Apply Global Transactional Compliance

Problem

Compliance regulation software and data are traditionally kept in the core data center. In widely dispersed enterprises, regulations change often, affected by an increasingly mobile workforce. Attempting to manage regional business regulations centrally creates a suboptimal user experience.

Solution

Guarantee timely, relevant regulatory compliance and optimal user experience by driving policy enforcement decisions to local regions through edge-based service chaining. Control data sovereignty and access with locally enforced policies reflecting geographic limitations and protections which often change. Ensure regulation policies are pushed to the edge through expanded compliance services. Leverage deployed edge security services (e.g., deep packet inspection) to enforce local compliance regulations. Deploy edge repositories that retain the latest compliance policies, protect all users from theft and attacks, and log all required events (e.g., non-repudiation audit logs) required by regional compliance. Ensure localized regulations are applied to inter-cloud interactions, especially data, where a cache at the edge between clouds may be required. This creates the ability to rapidly change business value chain partners through policy updates.

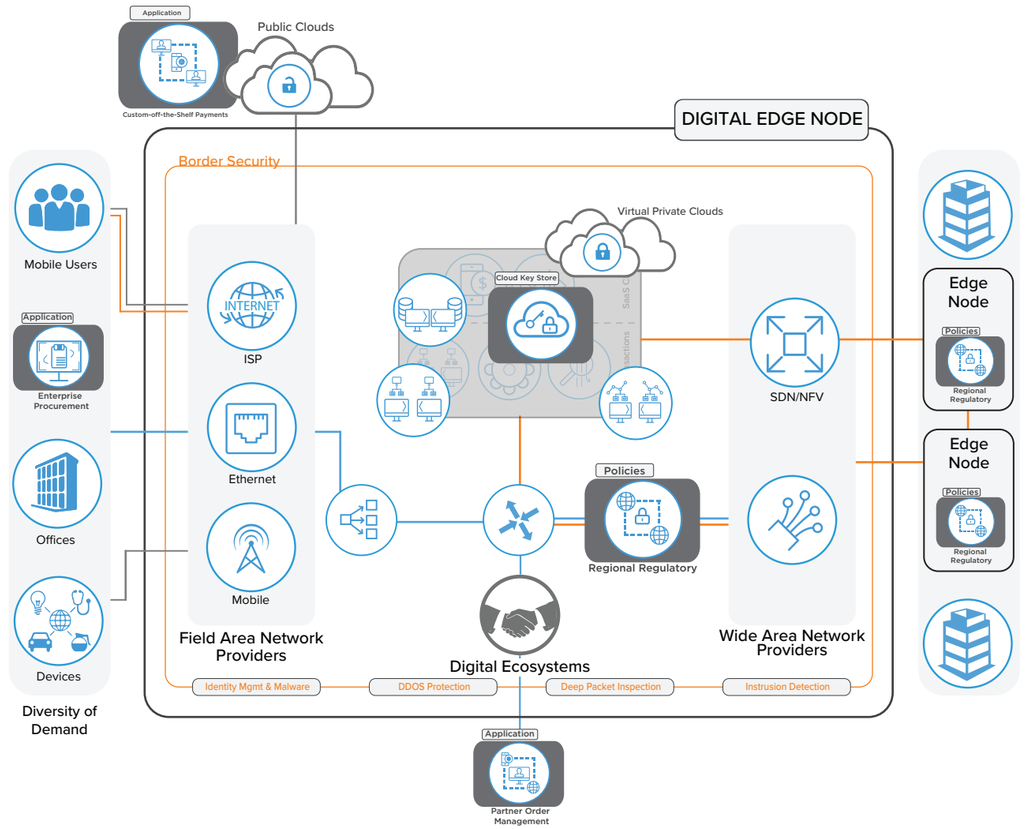
Constraints

1. Regulation software and policy data are 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. Certain local restrictions on data exposure prevent the transmission of information from leaving a region.
4. Regional policies usually apply only locally and change frequently, complicating central management.

Steps

1. Expand security service chaining at the edge by leveraging ecosystems to include recording services and data repositories that hold all local compliance policies (including auditing).
2. Install repositories to meet local/regional audit and logging compliance regulations.
3. Invoke policy-driven segmentation at the digital edge (an extension of the company firewall) where a cloud-based solution would be prohibited.
4. Ensure that local BYOD policies are enforced.
5. Install auditing features at the digital edge to ensure comprehensive security and user confidence.
6. Control the traffic across mesh connections with appropriate segmentation at the edge.

Reference View



Forces

- Regulations change rapidly across a global enterprise; most regulation changes occur regionally and should be enforced locally.
- The proliferation of a mobile workforce with myriad devices will stress centralized compliance enforcement.
- Regional regulations require transactional recording and can restrict viewing of data to that regional level.
- Dynamic new partner arrangements across the globe will have 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

- Regional regulatory compliance can be tailored and kept timely without performance delays.
- Privacy can be better protected by ensuring secure edge-to-edge connections over the mesh.
- Compliance services (such as end-point auditability and 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 services that were previously held back due to local regulation issues are expanded.

Potential New Challenges

- Unplanned volume growth can affect the performance of security services.