White paper
Confidential

From the Edge to the Cloud: Cisco in Defense

Understanding of the Problem

Several of the far-reaching objectives of the Defense Digital Modernization Strategy is connecting the mission edge with the data and analytics hosted in the cloud. Achieving this vision is not without challenges.

- First is that the mission edge spans in function and scope from forward deployed units engaged in combat operations through multi-domain regional command and control elements through forward and fixed logistics and sustainment centers to functional and national level operations and intelligence centers.
- Second is that the 'cloud' is not a single cloud but a cloud of clouds that includes mission dedicated, platform embedded assets; regionally distributed fit-for-purpose cloud environments; and hyper-scale general-purpose public cloud environments.
- Third is that diverse mission function drives diverse, fluid, sometimes event-specific constellation membership and functional forms.
- Fourth is that mission conversations take place simultaneously at multiple levels of security across significant distances that are differentially served by dedicated transport bandwidth.

While in aggregate, these challenges appear to be complex, individually they are each addressable with intelligent network architectures that are secure, adaptive, agile, and elastic. In this context:

- Secure refers to the ability to establish a root of trust and maintain continuity of trust throughout the multi-transaction data lifecycle across multiple architecture elements.
- Adaptive refers to the ability to operate in cyber-contested environments using real-time threat intelligence and trajectory analytics to adjust operating postures and path selection.
- Agile refers to the ability to support a secure, concurrent development-operations model in which mission assets are rapidly reconfigured in response to the changing battlespace.
- Elastic refers to the ability to scale rapidly to meet intense demand and the ability to position workloads to align with mission resiliency requirements and comply with latency thresholds

The reality is that these capabilities exist. Cisco's multi-year rotation from device centricity to architecture centricity has generated the ability securely create an integrating architecture that supports the data exchange that is at the core of a profound shift in tactical, operational, and strategic advantage.

The Medium of Maneuver for Operationalized Data

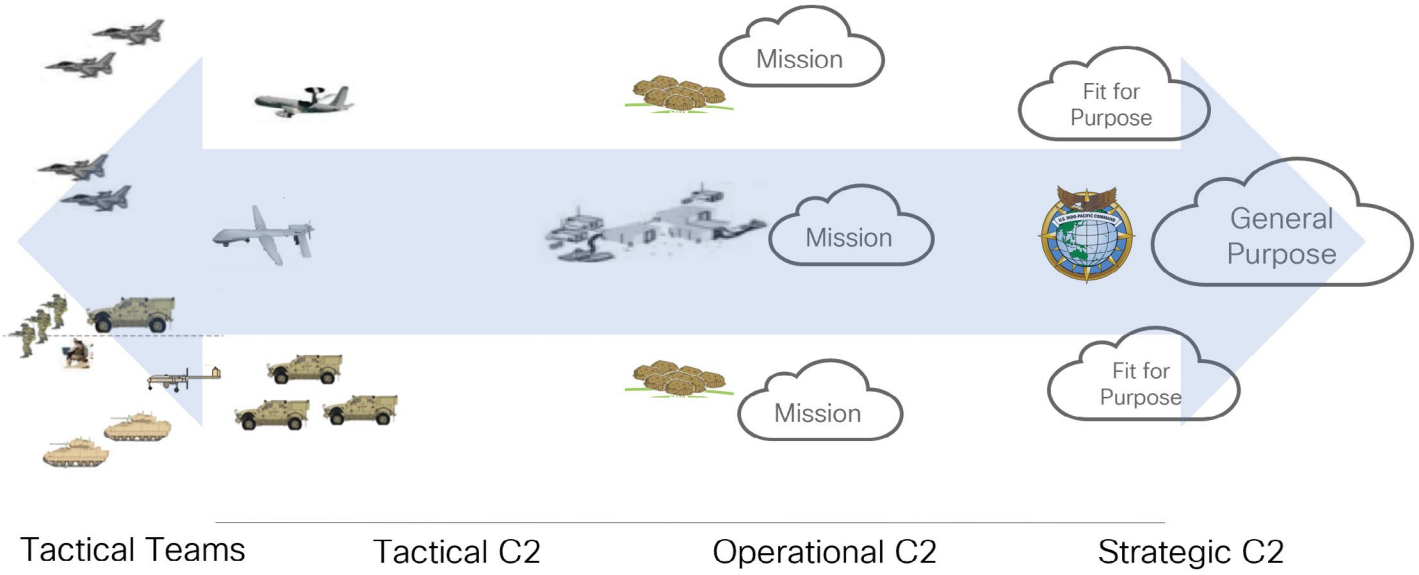
We see this integrating architecture as the 'medium of maneuver' for data. Within this medium of maneuver, data moves purposely and accountably from point-to-point, from mission constellation-to-mission constellation accelerating the operational tempo and increasing operational effectiveness - it is comprised of multiple network architectures that interface via cross-platform, secure data exchange mechanisms and orchestrated cloud-to-cloud interactions. The medium of maneuver for data features:

- Adaptive security architectures that implement advanced network segmentation and network access controls to prevent, detect, and respond to intrusions or malicious activity through continuous visibility and validation.
- Verifiable and customizable defensive technologies and techniques that help customers protect their data and workload assets from the edge to the cloud.
- Situational awareness of all when all of these network flows and device telemetry can be integrated and analyzed automatically – and understood in context to any threats.

The bottom-line is that the digital medium of maneuver connects advantage at the tactical level to the operational level accelerating the decision cycle and compressing the time necessary to overwhelm the adversary. At the strategic level, situational awareness of tactical impacts and operational tempo supports orchestration and integration of national level efforts to generate cascading effects that confound and cripple the adversary.

The Continuum of Connection Edge-to-Cloud

Distributed enterprise architectures have been around for about a decade and during that time Cisco has assisted customers as they debate the appropriate balance between centralization and localization of compute, storage, and networking assets. Through this experience, it has become evident that the vast majority eventually use a combination of both aligning the information technology architecture with the operational architecture. In many cases, customers respond to diverse, dynamic, and constantly evolving demand by building in flexibility and agility.



These architectures are built on a multi-cloud operations model that takes advantage of software defined networking supported by strategically distributed, converged hardware that maximizes network function virtualization and delivers host agnostic interoperability and with containers on a software-defined networking operational model – these architectures are secure, adaptive, agile, and elastic by design.

- Convergence and virtualization convert infrastructure into a flexible fabric rather than a hardscape. Flexible nodes host multiple functions that have been previously device specific.
- Containers are software packages that enable replication or movement of apps and reference data to any capable host. Containers perform consistently on a variety of operating systems.
- Software-Defined Networking simplifies condition-responsive orchestration of access control and application/data provisioning that creates a fully managed medium of maneuver for data.

Although not unique to military applications, additional operational requirements such as latency compliance, operational resiliency, and data rights must be addressed in the design of the future network architecture. These requirements call for hybrid cloud solutions establishing on-premise data center capability and capacity that benefit from central security policies, access management, and app standardization with significantly reduced overhead.

Transformation Is Founded on Trustworthy Systems

While positioning itself in the digital future, the Department of Defense will increasingly call on a range of globally distributed data sourced from fixed and mobile sites to combine with data and applications hosted in many clouds to support autonomous machine man-in-the-loop decisions/actions. We at Cisco know this territory and have served as the trusted partner for global organizations operating in the same environment. Our enterprise-level customers deliver business outcomes in multi-national banking, global manufacturing, worldwide shipping, and highly secure, time-sensitive military missions such as remote/split operations of globally deployed unmanned aerial vehicles. All have one thing in common – a trustworthy, secure, resilient, simple, and verifiable digital foundation. Cisco is the global leader in:

- Trustworthiness rooted in secure lifecycle management practices and secure supply chain constantly protected and verified via physical, logical, and technology-based methods.
- Cybersecurity based on a zero-trust posture ensuring real-time verification at the user, device, network, and application levels using AI powered identity management and behavior monitoring.
- Resiliency enabled by threat and quality of service aware routing, rapid mobility from-cloud to-cloud via container-native designs to assure for cloud connection, protection, and consumption.
- Simplicity inherent in graphic user interface-based access control and security policy deployment, one-touch provisioning, and visual confirmation of configurations & status.
- Verification capability enabled by telemetry-based audits of application performance and distributed data center policy compliance in the north-south and east-west directions.

With Cisco, every transaction from the edge to the cloud is based on trust.

Driving to Success in the Transformation Journey

Because we know that many digital transformations fail to meet expectations, we partner with our customers to maximize the potential throughout the journey. Through experience, we have identified keys to successful cloud journeys that apply in the adoption of hybrid and multicloud models essential to enterprise transformation:

- Embrace existing deployments: Between existing cloud enclaves and continuously emerging specialized requirements, the organization most likely already has a multicloud environment. Migrating all existing infrastructure and data to a single environment would be resource intensive and does not necessarily unlock major value. In these cases, a multicloud approach allows for simplified adherence to desired cyber security and governance standards.
- Incorporate resiliency: Operating in multiple environments reduces the overall probability of a complete outage. If a service in one environment goes down, additional highly scalable environments are readily available. Proper cloud visibility, operations, and management platforms simplify this process and automate many actions based on enterprise policy.
- Adhere to industry standards and preserve future flexibility: In well managed private, hybrid and multicloud model environments, users and their vendors adhere to industry standards that support progressive distribution strategies that adapt to emerging conditions, technologies, and user populations. Maintaining cloud mobility provides the ability for the participants to select the cloud approach that best meets the needs of each individual mission.
- Own security: In a hybrid and multicloud model, the most sensitive workloads can remain onsite and under complete control of the organization. Enterprise policy defines strict security standards that must be met and upheld by all cloud providers, which guarantees that any workload moved offsite will be secured to the appropriate level.
- Preserve location flexibility: Some workloads must be hosted near the end-user in order to meet the desired performance expectations. Other workloads have to reside in certain locations to meet data sovereignty or impact level requirements. A hybrid and multicloud model provides flexibility in finding a provider that best meets the mission needs.

Cisco's Approach to the Distributed Network Architecture

Increasingly, the distributed network architecture not only connects people and devices, it provides distributed computing capability from the edge, through the network, to the data center, and into private and public clouds. It provides ubiquitous access to data and enables generation of digital threads and the digital twins that can power the AI-enabled enterprise.

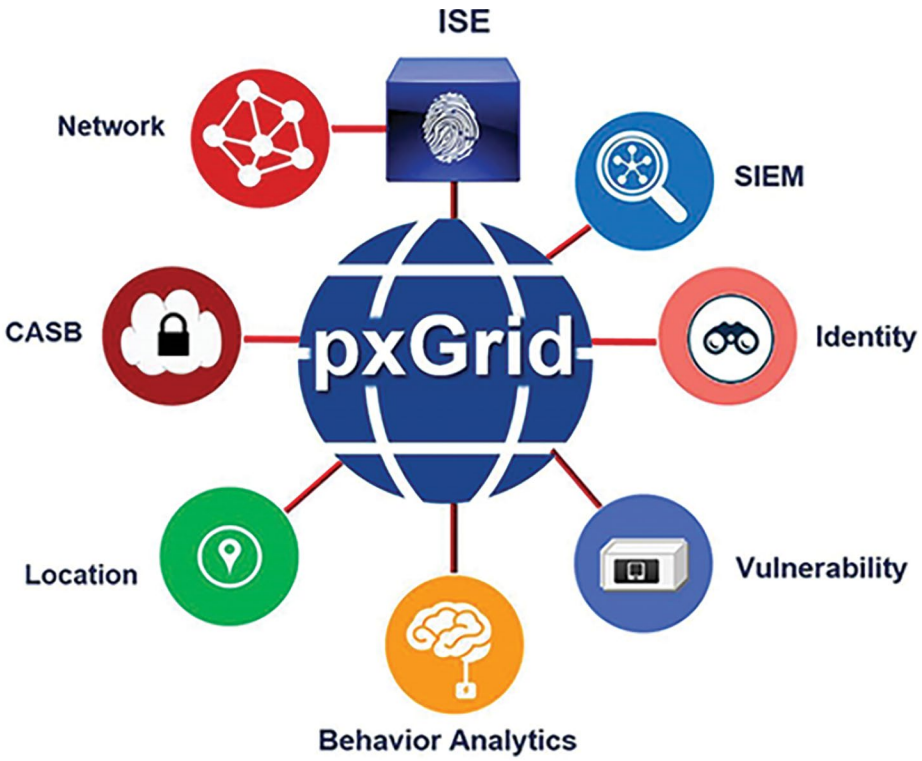
To make this possible, today's networks must extend beyond conventional uses and locations (often in harsh or extreme environments) over a variety of wired and wireless connections. Connecting with Cisco's Extended Enterprise extends your network, its access policies, and its cybersecurity capabilities to any and every edge.

Cisco's approach to forming the continuum of connection from edge-to-cloud is based on five principles:

- A zero-trust operational posture to establish source (user/endpoint/edge-device) authenticity in real-time via source qualification, registration, and context alignment. Once authenticated, sources are treated as identities and are subjected to zero-trust principles including granular micro-segmentation key in compartmentalizing users endpoints, edge-devices and/or data and applications.
- The zero-trust posture serves as the foundation for integrated, end-to-end cyber security that exploits real-time threat intelligence across a full range of integrated cyber security tools (intrusion detection/prevention, identity services, malware protection, behavior analysis, etc.) to extend enterprise protection to every participant at every location within the topology.
- Agile hardware technologies capitalize on network device, function, and application virtualization at every form factor from hyperconverged data center packages to vehicle mounted routers to device embedded switches. Agile hardware supports provisioning that places the right application and the right data in the right place at the right time.
- Advanced software defined networking capabilities inherent in application centric infrastructure that employs intent-based networking to support policy-based differentiation of user privileges by role, scope of access, and permitted actions. Intent-based networking supports session-by-session network adjustments aligning with the mission fabric similar to the manner in which airspace is dynamically aligned with the multi-domain battlespace.
- Real-time application performance monitoring to validate application and data interaction in multi-step processes. This capability supports real-time assessment to identify miscues and disconnects at their root cause (e.g., code change, data structure change, etc.) that lead to correction in minutes or hours vice traditional forensics that take days, weeks, or months.

Ensuring Interoperability in a Diverse Topology

At Cisco, we recognize that our customers often operate in multi-vendor networks environments, so we developed the industry-leading Platform Exchange Grid (pxGrid) to provide a unifying framework. This framework enables multivendor, cross-platform network system collaboration for security monitoring and detection; network policy management; asset and configuration oversight; identity and access services; and other IT operations. Cisco pxGrid enables ecosystem partners to integrate once, then share context either uni-directionally or bi-directionally with many platforms, without the need to adopt platform-specific APIs. At present over 80 vendors are incorporated.

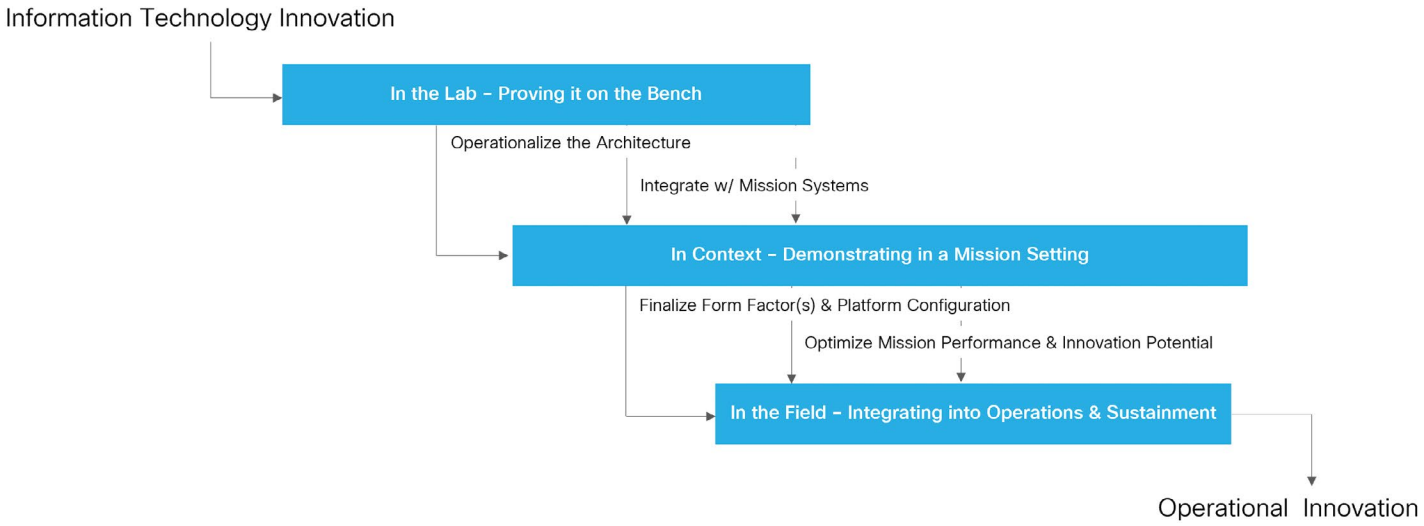


One of the benefits of Cisco's global presence is that we have seen customers deploy a multitude of cross-vendor solutions and have been able to identify those combinations that create 'better together' solutions. In other cases, we have found that multi-vendor solutions can actually reduce effectiveness and dramatically increase complexity as multiple and, in some cases, overlapping solution sets actually reduce performance and generate significantly higher training, management, and administration burdens.

Partnering in Operational Innovation

We, at Cisco, are innovators at our core – constantly looking for ways to optimize performance, maximize security, and reduce complexity of the network architecture such that it becomes part of the mission fabric. Our research and development efforts are focused to this end, but we realize that it's not only about the network. Although the network provides the foundational platform to enable mission operations, the applications and data are essential components any digital transformation effort must account for networks, applications and data holistically. We also recognize that in our DoD line of business our job is to identify the potential for innovation in information technology to enable innovation in a mission context and to actively participate in the experimentation that leads to new, more effective, lower risk operational concepts.

As a general practice, we see rapid discovery, integration, and normalization as a process (illustrated below) that is characterized by speed and measured in terms of operational relevancy.



Our engineers, architects, account managers, and defense strategists are focused on this idea every day and are standing at the ready to serve as your mission partners.

Conclusion

Cisco sees the potential of capitalizing on technologies proven in government and commercial settings within dedicated mission settings to close critical gaps in the edge to cloud continuum shifting the advantage in favor of those that can generate, share, and make sense of data at machine speed across the full continuum of connectivity from edge to cloud.