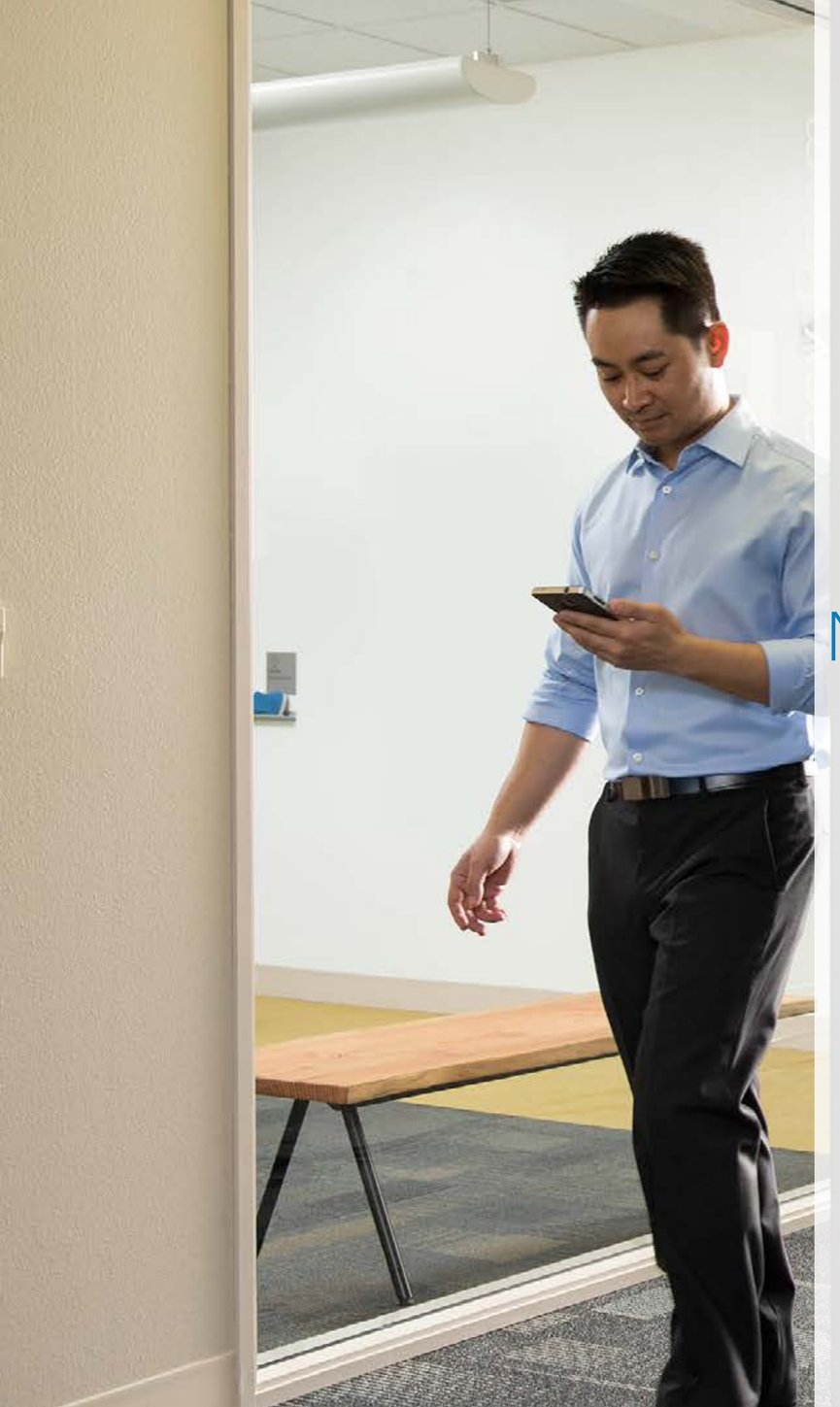


Cisco Digital Network Architecture (DNA) Readiness Model

Let’s get started

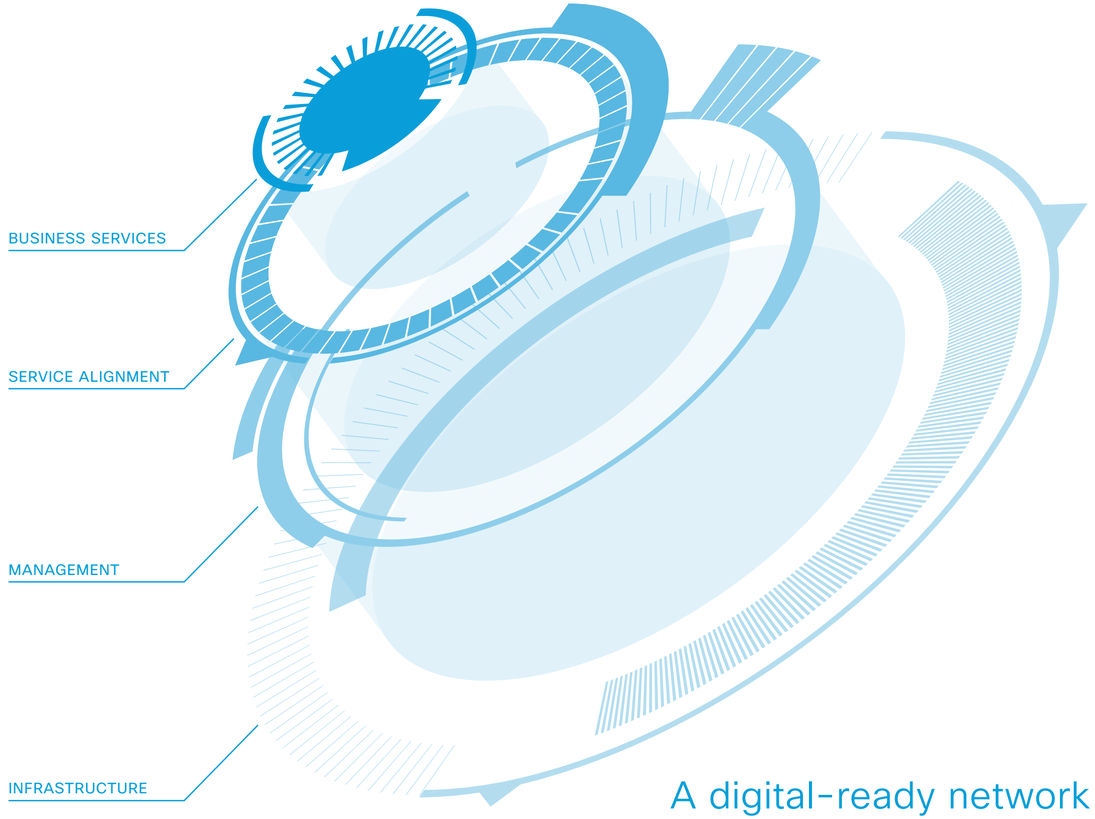
Share

Why Evolve to a Digital-Ready Network Architecture?

The digital value at stake from the overall private sector for 2015 to 2024 is estimated at an enormous **US $23.8 trillion.**[1]

Every aspiring organization, large or small, faced with the opportunities and challenges of digital business needs a digital-ready network. Agile, secure networks simplify IT and enable rapid innovation. Without a network that can actively enable and protect your business strategy, the applications, cloud services, and devices you deploy cannot live up to their potential.

Get a view into the DNA Readiness Model and how it can benefit you.



A digital-ready network dynamically aligns to meet the needs of the business.

1. Connected Futures Magazine: Private Sector Digital Value at Stake (PDF)

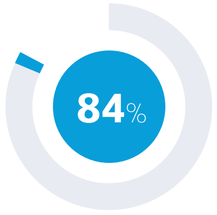
Trends Fueling Digital Business and the Digital Network

Security

The attack surface is increasing.

100% of the business networks analyzed by Cisco teams have traffic going to websites that host malware.

Ransomware is becoming rampant.

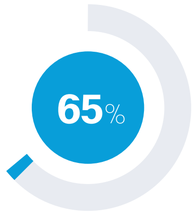


Big Data

84% of CEOs believe that big data is delivering high or very high business value to their organization.[2]

Big data storage will reach **73 ExaBytes** by 2019.[3]

2. PWC: 18th Annual Global CEO Survey
3. IDC: Worldwide Storage in Big Data Forecast, 2015–2019

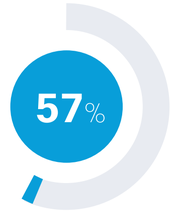


IoT

IDC forecasts as many as 30 billion IoT devices by 2020.[4]

65% of CEOs consider IoT strategic to their business.[5]

4. IDC: Worldwide Internet of Things Forecast Update, 2016–2020
5. PWC: 18th Annual Global CEO Survey

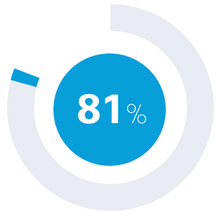


Cloud

57% of organizations are using or planning to use public cloud or private cloud solutions to support production workloads and services.[6]

For organizations, greater cloud adoption generates an average US $1.6 million in additional annual revenue and US $1.2 million in cost savings per cloud application.[7]

6 & 7. IDC InfoBrief, sponsored by Cisco, Don't Get Left Behind: The Business Benefits of Achieving Greater Cloud Adoption, August 2015



Mobile

81% of CEOs believe that mobility is strategic to their business, whether for improving the workforce experience or customer engagement.[8]

According to the 2016 Cisco VNI Mobile Index there will be an estimated 5.4 Billion mobile users by 2020.[9]

8. PWC: 18th Annual Global CEO Survey
9. Cisco VNI Mobile Index

"Given the promise of these accelerators to create new competitive opportunities or serve as catalysts to solving a wide range of global and commercial needs, having the right network architecture to support these workloads will be of paramount importance." [9]

61%

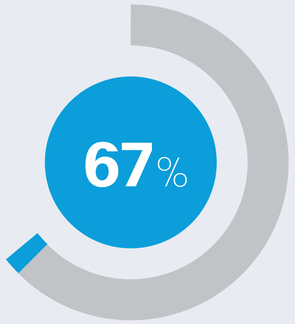
Customer Demands

61% of CEOs believe that changes in customer behaviors are responsible for promoting disruption in their industry.[10]

9. IDC: Insight (Doc #259317 / Sep 30, 2015) IT's 3rd Platform Drives Need for Network Innovation
10. PWC: 18th Annual Global CEO Survey

Network Evolution for Digital Transformation

According to Gartner, networks and communications have an important role to play in digital business and the Internet of Things (IoT). Organizations rank them higher in accelerating digital business than business applications, operational technology applications or cloud.[11] At the same time, however, "Less than 10% of enterprises that have implemented or plan to implement digital business have very clear integration between their network and digital business strategies."[12] And according to a Forrester survey, most organizations believe that it's IT leadership that has the expertise and experience to make sure that this integration between business and IT occurs: "Nearly 4/5 of business leaders believe that it is IT's responsibility to ensure the network can support the company's digital plans."[13]



67% of business leaders believe the current network is a bottleneck in Enterprise IT.[14]

What Does This Mean?

If digital transformation were not a reality, just continuing to focus on providing high performance and reliable connectivity might be sufficient. But that's not the case. Business leaders are now saying, "Thanks for all the years of service. But we need much more from the network if we are going to succeed in the digital era."

The business is expecting much more because rigid, complex, slow-to-deploy-and-configure networks can no longer do the job. The business is saying, "In the future, I need a network that 'hears and speaks' the language of the business." What does that mean? Well, when the business creates a new service or process, embarks on a project to improve customer relationships, adopts a new security policy, is faced with a new regulation, needs real-time data, enters the world of IoT, or embraces any other new initiative, the network must intrinsically understand what needs to be done—and then just do it. This transformation will require networks that are open and extensible and able to dynamically adjust based on business rules with little manual intervention.

11 & 12. Gartner, Jouni Forsman, Survey Analysis: Networks for IoT and Digital Business, September 2015, G00289837.

13 & 14. Verizon Commissioned Study carried out by Forrester Consulting, September 2015.

Changing the Fundamental Principles of Networking

Recognizing the need for a transformative network architecture, Cisco announced the Cisco® Digital Network Architecture (DNA). This architecture is based on a number of basic principles that contribute to delivering a network ready for the digital age.

Virtualize Everything

By decoupling hardware from software, give organizations freedom of choice to run any service anywhere, independent of the underlying platform: physical or virtual, on premises or in the cloud.

Designed for Automation

Automation makes networks and services on those networks easy to deploy, manage, adapt, and maintain, fundamentally changing the approach to network management. Controller-based networking simplifies management through abstraction and automation and provides a platform for consistent service alignment and policy enforcement. This approach accelerates application and service rollout while reducing risk. IT staff gain the time to focus on enabling business strategy instead of operations.

Pervasive Analytics

Provide insights into the operation of the network, IT infrastructure, and the business to help IT and the business make better, faster decisions using information that only the network can provide. Use the distributed power of the network to create value from the masses of data delivered through Internet of Things (IoT) initiatives. Respond quickly to contain threats by using the all-seeing network to identify anomalies.

Service Management Delivered From the Cloud

Unify policy and orchestration across the network, enabling both the agility of cloud and the security and control of on-premises solutions.

Open, Extensible and Programmable at Every Layer

Integrate Cisco and third-party technology, open APIs, and a developer platform to support a robust ecosystem of network-enabled and cloud-enabled applications. Enable open interfaces so that business applications and services can communicate service and policy requirements directly to the network.

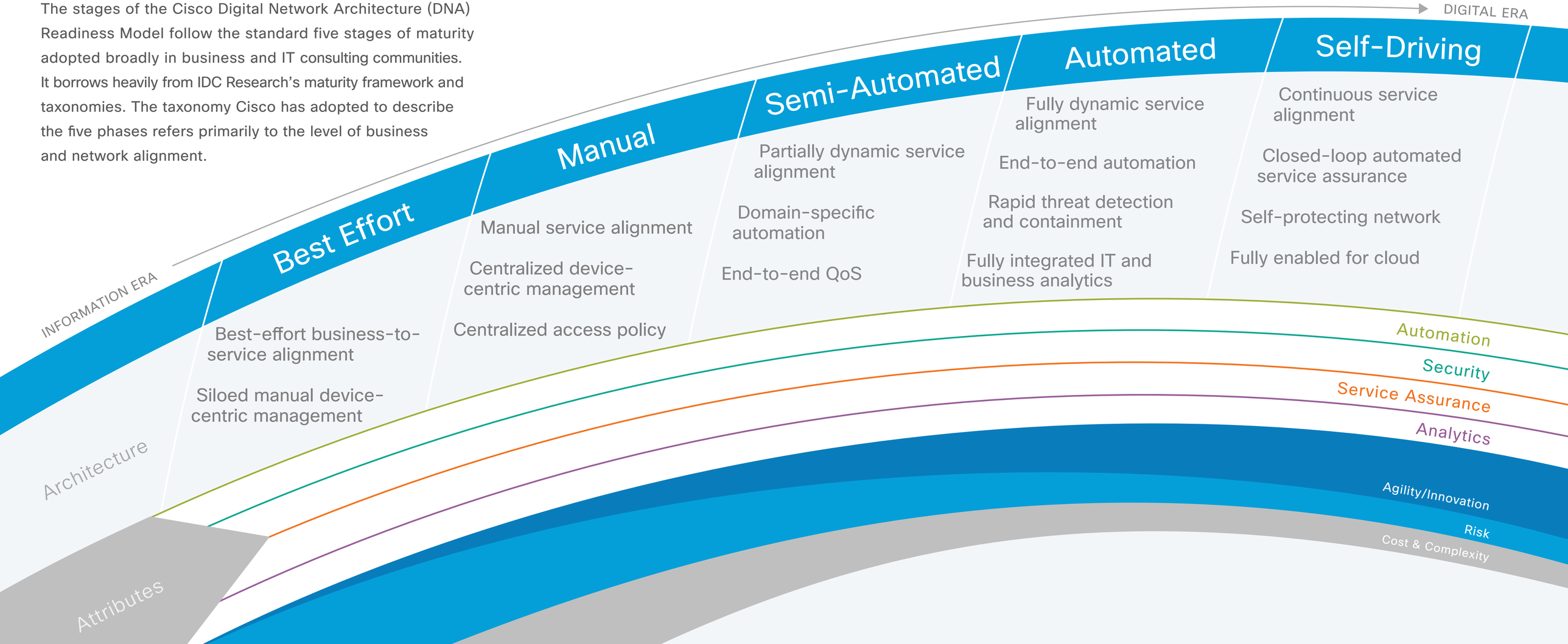
Why a Network Readiness Model?

Most organizations are early in their journey to a digital-ready network. And the evolution to a network that can fully meet the requirements of digital initiatives will require the coming together of many technologies and process changes over time. Just as data center consolidation, virtualization, and automation has been a multiyear journey for most organizations, we can expect that it will take some time for most organizations to complete the digital network journey. However, the journey delivers important near term gains on the road to network transformation.

The Cisco Digital Network Architecture Readiness Model has been created to help customers gain a clearer picture of where they are on this journey and gain visibility into the opportunities and benefits of evolving to the next stage. The model is intended as a framework and guide that each organization can use and customize to suit its own needs and priorities.

Cisco Digital Network Architecture Readiness Model

The stages of the Cisco Digital Network Architecture (DNA) Readiness Model follow the standard five stages of maturity adopted broadly in business and IT consulting communities. It borrows heavily from IDC Research's maturity framework and taxonomies. The taxonomy Cisco has adopted to describe the five phases refers primarily to the level of business and network alignment.



Stage 1: Best Effort

Siloed Hardware & Device Centric Architecture

Stage 1 2 3 4 5

CUSTOMER EXPERIENCE
CLOUD
ENTERPRISE
WORKFORCE EXPERIENCE
COLLABORATION
BUSINESS ANALYTICS
BUSINESS OPERATIONS
IOT
CUSTOMER

Application Service Levels | Security Policy & Compliance | IT Operations & Processes

Business
Digital Business
Applications
Business Service Requirements

POLICY

Service Alignment
Manual, Device-centric Policy

Fragmented, Manual, Device-centric Policy Alignment

Management
Localized, Siloed Device-centric

Wireless LAN Management
LAN Management
Firewall Management
Data Center Network Management
Branch Router / WAN Management

ABSTRACTION

Infrastructure
Hardware & Device-Centric

INTERNET/ CLOUD

CAMPUS
Wireless Access
Wireless Controller
Access
Core/ Distribution
Security
Edge
HARDWARE/DEVICE CENTRIC

WAN

DATA CENTER
Security
Edge
Network

WAN

BRANCH
Branch Access
WAN
HARDWARE/DEVICE CENTRIC

SERVICE ASSURANCE
AUTOMATION
SECURITY
ANALYTICS

Best-effort business-to-service alignment

Siloed device-centric management

Fragmented IT operations

Perimeter-focused security

Patchy service assurance coverage

Detail View >

Stage 1: Best Effort

Siloed Hardware & Device Centric Architecture

DETAIL

Stage 1 2 3 4 5

DETAIL VIEW

CUSTOMER EXPERIENCE
CLOUD
ENTERPRISE
WORKFORCE EXPERIENCE
COLLABORATION
BUSINESS ANALYTICS
BUSINESS OPERATIONS
IOT
CUSTOMER

Application Service Levels | Security Policy & Compliance | IT Operations & Processes

Business
Digital Business
Applications
Business Service Requirements

POLICY

Service Alignment
Manual, Device-centric Policy

Management
Localized, Siloed Device-centric Multiple Functionally Separate Systems

ABSTRACTION

Infrastructure
Hardware & Device-Centric

Business Group Views
Centralized Event Aggregation
Threat Detection Reporting
Basic Application Policies

Roles & Scope-based Access
Device-specific Event Analysis
Perimeter Threat Detection
WAN Application Prioritization
Wireless LAN Management
LAN Management
Firewall Management
Data Center Network Management
Branch Router / WAN Management

INTERNET/ CLOUD

OS 1
Wireless Access
Wireless Controller
OS 2
Access
Core/ Distribution
HARDWARE/DEVICE CENTRIC
Security
Edge
WAN
Security
Edge
Network
OS 3
Branch Access
WAN
HARDWARE/DEVICE CENTRIC

CAMPUS
DATA CENTER
BRANCH

SERVICE ASSURANCE
AUTOMATION
SECURITY
ANALYTICS

Stage 2: Manual

End-to-End Hardware & Device Centeric

Stage 1 2 3 4 5

CUSTOMER EXPERIENCE
CLOUD
ENTERPRISE
WORKFORCE EXPERIENCE
COLLABORATION
BUSINESS ANALYTICS
BUSINESS OPERATIONS
IOT
CUSTOMER

Application Service Levels | Security Policy & Compliance | IT Operations & Processes

Business
Digital Business
Applications
Business Service Requirements

POLICY

Service Alignment
Manual, Domain-centric Policy

Management
Centralized Management Device-Centric

ABSTRACTION

Infrastructure
Hardware & Device-centric

Manual, Domain-centric Policy Alignment

Wireless LAN
LAN
Router
Data Center Network
Centralized Device Management
Firewall Management

SaaS
Customers/Partners
INTERNET/ CLOUD

VPN
WAN

Wireless Access
Wireless Controller
Access
Core/ Distribution
Security
Edge
HARDWARE/DEVICE CENTRIC

Security
Edge
Network

Branch Access
Hybrid WAN
HARDWARE/DEVICE CENTRIC

CAMPUS
DATA CENTER
BRANCH

Manual business-to-service alignment

Centralized device-centric management

End-to-end manual IT operations

Centralized access policy

Wide-spread service assurance coverage

Detail View >

ACCESS CONTROL
SERVICE ASSURANCE
AUTOMATION
SECURITY
ANALYTICS

Stage 2: Manual

End-to-End Hardware & Device Centeric

DETAIL

Stage 1 2 3 4 5

DETAIL VIEW

CUSTOMER EXPERIENCE
CLOUD
ENTERPRISE
WORKFORCE EXPERIENCE
COLLABORATION
BUSINESS ANALYTICS
BUSINESS OPERATIONS
IOT
CUSTOMER

Application Service Levels | Security Policy & Compliance | IT Operations & Processes

Business
Digital Business
Applications
Business Service Requirements

POLICY

Service Alignment
Manual, Domain-centric Policy

Management
Centralized Management Device-centric

ABSTRACTION

Infrastructure
Hardware & Device-centric

Prioritized Event Management
Centralized Event Analysis
Access Policy
Centralized Access Control
Threat Detection Reporting
Network-wide Threat Detection
Application Type Prioritization
Network-wide Application Prioritization
Centralized Device Management
Data Center Network
Router
LAN
Wireless LAN
Firewall Management

SaaS
Customers/Partners
INTERNET/ CLOUD

OS 1
Wireless Access
Wireless Controller
OS 2
Access
Core/ Distribution
HARDWARE/DEVICE CENTRIC
Security
Edge
VPN
WAN
Security
Edge
Network
VPN
OS 3
Branch Access
Hybrid WAN
HARDWARE/DEVICE CENTRIC

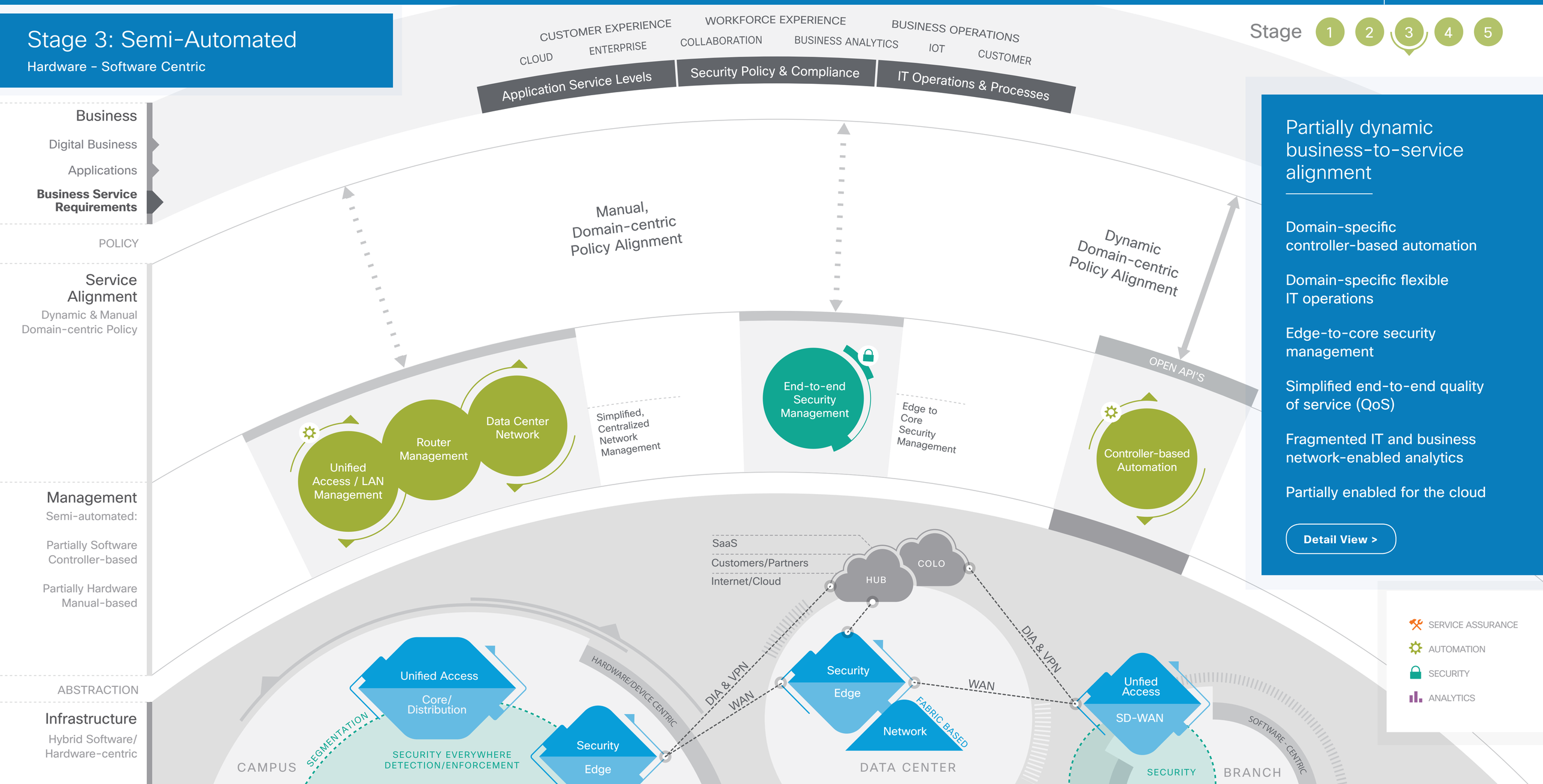
CAMPUS
DATA CENTER
BRANCH

ACCESS CONTROL
SERVICE ASSURANCE
AUTOMATION
SECURITY
ANALYTICS

Stage 3: Semi-Automated

Hardware – Software Centric

Stage 1 2 3 4 5



Partially dynamic business-to-service alignment

Domain-specific controller-based automation

Domain-specific flexible IT operations

Edge-to-core security management

Simplified end-to-end quality of service (QoS)

Fragmented IT and business network-enabled analytics

Partially enabled for the cloud

Detail View >

Stage 3: Semi-Automated

Hardware - Software Centric

DETAIL

Stage 1 2 3 4 5

DETAIL VIEW

CUSTOMER EXPERIENCE
CLOUD
ENTERPRISE
WORKFORCE EXPERIENCE
COLLABORATION
BUSINESS ANALYTICS
BUSINESS OPERATIONS
IOT
CUSTOMER

Application Service Levels | Security Policy & Compliance | IT Operations & Processes

Business
Digital Business
Applications
Business Service Requirements

POLICY

Service Alignment
Dynamic & Manual
Domain-centric Policy

Management
Semi-automated:
Partially Software Controller-based
Partially Hardware Manual-based

ABSTRACTION

Infrastructure
Hybrid Software/ Hardware-centric

Dynamic Policy

OPEN API'S

Application Prioritization

Anomaly Detection and Containment

E2E Service Management

Policy Management and Enforcement

Fragmented Analytics

- Network
- Location
- Security

Centralized Policy Orchestration

Software-orchestrated Quality of Service

OPEN API'S

Day 1

Day 0

Business Service Impact Analysis

Simplified, Centralized Network Management

End-to-end Security Management

Unified Access / LAN Management

Router Management

Data Center Network

Controller-based Automation

Open APIs

SaaS
Customers/Partners
Internet/Cloud

HUB

COLO

DIA & VPN

WAN

OS 1

OS 2

Unified Access

Core/ Distribution

SEGMENTATION

SECURITY EVERYWHERE DETECTION/ENFORCEMENT

CAMPUS

HARDWARE/DEVICE CENTRIC

Security Edge

Security Edge

Network

FABRIC BASED

DATA CENTER

OS 3

Unified Access

SD-WAN

SOFTWARE-CENTRIC

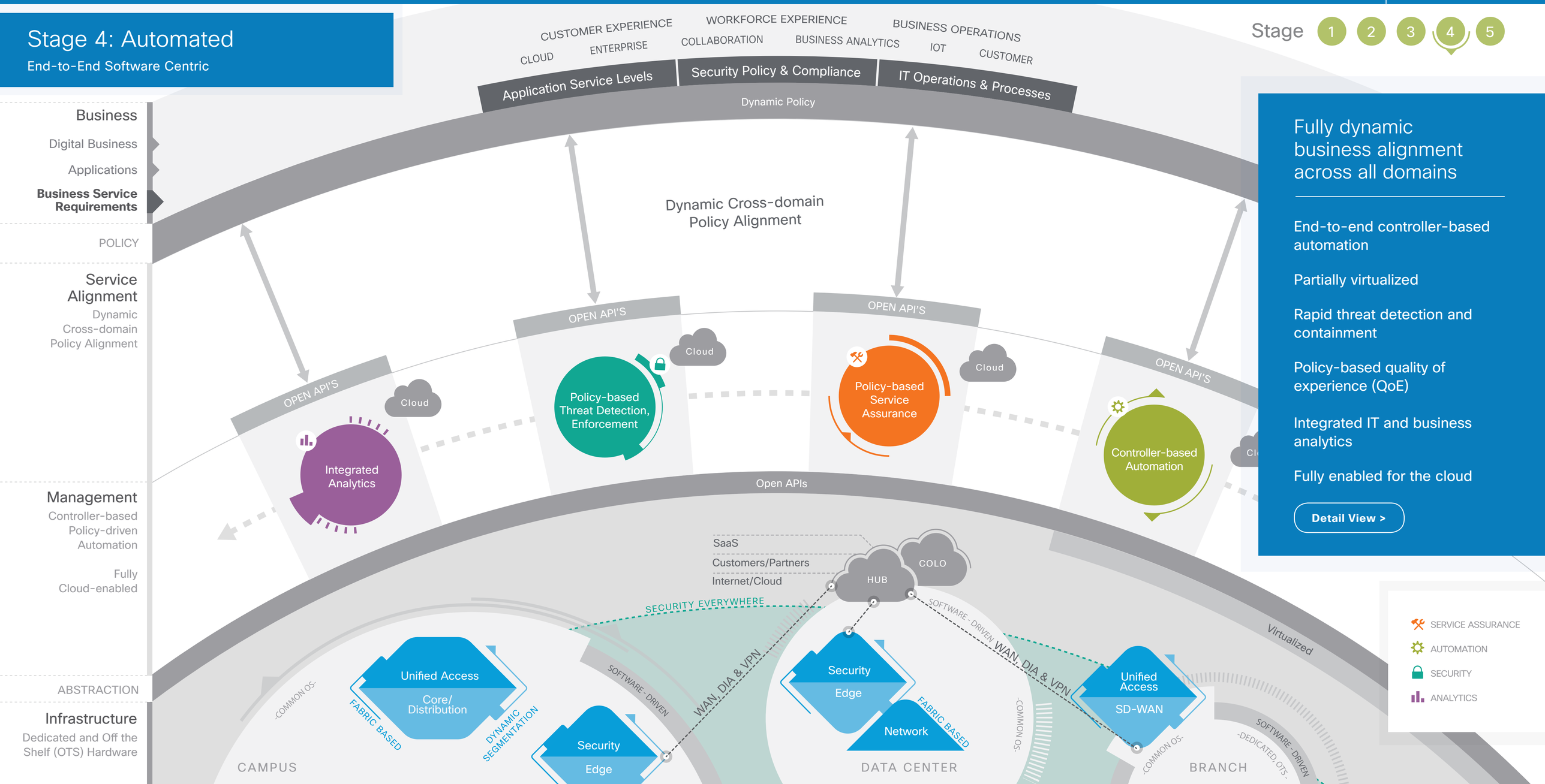
BRANCH

SERVICE ASSURANCE
AUTOMATION
SECURITY
ANALYTICS

Stage 4: Automated

End-to-End Software Centric

Stage 1 2 3 4 5



Fully dynamic business alignment across all domains

- End-to-end controller-based automation
- Partially virtualized
- Rapid threat detection and containment
- Policy-based quality of experience (QoE)
- Integrated IT and business analytics
- Fully enabled for the cloud

Detail View >

Stage 4: Automated

End-to-End Software Centric

DETAIL

Stage 1 2 3 4 5

DETAIL VIEW

CUSTOMER EXPERIENCE
CLOUD
ENTERPRISE
WORKFORCE EXPERIENCE
COLLABORATION
BUSINESS ANALYTICS
BUSINESS OPERATIONS
IOT
CUSTOMER

Application Service Levels | Security Policy & Compliance | IT Operations & Processes

Dynamic Policy

Business
Digital Business
Applications
Business Service Requirements

POLICY

Service Alignment
Dynamic
Cross-domain
Policy Alignment

OPEN API'S
BUSINESS
IT
IoT
Network
Location
Security
Real-time Business / Operations Analytics
Integrated Analytics
Cloud

OPEN API'S
Access
Security Policy Orchestration
Real-time Threat Containment
Policy-based Threat Detection, Enforcement
Cloud

OPEN API'S
E2E QoE
E2E Network Assurance
Dynamic Service Assurance
Policy-based Service Assurance
Cloud

OPEN API'S
NFV Orchestration
Day 0
Day 1
Day 2
Cross-domain Service Correlation and Impact Analysis
Controller-based Automation
Cloud

Open APIs

Management
Controller-based
Policy-driven
Automation

Fully
Cloud-enabled

SaaS
Customers/Partners
Internet/Cloud
HUB
COLO

NETWORK AS A SENSOR/ENFORCER

WAN, DIA & VPN

WAN, DIA & VPN

Virtualized

COMMON OS

Unified Access
Core/ Distribution
FABRIC BASED
DYNAMIC SEGMENTATION

SOFTWARE - DRIVEN

Security
Edge

CAMPUS

Security
Edge
Network
FABRIC BASED

DATA CENTER

SOFTWARE - DRIVEN

Unified Access
SD-WAN

COMMON OS

SOFTWARE - DRIVEN

BRANCH

SERVICE ASSURANCE
AUTOMATION
SECURITY
ANALYTICS

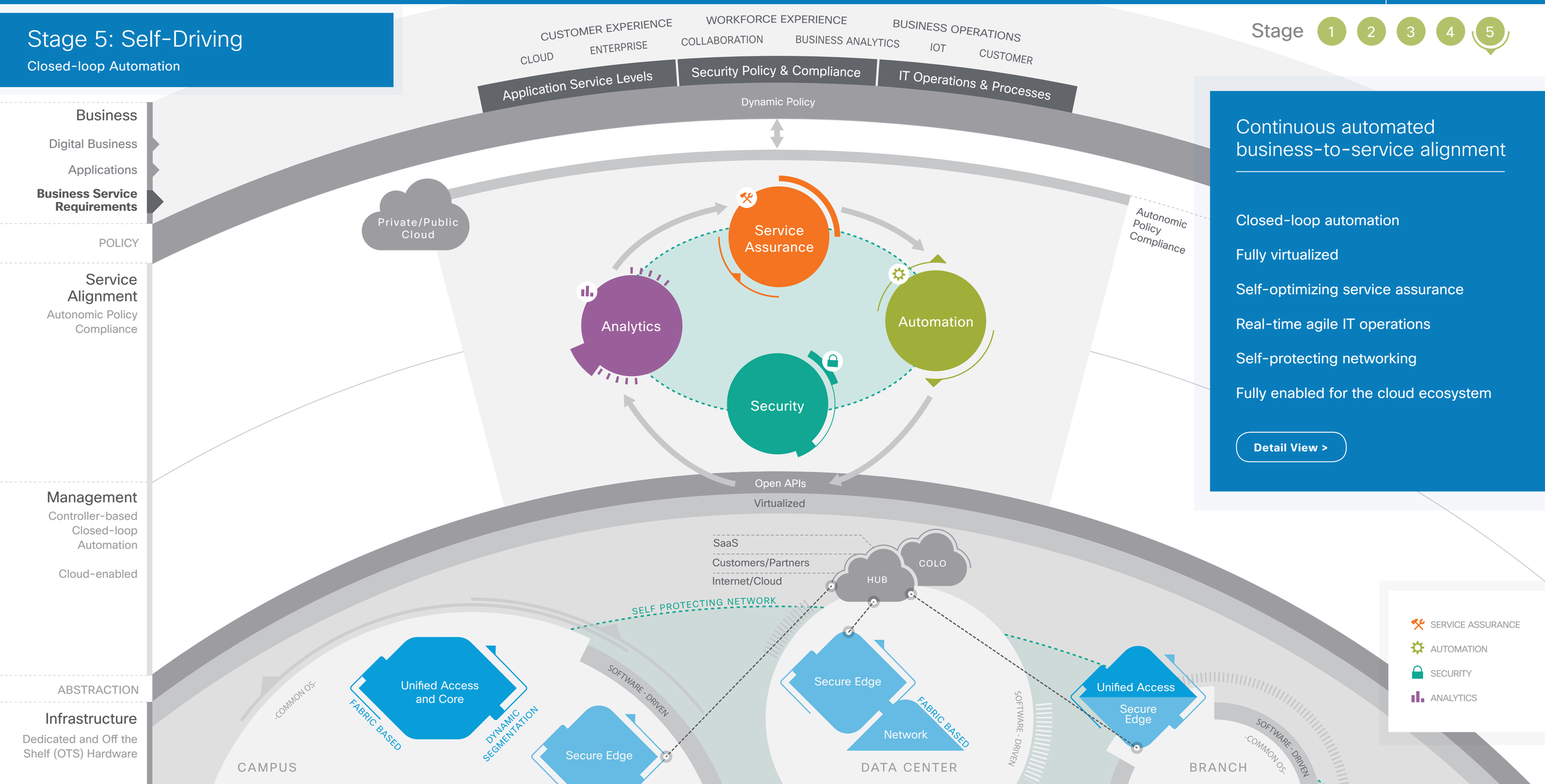
ABSTRACTION

Infrastructure
Dedicated and Off the Shelf (OTS) Hardware

Stage 5: Self-Driving

Closed-loop Automation

Stage 1 2 3 4 5



Continuous automated business-to-service alignment

- Closed-loop automation
- Fully virtualized
- Self-optimizing service assurance
- Real-time agile IT operations
- Self-protecting networking
- Fully enabled for the cloud ecosystem

Detail View >

Stage 5: Self-Driving

Closed-loop Automation

DETAIL

Stage 1 2 3 4 5

DETAIL VIEW

CUSTOMER EXPERIENCE
CLOUD
ENTERPRISE
WORKFORCE EXPERIENCE
COLLABORATION
BUSINESS ANALYTICS
BUSINESS OPERATIONS
IOT
CUSTOMER

Application Service Levels | Security Policy & Compliance | IT Operations & Processes

Dynamic Policy

Business

Digital Business

Applications

Business Service Requirements

POLICY

Service Alignment

Autonomic Policy Compliance across all domains

Management

Controller-based Closed-loop Automation

Cloud-enabled

ABSTRACTION

Infrastructure

Dedicated and Off the Shelf (OTS) Hardware

BUSINESS ECOSYSTEM

Business Intelligence, Threat, Market, Environmental & Other Data

Cloud-based IT Services: Analytics, Security, IoT

Cross-domain Service Orchestration

Closed Loop Policy-based Automation

Service Assurance

Analytics

Automation

Security

IT ECOSYSTEM

Cloud Providers, Telecom Providers, Corporate Systems

Public / Private / Hybrid Cloud Applications

Network Services (Virtual Network Functions)

Real-time Business / Operations Intelligence
Predictive and Self-optimizing Service Assurance
Continuous Security, Regulatory Compliance
Dynamic Business to IT Alignment
Universal Service Visualization

Open APIs

Virtualized

SaaS
Customers/Partners
Internet/Cloud

HUB
COLO

SELF PROTECTING NETWORK

-COMMON OS-
FABRIC BASED
Unified Access and Core
DYNAMIC SEGMENTATION
SOFTWARE-DRIVEN
Secure Edge
CAMPUS

Secure Edge
FABRIC BASED
Network
SOFTWARE-DRIVEN
DATA CENTER

Unified Access
Secure Edge
SOFTWARE-DRIVEN
-COMMON OS-
BRANCH

SERVICE ASSURANCE
AUTOMATION
SECURITY
ANALYTICS

Framework for Digital Network Readiness Model

Digital Network Architecture Readiness Model Categories

Improvements in capabilities are applied to each category across all five stages of the model.

Network Architecture Strategy

Define the approaches to the network's architecture, management strategy, lifecycle management, governance, and compliance at each stage of digital network readiness.

Automation

Adopt network automation capabilities to simplify operations and respond more quickly to new service requirements. By increasing the level of automation in networks, IT can focus more effort on delivering value to the business. Automation allows IT to lower the cost of operations while improving service levels and responding more quickly to new service requirements and deployments.

Network-enabled Service Assurance

Align Quality of Experience (QoE) with explicit and implied business intent. Service assurance applies to all applications (productivity, mobile, cloud, collaboration, IoT, etc.), services (business to business [B2B], business to consumer [B2C], machine to machine [M2M], peer to peer [P2P], rich media, operations, etc.), users, devices, and locations.

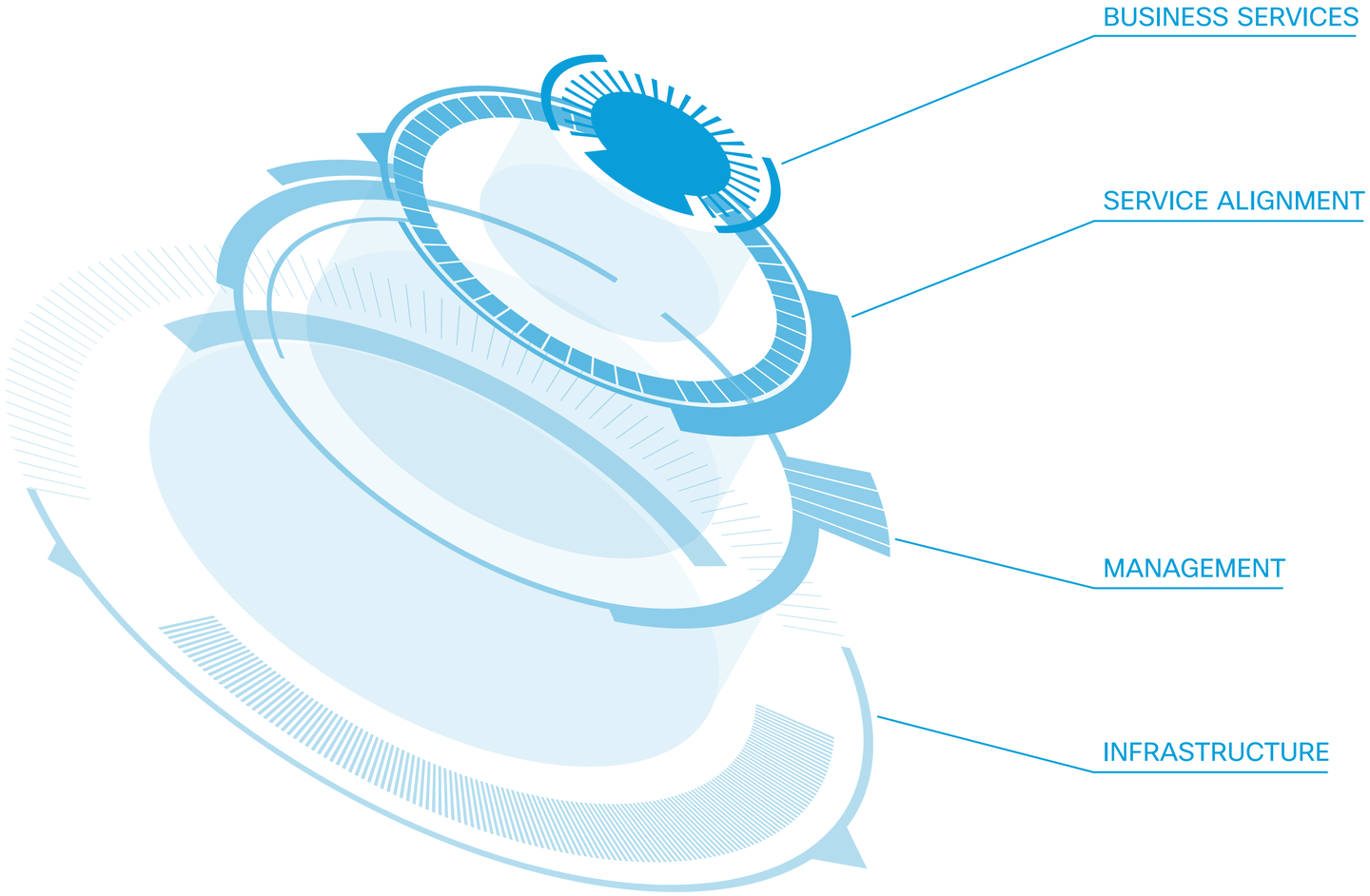
Network-enabled Analytics and Insight

Use the network as a powerful platform for business, IT, security, and OT insight. Improve operations, security and business intelligence by delivering valuable business, IT, OT and security-relevant data and by contextualizing who, where, when, what, how, and why devices, users and applications are using the network.

Network Security

Reduce risk and meet compliance requirements by using the network's capability to reach all users and devices and gain visibility into all traffic to rapidly detect and respond to threats and attacks. Network security provides a robust and indispensable foundation for an overall cybersecurity strategy. With the advent of mobility and cloud, network security needs to extend from the edge of the network through the core and to the cloud.

Readiness Model Stack



The broad set of business functions and associated applications that depend on the network, including functions associated with customer experience, workforce experience, and business operations.

The alignment between what the applications and the business require from the network and the services that the network can deliver. Service alignment is evolving from a best-effort manual alignment to very tight closed-loop integration between business requirements (for example IT operations, application service levels, and security policy and compliance requirements) and the underlying network.

The approach to managing network devices and network services, including the level of adoption of open and extensible controller-based policy-driven management and automation.

The physical and virtualized network and network security components of the enterprise network, including the campus, data center, WAN, and branch networks.

Business Outcomes

Improved results with each stage of the readiness journey

Improved Agility and Faster Innovation

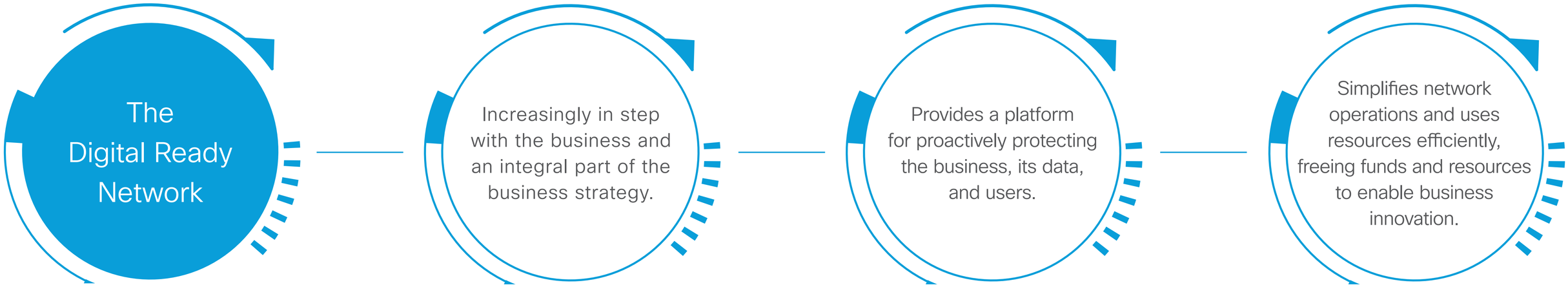
The increased pace of business requires a network that is an accelerator for change, not an obstacle. Fueled by a digital-ready infrastructure that can quickly respond to new business and application requirements and deliver valuable real-time insight.

Lower Security Risk

The increased risk of security attacks and breaches are the biggest drag on digital transformation. Without an infrastructure capable of dealing with emerging threats and attacks as they happen, the business cannot move with digital speed.

Reduced Cost and Complexity

The increased scale of networked applications, devices, and capabilities can lead to fast rising cost and complexity if unchecked.



Technology Attributes

Advance with each step of the readiness journey

Cloud Enabled

Digitization requires increased scalability, agility, and openness, which demands new ways of running the network. Shifting to a cloud-based approach (private, public, or hybrid) to deliver network services such as policy management, virtualized network functions, security, and analytics can increase the agility of a network, while making it more scalable and open to third-party innovations. At the same time, the network architecture needs to be properly designed to optimize secure user access to applications and services hosted in the public, private, or hybrid cloud.

Mobility Enabled

Mobile devices and applications are basic enablers of new ways of working, new ways of engaging customers, new business processes, and completely new business models. Therefore, a digital-ready network must be built with mobility in mind and enable an enhanced mobile experience from anywhere on any device. And of course, a digital-ready network needs to protect the business from the increased risk that comes with opening up networks and data to employee, customer, and guest devices.

IoT Enabled

For many industries, digital transformation is fueled by new IoT initiatives. From remote patient monitoring, to predictive maintenance, to asset tracking and more, IoT makes enhanced and totally new business models possible. To support these new IoT connected devices, applications, and processes, the network needs to adopt new capabilities that can provide the service levels and security they demand.

Business Service Requirements

When an organization creates a new service or process, embarks on a project to improve customer relationships, chooses a new security policy, is faced with a new regulation, needs valuable real-time data, enters the world of IoT, etc., the organization needs to help ensure that the network can conform to these requirements and policies. Traditionally, this assurance was achieved in a hit and miss, manual way, by IT attempting to manually translate the policy requirements into network configurations. This approach inevitably slows down and can even derail these initiatives because so much intent and time can be lost in the translation. To overcome these impediments, a digital-ready network needs to be able to adapt to continuously understand the policies and needs of the business and make the necessary changes on an ongoing basis. Business service categories that can be policy-driven include applications service levels, policy and compliance and IT operations.

Application Service Levels

The service levels required by an application or service need to be communicated either through policies or directly by the applications, so that the requirements of users and processes are consistently met. Digital organizations need a network that can deliver service levels aligned with explicit and implied business intent. Service assurance needs to be applied to all applications (productivity, mobile, cloud, collaboration, IoT, etc.) and services (B2B, B2C, M2M, P2P, virtualized, rich media, IoT, personal, etc.) across users, devices, and locations.

Policy and Compliance

Policy applies to the organization's security decisions about employee, partner, and visitor roles and responsibilities and about application, data, and network access and use. Policies need to covers all network systems and data in the organization as well as regulations defined by third-party governmental and trade organizations. Traditionally, policies have been applied as fragmented network security mechanisms through manually managed access policies and enforcement mechanisms. In an increasingly connected and mobile world with growing risk, digital organizations need ways to apply and enforce policies and achieve regulatory compliance in a real-time, dynamic and automated way.

IT Operations

For IT to keep up with the rate of change and with the new demands of the digital network, it needs to make its operations more agile and responsive. IT needs to replace time-consuming manual and error-prone processes with ones that are simpler and more automated. IT needs to create operating models and technology capabilities that allow much greater integration between business requirements and network services. Such capabilities include self-service service catalogs; day-zero, day-one, and day-two operations automation; and IT workflows.

Resources

Use the following resources for more information and to help guide you on your journey to digital network readiness.

Learn more about the Cisco Digital Network Architecture

Get an insider's perspective on how to use the DNA Readiness Model

Getting to a Digital Network Architecture - Blog

View Infographic from IDC Research

Cisco Digital Network Architecture Strategy and Analysis Services

Explore the Cisco DNA Technical Whitepaper

Review the DNA Checklist

DNA Checklist

Questions to Ask Your Vendor

Can you support our digital business ambitions?

- Do you have a vision and roadmap for networking that will support digital transformation?
- Do you help customers achieve a smooth network evolution to a software-delivered architecture?
- Can your network architecture deliver lower cost and complexity, reduced risk and enable faster innovation?
- Can your network deliver valuable IT and business analytics?
- Can your partners and services ecosystem help me evolve to a digital-ready network?
- Can you help with developing our network team's skill set to support a programmable network?
- Do you have a proven record as a trusted partner for the long term, to support IT through the journey to digital?
- Do you have a broadly adopted developers program?

How can your network technologies support our digital requirements?

Architecture

- Is your network architecture end-to-end, meaning from clients to cloud (access, core, WAN, branch office, data center, cloud)?
- Does your architecture enable end-to-end automation?
- Is your architecture open and standards-based?
- Is your architecture designed to support a controller-based programmable network?
- Is your architecture built to support virtualization?
- How does your architecture enable mobile, cloud, Big Data and IoT?

Automation

- Can your management system create and configure networkwide policy and services through standard APIs and traditional interfaces?
- Can your architecture automate policies across day zero, day one and day 2 operations?

Security

- Does your network provide security and protection for the edge and the core?
- Can your network act as a networkwide security sensor and intelligence dashboard?
- Can your network enforce contextual security policy and respond to contain threats?

Analytics

- Can your network provide clear visualization of activity, networkwide?
- Can your network identify threats and anomalies in real-time?
- Can your network support distributed and cloud-based IoT analytics?
- Can your network provide valuable real-time insights into customer and employee behaviors?

Service Assurance

- Can your architecture apply application quality of service (QoS) network wide?
- Can your architecture automate QoS policy across the network?