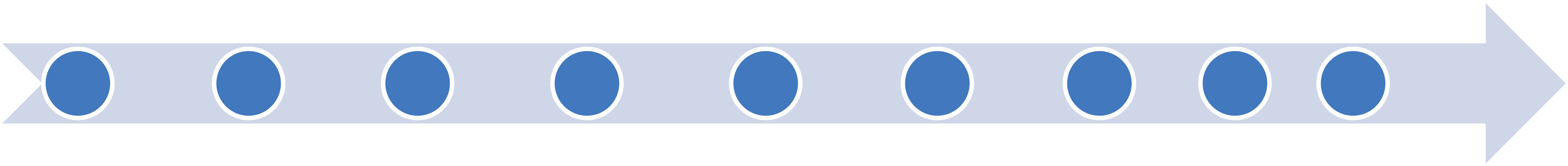
Performance: patented gateway technology that executes transactions natively within the OS, *delivering 30K TPS at wire speed*

DataPower Gateways help reduce TCO

- **Less security exposures** reduces time spent patching systems
- **Minimal performance tuning** reduces infrastructure and operational costs
- **Less hardware needed** to support workload which lowers capital expenditure



History of DataPower Gateway Innovation



IBM Acquires DataPower
2005

Web 2.0 (REST/JSON)
2010

DataPower Virtual Edition
2012

API Management
2013

REST Management API
2014

JavaScript Runtime (GatewayScript)
2015

DataPower Gateway for Linux
2016

Tenant Isolation
2017

API Gateway Service
2018

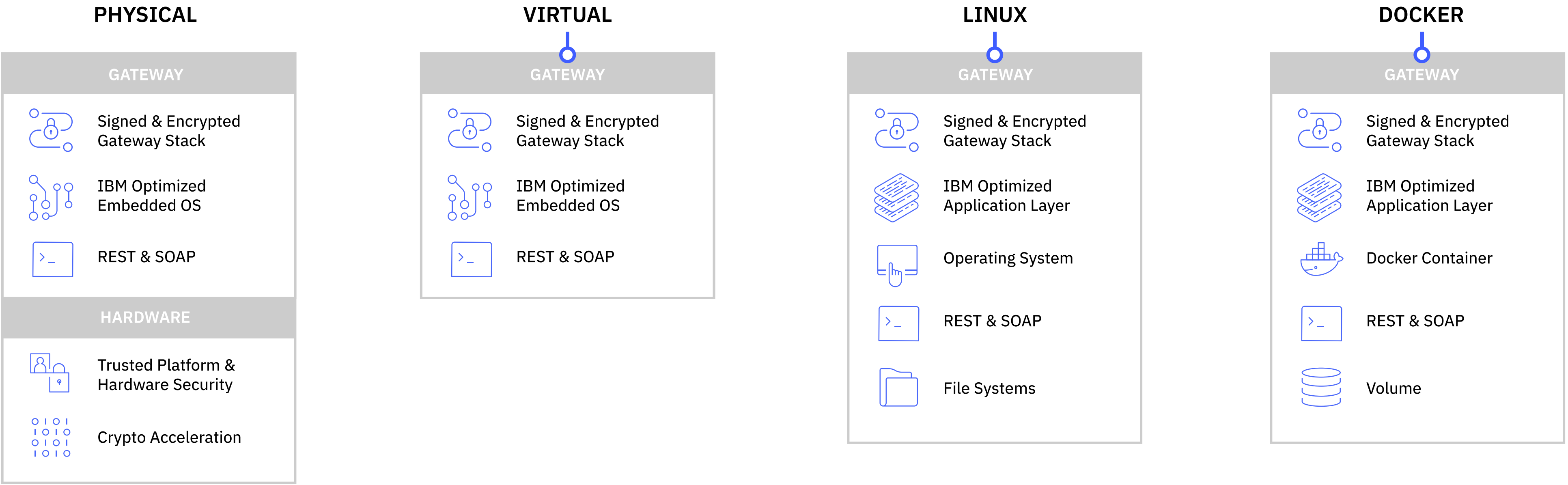
Gateway Innovations: Brand New Gateway Service for APIs

Key Innovations	Description
New DataPower X2 physical appliance	Next generation hardware architecture that provides increased cores, network & memory capacity
New Gateway Service for APIs	Built from scratch, re-architected Gateway Service to process API workloads at native kernel level
10X Performance boost	30,000 Trans/Sec with 8 ms latency
Optimized Self-healing & auto-scale	Self corrective distributed architecture for healing & scaling for usage spikes & runtime resiliency
New DataPower Operations Dashboard	Deep transactional insight for accelerating troubleshooting and firmware management for quicker upgrades
Istio integration	SLA-based micro services routing, security & performance

DataPower Gateways can deploy anywhere…

Physical appliances: All-in-one (HW / SW), DMZ-ready with physical security including crypto acceleration and optional hardware security module (HSM)

Software: virtual appliance, application (Linux) & container (Docker/Kubernetes) provide flexible deployment options for both cloud and on-prem environments



PHYSICAL

GATEWAY

- Signed & Encrypted Gateway Stack
- IBM Optimized Embedded OS
- REST & SOAP

HARDWARE

- Trusted Platform & Hardware Security
- Crypto Acceleration

VIRTUAL

GATEWAY

- Signed & Encrypted Gateway Stack
- IBM Optimized Embedded OS
- REST & SOAP

LINUX

GATEWAY

- Signed & Encrypted Gateway Stack
- IBM Optimized Application Layer
- Operating System
- REST & SOAP
- File Systems

DOCKER

GATEWAY

- Signed & Encrypted Gateway Stack
- IBM Optimized Application Layer
- Docker Container
- REST & SOAP
- Volume

Choosing the right Gateway form factor

Physical appliances provides the most comprehensive security combined physical with firmware security.

Virtual, Linux and Container offer “right sized” units of capacity, as few as 4 CPUs

Container provide ability to leverage auto-scaling and runtime health monitoring

Container is “cloud ready” to facilitate both public and private cloud based deployments

Next Generation DataPower Gateway (IDG) X2 Appliance

Up to 2X performance with next generation hardware architecture compared to IBM DataPower Gateways (IDG) for lower TCO

2X 10GbE network ports compared to IDG to accelerate application responsiveness

Up to 4X RSA operations with 2048-bit keys using the optional Hardware Security Module (HSM)

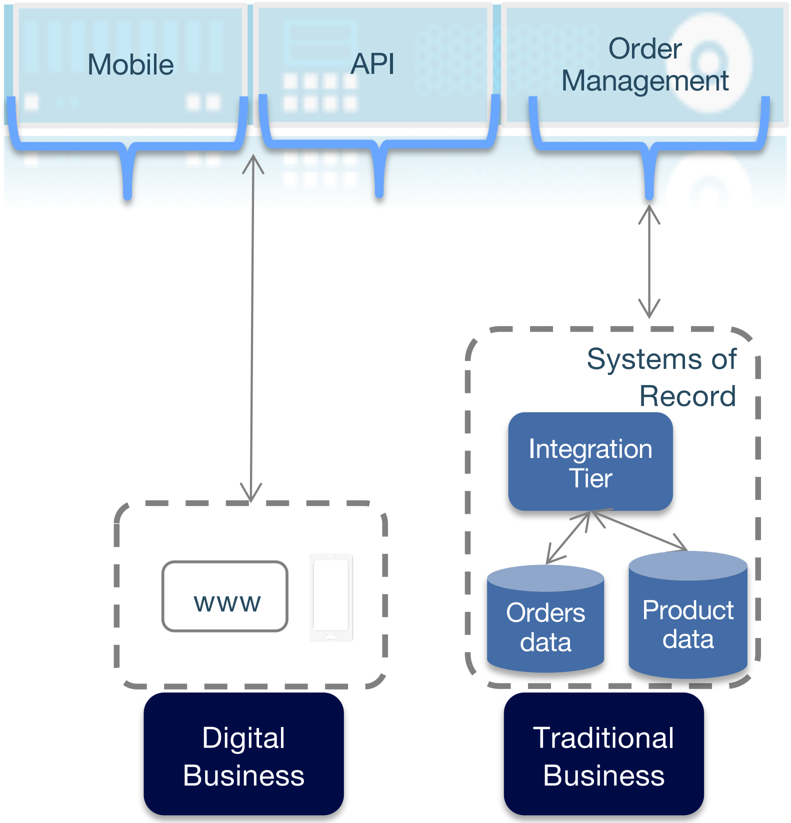
Enhanced memory and workload capacity available for higher performance and/or to run additional tenants

Tenant Isolation provides workload isolation and upgrade flexibility

Create tenants on DataPower physical appliances for workload isolation and enhanced runtime resiliency

- **Apply firmware upgrades** to the Digital workloads independently from traditional DataPower services
- **Upgrade tenants** without disrupting traditional DataPower services

Physical DataPower appliance partitioned into isolated tenants



DataPower Operations Dashboard

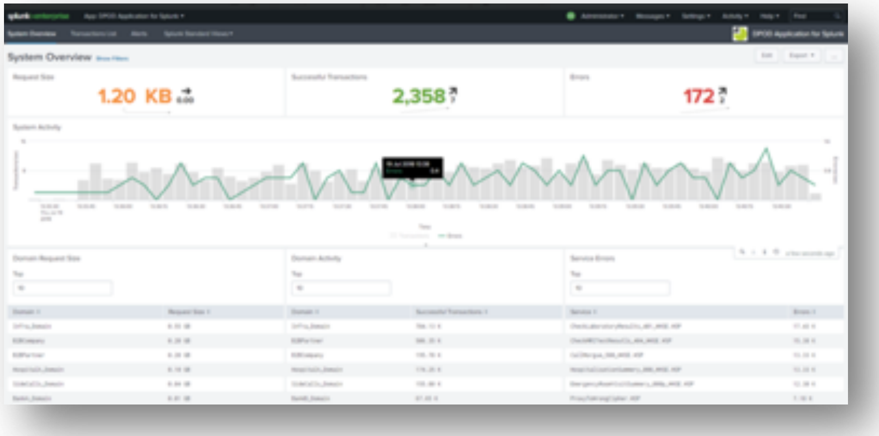
Enhanced Troubleshooting with DataPower Operations Dashboard

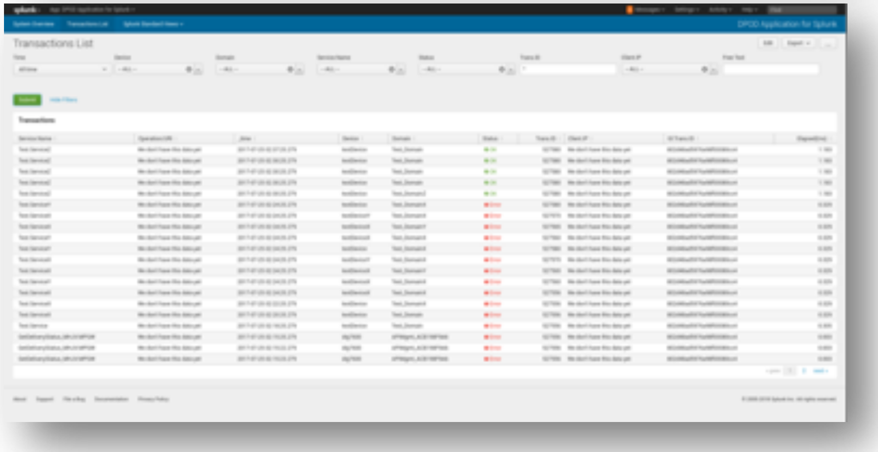
Powerful API diagnostics with detailed views across latency, version, policy, and consumer

Non-intrusive tracking of transactions across multiple gateways without any manual policy instrumentation

Supercharged performance for demanding workloads via new distributed, federated server architecture

Reduce Splunk licensing cost with DPOD plug-in for Splunk, empowering Splunk admins unique operational insight collected from DPOD



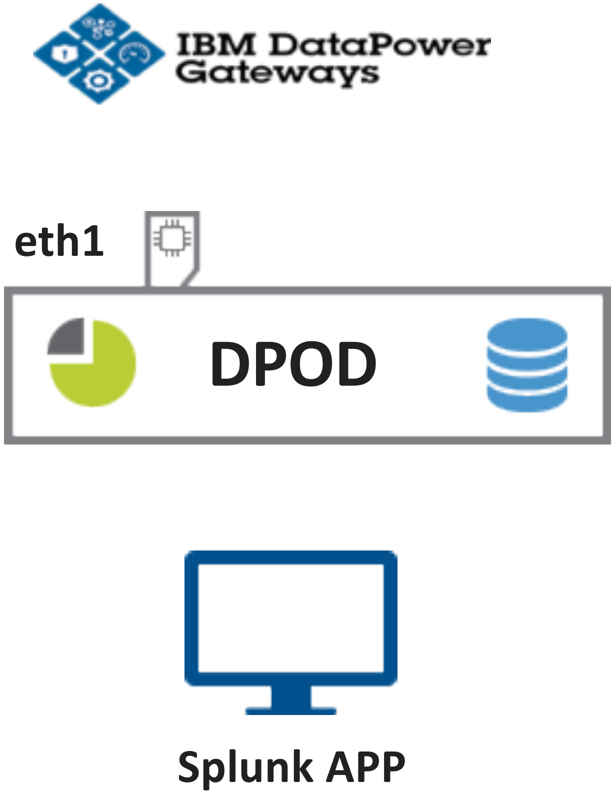


New DPOD plugin provides enhanced APM Integration

Application Performance Management (APM) solutions provide an enterprise view of system health and performance

Deep-transactional insight into API and Gateway transactions

New DPOD plug-in for Splunk empowers Splunk administrators with unique operational insights collected from DPOD and reduces licensing cost for Splunk



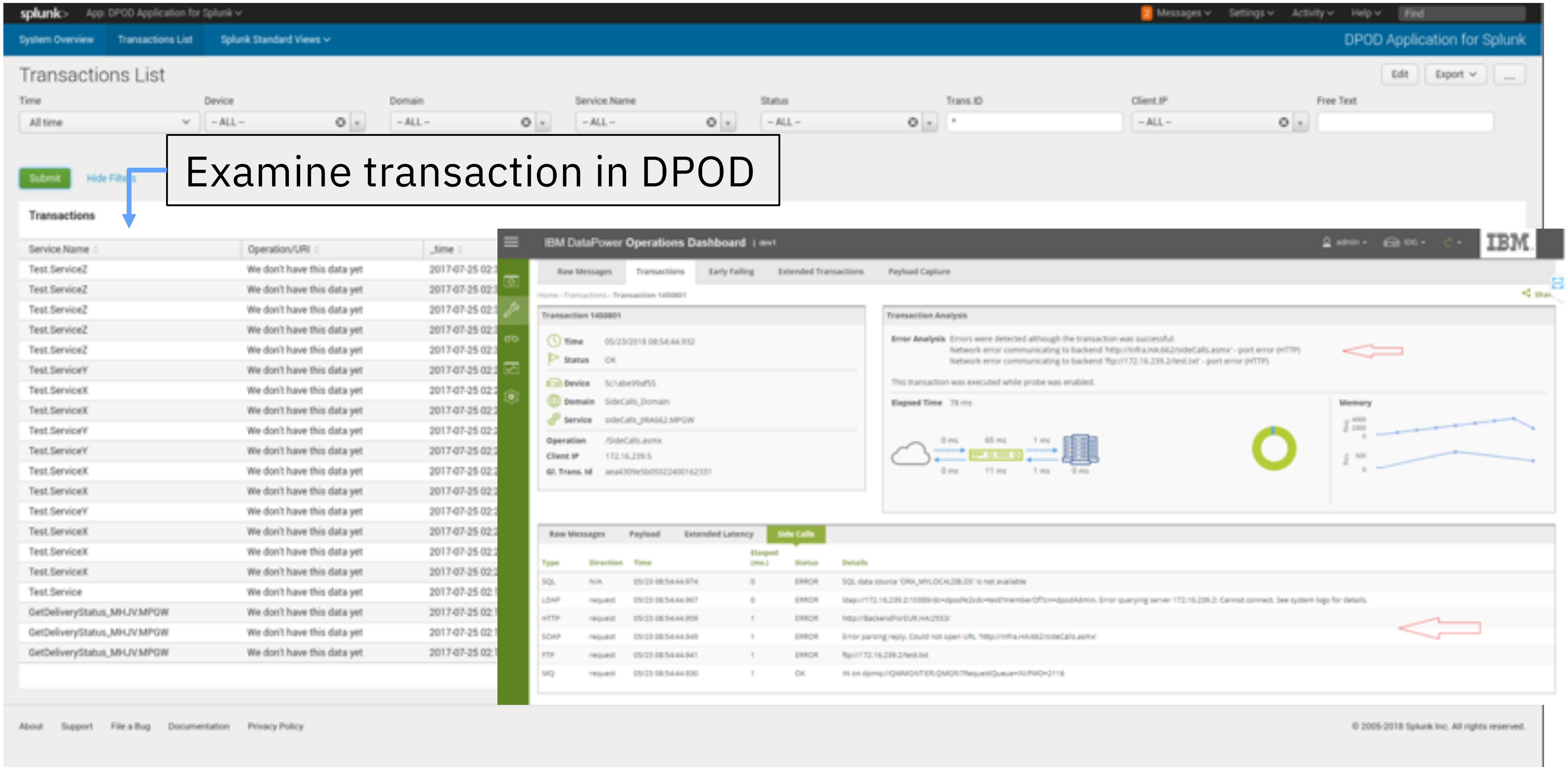
IBM DataPower Gateways

eth1

DPOD

Splunk APP

DPOD plugin for Splunk



Examine transaction in DPOD

Transactions List

Time: All time
Device: – ALL –
Domain: – ALL –
Service.Name: – ALL –
Status: – ALL –
Trans.ID: *
Client.IP: – ALL –
Free Text:

Transactions

Service.Name	Operation/URI	_time
Test.ServiceZ	We don't have this data yet	2017-07-25 02:3
Test.ServiceZ	We don't have this data yet	2017-07-25 02:3
Test.ServiceZ	We don't have this data yet	2017-07-25 02:3
Test.ServiceZ	We don't have this data yet	2017-07-25 02:3
Test.ServiceZ	We don't have this data yet	2017-07-25 02:3
Test.ServiceY	We don't have this data yet	2017-07-25 02:2
Test.ServiceX	We don't have this data yet	2017-07-25 02:2
Test.ServiceX	We don't have this data yet	2017-07-25 02:2
Test.ServiceY	We don't have this data yet	2017-07-25 02:2
Test.ServiceY	We don't have this data yet	2017-07-25 02:2
Test.ServiceX	We don't have this data yet	2017-07-25 02:2
Test.ServiceX	We don't have this data yet	2017-07-25 02:2
Test.ServiceY	We don't have this data yet	2017-07-25 02:2
Test.ServiceX	We don't have this data yet	2017-07-25 02:2
Test.ServiceX	We don't have this data yet	2017-07-25 02:2
Test.ServiceX	We don't have this data yet	2017-07-25 02:2
Test.Service	We don't have this data yet	2017-07-25 02:1
GetDeliveryStatus_MHJV.MPGW	We don't have this data yet	2017-07-25 02:1
GetDeliveryStatus_MHJV.MPGW	We don't have this data yet	2017-07-25 02:1
GetDeliveryStatus_MHJV.MPGW	We don't have this data yet	2017-07-25 02:1

Transaction 1450801

Time: 05/23/2018 08:54:44.932
Status: OK
Device: 5c1abe99af55
Domain: SideCalls_Domain
Service: sideCalls_JIRA662.MPGW
Operation: /SideCalls.asmx
Client IP: 172.16.239.5
Gl. Trans. Id: aea4309e5b05022400162331

Transaction Analysis

Error Analysis: Errors were detected although the transaction was successful:
Network error communicating to backend 'http://infra.HA:662/sideCalls.asmx' - port error (HTTP)
Network error communicating to backend 'ftp://172.16.239.2/test.txt' - port error (HTTP)

This transaction was executed while probe was enabled.

Elapsed Time: 78 ms

Memory

Type	Direction	Time	Elapsed (ms.)	Status	Details
SQL	N/A	05/23 08:54:44.974	0	ERROR	SQL data source 'ORA_MYLOCALDB.DS' is not available
LDAP	request	05/23 08:54:44.967	0	ERROR	ldap://172.16.239.2:10389/dc=dpod%2cdc=test?memberOf?cn=dpodAdmin. Error querying server 172.16.239.2: Cannot connect. See system logs for details.
HTTP	request	05/23 08:54:44.959	1	ERROR	http://BackendForEUR.HA:2553/
SOAP	request	05/23 08:54:44.949	1	ERROR	Error parsing reply. Could not open URL 'http://infra.HA:662/sideCalls.asmx'
FTP	request	05/23 08:54:44.941	1	ERROR	ftp://172.16.239.2/test.txt
MQ	request	05/23 08:54:44.930	1	OK	IN on dpmq://QMMONITER.QMGR/?RequestQueue=IN;PMO=2116

API Gateway

Service

New, Native API Gateway Service in DataPower

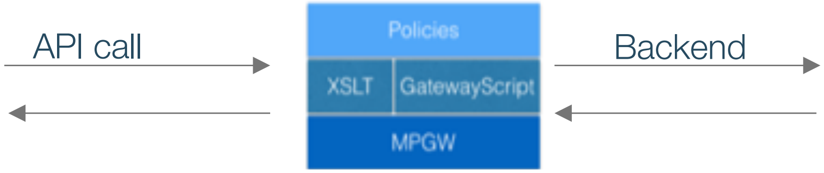
Up to 5X increased performance with natively built API Gateway using purpose-built technology for native OpenAPI/Swagger REST and SOAP APIs

Multi-cloud scalability and extensibility to help meet SLAs and improve client user experience

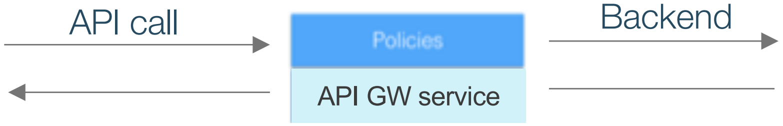
Optimized drag & drop built-in policies for security, traffic control and mediation including flexible OAuth, enhanced JSON & XML threat protection

Secure to the core with self-contained signed & encrypted image to minimize risk, plus proven security policies to quickly protect APIs

Before: DP Multi protocol Gateway Service



New: Native API Gateway Service



Policies for Enforcement on API Gateway Service

- **Gateway Script and XSLT policy support** provides flexible message mediation & dynamic security enforcement
- **Dynamic Routing support** through Conditional Policy
- **Enforce strong security** through Parse, JSON and XML Schema Validation policy
- **OpenID Connect** support to enable banks to meet PSD2 / Open Banking regulations
- **OAuth Token revocation** to enable self-service token management

API Gateway Service (APIGW)

Foundational	Security	Mediation
Invoke	API Key+	Map
Activity Log+	JWT Validate	JSON-XML
Rate Limit+	JWT Generate	Gateway Script
Throw	OAuth Policy	XSLT
Set Variable	Parse (Threat Detection)	
Conditional	Validate*	
	User Security	
	OpenID Connect*+	

+ Configured outside API Assembly   * Available as part of 2018.4.1.1

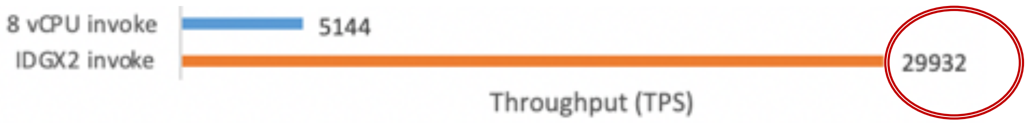
Single Gateway supports 30K TPS with 8 ms latency!

Natively built API Gateway using purpose-built technology for native OpenAPI/Swagger REST and SOAP APIs

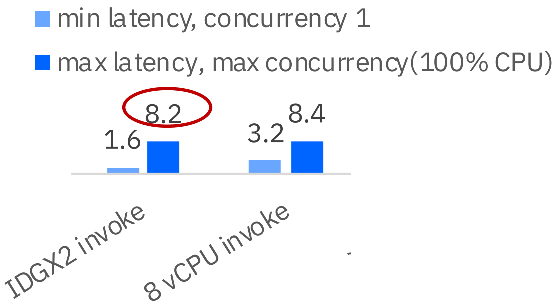
Multi-cloud scalability and extensibility to help meet SLAs and improve client user experience

IDG X2 physical appliances use the equivalent of 48 vCPU

Max Throughput @ 100% CPU



Latency(mS) @ Min/Max Concurrency

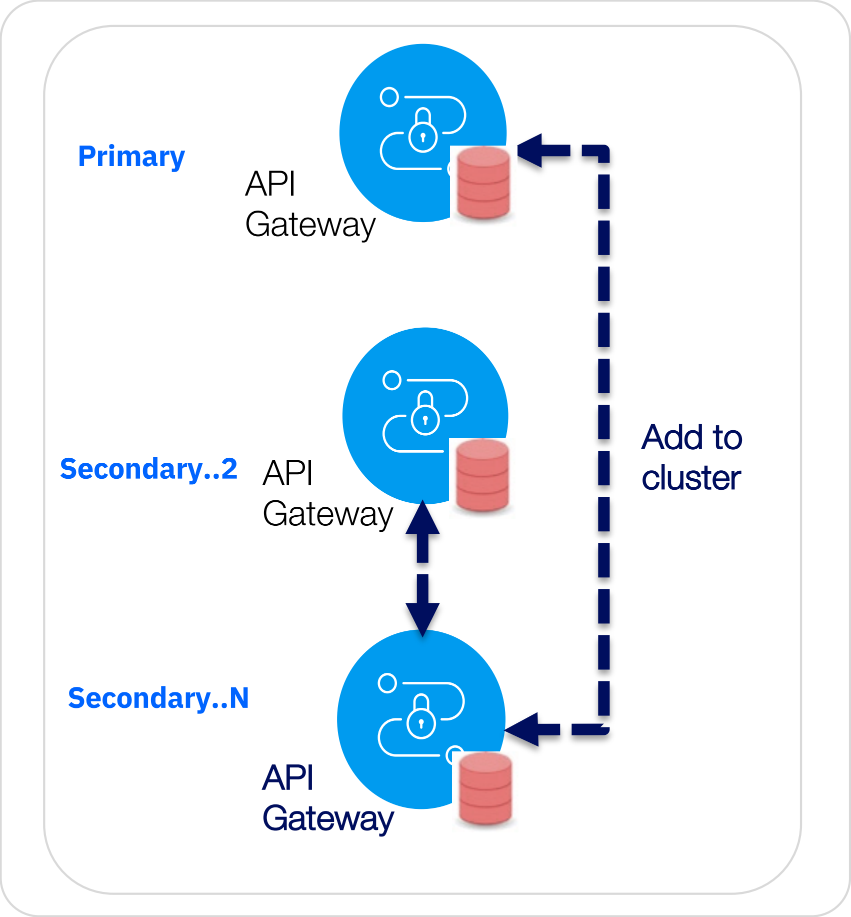


Runtime Scale for Usage Spikes

Scale API gateway clusters to adhere to SLAs and handle volume spikes

Autonomous gateway management, deploy gateways on multiple clouds without any operational impact

Self-healing gateways optimizing scaling for usage spikes to improve runtime resiliency



What’s Next

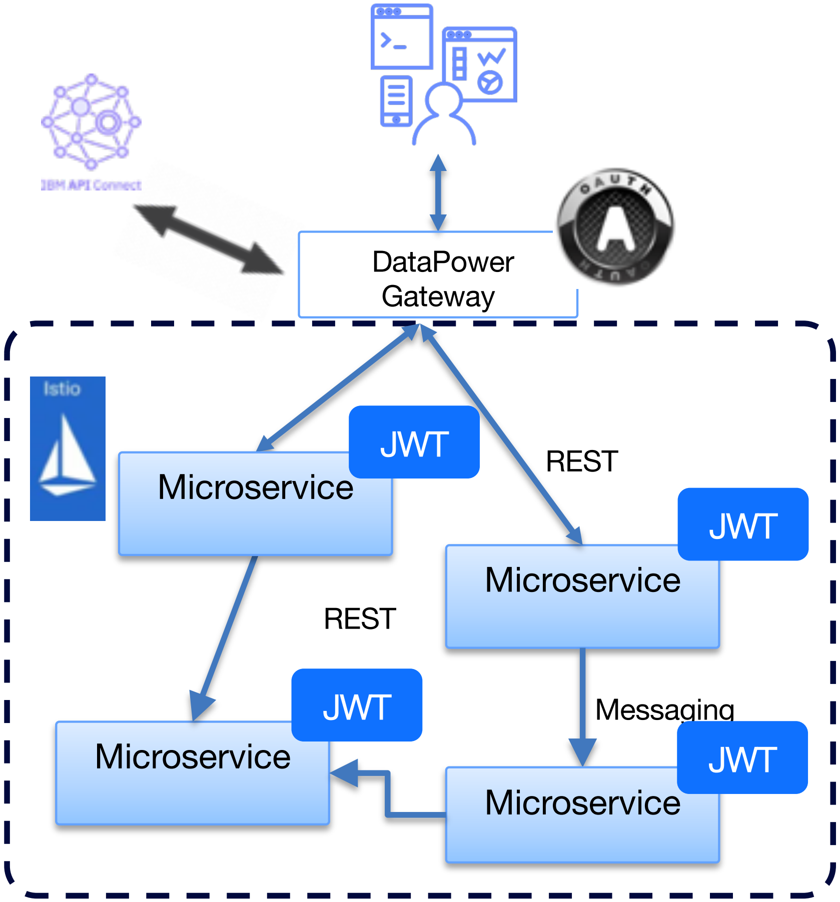
Istio Service Mesh Integration for Security, SLA & Resiliency

Istio ready architecture complimenting API management and microservices management

No code end to end security by combining ingress security (i.e. OAuth) with microservices security (i.e. JWT validation)

Intelligent and dynamic routing based on business logic via meta-data injected into the mesh provided by API Connect

First API management platform to propagate API security, rate limit from API Gateway into Istio for micro services SLA (i.e. Gold vs. Silver users)



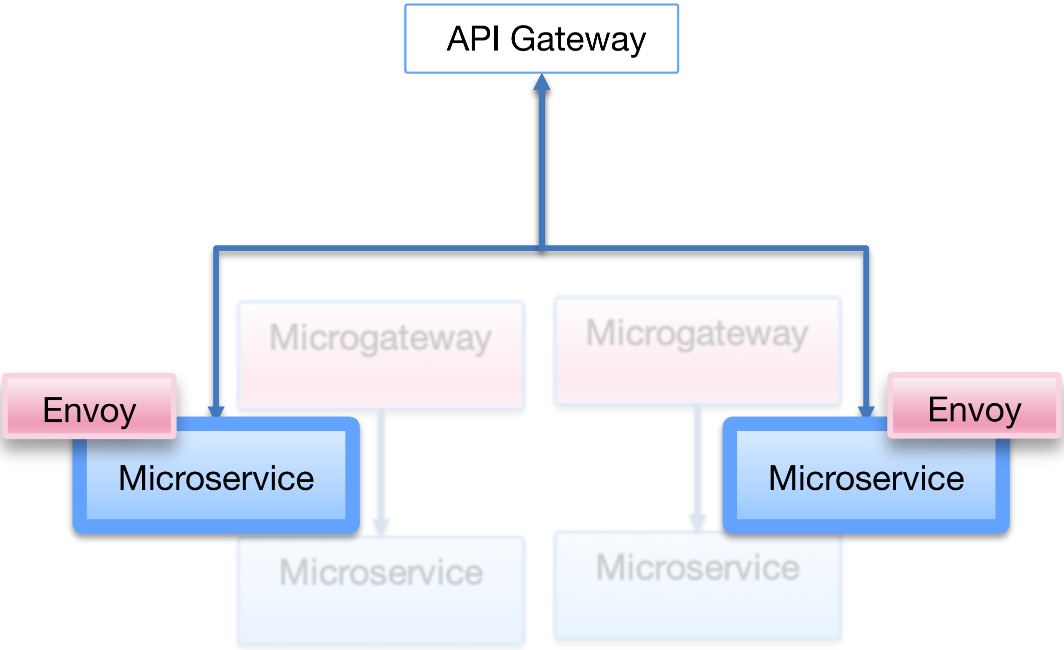
Istio versus Microgateway Point of View

Takeaway: Sidecar proxies replace Microgateways, enabling easier deployment as part of the underlying infrastructure

Shift from Monolith to Microservices architecture recommends smaller "micro" components (servers, databases, Gateways) to avoid single point of failure

Microgateway is a lightweight proxy co-located and packaged together with backend services

Service mesh architectures provide a sidecar proxy (ie Envoy) that includes similar function to a Microgateway and is co-located with backend services



Secure & Manage GraphQL Endpoints (Preview)

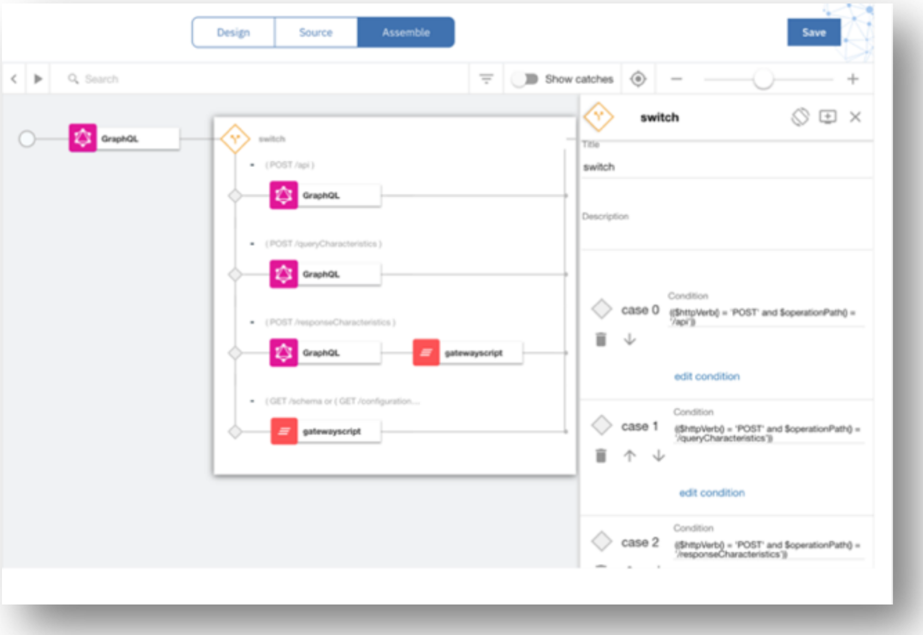
Next-Gen evolution of Gateway technology beyond Web services and REST with GraphQL support

Secure and Manage APIs with GraphQL backends, efficiently managing compute intensive services

Threat Protection against cyberattacks using advance query complexity analysis to prevent API-based attacks

Rate Limit GraphQL queries with consumer plans based on number of API calls & backend compute time

GraphQL



Title: switch

Description

case 0 — Condition: (($httpVerb() = 'POST' and $operationPath() = '/api'))

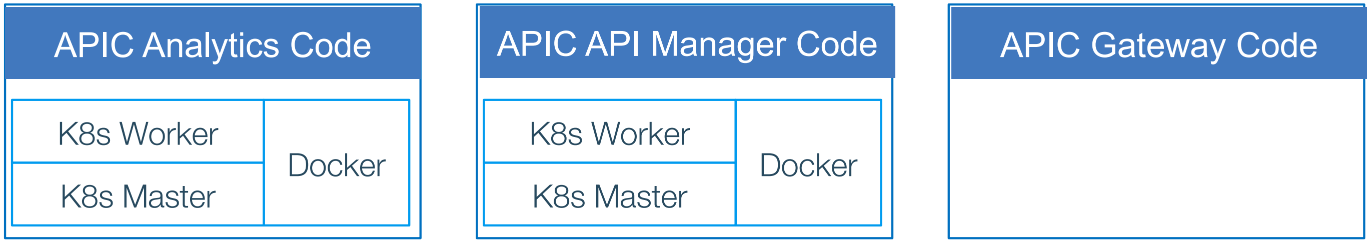
case 1 — Condition: (($httpVerb() = 'POST' and $operationPath() = '/queryCharacteristics'))

case 2 — Condition: (($httpVerb() = 'POST' and $operationPath() = '/responseCharacteristics'))

Best Practices

Topology

...



APIC Analytics Code

K8s Worker

K8s Master

Docker

APIC API Manager Code

K8s Worker

K8s Master

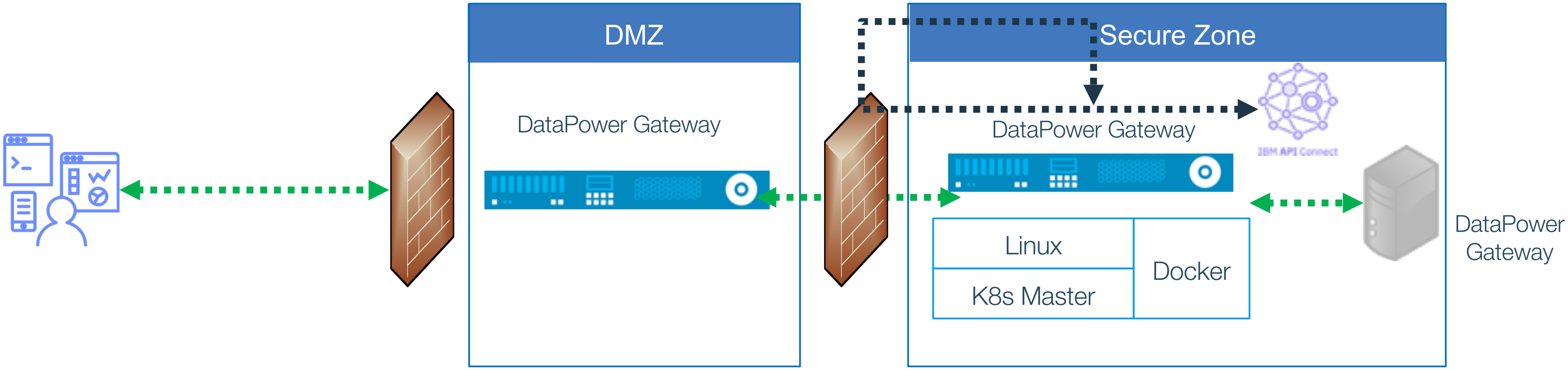
Docker

APIC Gateway Code

Analytics OVA: 2 cores

Manager OVA: 4 cores

Gateway OVA: 4 cores



DMZ

DataPower Gateway

Secure Zone

DataPower Gateway

Linux

K8s Master

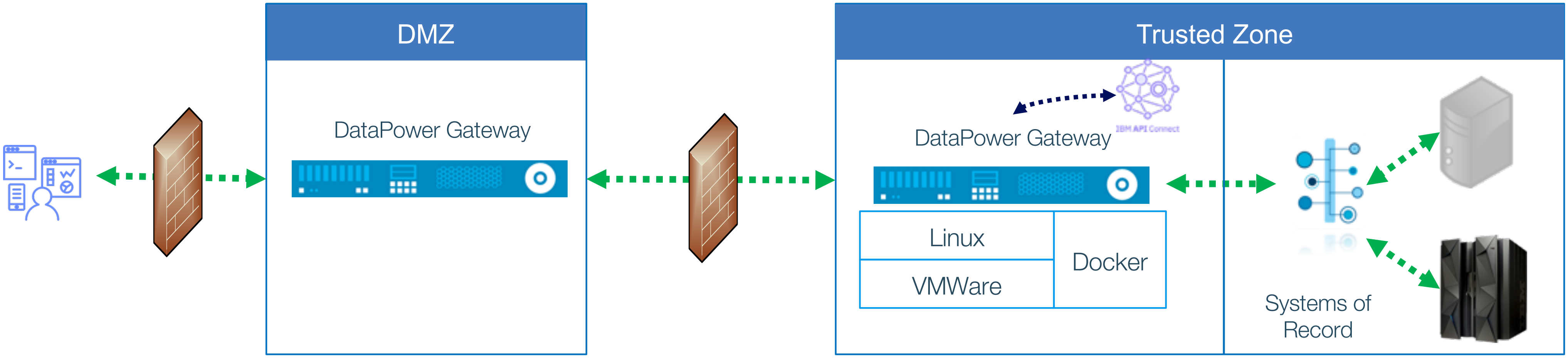
Docker

DataPower Gateway

Deployment Scenarios

DataPower Gateways are typically deployed in either the DMZ or Trusted Zone

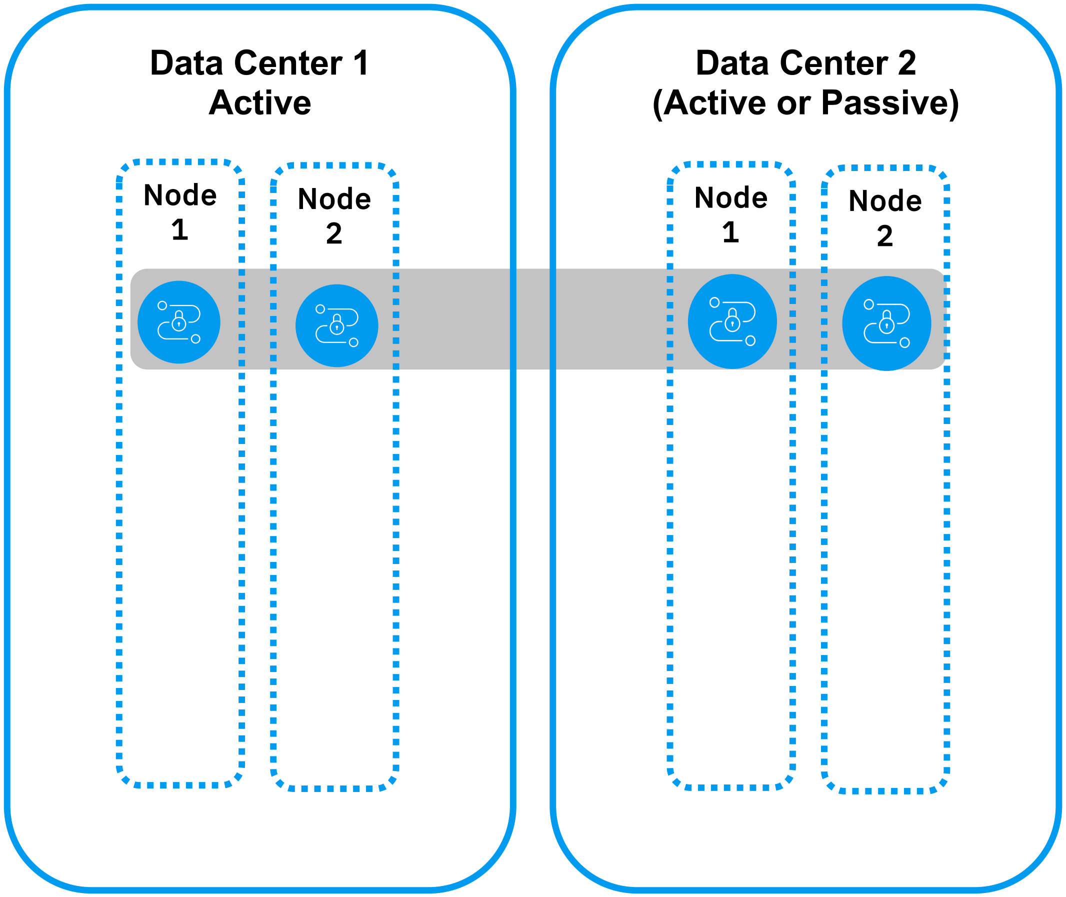
- Physical appliances are suitable for deployment in DMZ
- All form factors can be deployed in Trusted zone



Traditional Topology – Active for HA; Passive For DR

Traditional deployment consists of two data centers

- Two DataPower Gateways instances per Data Center
- Requires external load balancer to route traffic between data centers
- Optionally, use AO self-balancing to route traffic between DataPower Gateways within the data center
- Passive instances are pre-configured but without live traffic



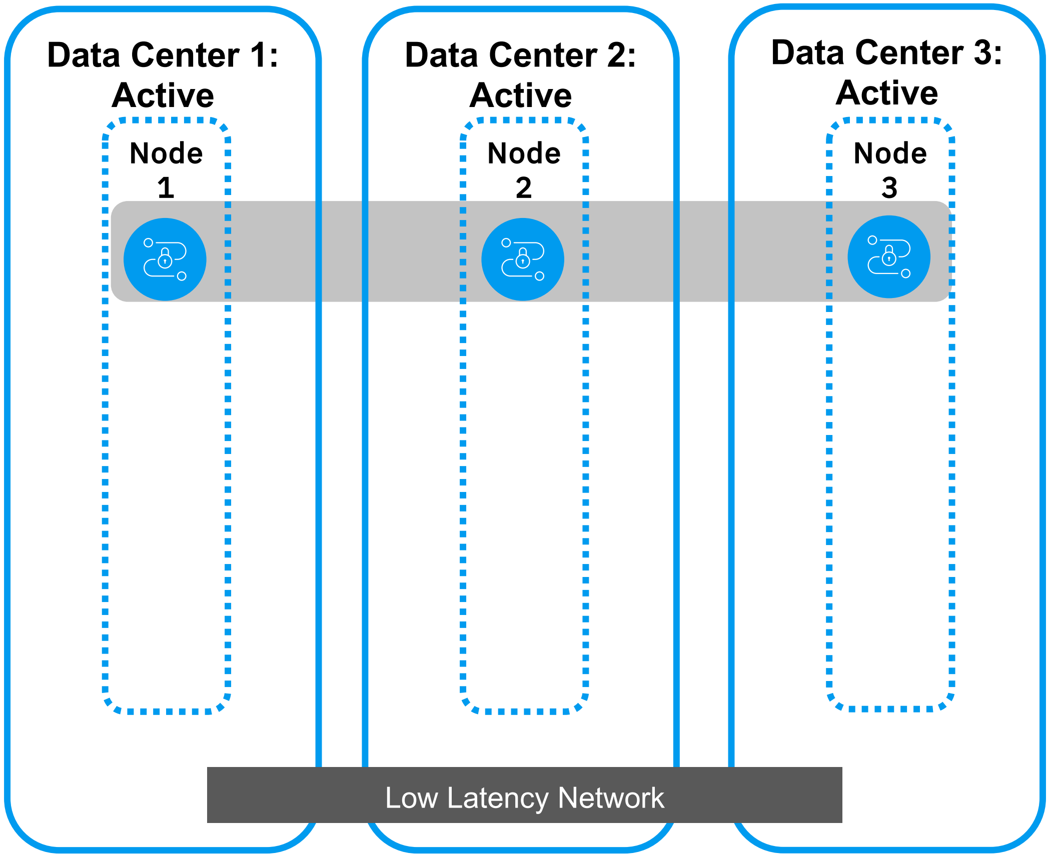
**Nodes represent physical appliances or VMs

Kubernetes Topology - Three Data Centers for HA

Deployment of three DataPower Gateway instances is required for HA in Kubernetes

Deployment with API Connect mandates three instances to ensure quorum

- Instances can be deployed within application domains / tenants to achieve quorum requirement



**Nodes represent physical machine or VMs

DevOps – Manage DataPower Configuration

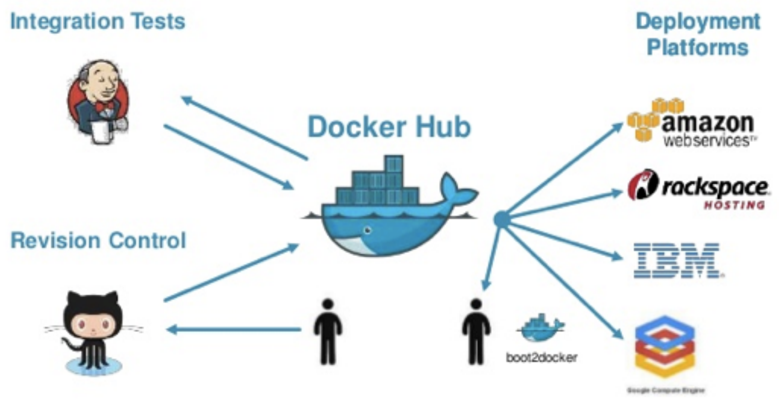
DataPower configuration is persisted on file system per domain

Programmatically modify configuration using following methods:

- Command Line Interface (CLI)
- SOAP Management interface (SOMA)
- REST Management interface (ROMA)

Manage environment / domain specific configuration

- Deployment policy objects
- DevOps pipeline to templatize and modify configuration



DevOps - Deploy DataPower Configuration

Deploy configuration and crypto material

- **Secure Backup/Restore** to manage configuration + crypto material
- **Import/Export** to management configuration only (keys managed separately if stored in cert/sharedcert folders)
- **Container/Linux only:** Map host machine volume (ie source control systems) to DataPower file system (local/config)

DataPower configuration management (DMAN) is an open source library based on Java and ANT that provides a wrapper to common DataPower management APIs

- https://github.com/ibm-datapower/datapower-configuration-manager/wiki/Quick-Start

Building Docker Images & Helm Charts

Create docker images to automate deployments of DataPower containers and automate provisioning

- Use `COPY` commands to push configuration to base image

Helm charts package Kubernetes configuration into a single archive, enabling tooling to deploy containers with user-driven values

- Example Helm chart available here: https://github.com/IBM/charts/tree/master/stable/ibm-datapower-dev
- Building your own Helm charts requires understanding of DataPower configuration and Helm / Kubernetes manifest files

`mycompany/datapower`

```
FROM ibmcom/datapower:latest
ENV  DATAPOWER_ACCEPT_LICENSE=true \
     DATAPOWER_WORKER_THREADS=2 \
     DATAPOWER_INTERACTIVE=true
COPY config/ /drouter/config/
COPY local/ /drouter/local/
EXPOSE 80 443 9090
```

```
docker run -itd \
   -v $PWD/config:/drouter/config:ro \
   -v $PWD/local:/drouter/local:ro \
   -e DATAPOWER_ACCEPT_LICENSE=true \
   -e DATAPOWER_INTERACTIVE=true \
   -e DATAPOWER_WORKER_THREADS=2 \
   -p  9090:9090 -p 80:80 -p 443:443 \
   --name datapower \
   mycompany/datapower
```

Key Management

Form factor drives the optimal approach to store sensitive information

- **Embedded & Network Hardware Security Module (HSM)** provides additional level of security using dedicated hardware
- **Virtual Appliances** store crypto material within flash memory with additional layer of security
- **Linux & Container** form factors map file system directories for easier DevOps

Use password aliases to mask sensitive information within firmware

Summary

- List of DataPower Gateway innovations
- DataPower Operation Dashboards overview
- API Gateway policies and performance
- Identify use cases for deployment within Istio
- Best practices for deploying DataPower Gateways for HA, including Kubernetes
- Architectural guidance for managing DataPower configuration

Notices and disclaimers

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

IBM®