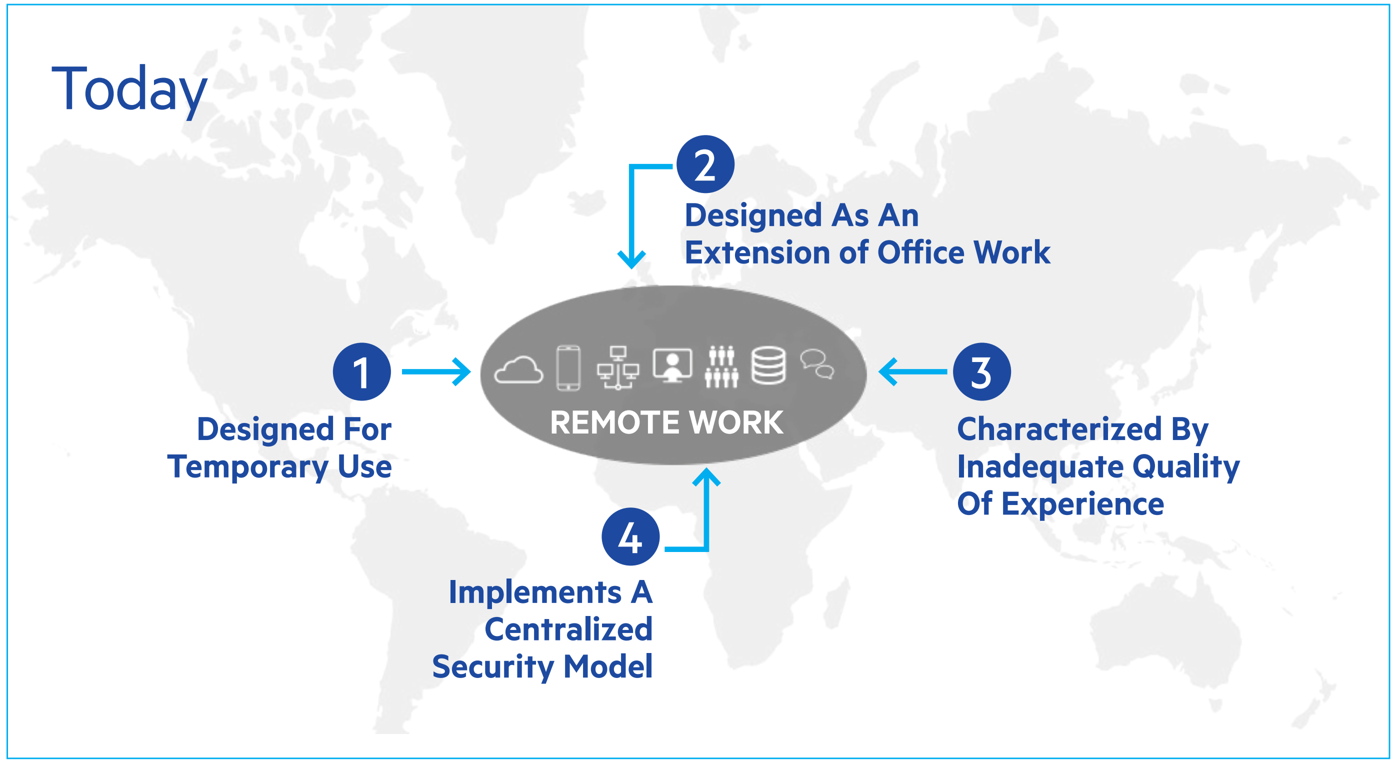
PERVASIVE DATACENTER ARCHITECTURE (PDx™)

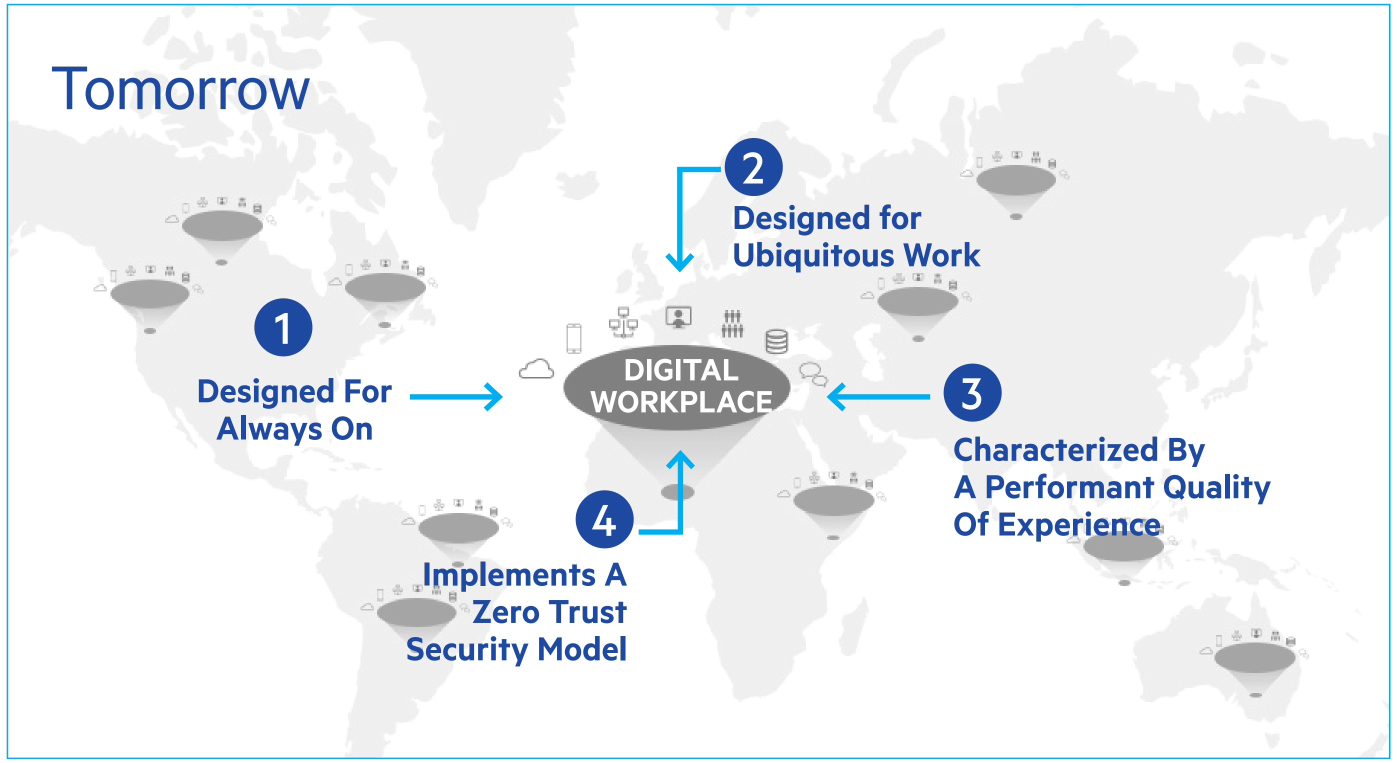
DIGITAL WORKPLACE

BLUEPRINT

INTRODUCTION

Many of today's remote worker architectures are not suited to the modern digital workplace. Having been deployed as an extension of the classic centralized IT infrastructure stack, they are not optimized for latency-sensitive and data-intensive modern application workflows. Furthermore, the inflexible nature of a centralized security stack, and the performance challenges of centralized data repositories and application hosting have a negative impact on the quality of experience. The modern digital workplace experience is designed for ubiquitous, performant, and always-on secure access to data and applications.


Today
2 Designed As An Extension of Office Work
1 Designed For Temporary Use
REMOTE WORK
3 Characterized By Inadequate Quality Of Experience
4 Implements A Centralized Security Model


Tomorrow
2 Designed for Ubiquitous Work
1 Designed For Always On
DIGITAL WORKPLACE
3 Characterized By A Performant Quality Of Experience
4 Implements A Zero Trust Security Model

1 Increased usage results in compute bound performance bottlenecks

2 Backhauls the user to centralized systems, resulting in network bound performance bottlenecks

3 Users unpredictability routed across Internet negatively impacts customer/ employee experience

4 Centralized security enforcement via backhaul doesn't address vulnerability points or improve security posture

1 Capacity is hosted at points of presence and interconnected to clouds to create elasticity

2 Traffic is consolidated at points of presence and interconnected to local services optimized for latency, throughput and ubiquity

3 Users, things, networks and capacity are integrated within proximity of centers of data exchange to optimize workflow & experience

4 Security controls are hosted and interconnected at points of presence to enable policy enforcement at ingress/egress points

©2020 Digital Realty Trust, Inc.

SOLUTION

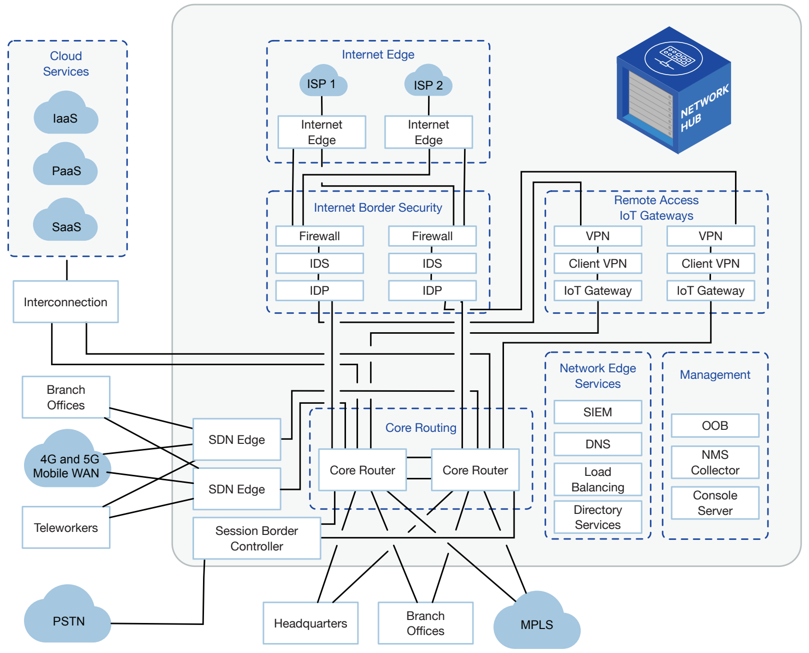
STEP 1 REWIRE THE NETWORK

1 Designed for Always On

2 Designed for Ubiquitous Work

ACTION: IMPLEMENT NETWORK HUB

Deploy network hubs to optimize traffic flows, host capacity and connect to clouds and service providers at points of presence.



- + Interconnect ecosystems of networks, clouds and partners
- + Secure multi-cloud access with direct interconnection (physical and virtual)
- + Segment, tailor and provision interconnection matched to business needs in terms of type, speed, destination, participant or time of day

OUTCOME

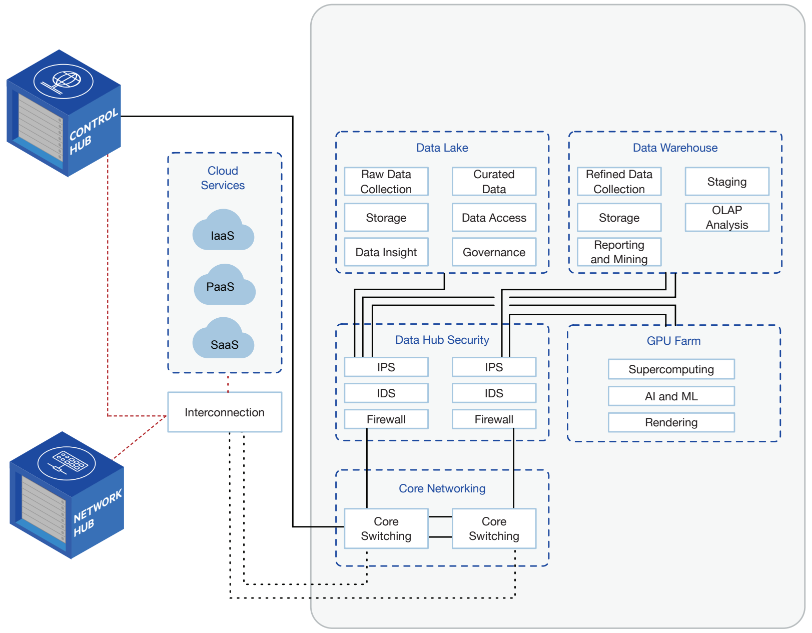
- + Reduce latency and increase throughput
- + Increase bandwidth per employee cost-effectively
- + Enable performant multi-cloud connectivity

STEP 2 OPTIMIZE DATA EXCHANGE

3 Performant Quality of Experience

ACTION: IMPLEMENT DATA HUB

Deploy data hubs at points of presence to leverage centers of data exchange.



- + Solve global coverage, capacity and connectivity needs
- + Deploy tailored infrastructure matched to business need irrespective of size, scale or configuration
- + Operate deployments as a seamless extension of global infrastructure with consistent experience, security and resiliency

OUTCOME

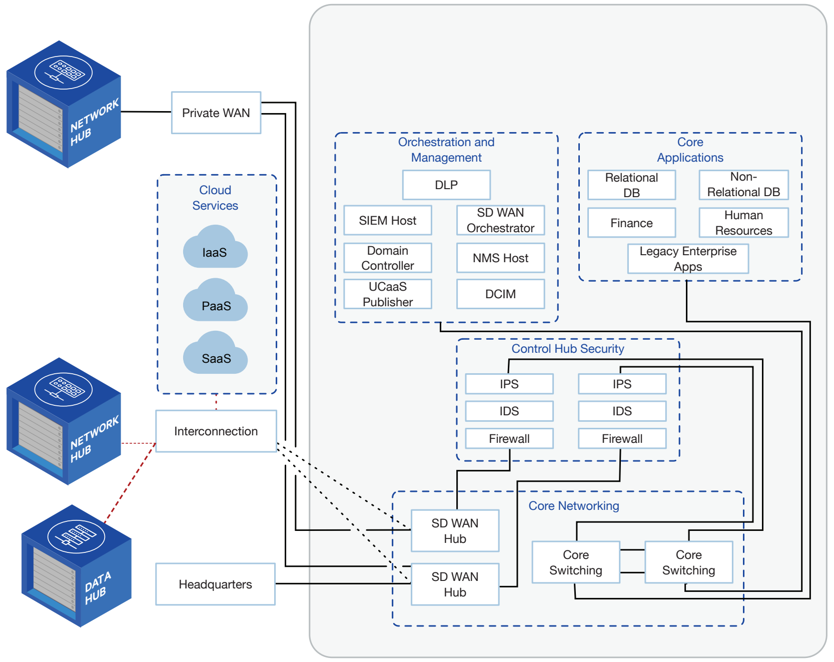
- + Implement distributed data staging and aggregation
- + Deploy regional data lakes and distributed data warehouses
- + Maintain compliance and sovereignty

STEP 3 IMPLEMENT HYBRID IT CONTROLS

4 Zero Trust Security Model

ACTION: IMPLEMENT CONTROL HUB

Deploy control hubs to distribute security policy enforcement and inspection.



- + Host IT and security controls and enable policy enforcement at data ingress/egress points to maintain data compliance and sovereignty
- + Deploy tailored infrastructure footprints to accommodate special purpose security, telemetry and logging infrastructure configurations
- + Operate deployments as one seamless, secure global data center infrastructure

OUTCOME

- + Reduce IT vulnerability points and improve security posture
- + Deploy telemetry and apply policy at points of ingress/egress
- + Reduce operational complexity and simplify infrastructure management

©2020 Digital Realty Trust, Inc.

SOLUTION STEP 1

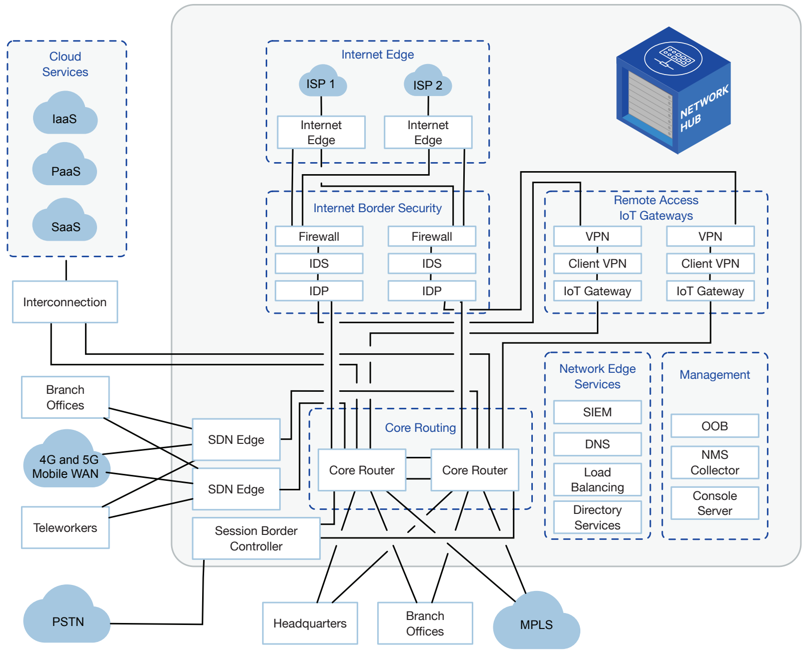
REWIRE THE NETWORK

1 Designed for Always On

2 Designed for Ubiquitous Work

ACTION: IMPLEMENT NETWORK HUB

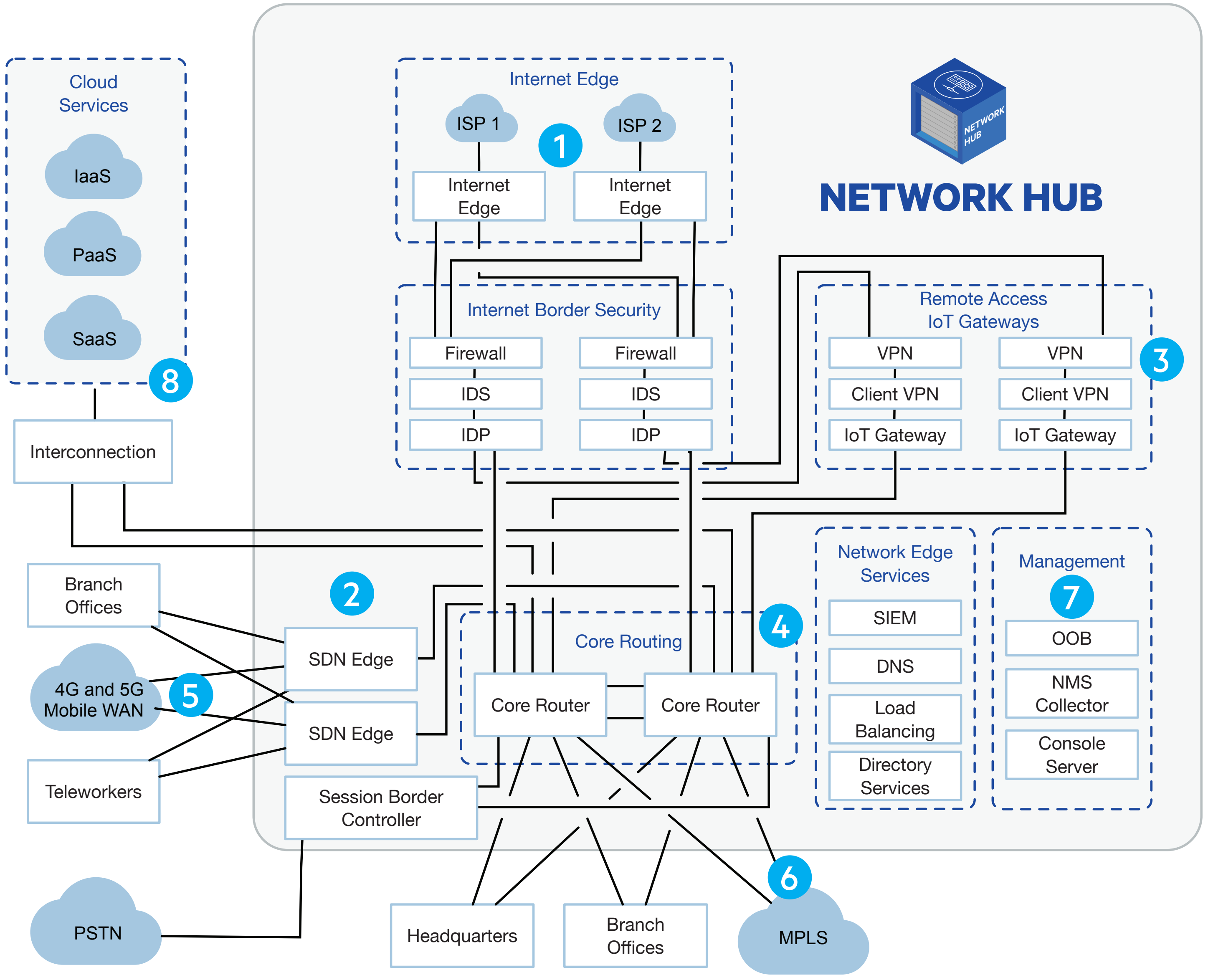
Deploy network hubs to optimize traffic flows, host capacity and connect to clouds and service providers at points of presence.



+ Interconnect ecosystems of networks, clouds and partners
+ Secure multi-cloud access with direct interconnection (physical and virtual)
+ Segment, tailor and provision interconnection matched to business needs in terms of type, speed, destination, participant or time of day

OUTCOME

+ Reduce latency and increase throughput
+ Increase bandwidth per employee cost-effectively
+ Enable performant multi-cloud connectivity



1. Multiple ISPs and Internet Exchanges are connected to edge routers to provide redundant Internet access to the customers' environment.
2. Enterprise security stack is deployed to border between the enterprise network and Internet resources.
3. IoT, VPN, and Client VPN devices are deployed behind the enterprise security stack to provide gateway services to remote devices, users, and partners.
4. Network Core layer provides enterprise routing and segmentation. Highly scalable data center routing and switching platform ties all enterprise resources together.
5. Tie remote locations and users to the enterprise using reliable and cost effective network solutions such as broadband internet, Cellular (4G or 5G), or other WAN technologies.
6. Leverage services, such as carrier ethernet to tie remote locations as well as headquarter locations to the Network Hub. Leverage services such as carrier ethernet to tie remote locations as well as headquarter locations to the Network Hub. Leverage MPLS network where required or as part of the migration strategy to a modern SDN architecture.
7. Critical applications services can be located inside of the Network Hub to reduce latency and provide a distributed architecture for these services.
8. Securely interconnect to cloud ecosystem, including leading IAAS, PAAS and SAAS providers. Build hybrid and multi-cloud deployments. Provide cloud services with enterprise security stack and controls adjacent in the hub.

©2020 Digital Realty Trust, Inc.

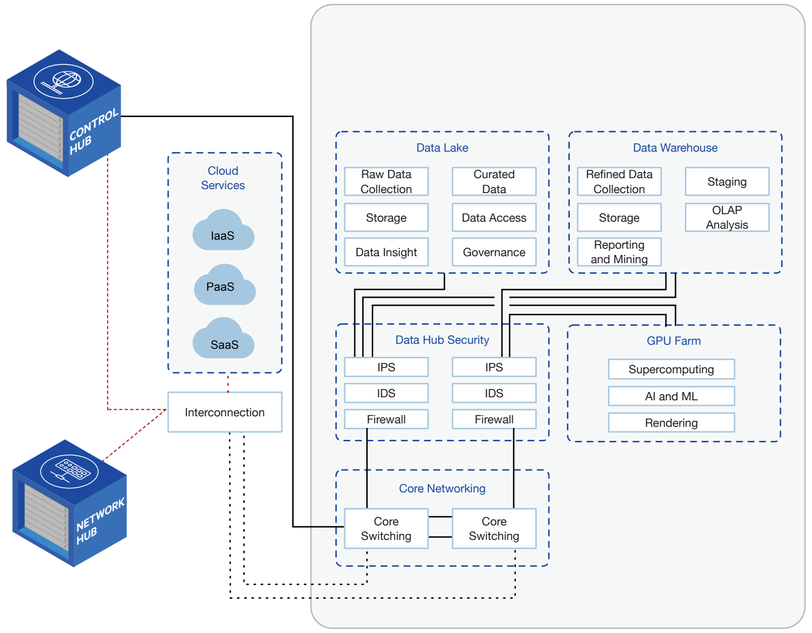
SOLUTION STEP 2

OPTIMIZE DATA EXCHANGE

3 Performant Quality of Experience

ACTION: IMPLEMENT DATA HUB

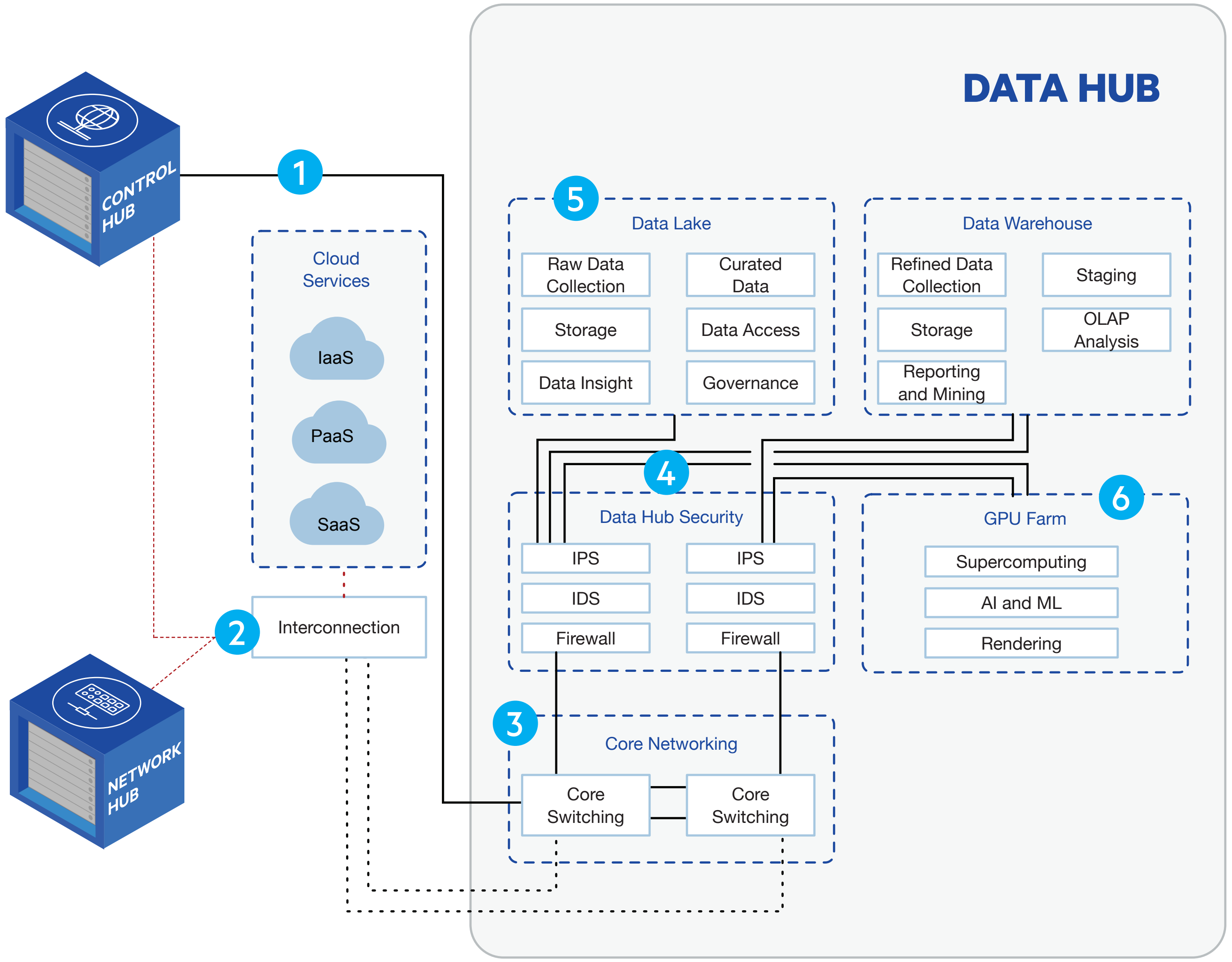
Deploy data hubs at points of presence to leverage centers of data exchange.



+ Solve global coverage, capacity and connectivity needs
+ Deploy tailored infrastructure matched to business need irrespective of size, scale or configuration
+ Operate deployments as a seamless extension of global infrastructure with consistent experience, security and resiliency

OUTCOME

+ Implement distributed data staging and aggregation
+ Deploy regional data lakes and distributed data warehouses
+ Maintain compliance and sovereignty



1. The Data Hub located in close proximity to the Control Hub connects using a Campus Connect or Metro Connect.
2. An out of market Control Hub connects back to the Data Hub using Service Exchange. Trusted data from Network Hubs flow to the Data Hub for further analysis and modeling.
3. The Core Switching infrastructure terminates connectivity into the Data Hub and enables access to the cloud for deep analytics and archival storage.
4. Due to the value and sensitivity of enterprise data, access needs to be strictly controlled and logged.
5. Data Lakes analyze and curate raw data for Data Scientists to use. Refined Data sits in the Data Warehouse for Business Professionals to use.
6. HPC GPU Farm, located directly adjacent to data stores for direct access. GPU Farms enable AI Development, Media Content Creation, complex modeling and simulations.

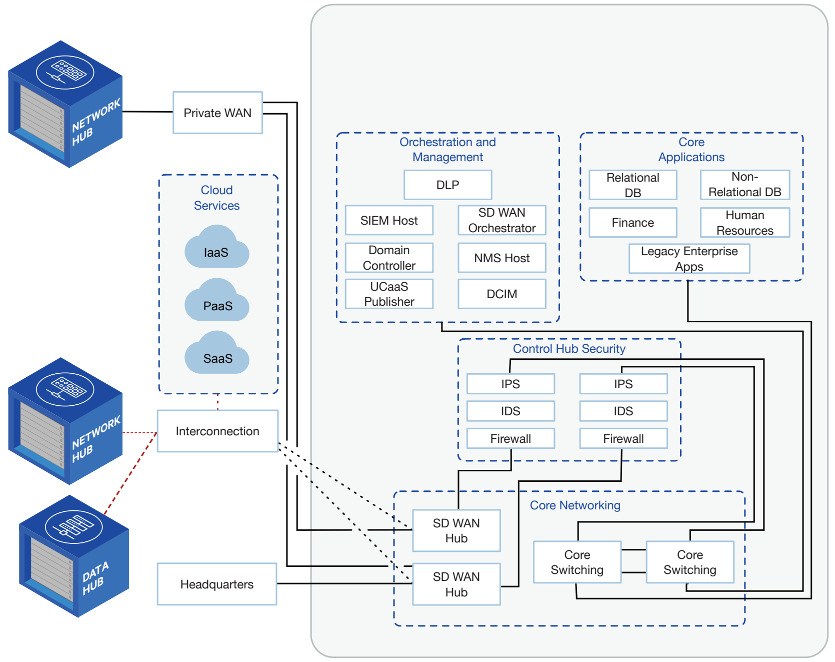
SOLUTION STEP 3

IMPLEMENT HYBRID IT CONTROLS

4 **Zero Trust Security Model**

ACTION: IMPLEMENT CONTROL HUB

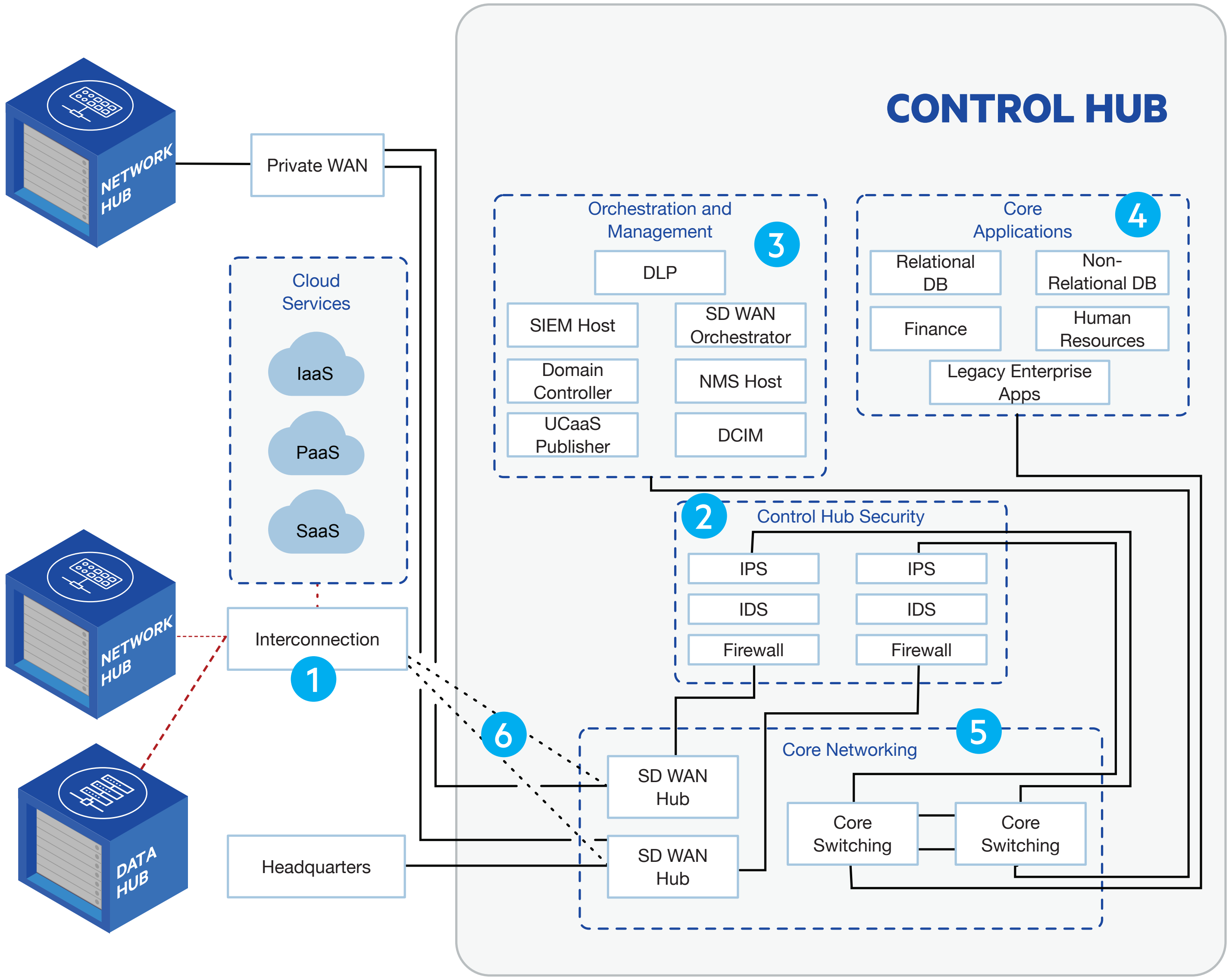
Deploy control hubs to distribute security policy enforcement and inspection.



- Host IT and security controls and enable policy enforcement at data ingress/egress points to maintain data compliance and sovereignty
- Deploy tailored infrastructure footprints to accommodate special purpose security, telemetry and logging infrastructure configurations
- Operate deployments as one seamless, secure global data center infrastructure

OUTCOME

- Reduce IT vulnerability points and improve security posture
- Deploy telemetry and apply policy at points of ingress/egress
- Reduce operational complexity and simplify infrastructure management



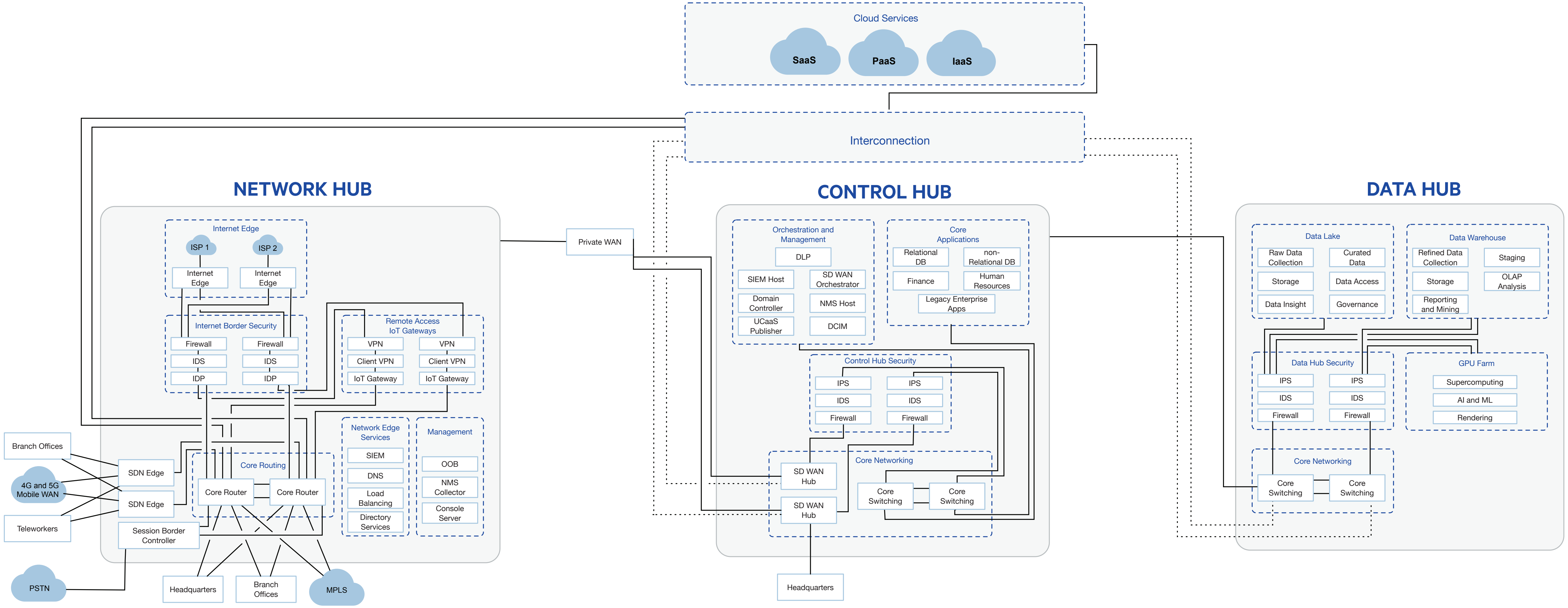
1. Regional Hubs connect over Internet access to reach centralized applications. Threat intelligence and other security systems events feed into the SEIM Host.
2. An additional security stack sits at the Control Hub to limit and authorize access to core business applications.
3. Orchestration and management instances that configure, manage and update resources deployed at the Network Hubs and corporate locations.
4. Legacy Applications supporting business organizations that are not suited for a Network Hub or the Cloud can be located in the Control Hub.
5. The Core Networking Zone aggregates traffic from the Network Hubs and Headquarters and providers routing and segmentation.
6. Connectivity from the Network Hubs to the Control Hub include Service Exchange, MPLS, DWDM, EVPL and Internet.

©2020 Digital Realty Trust, Inc.

TARGET STATE ARCHITECTURE

Summary

A purpose built architecture for the digital workplace provides ubiquitous, performant, always-on secure access to data and applications. By implementing Network, Data and Control Hubs, users, things, networks and capacity are integrated within proximity of centers of data exchange to optimize workflow & experience. By architecting and deploying your digital workplace on PlatformDIGITAL™, you solve for coverage, connectivity, capacity and control.



Cloud Services
SaaS
PaaS
IaaS
Interconnection
Private WAN

NETWORK HUB
Internet Edge
ISP 1
ISP 2
Internet Edge
Internet Edge
Internet Border Security
Firewall
IDS
IDP
Firewall
IDS
IDP
Remote Access IoT Gateways
VPN
Client VPN
IoT Gateway
VPN
Client VPN
IoT Gateway
Network Edge Services
SIEM
DNS
Load Balancing
Directory Services
Management
OOB
NMS Collector
Console Server
Core Routing
Core Router
Core Router
SDN Edge
SDN Edge
Session Border Controller
Branch Offices
4G and 5G Mobile WAN
Teleworkers
PSTN
Headquarters
Branch Offices
MPLS

CONTROL HUB
Orchestration and Management
DLP
SIEM Host
SD WAN Orchestrator
Domain Controller
NMS Host
UCaaS Publisher
DCIM
Core Applications
Relational DB
non-Relational DB
Finance
Human Resources
Legacy Enterprise Apps
Control Hub Security
IPS
IDS
Firewall
IPS
IDS
Firewall
Core Networking
SD WAN Hub
SD WAN Hub
Core Switching
Core Switching
Headquarters

DATA HUB
Data Lake
Raw Data Collection
Curated Data
Storage
Data Access
Data Insight
Governance
Data Warehouse
Refined Data Collection
Staging
Storage
OLAP Analysis
Reporting and Mining
Data Hub Security
IPS
IDS
Firewall
IPS
IDS
Firewall
GPU Farm
Supercomputing
AI and ML
Rendering
Core Networking
Core Switching
Core Switching

The Digital Workplace Blueprint is part of a library of blueprints and repeatable implementation patterns that make up the Pervasive Datacenter Architecture (PDx™). By practitioners, for practitioners, PDx™ was created by codifying 100's of production deployment combinations to enable companies to accelerate deployment and improve precision of their infrastructure to scale digital business globally. PDx™ provides a step-by-step strategy to enable firms as they architect a decentralized IT infrastructure to remove data gravity barriers and accommodate distributed workflows at centers of data exchange in support of digital business.

Digital Realty Trust, Inc. owns or licenses all copyright rights in all content, including, without limitation, all text, images, videos, and graphics in this document, to the full extent provided under the copyright laws of the United States and other countries. You are prohibited from copying, reproducing, modifying, distributing, displaying, performing, or transmitting any of the content in this document for any purposes.

DISCLAIMER

THE CONTENT HEREIN AND SERVICES BY DIGITAL REALTY ARE PROVIDED TO YOU ON AN “AS IS” AND “AS AVAILABLE” BASIS, EXCEPT AS SET FORTH IN A DEFINITIVE AGREEMENT BETWEEN YOU AND DIGITAL REALTY. EXCEPT AS EXPRESSLY PROVIDED, TO THE FULL EXTENT PERMISSIBLE BY LAW, DIGITAL REALTY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. [DIGITAL REALTY DOES NOT WARRANT THAT SERVICES, CONTENT, PRODUCTS, OR ANY OTHER INFORMATION PROVIDED OR OTHERWISE MADE AVAILABLE TO YOU BY DIGITAL REALTY ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS.] TO THE FULL EXTENT PERMISSIBLE BY LAW, DIGITAL REALTY WILL NOT BE LIABLE FOR ANY DAMAGES OF ANY KIND, INCLUDING, ANY LOSS OF PROFITS, LOSS OF USE, BUSINESS INTERRUPTION, OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES OF ANY KIND IN CONNECTION WITH SERVICES, CONTENT, PRODUCTS, OR ANY OTHER INFORMATION PROVIDED OR OTHERWISE MADE AVAILABLE TO YOU BY DIGITAL REALTY.

Pervasive Datacenter Architecture (PDx™) Blueprint - DIGITAL WORKPLACE

©2020 Digital Realty Trust, Inc