



U.S. FEDERAL GOVERNMENT BLUEPRINT

Design Principles

- Architecture dynamically adjusts to meet mission-critical needs.
- A vendor marketplace enables cost and performance competition.
- Collaboration is global, mobile and user-centric.
- Geographically dispersed, real-time collaboration workflows are sensitive to jitter and latency.
- Collaboration is interactive, multicloud and secure.
- Flexible consumption spending models are required.
- Collaboration services are localized wherever possible.
- End users and devices are vulnerable to attacks and identity theft.

Critical Platform Elements

Global location coverage – Ability to place control points near customers, employees and partners for responsiveness and compliance.

Interconnection and ecosystems – Greatest choice in networks, clouds, partners and ecosystems with dynamic exchange options.

Integration and control – Leverage proximity and low latency to integrate physical and virtual services from a marketplace of leading options.

Enterprise

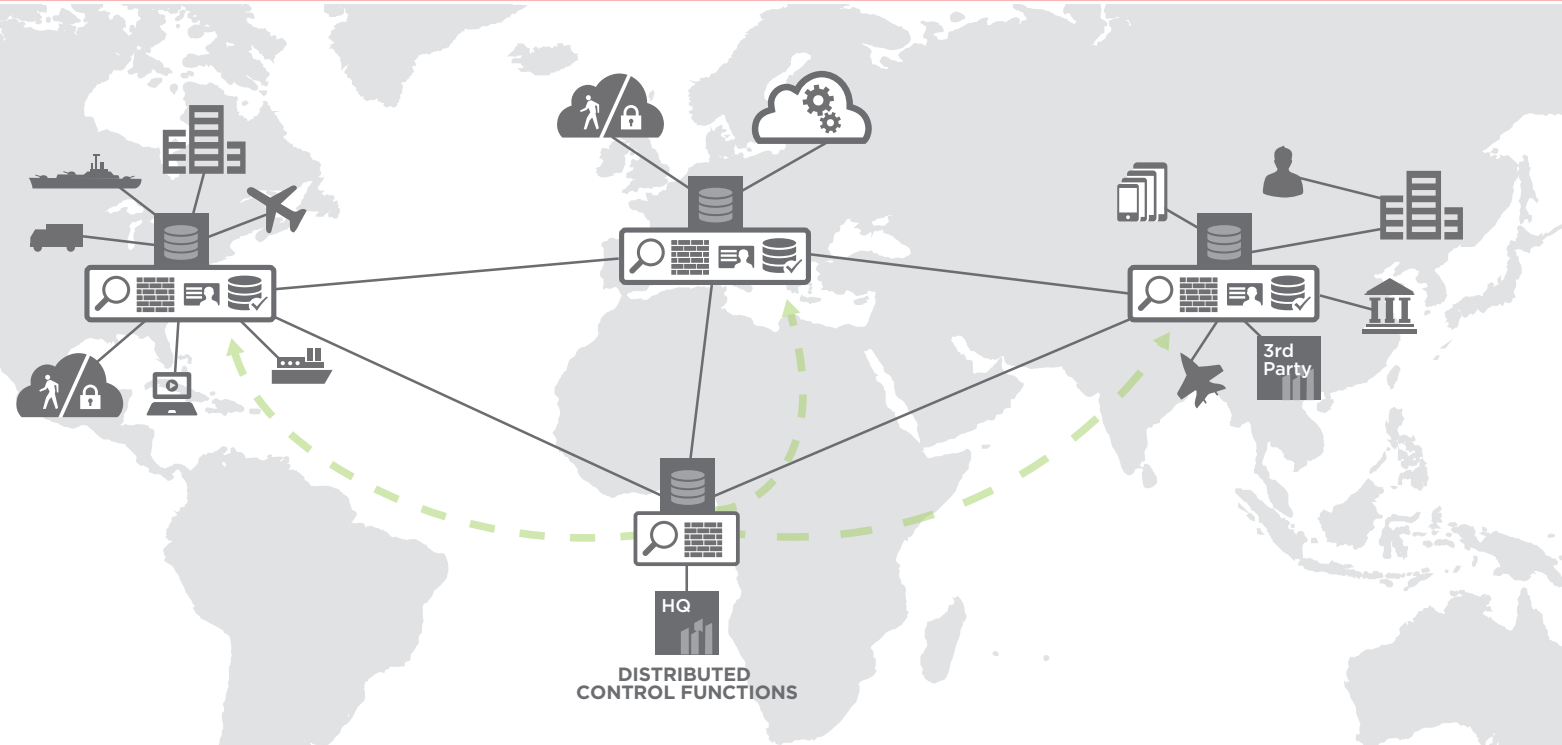
Government agency missions require meeting their constituents' expectations of fast response to new needs. However, most agencies run on aging and costly infrastructure that can't accommodate new capabilities at scale, nor collaborate across agencies efficiently. Digital transformation is the path to optimize those capabilities.

Provider

Service providers must offer integrated solutions that enable agencies to quickly deploy and scale open, API-based cloud services at the digital edge, facilitating better collaboration and information sharing that streamline operations while providing real-time, intuitive user experiences.

Managed Services

MSPs must provide architectural program management, deployment and strategic planning guidance to agencies navigating distributed security; holistic, multicloud integration; open, secure and compliant collaboration; and dynamic data sharing that meets future "smart nation" mission goals.



Advantages of a Digital-Ready Platform

Capabilities

- Securely share responsive content and application services across clouds.
- Dynamically rewire connections to new partners, agency interfaces and data channels.
- Optimize the use of encryption for data at rest and in motion.
- Manage regulatory compliance at local edge nodes where most changes occur.
- Achieve resilience, responding to outages and network congestion, by dynamically rerouting traffic.
- Maintain a seamless experience for collaboration services across geographically distributed centers and devices.
- Scale volume and tailor user experience to meet local needs as usage grows with demand.
- Obtain fast insights from actionable data to adjust to demand.
- Build the IoT foundation for a smart nation.

Virtual and Physical Stack



Leverage colocation control points for hybrid deployment models of fit-for-purpose services that are both appliances and ecosystem cloud-delivered, to create optimized collaboration and data sharing.

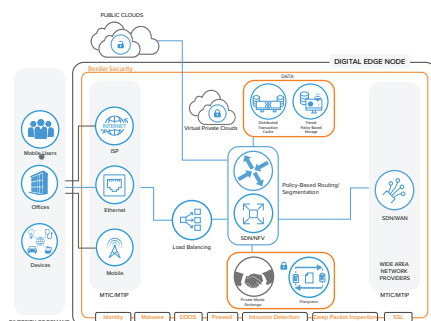
PLAYBOOK STRATEGY

1ST Re-architect the Information Exchange

Establish new collaboration and data sharing capabilities by rewiring your centralized network to a distributed, interconnected fabric of private exchange control points adjacent to dense clusters of clouds and information exchanges. Secure them with distributed controls, distributing workloads while optimizing capacity.

Types of control functions involved:

- Network function virtualization (NFV).
- Policy-based segmentation and routing.
- Network load balancing.
- SDN/WAN.
- MTIC/MTIP-compliant localized border security, including inspection zones, SSL termination, malware & DDOS protection, next-generation firewall, identity management.
- Private agency information exchange.

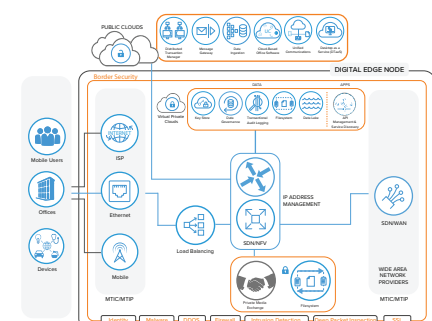


2ND Integrate Capabilities with Multicloud

Deploy hybrid multicloud infrastructure into localized control points to simplify application, data and multicloud integration and streamline interagency operations. Deploy applications into clouds, choosing API-based services for elasticity. Integrate compliant partners, and develop flexible, consumption-based spending contracts.

Types of control functions involved:

- IP address management.
- Cloud key store.
- Distributed file system.
- Localized data governance.
- Object store and data lakes.
- API manager.
- Message gateway.
- Distributed transaction/workflow manager.
- SaaS-based office suite.
- Desktop as a service.
- Unified communication.

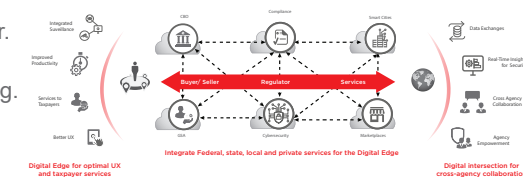


3RD Enable Digital Government

Create efficient, integrated, seamless interagency collaboration with SaaS-based office suites and information exchanges. Build a smart nation with sensor-based trend analysis creating actionable insights regionally and nationally. Ensure agency mission resilience with integrated, policy-based disaster recovery tools.

Types of elevated capabilities involved:

- Mobile application services.
- Device management.
- Distributed application update coordinator.
- Data integration and pipeline manager.
- Data ingestion, aggregation and scrubbing.
- Analytics dashboard.
- IOT aggregation gateways.
- Real-time complex event processing manager.
- Disaster recovery manager.
- Global data consistency replication manager.





Problem

IT consolidation and requirements for interactive services require government agencies to securely share data. Siloed legacy technology stacks constrain the ability to scale, reduce costs or improve user experience. IT architectures must securely integrate digital technologies, clouds and federal agencies to optimize collaboration, federate information sharing and analysis, and engage users.



Solution

By re-architecting IT infrastructures, federal agencies can accelerate digital transformation and meet growing demands. Begin by evolving centralized networks to a distributed, interconnected fabric of control points (hubs) in strategic locations where partners, agencies and clouds interact. Then, deploy policy and security control services in these colocation hubs, and interconnect to required clouds and agencies using the controls to segment direct traffic flows. Next, implement distributed transactional caches (for audit logging) in the control hub, and interconnect to partners and private data exchanges at these secured control points. As you rewire your topology, scale for capacity through software controls that respond to demand. This fabric lays the foundation for multicloud integration and enhanced platform capabilities such as integration with collaborative communities of interest using federated information sharing.



Providers



Managed Services

Offer integrated building-block stacks of functionality that are configurable based on expected capacity and regulatory needs. These include converged infrastructure, tiered storage and software appliances that utilize NFV and SDN to optimize usage and accommodate private data exchanges.

Provide program management and architecture guidance along with infrastructure and data management skills augmentation to assist with initial stages of mission-critical transformation.



Constraints

1. Traditional, centralized agency architectures, some of which are 40+ years old, are incapable of handling new distributed data and security requirements.
2. Current architectures cannot efficiently scale to meet changing needs.
3. Legacy systems are difficult and costly to upgrade, and expensive to replace.
4. Most legacy systems are siloed and closed, unable to address changing collaboration and data-sharing requirements.
5. As cyber threats increase in frequency, severity and variety, it becomes increasingly difficult to simultaneously secure legacy systems and enable collaboration.
6. Integrating new technologies (mobile, cloud, social, IoT) into rigid IT and network infrastructures is costly and complex.
7. Data governance must be maintained while information is shared.



Steps

1. Identify optimal locations — Determine mission goals per metro or region. Identify target partners and exchanges required. Establish a regional presence by creating a control hub in strategic locations. Leverage the Equinix Marketplace to select appropriate interconnections.
2. Deploy security and control services — Modify and migrate centralized security and operational control services to the interconnected hub. Use NFV and security ecosystem partners to introduce defense-in-depth (e.g., MTIC/MTIP, intrusion detection, policy-based segmentation).
3. Interconnect agencies, clouds and partners — Programmatically discover and interconnect with required agencies, clouds, networks, and other partner providers and suppliers. These private, secure connections travel through the control hub, leveraging security levels to ensure real-time compliance.
4. Implement private data exchange — Use interconnections to build a private information exchange, tailored by mission goals, regions and demographics. Leverage SDN to optimize responsiveness and security.
5. Scale for digital capacity — Distribute information through a service fabric comprised of digital edge nodes. Add services from compliant partners and MSPs within Equinix Marketplace, scaling to meet demand.



Forces

- Government is experiencing rapidly compounding communication growth.
- Geographically dispersed participants require real-time collaboration.
- User consumption of large amounts of data is changing how agency missions are executed.
- Improved employee engagement is critical to mission success.
- Growing user expectations (always-on, automated systems, self-service) impacts recruitment.
- Seamless interagency collaboration is critical for mission success.
- Cyber threats continue to rise.

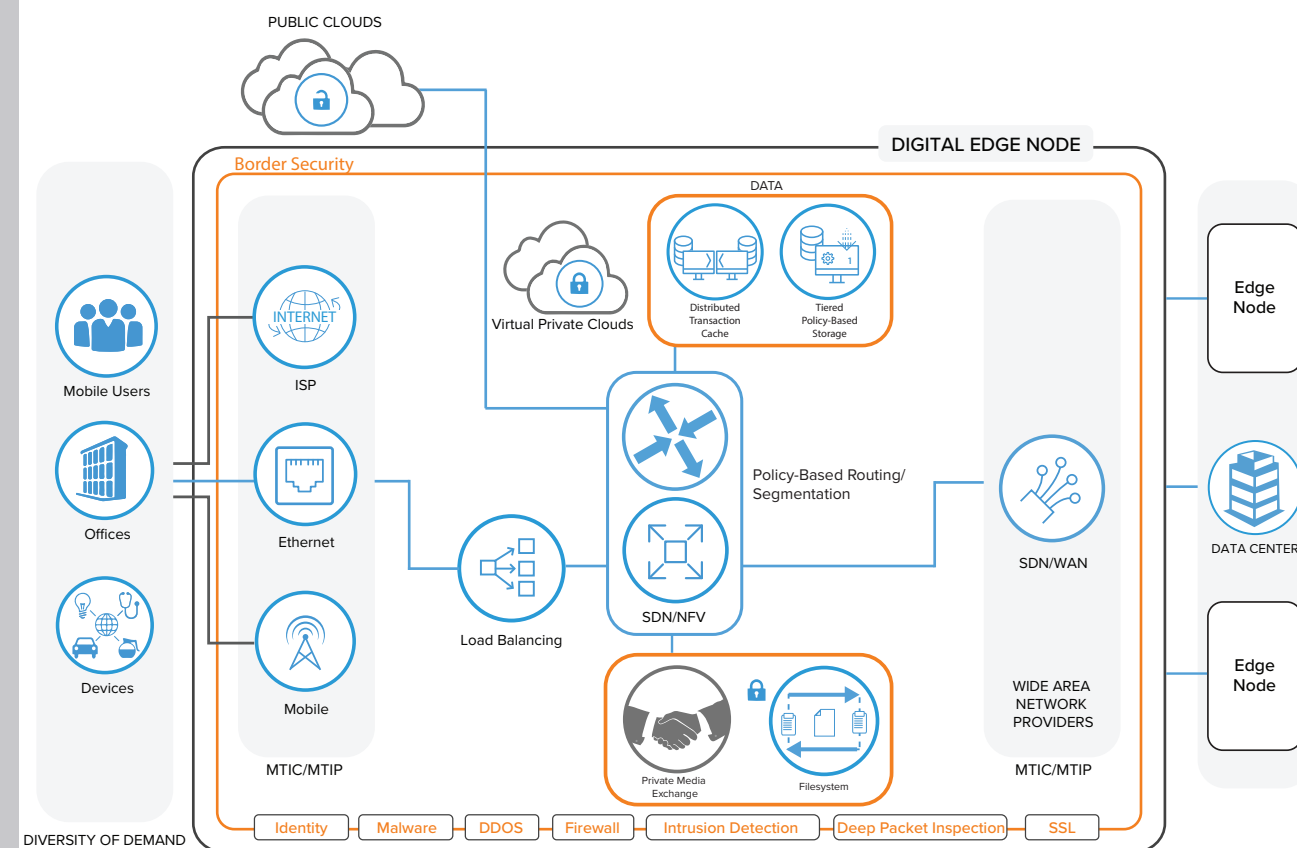


Outcomes

- Integrated security strategies ensure privacy and regulatory compliance.
- Efficient collaboration, data exchange and user engagement optimize service delivery.
- Support of geographic dispersion increases efficiency.
- Rapid onboarding of partners and new agency connections increases operational agility — costs are aligned to growth and need.
- Trusted, private network is extended to the edge for all traffic.
- IT is re-architected with distributed interconnection hubs, accelerating collaboration among people, systems, data and clouds.
- Direct and secure interconnection among organizations, partners and clouds maintains data safety and compliance.
- Cyber threat exposure is reduced with less internet exposure.
- Rewiring for future needs is simplified.
- Scaling is policy-based, driven by demand.



Reference View



Controls



- Network function virtualization (NFV).
- Policy-based segmentation and routing.
- Network load balancing.
- SW defined network (SDN)/WAN.
- Transactional data cache.

- MTIC/MTIP-compliant, localized border security (inspection zones, SSL termination, malware and DDOS protection, next-generation firewall, identity management).
- Localized, tiered, policy-based storage.
- Private agency information exchange.



Problem

Collaboration across multiple, cloud-based platforms creates poor experiences for agencies, partners and constituents alike. Legacy applications within traditional infrastructures are difficult to migrate to cloud. Rigid cost structures create inefficiencies, while initiatives such as integrating partners and expanding services become overly complex, discouraging innovation.



Solution

Reduce cost and complexity by integrating traffic flows from WAN and cloud. Increase collaboration by integrating multicloud and hybrid services in a secure, low-latency manner while migrating or replacing legacy applications at the edge. Colocate in-band security services at the edge node, enabling applications to safely interact across clouds. This improves performance and security while enabling pay-as-you-go cost models. Low-latency, cloud-to-cloud, SaaS-based interaction at the edge significantly reduces delays. Apply role-based access, cloud-based key management and deep packet inspection to traffic entering the digital edge node. Once verified and allowed to enter, inter-cloud traffic can be optimized to reduce data leakage and prohibit unauthorized access to outbound traffic. Each agency can decide how to deploy data, using a hybrid of policy-based, tiered storage in a virtual private cloud (VPC), along with some cloud-based storage. Utilizing SDN/SD-WAN and NFV, implement API-based services that leverage Equinix Marketplace to compose new applications quickly from trusted partners, establishing the foundation for application-centric architecture.



Providers



Managed Services

Supply tailorable, integrated software solutions that simplify hybrid and multicloud connectivity and compliant security. Develop integrated, distributed file storage solutions for private control hub deployment as an alternative to intercloud transfers. Publish API and data management services.

Guide the transformation process with multi-agency and vendor program management. Pilot new data and workload and operations integration with standards-compliant data governance models, driving portfolio rationalization and migration to SaaS.



Constraints

1. Maintaining complex privacy, security and compliance systems in a dispersed, cloud environment increases risk with fragmented controls and expanded attack surfaces.
2. Custom connections to each cloud-based service delays deployment, increases cost and operational complexity.
3. Legacy applications and isolated data impede information sharing.
4. Identity and key management across clouds must be solved to address federal compliance standards.
5. Agencies cannot keep up with the demand for new application services.
6. As cloud consumption grows, fixed cost models create budget overrun and/or operational risk.
7. As more legacy-based services and applications are pushed to hybrid and multicloud, their interactions are impacted by performance and security constraints, impoverishing user experience.
8. Integrating compliant partners is complex and time consuming.



Steps

1. Deploy hybrid multicloud infrastructure — Reduce multicloud connectivity complexity and cost. Ensure secure, low-latency communication by establishing localized IP address management via standards-compliant flow segmentations in the control hubs. Localize file storage in the hubs, minimizing data leakage and costly intercloud data transfers. Deploy a localized cloud key store to secure identity management.
2. Deploy applications in clouds — Incrementally replace legacy applications with equally functional, SaaS-based services in the control hubs. Securely integrate new, cross-cloud workflows while keeping sensitive data under your control.
3. Integrate compliant partners — Leverage the ecosystem for fully compliant partners that can enhance an offering with new capabilities. Build new multicloud workflows tailored for each agency and region.
4. Choose API-based services built for elasticity — Improve innovation and agility with new services composed of standards-compliant functions discoverable via APIs, reducing the burden and cost implications of building in-house.
5. Contract with spend flexibility — Build policy-based, “pay-as-you-use” consumption models.



Forces

- Mandates to increase operational and cost efficiency by going cloud-first shift data distribution and security approaches.
- Agencies must collaborate with each other, the private sector and citizens.
- Risk of not fulfilling changing agency mission is reshaping priorities.
- Loss of collaboration ability can impede mission integrity.
- Growth in cloud usage, data consumption and partner interactions burden current architectures.
- Owning the end-to-end experience of collaboration services is not feasible.

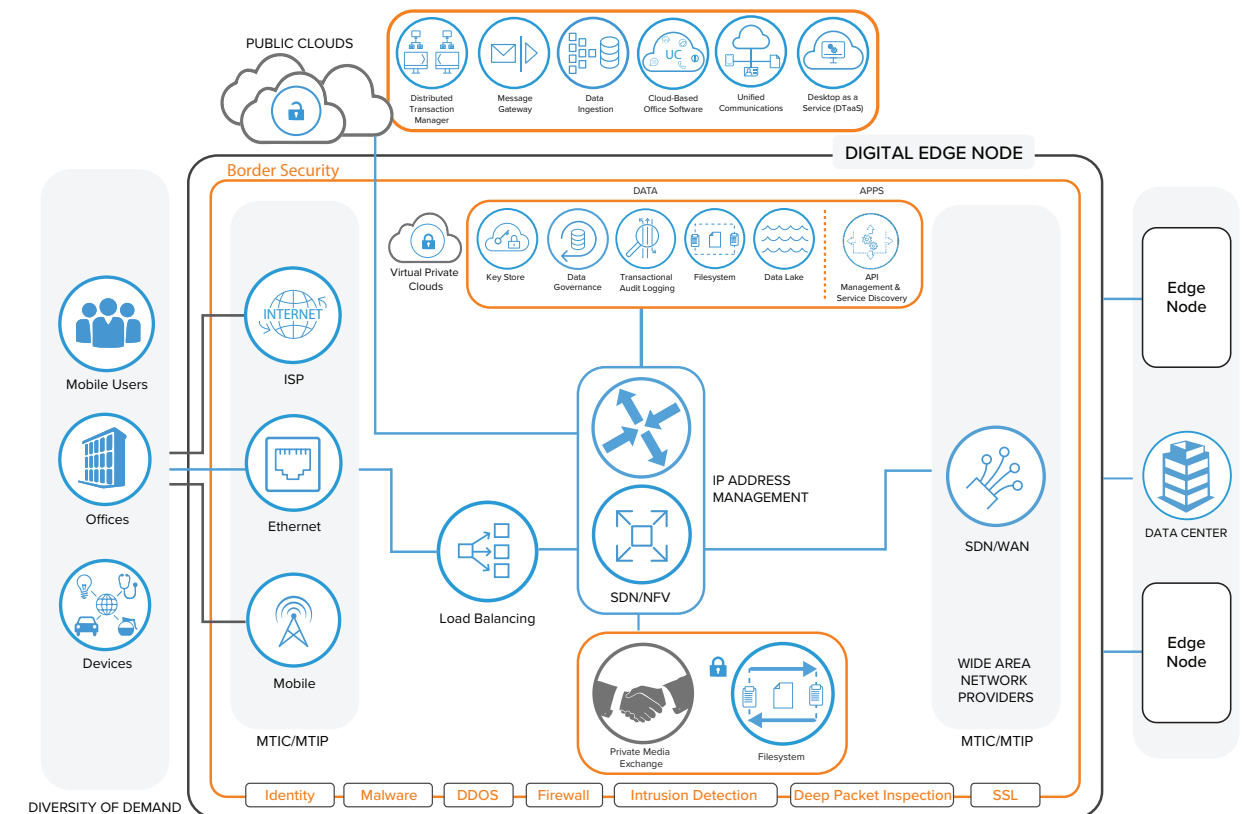


Outcomes

- Delivery and consumption of timely and effectual information.
- Reduced operational complexity for cloud connections.
- API-based discovery and composition for reduced complexity and cost and accelerated innovation.
- Rapid partner onboarding with improved security.
- Policy-driven inter-agency workflows supported by edge controls.
- Federated information sharing between cloud-based applications for responsive, secure and cost-effective access.
- Migration or replacement of legacy applications facilitated by discoverable SaaS services combined through API-based calls.
- New infrastructure consumption models with policy-based usage saves money while ensuring responsiveness to demand spikes.



Reference View



Controls



- IP address management.
- Cloud key store.
- Distributed file system.
- Localized data governance.
- Object store and data lakes.
- API manager.
- Message gateway.
- Distributed transaction/workflow manager.
- SaaS-based office suite.
- Desktop as a service.
- Unified communication.



Problem

Government agencies are unable to engage in distributed data sharing with partners or obtain actionable insights to trending events. They are unable to coordinate their missions with reliability across time zones or optimize user experience across mobile platforms.



Solution

Rewire new capabilities with trusted, resilient connections. Meet mission needs as technology changes and new challenges and threats emerge. Adapt across time zones, collaborate with agencies and enable new partner contracts. Adapt to changing traffic patterns, new regulations, technical innovations (e.g., smart nation initiatives) and capability requirements to support new mission objectives; including the ingestion, aggregation and scrubbing of massive amounts of sensor-based data. Optimize mobile user experiences. Leverage an ecosystem of trusted, standards-compliant partners and services enacted through real-time configuration control. Store the policies in local data repositories at the edge. Route traffic efficiently and safely, driving traffic to the interconnected fabric of control hubs. Anticipate macro and regional trends by building a connected set of complex event processors to analyze aggregated data and create actionable insights that can be directed via policy across an interconnected, self-healing fabric.



Providers



Managed Services

Offer integrated data engineering functions that enable IoT data scrubbing, complex event processing and data governance. Integrate secure mobile device management. Develop IoT gateways. Offer analytic dashboards. Provide seamless, real-time disaster recovery across the fabric.

Build and execute a long-term, strategic plan of continuous innovation with insights from actionable data to fulfill new mission objectives. Invoke parallel change agent teams to integrate the transformation process, balancing global and local initiatives to drive strategic changes.



Constraints

1. Managing a mobile workforce and remote partner interactions from centralized locations creates user experience and security problems.
2. Real-time, dynamic data sharing across agencies and partners challenges centralized operational procedures and security policies.
3. Centralized data capture and analytics that are geographically distant from distributed partner agencies, private sector and non-profit organizations, mobile citizens, and assets inhibits real-time analyses and insights.
4. Incorporating new technologies (mobile, cloud, social, IoT) into legacy systems, under constrained budgets and increased security and compliance regulations impedes mission objectives.
5. Achieving mission resilience in a distributed, hybrid multicloud environment is especially challenging as data replication controls can become isolated and fragmented.



Steps

1. Optimize web and mobile UX — Integrate and deploy API release management tools designed to work across multiple devices and protocols. Emphasize rapid delivery with security compliance sandbox testing for beta releases. Deploy user experience policies to enforce regional configurations.
2. Share data with other agencies — Deploy data ingestion and integration managers into the control hub. Use data governance policies across data pipelines for inter-agency and partner exchange.
3. Achieve fast and agile insights with actionable data — Leverage SaaS-based analytic modeling tools to examine regional, national and global trends using data aggregated in the hubs. Develop and deploy complex event processors to drive actions, workflows and alerts.
4. Create smart nation foundation — Deploy IoT gateways in each control hub, using data lakes as staging areas for aggregation and scrubbing. Integrate with complex event processors to derive trends, actionable insights or threats.
5. Achieve mission resilience — Implement localized disaster recovery managers at each hub, leveraging a global data consistency replication manager that works across the fabric.



Forces

- The smart nation initiative requires large-scale digitalization and the integration of IoT.
- Smart nation will force the expansive distribution of complex event modeling and data governance.
- Citizens are expecting personalized public services, tailored to their needs, and these needs will change during disasters.
- Interagency collaboration and sharing needs to become real time.
- Agencies must address the growing mobility of employees, partners and citizens to fulfill missions.

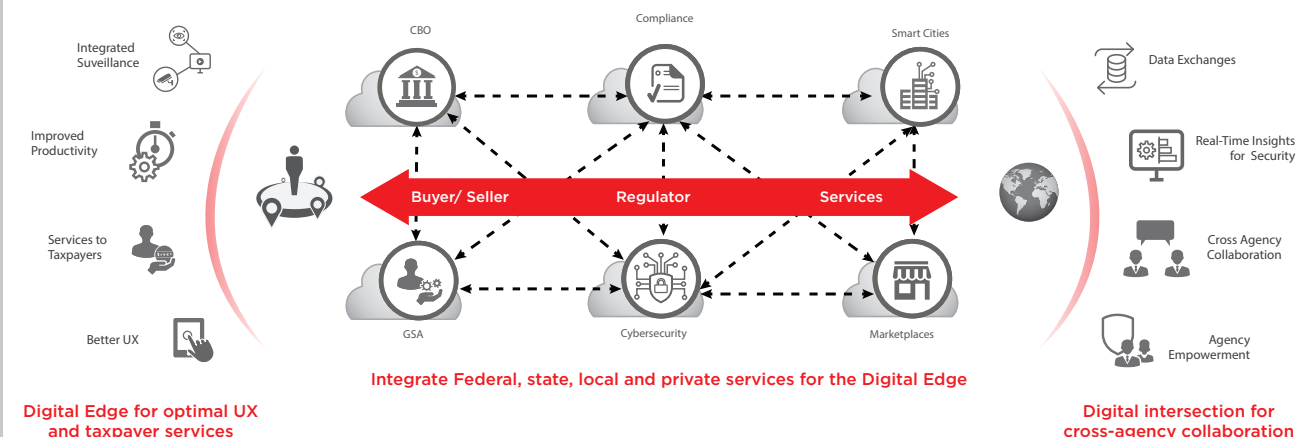


Outcomes

- User experience is optimized across device types, with frequent, safe application updates tailored to regional needs.
- Inter-agency data exchanges are tailored to local requirements.
- Localized and secure real-time data processing and analytics enable faster insights and effective service delivery.
- Sensor data is aggregated, normalized, scrubbed and analyzed locally for trends and actionable events to facilitate smart nation initiatives.
- Policy-driven, real-time disaster recovery and operational continuity across the service fabric ensures continuous resilience within and across agencies.



Reference View



Controls



- Mobile application services.
- Device management.
- Distributed application update coordinator.
- Data integration manager.
- Data ingestion aggregation and scrubbing.
- Data pipelines.
- Analytics dashboard.
- IOT aggregation gateways.
- Real-time complex event processing manager.
- Disaster recovery manager.
- Global data consistency replication manager.