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*].

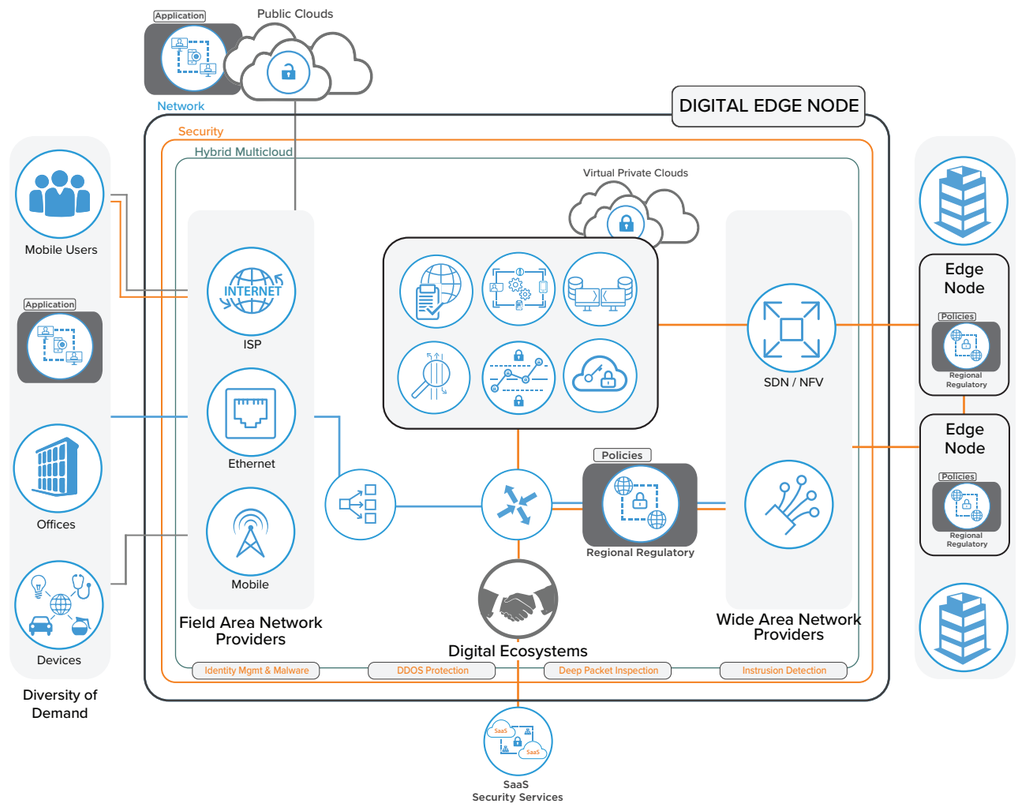
Constraints

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.

Reference View



* Security Blueprint — IOAKB.com

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.