Protect Content Compliance

Problem

Compliance regulation software and data have traditionally been kept in the core data center. In widely dispersed enterprises, regulations often change, reflecting local needs including a growing mobile workforce. Regional personalization requirements cannot be managed centrally as user experience requirements are not met.

Solution

Guarantee timely and relevant regulatory compliance and brand-enhancing personalization services 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 change the most often. Ensure that 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., auditable file changes) required by regional compliance. Ensure localized regulations are applied to inter-cloud interactions. Enable dynamic changes to personalization for content delivery. This allows for shifting business needs and changes that can be extended as needed to business value chain partners.

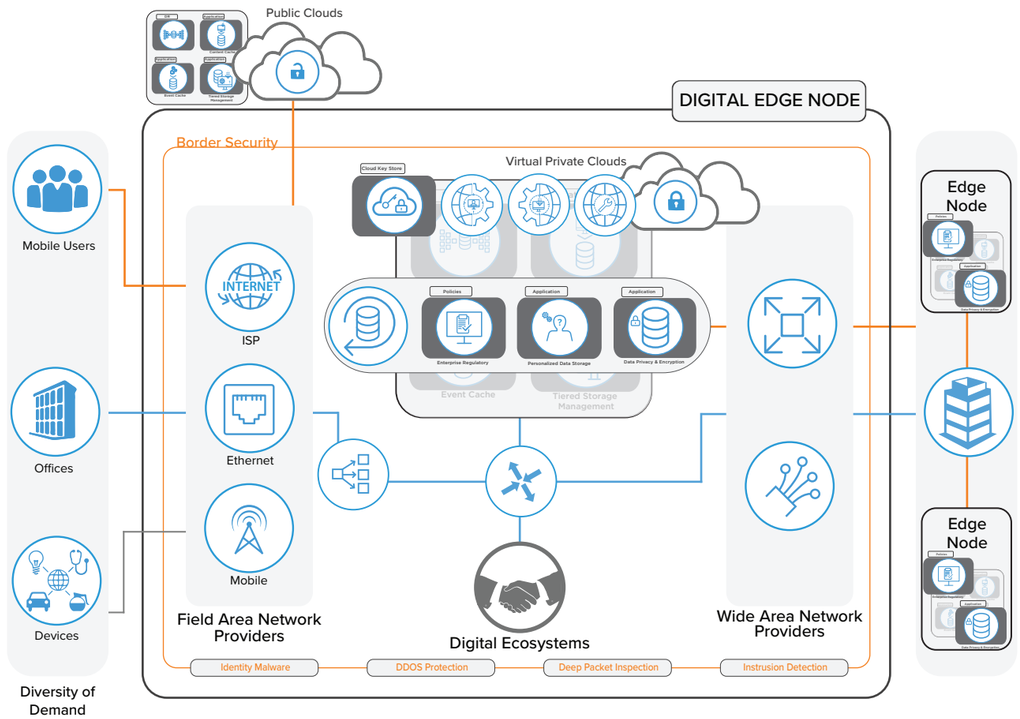
Constraints

1. Regulation software is deemed too important to be distributed outside company firewalls, but keeping it centralized delays file access and delivery. Backhauling all regulation checks to a centralized data center creates a poor user experience.
2. Traditional centralized compliance is unsustainable in a global dispersed network where many of the enforcement policies reflect regional concerns.
3. Some compliance services (e.g., data sovereignty checks) present performance problems in multicloud interactions if they are not enforced at a regional level.
4. The traffic volume in a large population center from the public internet creates a significant threat.
5. Most compliance changes originate regionally, making timely enforcement a complex challenge.
6. Application interaction for content creation across the value chain will suffer from critical response time issues.
7. Regional personalization requirements cannot be effectively managed centrally.

Steps

1. Expand security service chaining at the edge by leveraging partner ecosystems to include encryption 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. Control traffic across mesh connections with appropriate segmentation at the edge.
6. Install repositories and leverage service chaining to provide nuanced, scalable and localized personalization services.

Reference View



Forces

- Regulations change rapidly across a global enterprise, but most regulation changes occur regionally and need to be enforced locally.
- Control must be asserted to protect against theft, attacks and information loss.
- Some regulations restrict viewing of data at a regional level.
- Audit features are critical for holistic security and user confidence, but can hurt user experience by introducing latency.
- The need for non-repudiation (e.g., buying content) needs to be balanced with the need for exceptional performance.
- Regionalized personalization is a critical success factor in content delivery.
- Content creation drives new business value chain partners and opportunities.

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.
- Automated workflows and compliance services (such as end-point auditability and security analytics) are easier to maintain and enforce because of improved response times.

Business

- Costs and reputational risk are better controlled using local services at the edge.
- Cloud services that were previously rejected due to local regulation issues can be utilized.
- Business value chain partners can be safely and quickly added and removed.
- Personalization services can be administered and applied locally for optimal user experience.