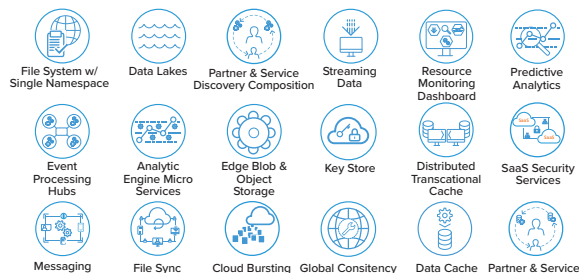




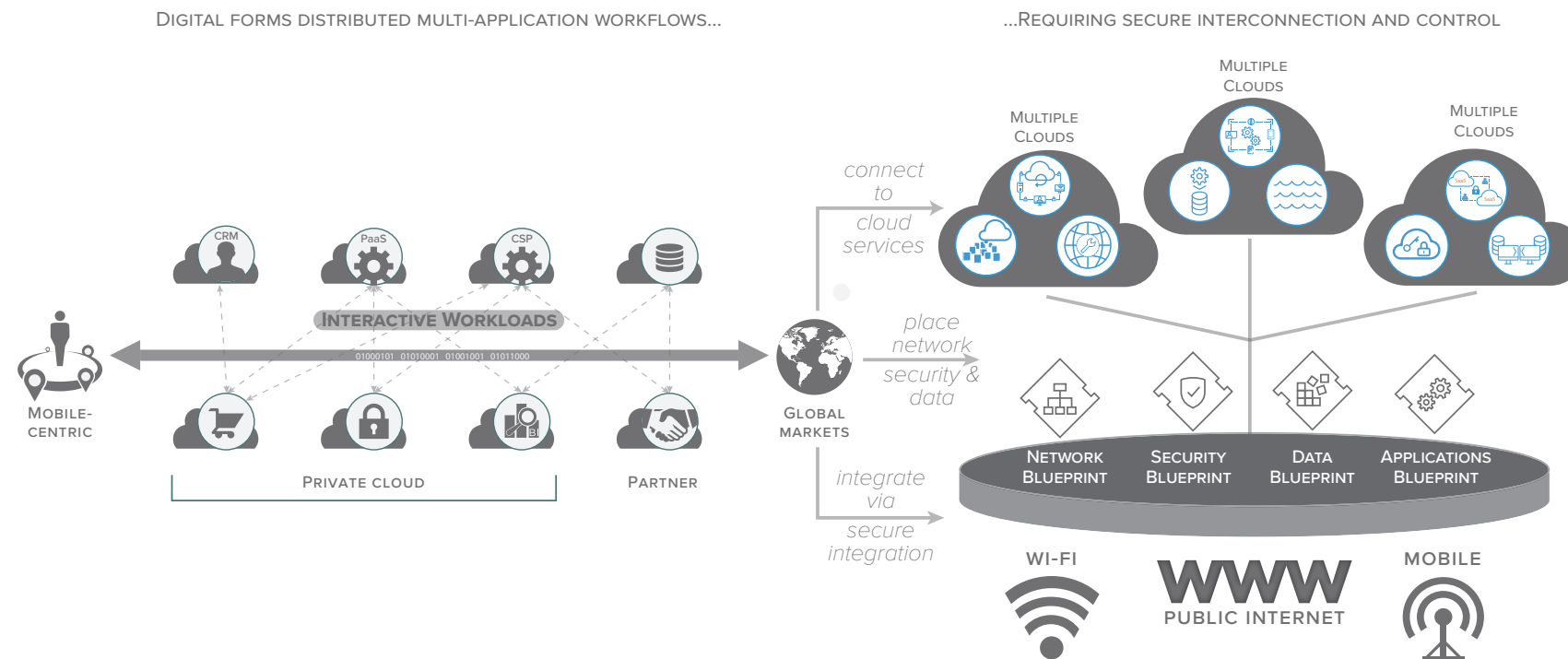
Design Principles

- Platform (cloud & network neutral).
- Scale (dynamic & automated).
- Workflows (study, measure & optimize).
- Integration (APIs for networks, clouds, apps).
- Latency (measure & minimize).
- Security (trust-nothing model).
- Governance (compliance & policy enforcement).
- Data Protection (privacy & placement).
- Orchestration (all actions pre-determined).
- Dynamic change (everything is temporary).

Edge Node Components



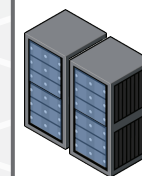
The demands of digital are forcing enterprises to re-architect their IT infrastructure. The speed of technology and business change combined with increased traffic volumes and mobile technology require a multicloud-enabled IT delivery platform, linked to traditional infrastructure. To do this efficiently, at scale, requires distributed IT exchange points (Digital Edge Nodes) that enable private, secure, low-latency communication among multiple clouds and SaaS services providing vendor-neutral network and cloud choice across geographic regions. Derived from hundreds of successful implementations, an Interconnection Oriented Architecture® provides enterprises a control point and places IT back in the center of the architecture.



Capabilities

- Secure, scalable multicloud connectivity.
- Low-latency workflow integration across multiple clouds.
- Common control point for adjacent network and security services across all the clouds and SaaS.
- Multicloud access to colocated private data and services.
- Cloud- and network-neutral choice.
- Improved user experience.
- Substantially lower data ingress/egress cloud provider charges.
- Dramatically lower risk profile with dedicated private connections.

Edge Node Deployment



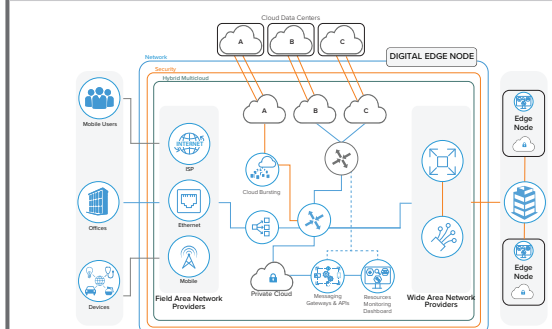
Mix physical and virtual appliances supporting services for Network, Security: typically one cabinet. Cabinets required for Applications and Data depend on application characteristics and data, with 1PB requiring ~5 cabinets.

DESIGN PATTERNS

1 STEP 1

Optimize for multicloud application workflows by placing edge nodes (traffic exchange points) close to users and clouds; localize traffic with direct, secure, low-latency interconnection to segment and integrate traffic flows.

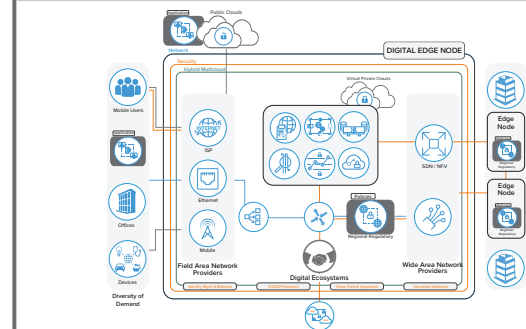
Simplify Multicloud Connectivity & Operations



2 STEP 2

Enforce compliance with a trust-nothing security model (applied to flows across all parties) with policy-based border control, packet inspection and real-time security analytics. Tailored to the level of security and compliance required by each flow.

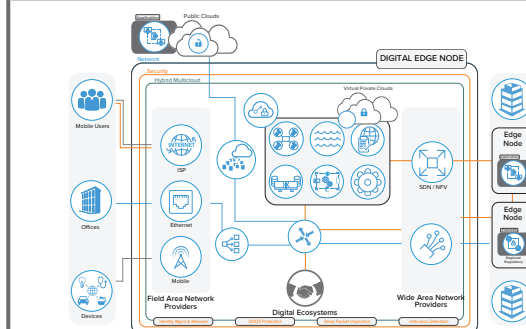
Increase Multicloud Security Effectiveness



3 STEP 3

Avoid the need to place sensitive data in the cloud, or move large data sets between clouds, by colocating private data in the edge node to provide secure, low-latency access from multiple cloud platforms.

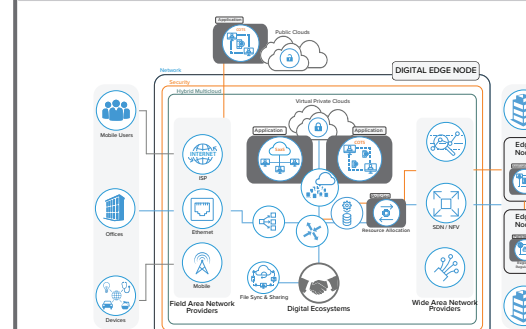
Minimize Costly Inter-cloud Data Transfers



4 STEP 4

Solve for growth in traffic, data volumes and processing by distributing workloads across geographically placed edge nodes, in proximity to users and cloud availability regions. Load balance resources for scale and continuity.

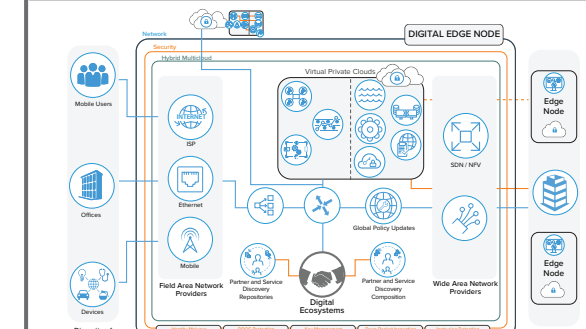
Scale Geographical Multicloud Demand



5 STEP 5

Interconnect with customers and partners for direct commerce and data exchanges. Establish new flows (business service chains) and continually adapt to changes in regulations, technologies and emerging partners and markets.

Build Multicloud Business Platforms





Simplify Multicloud Connectivity & Operations



Problem

Individually connecting multiple clouds over WAN is operationally complex and costly, resulting in unreliable cross-cloud application interaction performance and poor visibility. Managing increasing volumes isn't solved by public internet offloading (risk) or expanding WAN usage due to physics (distance) that increase latency and reduce bandwidth.



Solution

Success in the digital economy depends on the flexible integration of multiple, cloud-based services or workloads into new digital business models. These microservices—comprised of many services orchestrated across a multitude of applications—are the future of competitive digital businesses. The traditional enterprise backbone connections to each cloud must be re-architected to an Interconnection Oriented Architecture where clouds are connected at secure distributed edge nodes that are vendor-neutral IT exchange points for clouds and networks. Direct, private, secure connectivity to an edge node enables one-to-many connections to all clouds at the node, reducing setup time and costs through vendor choice. Traffic flows are segmented at the edge to optimize inter-cloud traffic using SDN, reducing enterprise backbone congestion and cloud ingress and egress costs. Cloud resource management and monitoring services are leveraged through edge-based partner ecosystems, enabling cross-cloud brokering and cloud bursting.



Constraints

1. Traditional infrastructure architecture is based on network isolation with a perimeter around the enterprise; a move to cloud stresses that design.
2. Extending the existing network backbone to individually connect to various clouds limits network connectivity options and choice.
3. Resource costs and time required to install links, equipment purchases and contracts impedes speed to market and ROI.
4. Cloud-based workloads are traditionally considered islands of compute that limit the responsiveness and flexibility required to compete in the digital economy.
5. Operational management becomes more difficult across multiple, independent cloud connections outside the enterprise backbone (where each connection needs a test cycle) and visibility across components and clouds is limited.



Steps

1. Using the guidance from Steps 2 and 3 of the Network Blueprint, [Network 2, 3*], pick the target application workloads (COTS, SaaS or bespoke). Assess traffic bandwidth demands. Aggregate and segment network interconnections into each chosen public/private cloud, using SDN as needed.
2. Migrate bespoke applications to target clouds and establish an API registry. Employ container management to manage their life cycles.
3. Install and connect data caches at edge nodes to facilitate rapid cross-cloud interactions.
4. Employ policy-based acquisition of services including cloud resource monitoring and dynamic resource allocation, leveraging digital services ecosystems.
5. Leverage cross-regional ecosystems to employ optimal partner services across clouds.



Forces

- A majority of enterprises (85%) employ multiple clouds with 58% being hybrid clouds—the base for digital economy platform construction.
- Hybrid multicloud connection complexity impedes adoption as cloud providers have a hard time managing bespoke connections, impeding economies of scale.
- Shadow IT continues to add cloud deployments, creating operational risk.
- The increase in mobile users has created interactions with more SaaS-based applications.
- The choice of SaaS drives cloud platform choice.
- Applications with many legacy enterprise application connections are being targeted for cloud deployment, creating security and performance challenges.



Results

Technical

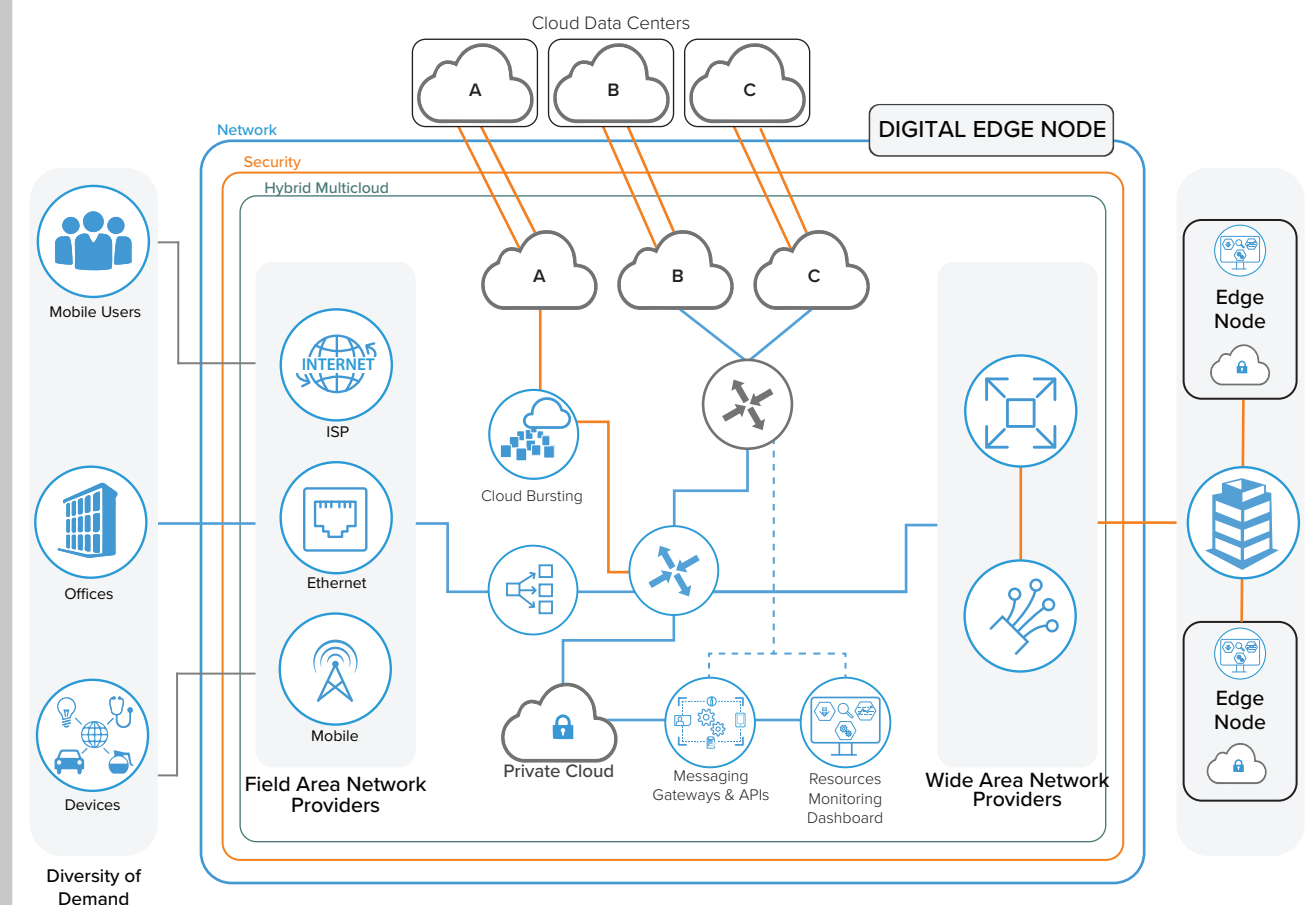
- Cross-cloud connections are secure and segmented for traffic optimization with high bandwidth and minimal latency.
- Multicloud connection complexity is simplified—provisioning new connections takes hours, not weeks.
- Cross-cloud and operational visibility is improved by leveraging partner ecosystems' monitoring tools.
- Workload integration is optimized as required resource demand changes.

Business

- Increased flexibility and choice of cloud and network providers at the edge reduces cost.
- Consistently enhanced user experience based on local needs and customs.
- Enhanced business strategy, operations and execution in real time via new partner ecosystems enables new global business models, expanding reach.



Reference View



* Network Blueprint — IOAKB.com



Increase Multicloud Security Effectiveness



Problem

Distributed hybrid multicloud environments cannot be secured with traditional centralized security services, as delays harm inter-cloud application performance. Multicloud identity management is complex and error-prone, and centralized management hurts user experience.



Solution

Establish a secure edge perimeter (an extension of the enterprise firewall), by leveraging edge-based partner ecosystems to deploy fundamental security services (e.g., border security, deep packet inspection and DDOS, malware and intrusion protection) [Security 1,2*]. Install a compliance policy repository to manage network segmentation restrictions, preventing restricted data leakage to or from clouds [Security 3*]. Install edge repositories to ensure that data prohibited from being stored in the cloud can be rapidly, seamlessly accessed by cloud-based applications to meet performance requirements. Create a federated cloud ID key management store to simplify inter-cloud interactions [Security 4*]. Store, synchronize and enforce regional compliance policies at the edge, including data scrubbing rules, ensuring they are timely and relevant. Run data gatekeeper programs in edge nodes to protect all users from theft and attacks while logging all required events (e.g., non-repudiation audit logs) required by regional compliance [Security 5*].



Constraints

1. Regulation software and policy data is considered too important to be distributed outside company firewalls, but keeping it centralized inhibits effective partner transactions and collaboration due to significant delays associated with backhauling all regulation checks to a centralized data center.
2. Some compliance services (e.g., national jurisdiction of data) present performance problems in multicloud interactions if they are not enforced at a regional level.
3. Regional policies usually apply only locally and change more frequently, complicating central management.
4. Due to bandwidth limitations and multicloud connectivity complexity; the internet is offered as a viable option for sensitive data due to implementation lag times, creating security risks to meet time-to-market conditions.



Steps

1. Establish comprehensive border security at the edge, including DDOS, malware protection and packet inspection [Security 1,2,3*].
2. Install a cloud key store and ID management solution [Security 4*] with proper encryption for cross-cloud interactions.
3. Invoke policy-driven segmentation at the digital edge (extending company firewall(s)) when cloud-based solutions would be prohibited.
4. Expand security service chaining at the edge, leveraging ecosystems and cloud-based SaaS for recording services and data repositories that hold all local compliance policies, including auditing.
5. Install predictive security analytics [Security 5*] to discern systematic intrusion detection.
6. Leverage edge-based data repositories, enabling cloud-based applications rapid access to data prohibited from cloud-based storage.



Forces

- As more data is exchanged across clouds, sensitivity and regulations associated with the data must be addressed, which requires network segmentation of message and data flows to meet compliance rules for safety and privacy (e.g., PCI-DSS & HIPAA).
- Regulations change rapidly across a global enterprise—most regulation changes occur regionally and should be enforced locally.
- Mobile workforce proliferation (urbanization) with myriad devices stresses centralized compliance enforcement.
- Dynamic new partner arrangements across the globe will require local compliance checks.
- The need for non-repudiation in a cross-value chain coordination project must be balanced with the need for exceptional performance.



Results

Technical

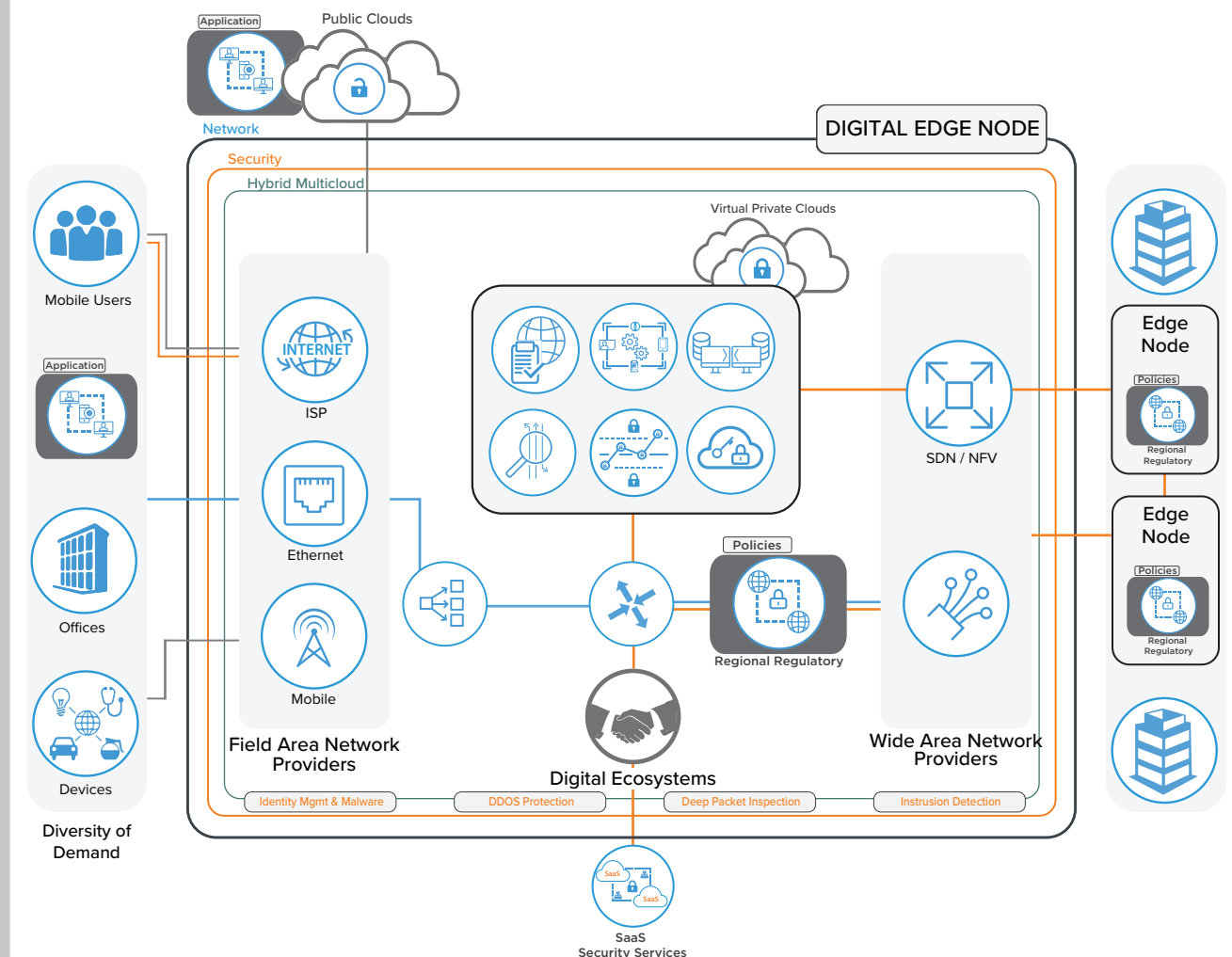
- Edge-based security ensures data and message flows adhere to policy restrictions.
- All cloud-based applications have low-latency access to data at the edge, improving performance without compromising data sovereignty policies.
- Regional regulatory compliance is tailored and kept timely without performance delays.
- Privacy is protected by ensuring secure, edge-to-edge connections over the mesh.
- Compliance services (i.e., end-point auditability/security analytics) are easier to maintain and enforce because of improved response time.

Business

- Costs and reputational risk are better controlled using local services at the edge.
- Cloud-based services that were previously restricted due to local regulations are expanded.



Reference View



* Security Blueprint — IOAKB.com



Minimize Costly Inter-cloud Data Transfers



Problem

Data transfers between multicloud environments have grown exponentially due to increased application migrations and the need to gather large user data sets, causing interaction performance delays, large increases in costs and added data management complexity.



Solution

Addressing the growing data gravity problem in hybrid multicloud environments requires implementing a set of edge-based storage tactics that include distributed caches to reduce inter-cloud response time and low-latency data connections between clouds and edge repositories containing data sets too large to move. In addition, policy-based storage management must be leveraged from edge-based ecosystem partners so that storage choices are available, enabling costs to be related to application QoS requirements. Repository management should be simplified by assigning a single namespace for all repositories. Further minimize data transfer complexity by leveraging ecosystem services for data aggregation, scrubbing and integration. Tailor for each node, and ensure that caching and synchronization will work across the interconnected mesh of edge nodes with other cloud deployments to solve for redundancy through manageable disaster recovery (DR) transfers and unexpected demand spikes or congestion.



Constraints

1. Large and frequent data transfers between clouds is very costly (e.g., \$86k/PB/year), and centralized data transfers consume most available bandwidth, creating cost and performance pressures.
2. Files are multi-sourced in many formats, creating significant data management problems
3. Large-scale data transmission for cloud-based applications creates response time lags that impede user experience.
4. Regional rules regarding data collection and scrubbing vary greatly and must be enforced locally.
5. Cloud-based applications may have local instances that require synchronization of data or behavioral trends.



Steps

1. Install or expand a data cache [Data 1*] and distributed repositories [Data 2*] at the digital edge node so that large data sets can be placed in policy-driven, tiered storage (including storage appliances) for multicloud access, minimizing frequent time-consuming data transfers between clouds.
2. Create a single namespace for all edge-stored data, facilitating file management.
3. Establish low-latency connections to the data sets for each application.
4. Ensure that local data collection, aggregation and scrubbing policies are enforced for security and performance reasons (e.g., IoT data deluge) [Data 3,4,5*].
5. Implement a dispersed, self-healing DR strategy using a data replication and synchronization engine so that each digital node has multiple connections, preventing a single point of failure.



Forces

- The digital economy is driven by creating value from data which will be transmitted at 600 TB/sec by 2020, surpassing internet capacity.
- Interconnection traffic at IT exchange points (digital edge nodes) will grow at 45% per year, 2x greater than internet traffic and 10x greater than MPLS traffic.
- This data deluge will be created and consumed locally, with expectations of near-real-time user experience.
- Cloud-based applications must access large data sets rapidly to support real-time systems of engagement and insight which are brand and revenue differentiators.
- The migration of applications to hybrid multicloud platforms is accelerating, requiring proximate data.



Results

Technical

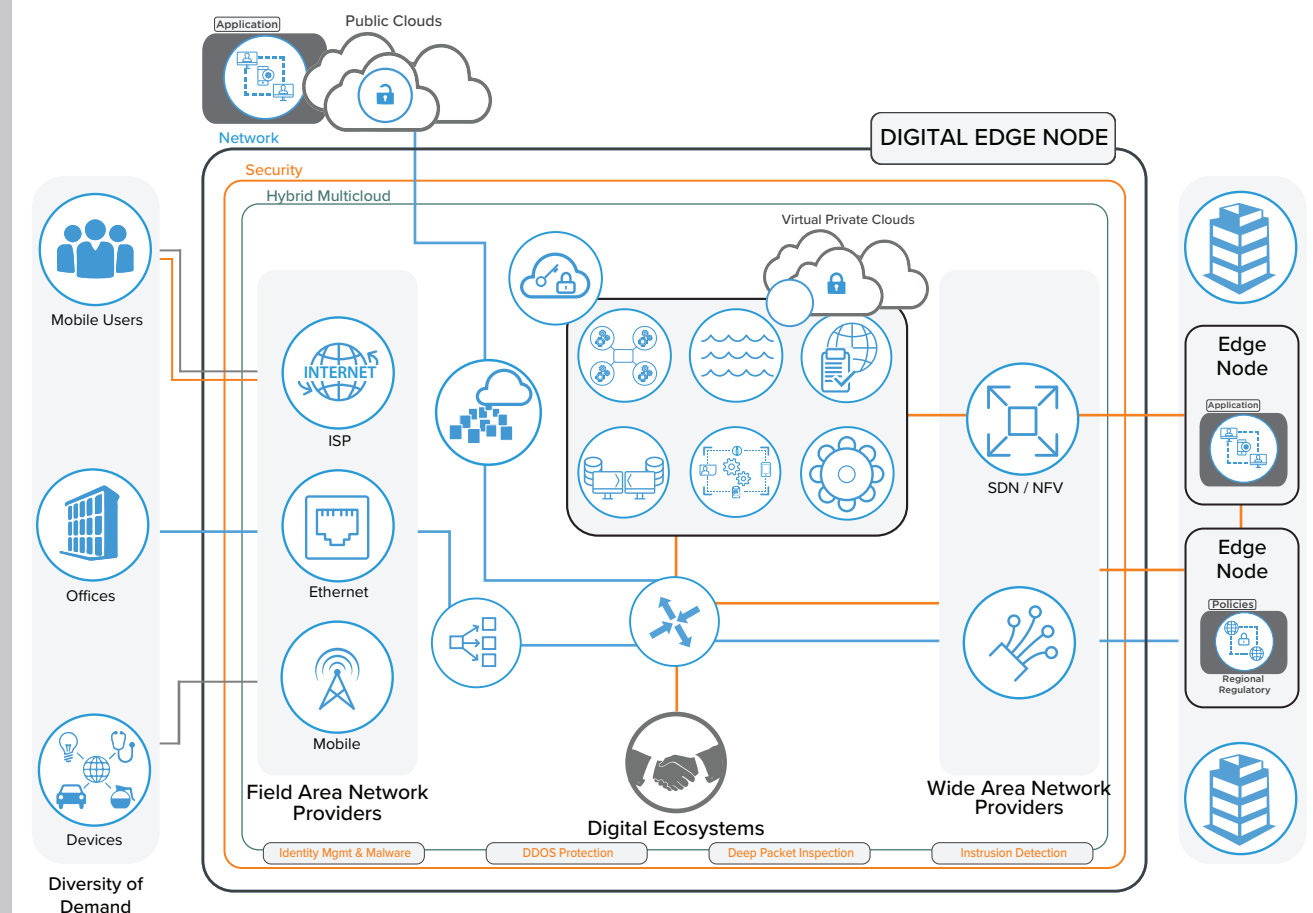
- Multiple applications across multiple clouds access data faster (milliseconds) without the need for large, frequent transfers.
- Interconnected edge-based ecosystems provide flexible storage and data management choices.
- Localized, edge-based data gathering, scrubbing and aggregation improves performance and user experience and reduces enterprise backbone congestion.
- Edge data caching enables efficient synchronization updates and DR across regions through a mesh of interconnected edge nodes.

Business

- Inter-cloud data transit costs are reduced.
- Improved application response times increase business competitiveness and create new opportunities.



Reference View



* Data Blueprint — IOAKB.com



Scale Geographical Multicloud Demand



Problem

Exponential traffic volume growth between cloud-based applications adversely affects user experience because it congests traditional centralized MPLS network topologies. Offloading traffic to the public internet is not secure, and dedicated connections to individual clouds are financially and operationally unsustainable.



Solution

Adapt to changing business needs and support new business models across time zones, with shifting traffic patterns and new regulations. Leverage edge-based ecosystems of service providers (cloud, network, SaaS) that can tailor resources and services based on business-driven policy decisions invoked via real-time configuration control (SDN/NFV). Drive inter-cloud traffic through the edge node via virtual interconnections to clouds. Minimize inter-cloud data transfer and store service quality policies in local data repositories at the edge node; drive traffic demand to the interconnected edge node mesh where digital ecosystems route traffic to other nodes most efficiently. Dynamically rewire services and connectivity, continually adapting to planned and unplanned business and technical environment shifts. Adjust cloud utilization across and within edge nodes to reflect usage and cost policies.



Constraints

1. Multicloud resource management is complex if each connection is separately managed with each cloud-based application having different needs over time.
2. Dynamic volume, bandwidth and infrastructure resource policy management wasn't considered feasible in traditional IT experiences.
3. Fear of inadequate cloud resource infrastructure causes firms to over-provision in fixed-price arrangements; yet, growing digital economy-based demand is dangerously unpredictable.
4. Distributed multicloud application proliferation requires resiliency tactics other than centralized failovers.
5. Multicloud workloads must interact in real time with resilient connections.
6. Diverse workload interactions (e.g., collaboration, transactions and analytics) require sophisticated QoS transmission policies ensuring delays don't degrade user experience.
7. Long distances impede high throughput and responsiveness in MPLS networks despite the use of SD-WAN.



Steps

1. Employ edge-based cloud ecosystems. Virtually cross connect dedicated circuits to clouds on demand.
2. Use SDN/NFV to segment traffic with different bandwidths based on application QoS needs.
3. Install cloud balancing with cloud bursting capabilities, ensuring effective resource utilization.
4. Install cloud resource monitoring and accounting to align and inform cloud-balancing policies.
5. Solve for exponential growth of demand across the distributed enterprise, deploying applications in geographically dispersed clouds through a mesh of interconnected digital edge nodes, leveraging partner ecosystems where private, one-to-many connections can be established.
6. Tailor each node for local services, enabling control of performance and cloud utilization scaling on demand.
7. Leverage predictive analytics and inform resource allocation policies across the distributed enterprise.



Forces

- Time to market combined with a compelling need to minimize the IT debt of aging infrastructure is driving new business applications to be delivered via cloud platforms to remain competitive in the digital economy.
- Expansion into new geographic markets with new partners cannot wait months for standard IT deployments.
- Providing relevant, timely value for cloud-based systems of insight and engagement across the proliferation of devices and their expanding capabilities to a growing mobile workforce is unsustainable using traditional centralized network architectures.
- Demand fluctuates sufficiently to challenge assumptions about capacity management in traditional architectures.
- Centrally planned capacity management cannot meet demand.



Results

Technical

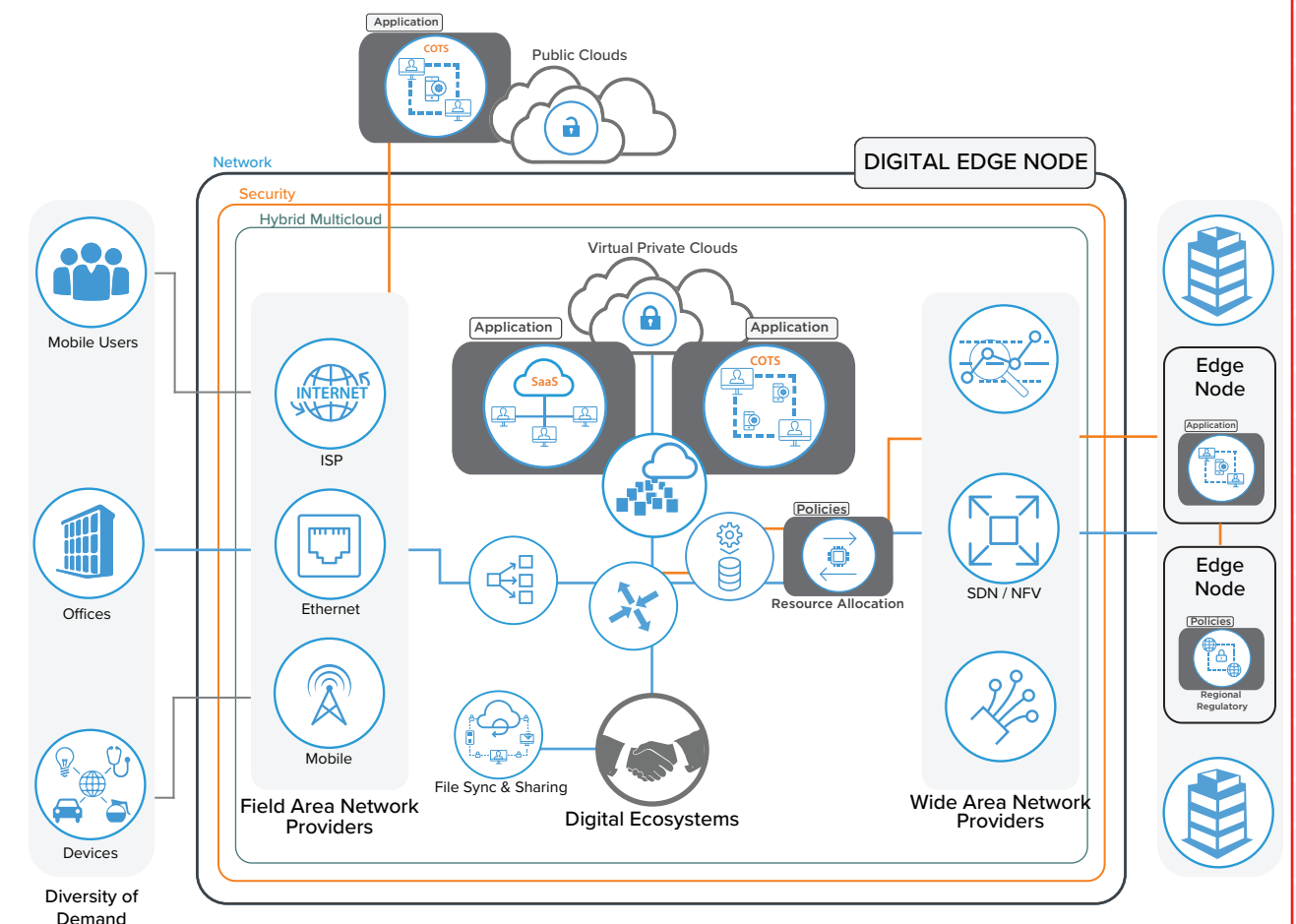
- Most traffic is localized using optimal paths via edge nodes to users of cloud-based workloads. Backhaul to corporate data centers is minimized.
- Cloud resource usage is dynamically tied to demand.
- Dynamic routing enables self-healing in the case of local bottlenecks.
- Adding more bandwidth is programmatic, increasing flexibility and agility.

Business

- Dynamic, real-time enterprise able to respond to changing demand by flexibly adjusting infrastructure supply—saving resources and reducing waste without re-architecting.
- Real-time and predictive analytics inform digital economy business strategies.
- Partnerships enable regionally tailored business models on a global scale.
- Planning for periodic shifts in demand is a policy versus engineering issue.



Reference View





Problem

Competing in the digital economy requires increased speed of change, global reach and reliability to enable cost centers to offer services that traditional centralized multicloud connectivity cannot sustainably offer due to cost and operational complexity.



Solution

Growing global hybrid multicloud utilization enables the enterprise to respond to changes in business models, demand volume, technology and regulations, control operational costs and adapt to shifting cloud providers and SaaS innovation. Interconnected edge node ecosystems allow new ventures with new technologies and business models using edge nodes as launching points. Partnerships enable regionally tailored business models on a global scale. Data placed at the edge facilitates multicloud data governance and greatly simplifies identity management across clouds and national jurisdictions. Multicloud workloads enjoy low-latency access to data at the edge, improving performance.



Constraints

1. New business models and technology innovation require major rework of network models and cloud connectivity.
2. Traditional cloud and network service connections are often fixed, limiting the responsiveness required to adjust dynamically to unpredictable demand.
3. Developing a distributed hybrid multicloud business platform requires a new set of architectural assumptions about distributed capacity management.
4. Assumptions about the need to custom-build all strategic applications and services hurt digital economy competitiveness.
5. A mindset change is required to architect a discoverable services model leveraging a fluid set of interconnections in a networked ecosystem that responds to changing needs.



Steps

1. Extend and productize API management [Application 1] from internally oriented to external-facing, where enterprise services are made available for discovery in edge node business ecosystems.
2. Monetize previously developed edge-based application services into publicly available services.
3. Expand how partner ecosystem services are leveraged to create new services at each edge node.
4. Construct a digital edge platform across the interconnected mesh of edge nodes, expanding reach.
5. Leverage predictive analytics to examine trends that indicate the need for new services.



Forces

- Technology change rapidly accelerates the range and impact of potential new business models; speed of change and time to market are the digital economy's sustainable competitive advantages.
- Cost pressures are forcing the migration of more enterprise backbone-based services and workloads to the cloud in more locations.
- Platforms and ecosystems are the foundation of value creation in the digital economy.
- Composing value chains from discoverable services in partner chain ecosystems at digital edge nodes replaces custom development as the strategic differentiator across the global digital enterprise, enabling targeted disruption in selected markets, while adapting to regional changes.



Results

Technical

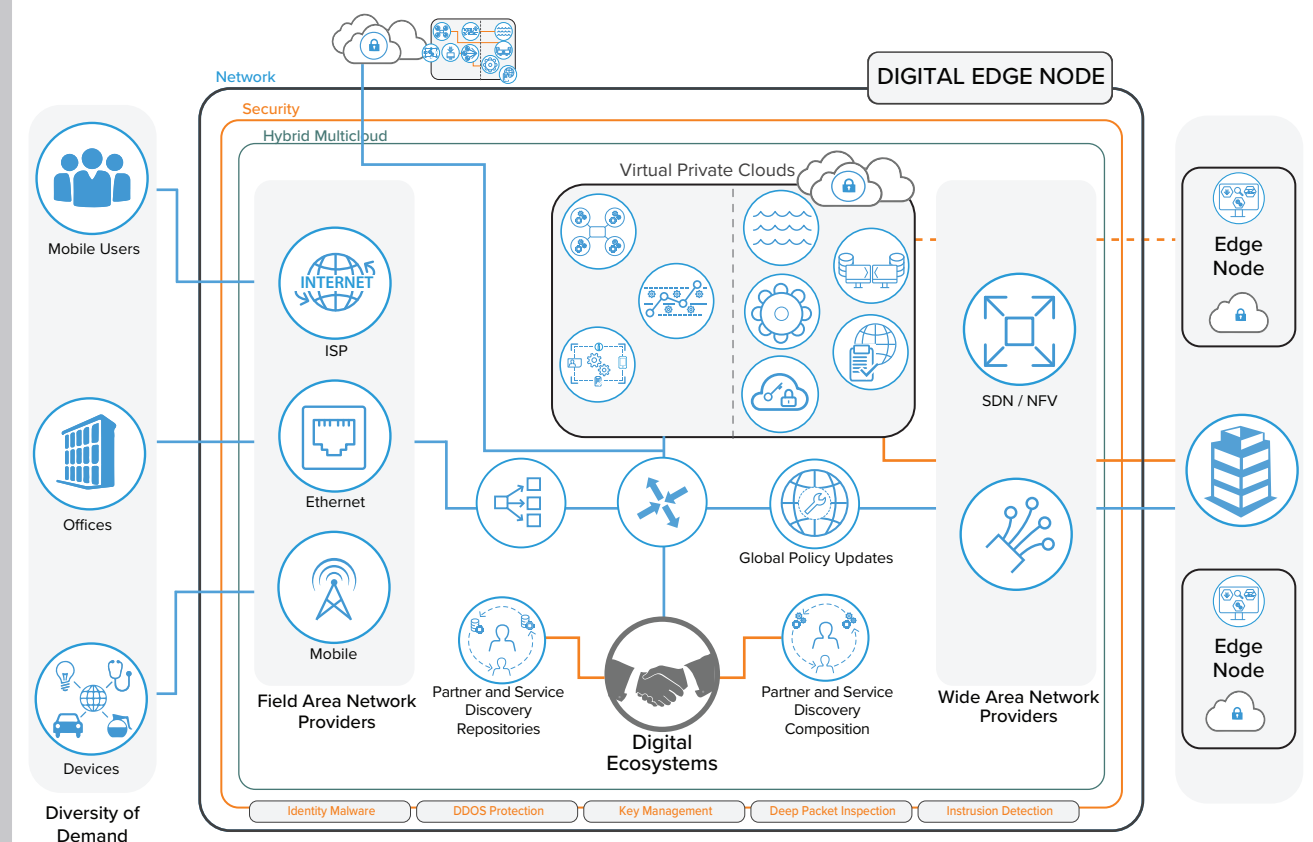
- API management is productized to include edge-based partner ecosystem discovery.
- The building blocks for a distributed digital business platform are established to compose business services faster.
- Cloud-based services are available across the interconnected edge nodes across regions.
- Virtualized service interconnections are adjusted to needs by region and demand.

Business

- Competing in and disrupting the digital economy is strategically feasible.
- Time-to-market introduction of new services is greatly improved across regions.
- Development mindset is aligned with the rapid changes in the digital economy, where leveraging partner ecosystems for new features is a first choice.



Reference View



* Application Blueprint — IOAKB.com