IBM DataPower Gateway

DataPower 201

IBM DataPower Gateway
is the industry-leading Security & Integration gateway that help provide Security, Control, Integration, and Optimized access to a full range of API, Mobile, Web, SOA, B2B, and Cloud workloads.

Gateway trends

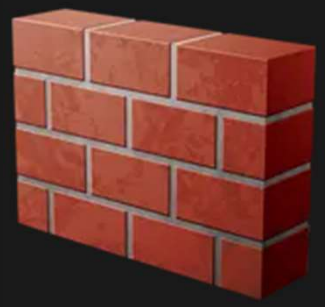
Cloud native architecture is driving the need for application-scoped gateways with minimal footprint

Adoption of latest standards require support for most modern protocols such as Kafka, AMQP, and HTTP/2 (gRPC)

Customers are seeking to simplify and automate operations including Gateway configuration deployment

Modern & consistent UXs are improving productivity driving new change in Gateway UX

End-to-end security with DataPower Gateways



Secure

- Latest Industry standard transport and events-based messaging
- Advanced Authentication, Authorization, and Audit
- Modern message protection with digital signature and encryption
- Transport protection with SSL/TLS processing

Control

- Rate limiting for quota enforcement
- Traffic control for service and application protection
- Extensive routing and error handling

Integrate

- Bridge latest and traditional protocols
- Payload Transformation offloading intensive and common operations
- Combine modern event- based and API workloads with traditional services

Optimize

- Caching for faster application response time and improved system throughput
- Load Balancing and advanced routing for processing traffic based on load and topology
- Custom acceleration to achieve highest levels of performance

History of Gateway Innovation

2005 IBM Acquires DataPower

2010 Web 2.0 (REST/ JSON)

2012 DataPower Virtual Edition

2013 API Management

2014 REST Management API

2015 JavaScript Runtime (Gateway Script)

2016 DataPower Gateway for Linux

2017 Tenant Isolation

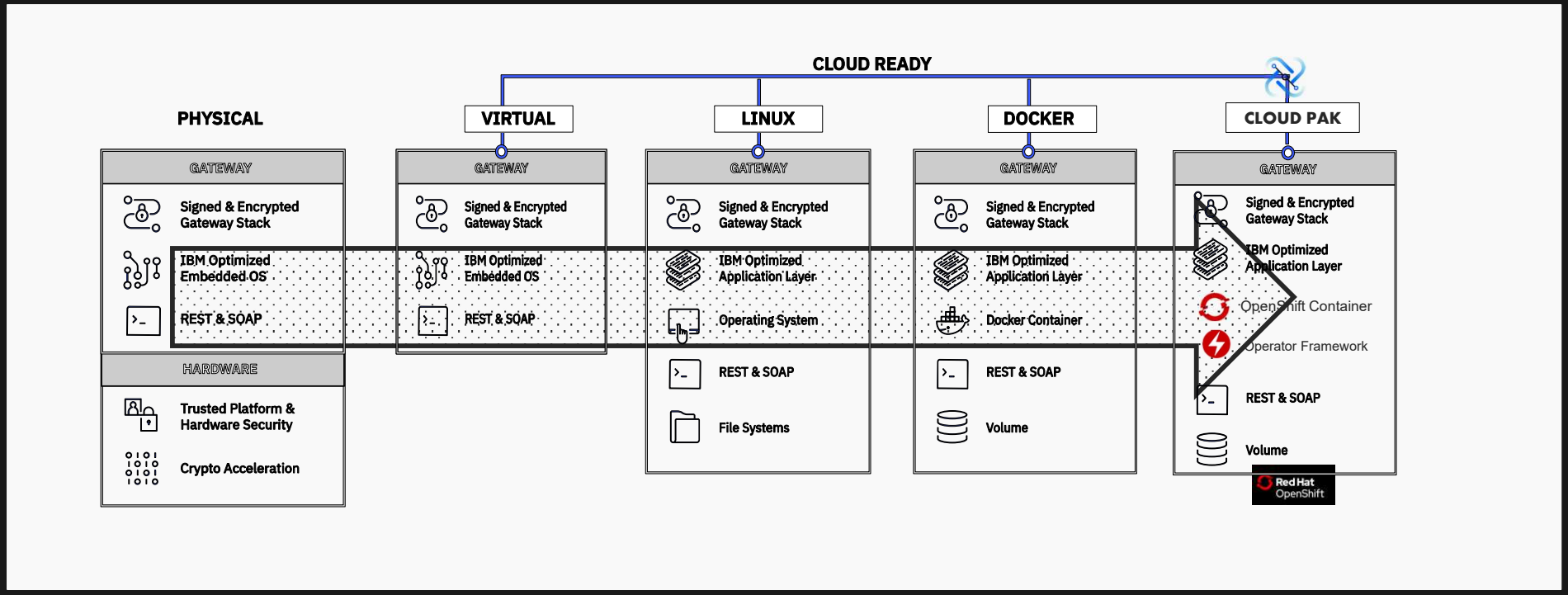
2018 API Gateway Service

2019 Security enforcement policies

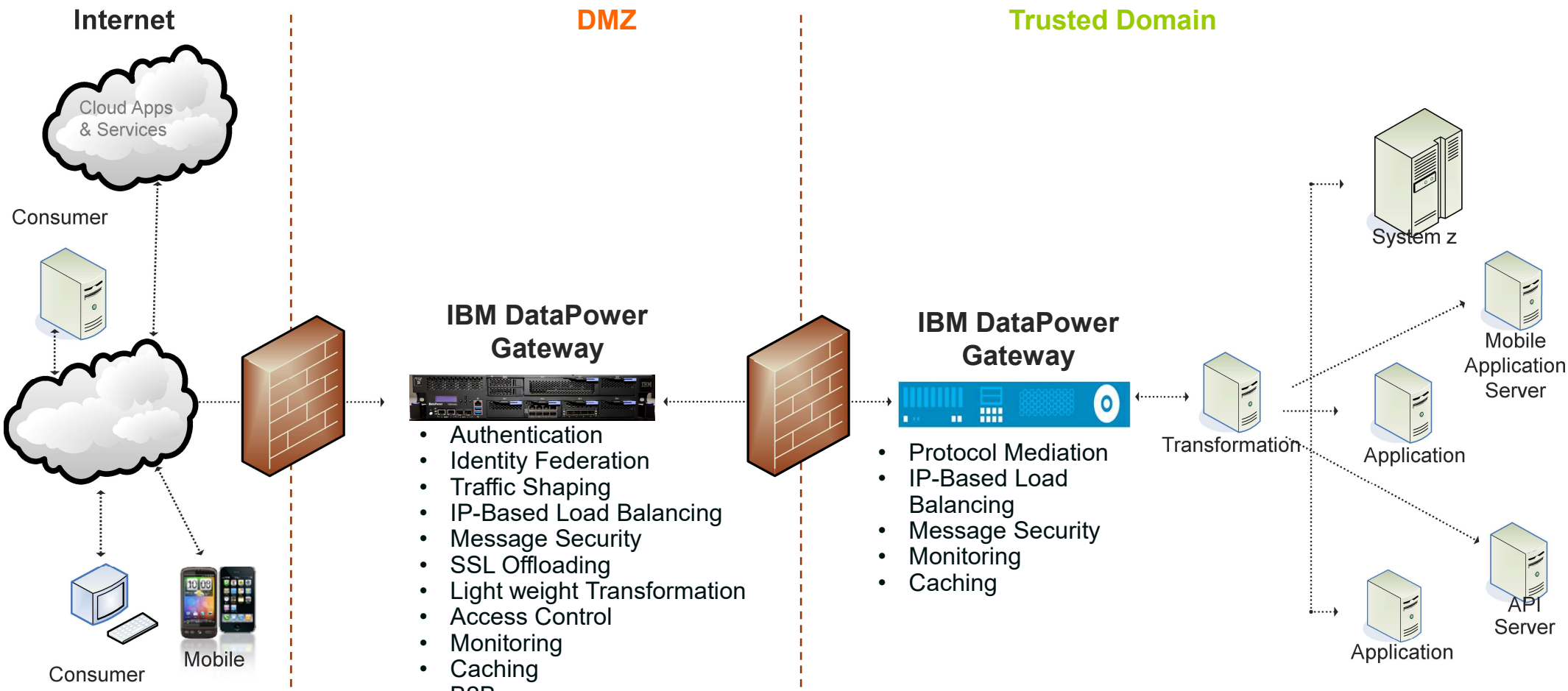
2020 Modern events-based messaging

Gateway choice and flexibility

Deploy Everywhere – Shift to Containers and Application Scoped Gateways



Core Use Cases



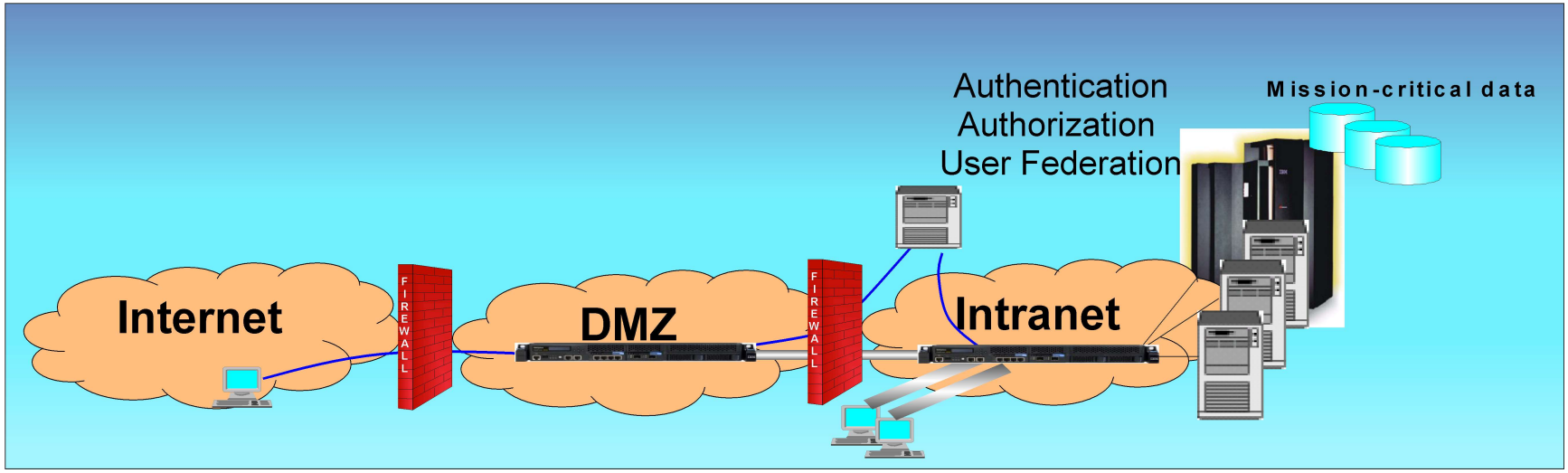
Deep Dive into Gateway Capabilities

Security

- Industry standard protocols including OAuth, SAML, XACML, JWT, WS-Security, LTPA, and Kerberos to secure access to applications
- Authentication, Authorization, and Auditing to converge security enforcement
- Token translation to easily integrate between many security protocols
- Message protection with digital signature and encryption capabilities
- Transport protection with SSL/TLS processing

Security - Data and End Point Protection

- ✓Secure access to Web and legacy applications
- ✓Converged security enforcement
- ✓Rock solid DataPower platform
- ✓Leverages enterprise security and policy managers

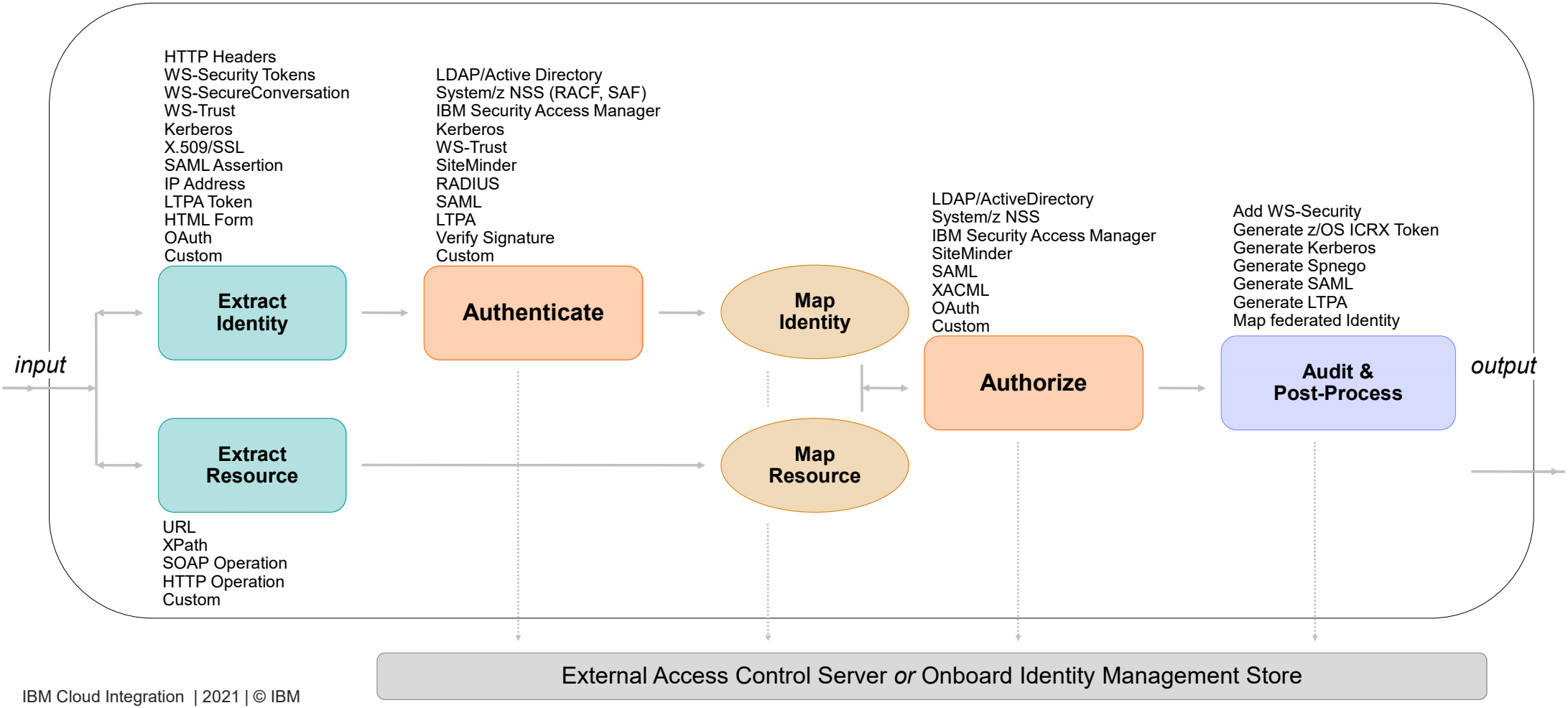


- **Protect data and other resources on the appliance and protected servers**
  - **System availability**
    - Protect against unwanted access, denial of service attacks, and other unwanted intrusion attempts from the network
    - Only allow “valid” messages through
  - **Identification and Authentication**
    - Verify identity of network users
  - **Authorization**
    - Protect data and other system resources from unauthorized access

- **Protect data in the network using cryptographic security protocols**
  - **Data End Point Authentication**
    - Verify who the secure end point claims to be
  - **Data Origin Authentication**
    - Verify that data was originated by claimed sender
  - **Message Integrity**
    - Verify contents were unchanged in transit
  - **Data Confidentiality**
    - Conceal clear-text using encryption
  - **Threat Protection**
    - SQL,XPATH injection
    - JSON and XML Protection
    - Custom message filtering

Security - Authentication, Authorization, and Auditing (AAA)

Flexible control framework utilizing industry standard protocols



Deep Dive into Gateway Capabilities…

Control

- Rate Limiting to enforce quota
- Traffic Control to protect services and applications from over-utilization
- Content-Based Routing
- Flexible Error handling

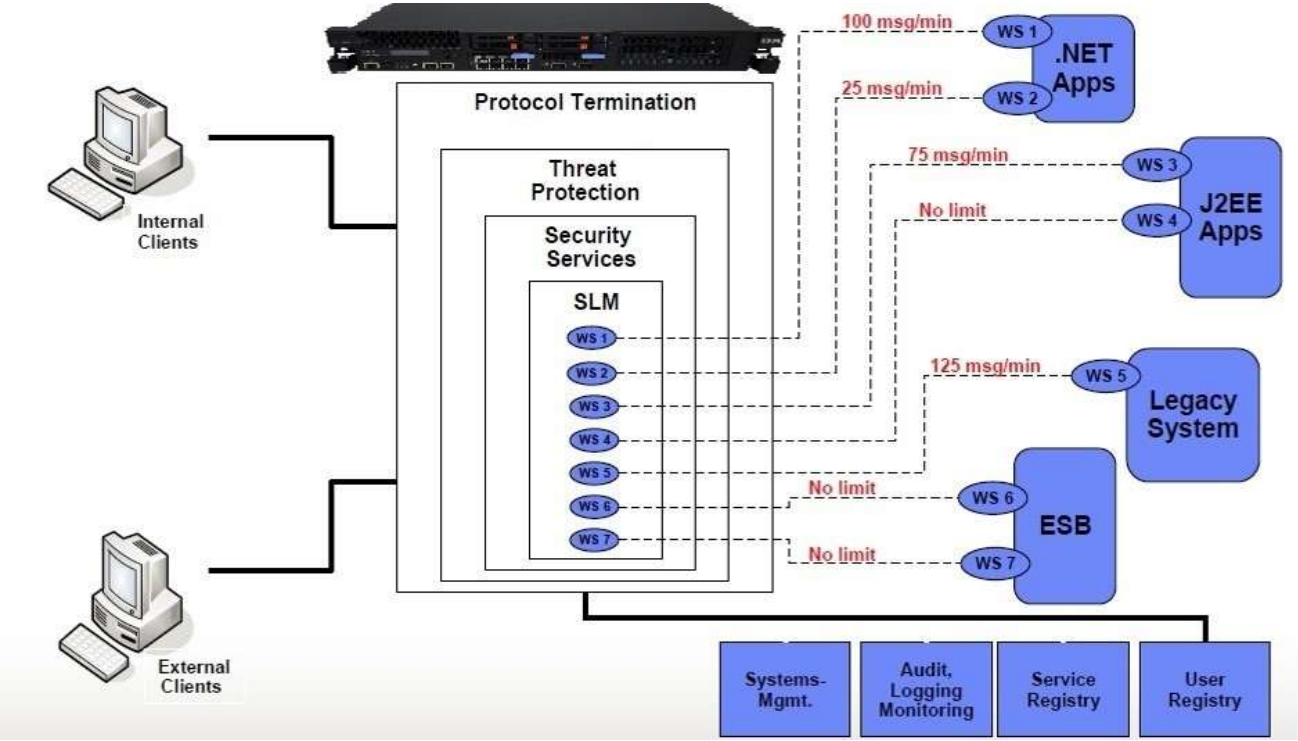
Control - Dynamic Routing

- Dynamically route based on any message content
  - Attributes such as the originating IP, requested URL, protocol headers, etc.
  - Data within the message such as SOAP Headers, XML, Non-XML content, etc.

- Query a repository for routing information
  - XML files, Databases, Web Servers, and others

Control - Rate Limiting and Re-Routing

- Protect services and applications from over-utilization and enforce quota
  - Frequency based on concurrency OR based on messages per time period
  - Take action when exceeding a custom threshold:
    - Notify (or log), Shape (or delay), Throttle
- Failure and Latency Re-routing
  - Based on back-end or total latency. Rerouting to secondary Datacenter/Cloud when average thresholds exceeded.
  - Route to secondary Data Centers based on service availability through built-in back end load balancing functionality



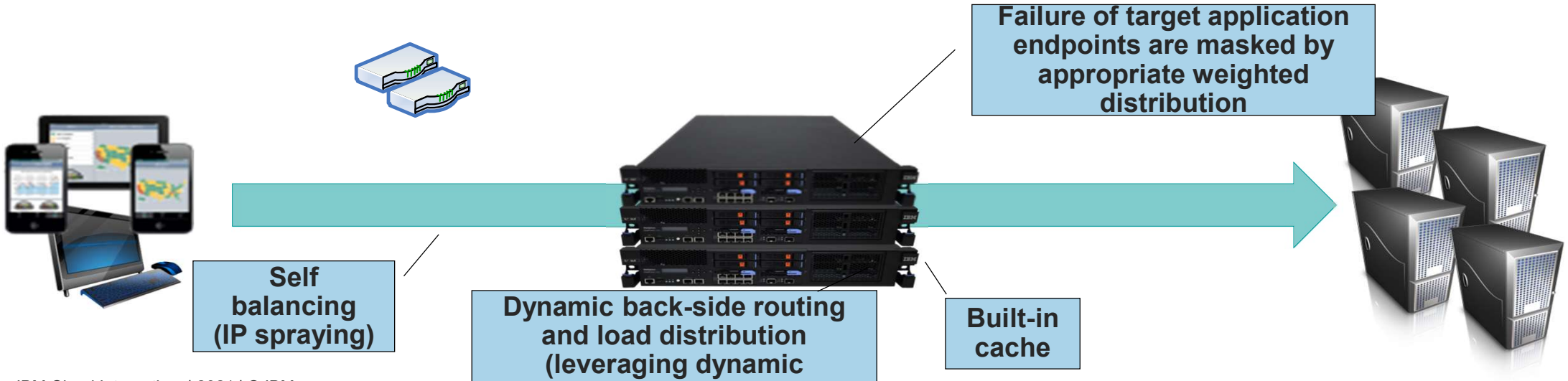
Deep Dive into Gateway Capabilities…

Optimization

- SSL/TLS Offload and Connection Pooling
- Intelligent load distribution by leveraging dynamic runtime conditions to distribute load based on topology and workload
- Front Side self load balancing
- Caching (Local and External) for faster application response time and improved system throughput
- Custom GatewayScript and XSLT acceleration to achieve highest levels of performance

Optimization – Transaction Distribution and Cache

- **Self Balancing:** Self balance across a cluster of appliances
  - Replace front-end IP load balancer
  - Enables connections to be preserved, without loss, during failover scenario
- **Dynamic** and **Intelligent Load Distribution** to backend systems
  - Replace backend load balancer
- Auto-discovers application targets and distributes load using **On-Demand-Routing** dynamic feedback mechanism
- Provides several options for enabling **Session Affinity**
- **Cache application response** data locally or in a caching grid



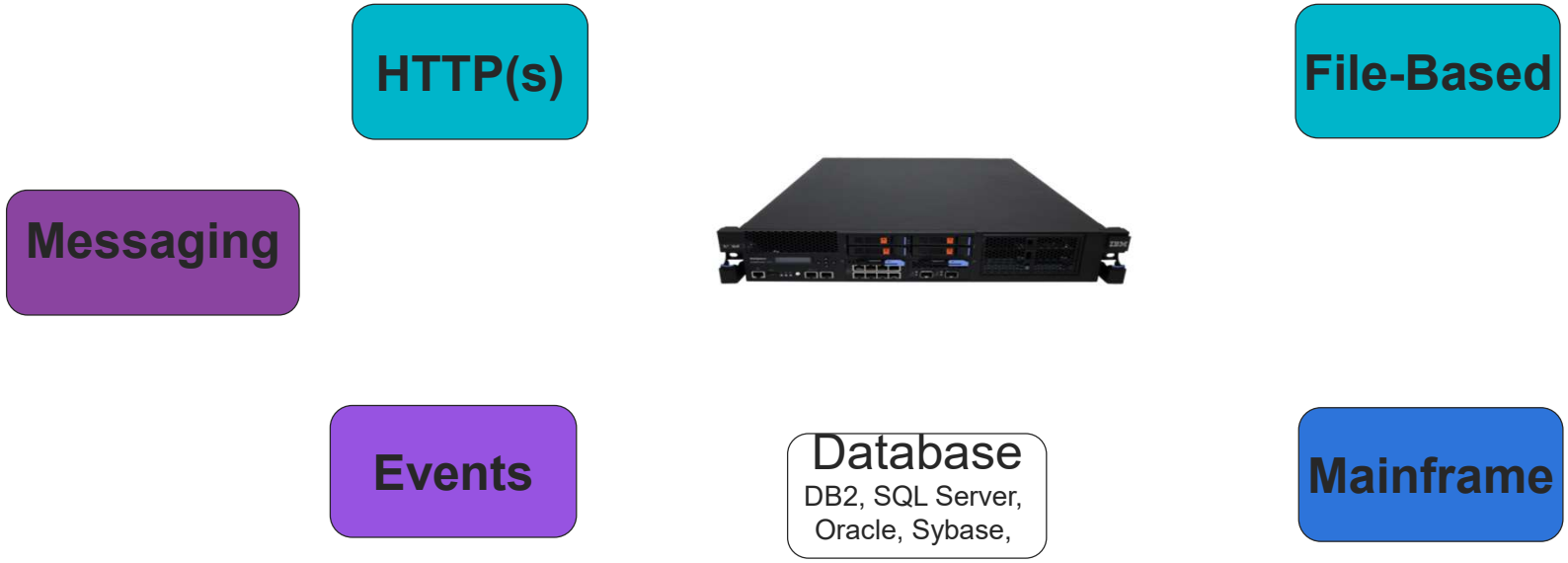
Deep Dive into Gateway Capabilities

Integration

- Transform Payloads (JSON,XML,CSV,..) to offload intensive and common processing
- Bridge Transports (HTTP,MQ, Kafka, AMQP, SFTP,..)
- Database Connectivity (DB2,Oracle,..) and file delivery of information sensitive data
- B2B Integration to provide secure proxy solution in the DMZ with AS1, AS2, AS3, AS4, EDIINT, … protocols

Integration - Transport Protocol Translation

- **Integrate disparate transport protocols** with extreme ease
  - No dependencies between inbound “front-side” and outbound “back-side”
  - Examples: HTTP(s), IBM MQ, AMQP, Kafka, WebSphere JMS, Tibco EMS, SFTP, FTP(s), NFS, IMS, Database (DB2, Oracle, Sybase, SQL Server)
- **Support synchronous, asynchronous**, pub-sub, assured-delivery, once-and-only once message patterns



Integration - Content Transformation

- Transform message and header content
- High speed transformation provided via GatewayScript (JavaScript) and XSLT
- IBM Transformation Extender runtime engine for graphical mapping support

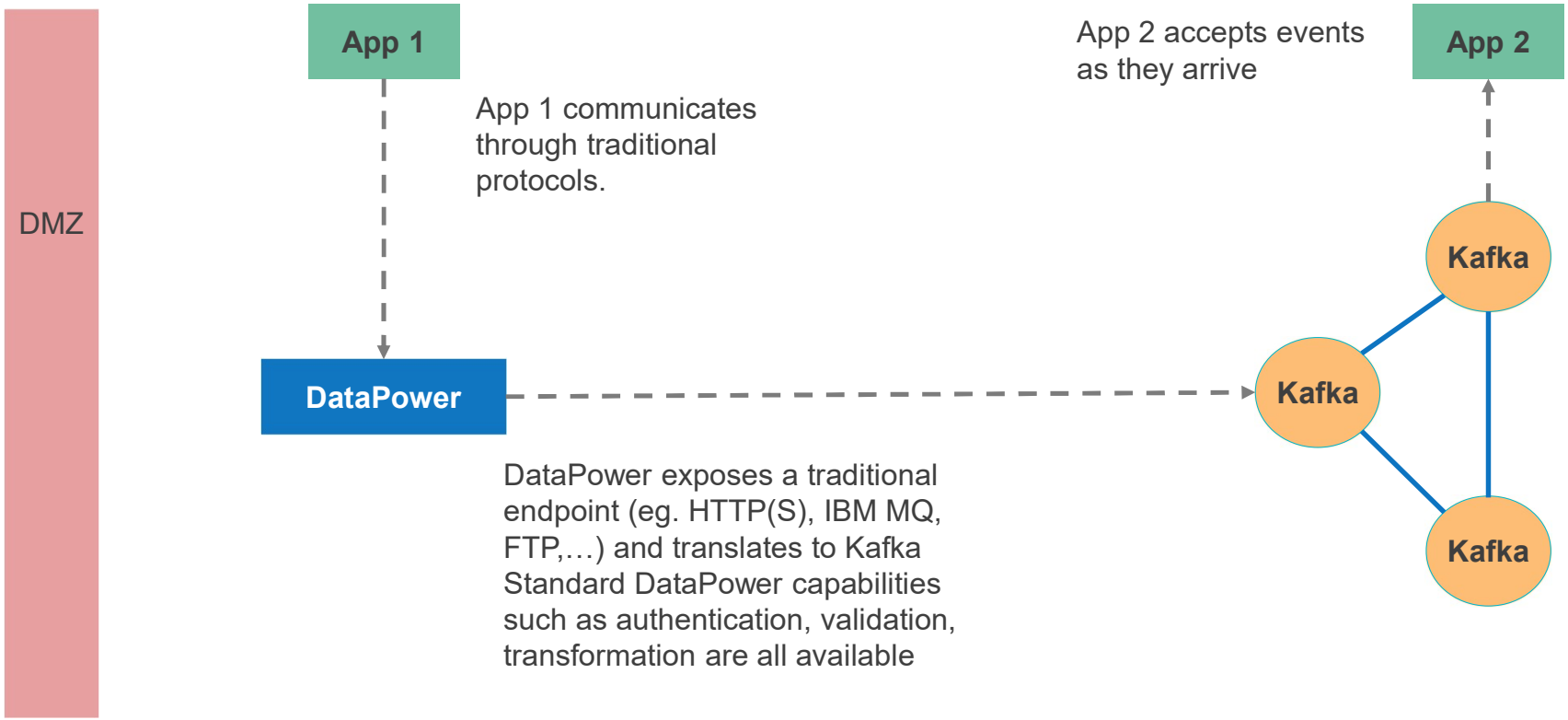
Modern Messaging with Event Driven Architectures and Transport Protocols

Mediate between synchronous and asynchronous protocols without worrying about the underlying protocol details

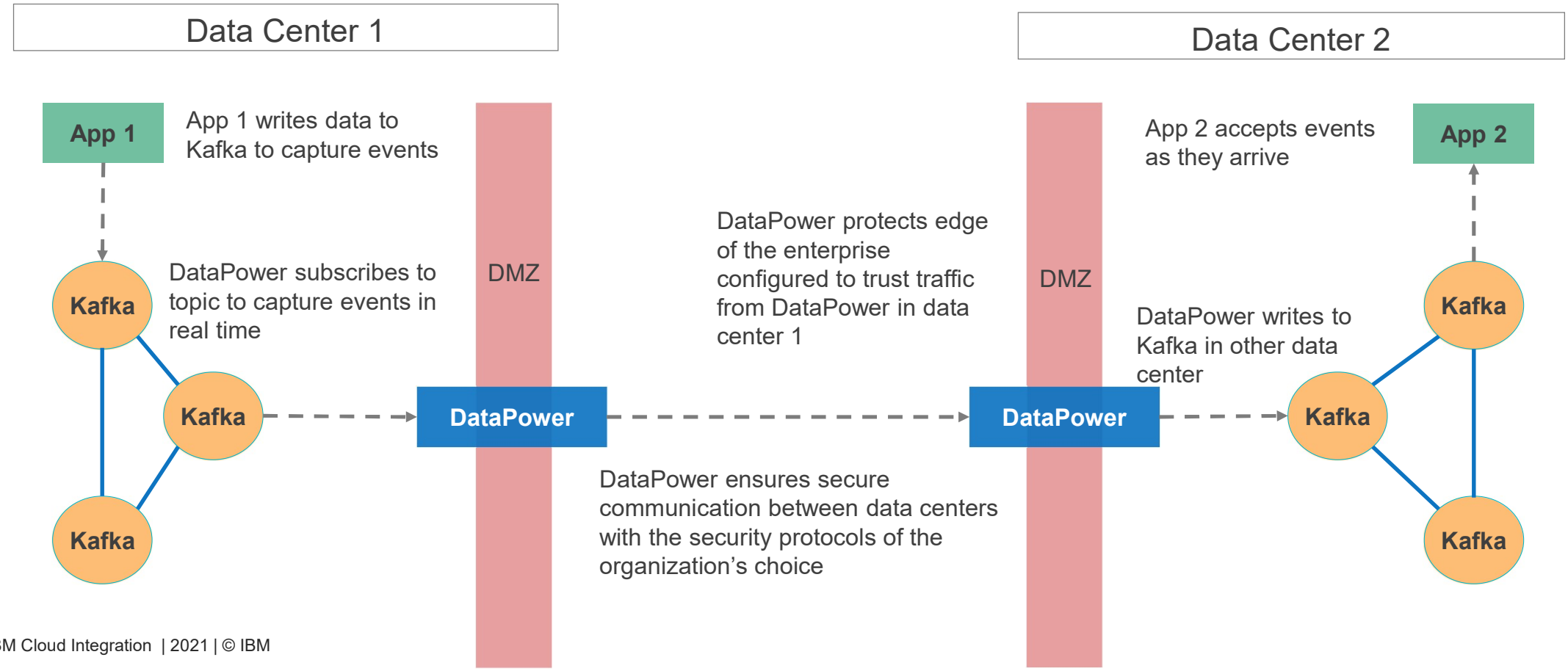
Increased message reliability using AMQP & MQ to provide confidence in delivery of mission critical analytics data

High Speed HTTP/2 web protocol for modern API's/Services including gRPC support

Use Case - Protocol Translation to Kafka

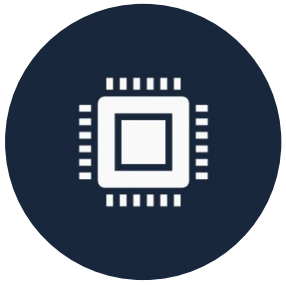


Use Case - Secure Kafka communication between Data Centers



Native AMQP Support

Supports IBM DataPower policies for ease of transformation, validation, encryption, authentication and other security policies



Bridge disparate transport protocols, such as HTTP, IBM MQ, SFTP and Tibco EMS with AMQP

Message reliability providing confidence in delivery of mission critical data

Safeguard for over utilization of resources and optimized workload delivery

Modules - Extensible Gateway Platform

Application Optimization Module
- ❑ Frontend self-balancing
- ❑ Backend intelligent load distribution
- ❑ Session affinity
- ❑ z Sysplex Distributor integration

Integration Module
- ❑ Any-to-Any transformation (tool based)
- ❑ Database connectivity
- ❑ Mainframe IMS connectivity

Tenant Isolation Module
- ❑ Enables partitioning of physical gateway
- ❑ Each tenant runs independently
- ❑ Each tenant can run different firmware levels
- ❑ Isolates CPU and memory to each tenant

B2B Module
- ❑ B2B DMZ gateway
- ❑ EDIINT AS1,AS2,AS3, AS4, ebXML
- ❑ Partner profile management
- ❑ B2B transaction viewer
- ❑ Any-to-Any transformation (tool based)
- ❑ Database connectivity

TIBCO EMS Module
- ❑ Integrate with TIBCO EMS messaging middleware
- ❑ Support for queues & topics
- ❑ Load balancing & fault-tolerance

IBM DataPower Gateway (Base)

Secure
- Authentication, authorization
- Security token translation
- Service / API virtualization
- Threat protection
- Message schema validation
- Message filtering
- Message digital signature
- Message encryption
- AV scanning integration

Integrate
- Transport protocol bridging
- Message transformation
- Message enrichment
- MQ Message Support
- AMQP Message Support
- Kafka Support
- Hybrid cloud connectivity
- JavaScript, JSONiq, XSLT, XQuery

Control & Manage
- Quota & rate enforcement
- Latency monitoring and optimization
- Content-based routing
- Message accounting
- Integration w/ governance, management & monitoring platforms

Optimize & Offload
- SSL / TLS offload
- Hardware accelerated crypto
- JSON, XML offload
- Local response caching
- Distributed caching with WXS
- Backend load balancing

Deployment and Operations

DevOps – Manage Gateway Configuration optimized for platform

Currently for appliances

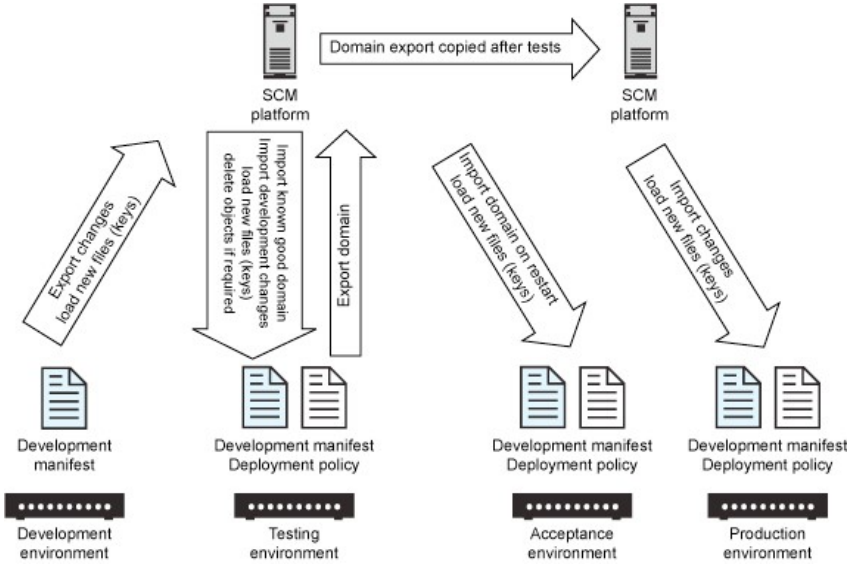
DataPower configuration is persisted on a file system or remotely with logical separation (domain)

Programmatically modify configuration using:

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

Manage environment/domain specific configuration:

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

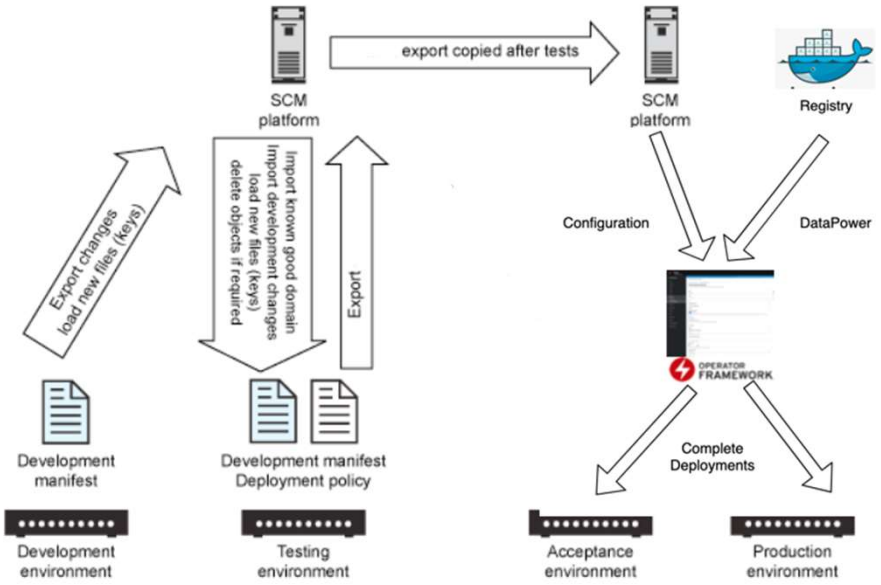


DevOps – Manage Gateway Configuration optimized for platform

For clouds and containers

DataPower configuration is built from your current configuration or other DataPower

Configuration information integrated with DataPower image using Kubernetes Operators and deployed



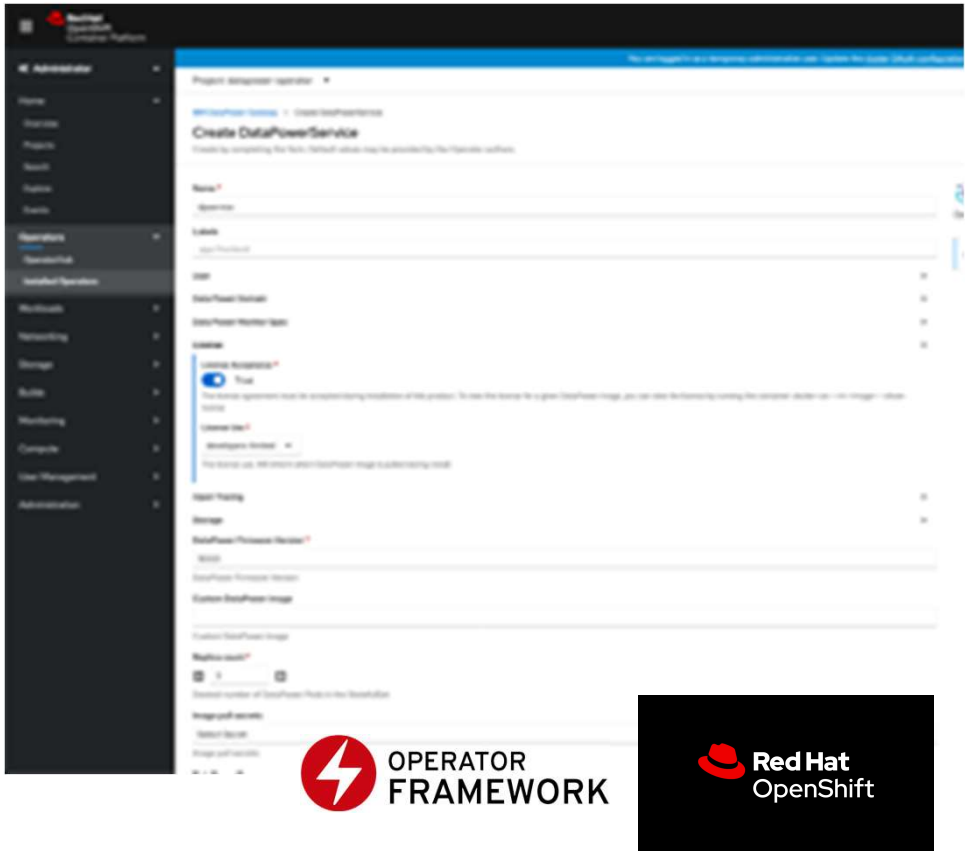
RedHat OpenShift Operators

DataPower extends the vision of containerized deployment with its support for RedHat OpenShift Operators. Operators ease deployment and management by combining a simplified administrative user experience with an automated deployment and monitoring system

Containerized DataPower Deployments

Simplified General Gateway Configuration

Streamlined DataPower Operations Management



Key Management

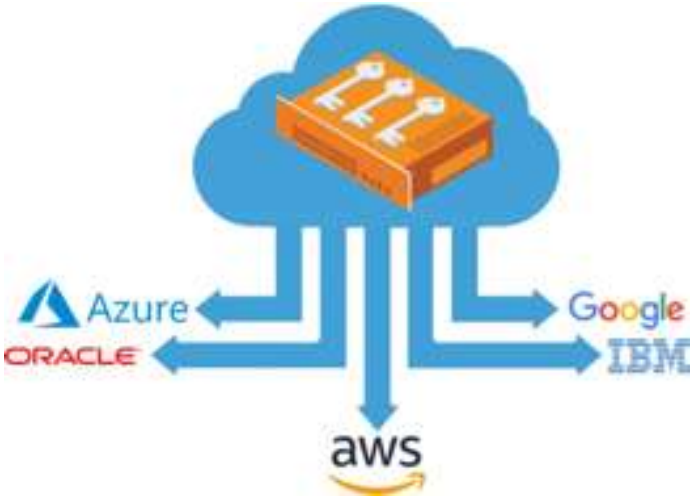
Form factor drives the optimal approach to store sensitive information

- Embedded hardware or network security module 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

DataPower Modernization

- **Auto scaling of Gateway** pods based on load
  - Integration with service Mesh/Istio
  - Control deployment to optimize licensing costs
  - Control level of resource use of components

- **Integrate with Cloud HSM providers** for
  - Highest levels of crypto security in public cloud (Azure and IBM Cloud)
  - Key Management and Offload TLS operations

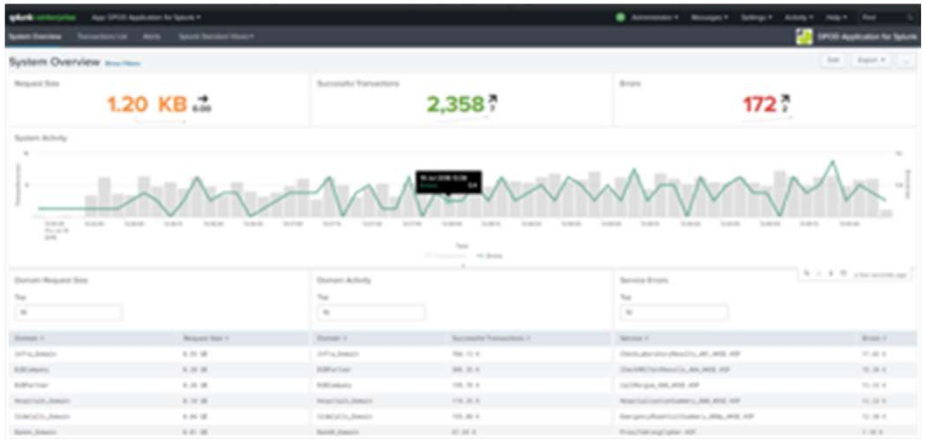


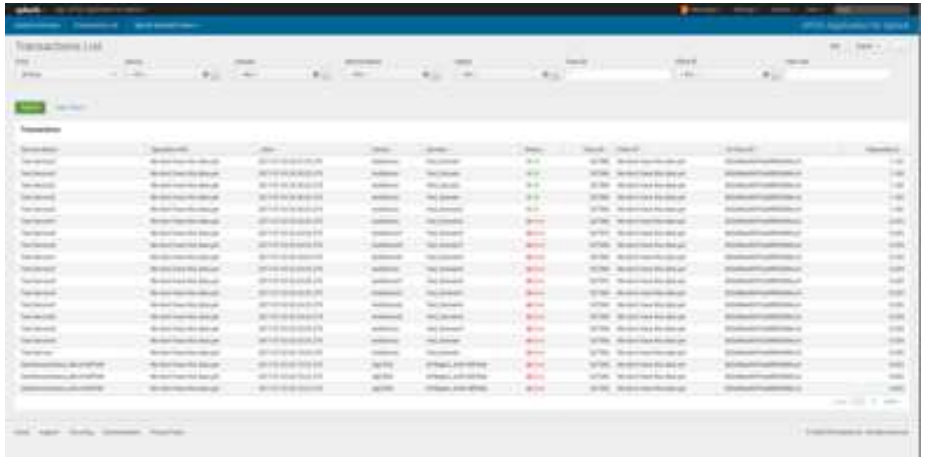
- **Custom header value** support for JSON Web Encryption

DataPower Operations Dashboard

Troubleshooting with DataPower Operations Dashboard

- **Powerful** DataPower and API diagnostics with detailed views across latency, version, policy, and consumer – provides first failure data capture to speed problem diagnosis
- **Non-intrusive tracking** of transactions across multiple gateways without any manual policy instrumentation
- **Supercharged performance** for demanding workloads via new distributed, federated server architecture
- **Robust Configuration Management** to simplify day to day operations
- **User control** to provide secure access via roles



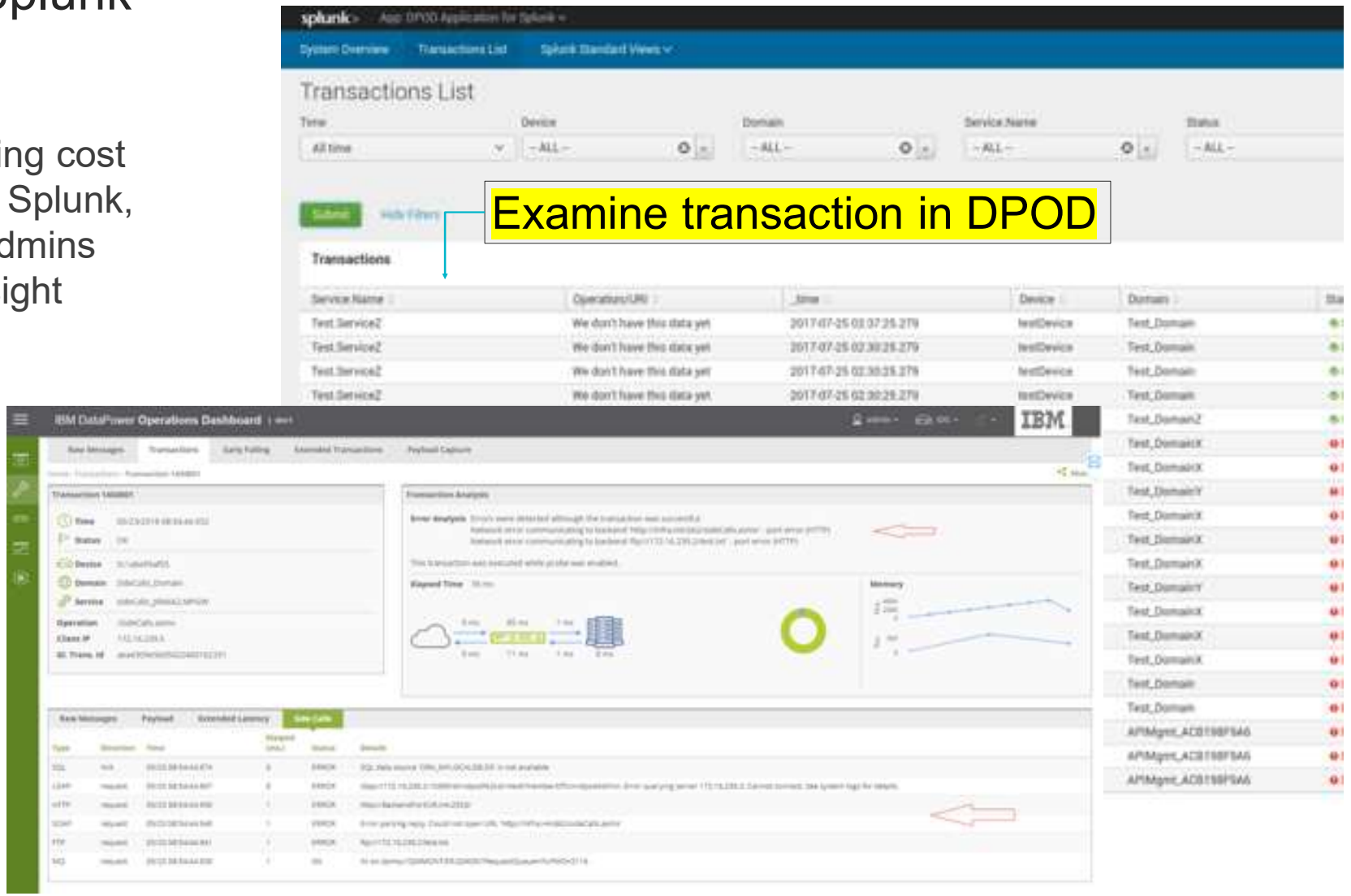


DPOD Plugin Provides Enhanced APM Integration

- Application **Performance Management (APM)** solutions provide an enterprise view of system health and performance
- **Deep-transactional insight** into API and Gateway transactions

DPOD plugin for Splunk

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



Thank you