IOA® KNOWLEDGE BASE

Solve for Data Sovereignty & Compliance

Problem

Compliance software and data have traditionally resided in the core data center. Global enterprises' regional regulations change often, reflecting local needs including how user information must be collected, stored and utilized in real time, which affects user experience.

Solution

To ensure secure and efficient processing of regulatory compliance for data gathering, cleansing, retention and access, regulatory enforcement is pushed to the digital edge where collection occurs and where regionally relevant policies can be stored securely and efficiently. Control multicloud analytic interactions with locally enforced policies reflecting geographic limitations and protections where they change most often. Expand compliance service chaining, especially the cleansing of collected user data, and leverage existing edge security services (e.g., deep packet inspection) to enforce local compliance regulations. Deploy edge repositories that retain the latest compliance policies to protect users from theft. Log analytic decision-making for business audit and non-repudiation purposes. Enhance remote access management to enable effective, cross-regional, multicloud collaboration of complex modeling engines.

Constraints

1. Regulation software is deemed too important to be distributed outside company firewalls, but keeping it centralized delays file access and delivery due to backhauling all regulation checks to a centralized data center, hurting user experience.
2. Traditional centralized compliance is unsustainable in a global, dispersed network where many 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. Data collection from mobile devices over the public internet in large population centers represents a significant threat vector.
5. Most compliance changes are regional, making timely enforcement a complex challenge.
6. Nuanced regional engagement personalization and data scrubbing cannot be effectively managed from a central location.

Steps

1. Install repositories to meet local/regional audit and logging compliance regulations.
2. Expand security service chaining at the edge by leveraging ecosystems to include encryption services and data repositories that hold all local compliance policies, including auditing of decisions.
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, especially for data collection anonymizing.
5. Control traffic across mesh connections with appropriate segmentation at the edge, ensuring data sovereignty.
6. Install repositories and leverage service chaining to provide nuanced, localized systems of engagement personalization services.
7. Install secure remote-access management for modeling and collection.

Forces

- Regulations change rapidly across a global enterprise, but most regulation changes occur regionally and should 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, including the anonymizing of collected data.
- Audit features are critical for holistic security and user confidence, but can hurt user experience by introducing latency in systems of engagement.

Results

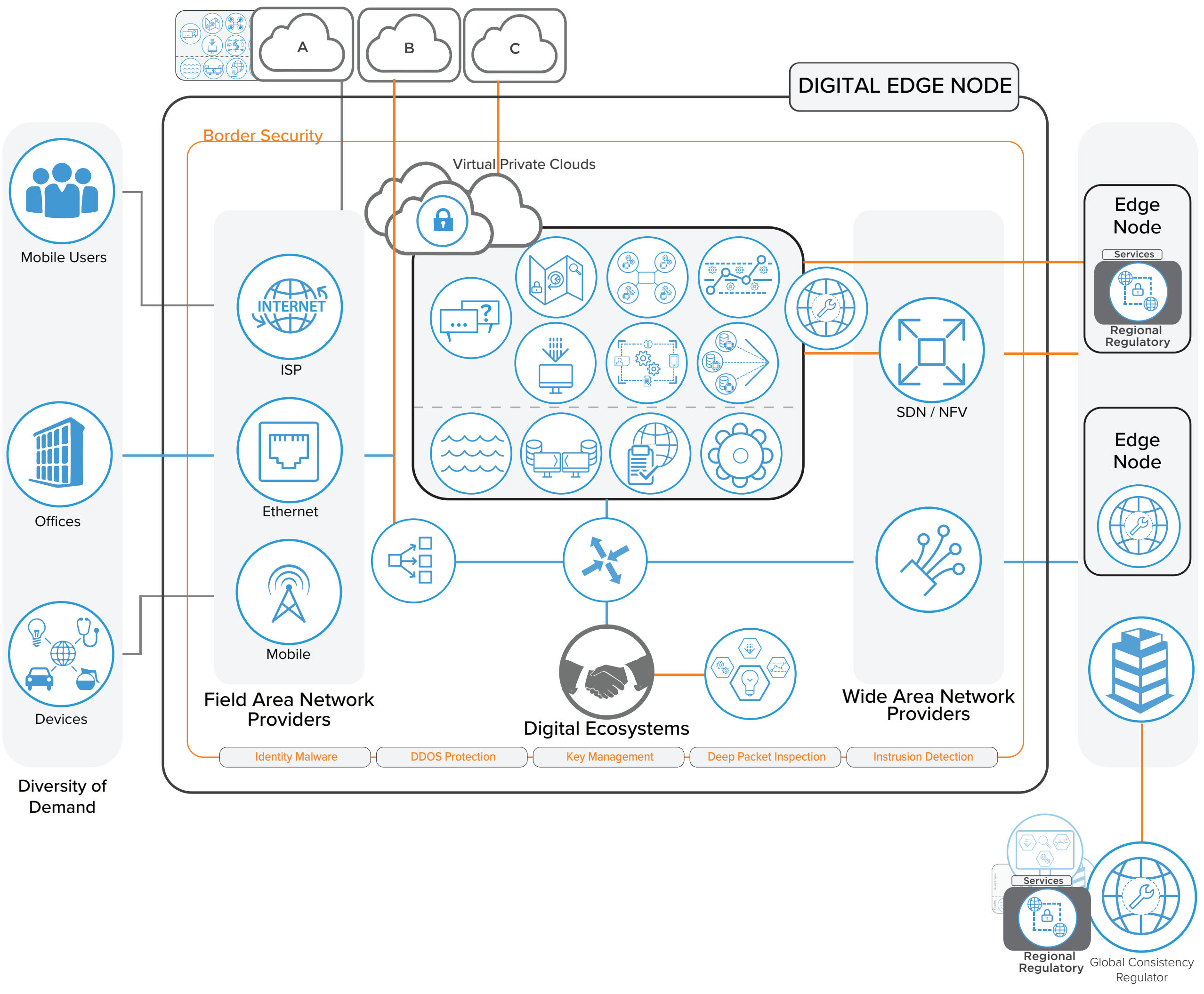
Technical

- 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 data anonymizing) 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, making it easier to adapt to regulatory change.
- Cloud services that were previously held back due to local regulation issues can be expanded.
- Value is enhanced due to better policy-based security.
- Personalization services can be administered and applied locally.
- Data loss/theft is minimized; accessibility is not.

Reference View


A
B
C
DIGITAL EDGE NODE
Border Security
Virtual Private Clouds
Mobile Users
Offices
Devices
Diversity of Demand
INTERNET
ISP
Ethernet
Mobile
Field Area Network Providers
Digital Ecosystems
SDN / NFV
Wide Area Network Providers
Identity Malware
DDOS Protection
Key Management
Deep Packet Inspection
Instrusion Detection
Edge Node
Services
Regional Regulatory
Edge Node
Services
Regional Regulatory
Global Consistency Regulator