



INSIGHTS | WHITE PAPER

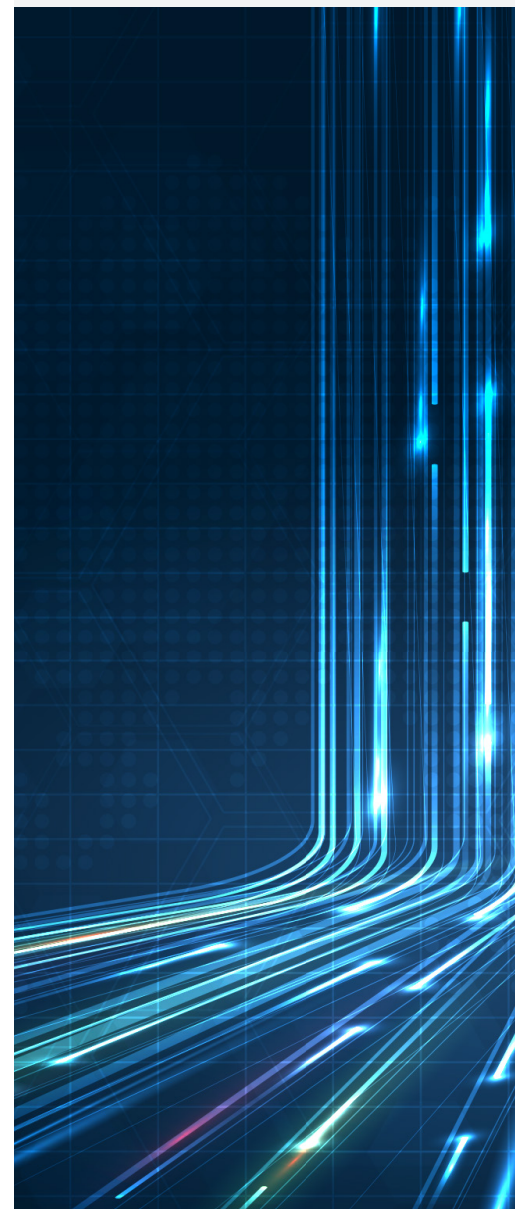
Cisco ACI: A Catalyst for Digital Transformation

Digital transformation is the strategic integration of technology to reimagine or create new business processes. Fueled by technology trends like artificial intelligence (AI), cloud computing, and Internet of Things (IoT), it positions organizations to continuously adapt to evolving user behaviors. This transformation unlocks a multitude of benefits, including:

- **Streamlined IT Resource Management:** Improve visibility, control, and management capabilities over IT resources
- **Enhanced Scalability:** Build flexible and scalable infrastructure to support business growth and expansion
- **Increased Productivity:** Simplify processes and workflows for improved operational efficiency and performance
- **Fortified Security:** Safeguard critical assets, including data and systems, from evolving threats
- **Elevated Customer Experience:** Deliver exceptional experiences through digital channels that keep customers engaged
- **Cost Optimization:** Reduce costs while allocating resources to maximize business value

By prioritizing digital transformation, organizations gain a competitive edge:

- **Thriving Distributed Workforce:** Maintain seamless connectivity and enhance collaboration regardless of location
- **Adaptability and Agility:** Respond quickly to changing market demands and emerging opportunities
- **Resource Flexibility:** Deploy resources swiftly and strategically to meet evolving business needs
- **Data-Driven Decision Making:** Leverage data insights for faster, more informed decisions
- **Accelerate Innovation:** Prioritize ongoing customer focus and align with changing market demands while fostering a culture of innovation
- **Drive Revenue Growth:** Identify new revenue streams and opportunities through digital products and services



The Roadblocks To Digital Transformation

The post-pandemic era has ushered in an unprecedented acceleration of innovation within the digital landscape. This rapid growth has led to a significant increase in applications and cloud adoption, underscoring the importance of robust and adaptable infrastructure. Traditional, siloed networks struggle to keep pace with these evolving demands. Manual configuration tasks are prone to errors, time-consuming, and inefficient, which impedes agility and drives up operational costs. Moreover, the manual provisioning of processes introduce delays in application deployment, hindering time-to-market initiatives. Inconsistent security policies across disparate network segments create vulnerabilities and pose compliance challenges. Additionally, limited visibility into network traffic and application performance complicates proactive problem-solving efforts. These challenges are further exacerbated as organizations expand to complex hybrid and multicloud environments.

The Digital Imperative: Rethinking Networks for Agility and Security

The global pandemic highlighted the critical role that technology plays in organizational survival. This has led to growing recognition that digital transformation requires a holistic approach with robust networking at its core. In today's hybrid and multicloud world, networks are no longer peripheral; they are the foundation upon which modern applications are built. These networks connect microservices, functions, and data into mission-critical business services that enable cutting-edge experiences like 8K ultra-high definition video streaming, immersive VR/AR applications, high-frequency stock trading, gaming, self-driving vehicles, AI/ML-driven automation, IoT, and 5G-powered use cases. To support these advanced applications, industry leaders are prioritizing network agility and security.

Software-defined networking (SDN) frameworks offer a strategic solution. SDN revolutionizes network management by decoupling the control plane (network intelligence) from the data plane (packet forwarding hardware). Traditionally, these functions were inseparable within network devices. SDN centralizes control on a software controller, enabling programmatic

configuration and automation. This empowers enterprises to achieve network agility across data centers and cloud environments, ultimately propelling digital transformation and business success.

Cisco ACI: The Catalyst for Secure and Agile Digital Transformation

This white paper explores how Cisco Application Centric Infrastructure (ACI) acts as a powerful catalyst for digital transformation, enabling organizations to work smarter, faster, and more efficiently. Cisco ACI, a leading secure, open, and comprehensive SDN solution, bridges the gap between traditional, siloed networks and the agility, security, and efficiency required for success in the modern digital age. The platform simplifies data center network management and enhances security by providing a centralized application-centric approach. It delivers a network policy-based framework, extending to WAN, campus networks, on-premises data centers, and cloud environments, enabling companies to dynamically provision networks, provide pervasive security, and automate network infrastructure services. Automation and policy-based control drive agile IT operations, streamline application deployment, and accelerate digital transformation. With Cisco ACI, organizations can:

- **Optimize the Network:** Simplify and automate operations across multisite, multicloud data center networks with centralized common policy.
- **Protect the Business:** Enhance business continuity and accelerate disaster recovery with pervasive security, zero-trust principles, and automated policy enforcement.
- **Accelerate Multicloud:** Scale with seamless connectivity to any workload anywhere, on-premises to cloud.

Positioning the Network as a Strategic Asset: The Benefits of Cisco ACI

As data volumes surge and network speed and agility demands intensify, networking professionals are transforming how they broker, connect, build, and govern their networks across expansive cloud ecosystems, in addition to data centers. As an enterprise-class SDN

solution, Cisco ACI provides complete control over the entire network, from data center to cloud. The platform simplifies IT infrastructure and operations by automating the network for improved reliability, scalability, and performance. It also offers comprehensive security to enhance business continuity, and accelerates the adoption of cloud or multicloud environments, enabling IT teams to quickly respond to evolving network demands.

With a flexible yet highly available network infrastructure, Cisco ACI allows agile application deployment within a site as well as across multiple sites, global data centers, and cloud environments. Organizations can manage complexity, maximize business benefits, and deploy workloads in any location, small and large, on-premises and remote locations, in private and public clouds, satellite data centers, and 5G-enabled telecom edges. Cisco ACI transforms the network into the cornerstone for digital transformation, delivering a comprehensive range of benefits.

- **Simplified Network Management:** Cisco consolidates multiple disparate networks into a single logical network with a centralized view. This single point of management provides control over the entire data center network, including physical and virtual infrastructure, applications, and services. The solution automates common network management tasks, including provisioning new devices, configuring port settings, and applying security policies. A central point of control eliminates the need for error prone manual configuration, while the reduced number of devices to manage and monitor facilitates easier troubleshooting.

Additionally, Cisco ACI optimizes network utilization by automatically distributing traffic across multiple paths, ensuring that resources are used efficiently. This holistic approach streamlines operations, reduces complexity, and frees up valuable IT resources to focus on strategic initiatives.

- **Consistent Application Behavior:** Organizations can ensure consistent application performance across the entire network by defining and enforcing common policies through an automation-driven approach. This guarantees that applications perform predictably and reliably, whether deployed on-premises, in a private

cloud, or a public cloud environment. Consistent performance allows businesses to smoothly integrate and manage new applications, accelerating digital transformation initiatives

- **Increased Agility and Scalability:** With Cisco ACI, enterprises can rapidly evolve with quick and easy provisioning of new applications and services through automated workflows that eliminate manual configuration steps. The solution scales linearly enabling it to support a large number of devices and users without compromising performance, making it ideal for enterprise-wide deployments. This scalable architecture ensures that the network can grow to meet changing and expanding business needs.
- **Enhanced Security Posture:** The platform enables companies to establish a consistent security posture at scale across multicloud environments. A policy-based approach allows teams to define and enforce granular security controls across the entire network. Cisco ACI goes beyond basic security by analyzing data center components to identify and mitigate potential security threats proactively.

Leveraging zero-trust principles and advanced features like microsegmentation, the solution fortifies the network against evolving threats. Built-in security features include role-based access control, limiting user access to authorized resources, and intrusion detection and prevention to identify and block malicious traffic.

- **Seamless Multicloud Integration:** Cisco ACI empowers organizations to embrace a multicloud strategy with confidence. The platform provides seamless connectivity to any workload anywhere from on-premises to cloud-based infrastructure. Security teams can extend their policies and security controls to public cloud environments, ensuring a consistent user experience across all cloud deployments.

A Policy-Based Approach

Traditional network configuration relies on IT professionals to manually configure network devices based on technical specifications. This complex, time-consuming process is prone to errors. Cisco



ACI revolutionizes this approach with policy-driven automation for network configuration, where application requirements define network infrastructure. By capturing high-level business goals and translating them into the automated network constructs necessary to dynamically provision the network, security, and infrastructure services, Cisco ACI simplifies network management and frees up IT resources to focus on strategic initiatives. Here's how policy-driven automation streamlines the process and ensures consistent results:

1. **Capture Business and User Intent:** Cisco ACI allows IT teams and business stakeholders to define high-level business goals and user requirements. This could include ensuring secure and high-performance access to a specific application, such as a CRM marketing application.
2. **Translate Intent into Policy:** Cisco ACI then translates this business intent into a comprehensive network policy. This policy dictates the specific security measures, performance requirements, network configuration, and resource allocation necessary to accomplish the established goals. For example, the policy might specify firewall rules, bandwidth allocation, and quality of service settings for the CRM application.
3. **Dynamic Provisioning:** The network policy is then used to automatically provision and configure the required network infrastructure components (switches, firewalls, VLANs, etc.) and security services. This eliminates the need for manual configuration and streamlines the deployment process.

Benefits for Digital Transformation

- **Faster Application Deployment:** Automation speeds up network configuration and deployment, accelerating the application development lifecycle and enabling faster time-to-market.
- **Simplified Management:** Policy-driven automation and centralized management simplify network complexity by providing a streamlined approach to managing network policies. This is especially beneficial when managing workloads across diverse cloud environments. IT teams are able to shift their focus to innovation and advancing organizational goals.

- **Flexibility:** Implementing the entire network as code makes it easy to update policies and configurations to align with evolving business needs. This ensures the network can quickly adapt to keep pace with changing application requirements and better support digital transformation initiatives.

How Cisco ACI Works

Cisco ACI is an application-centric infrastructure that enables organizations to design and build their data center network around specific applications requirements. This is facilitated by the ACI Fabric Operating System (OS), which runs on all systems within the ACI network. This shared OS allows the various network switches to seamlessly translate policies into infrastructure elements. Cisco ACI operates on the fundamental principle of decoupling the data forwarding plane (responsible for moving packets) from the control plane (responsible for network configuration and policy enforcement). This separation unlocks enhanced agility and scalability. Network administrators gain centralized control through a policy module, enabling them to automate and simplify network configuration, deployment, and management. The core building blocks of Cisco ACI include the Cisco Nexus 9000 series switches, handling the data forwarding, and the Cisco Application Policy Infrastructure Controller (APIC), managing the control plane.

- **Cisco APIC:** As the main architectural component of the Cisco ACI solution, the centralized, clustered infrastructure controller serves as the unified point for automation and management within the scalable, multitenant ACI fabric. Responsible for policy enforcement and health monitoring across physical, virtual, and cloud infrastructures, the APIC appliance optimizes performance and unifies operations across all environments. The controller framework enables broad ecosystem and industry interoperability between the Cisco ACI environment and management, orchestration, virtualization tools, and L4-L7 services from a wide range of vendors. An open, standards-based application programming interface (API) exposes the ACI policy module to external applications and orchestration tools. While automation is a core strength, the APIC also provides an intuitive web-based user interface for manual configuration and monitoring tasks when needed.

- Cisco Nexus 9000 Series spine and leaf switches:**
 The Cisco Nexus 9000 Series switches form the high-performance foundation of Cisco ACI, delivering low-latency switching to meet the needs of modern data center and cloud-based applications. Supporting speeds of up to 400G/800G, these switches are built to handle demanding workloads efficiently. The Nexus 9000 Series utilize a “fat-tree” network architecture, ensuring high-bandwidth connectivity between leaf and spine switches. Each leaf switch connects directly to all spine switches, providing redundancy and efficient data paths. All other devices in the network connect to the leaf switches for streamlined communications. Modular and fixed-configuration switch options offer compatibility with existing networks through NX-OS mode, while also enabling full access to Cisco ACI features when configured in ACI mode.
- Leaf switches serve as Top-of-Rack (ToR) switches, providing connectivity between servers and external networks, acting as the access layer for the fabric. They are fully programmable, allowing for customization to meet specific application needs. Leaf switches support Layer 2 and Layer 3 protocols, along with quality of service (QoS), security features, and virtualization capabilities.

- Spine switches function as aggregate Layer 3 points, delivering high-bandwidth connectivity between leaf switches. They ensure efficient data flow throughout the network. Like leaf switches, spine switches are fully programmable and support all Layer 2 and Layer 3 protocols.

Within the Cisco ACI fabric, all endpoints, including APICs themselves, connect to the network via leaf switches. These leaf switches then interconnect with spine switches in the backend, forming a high-performance network foundation. This modular architecture provides versatile deployment options: on-premises for policy-driven management of existing data centers, cloud-based (including public, private, and hybrid) for consistent policy enforcement across the entire IT infrastructure, and SD-WAN edge for managing and securing branch office connectivity with the same policy-driven approach. By leveraging these deployment models, organizations can achieve consistent policy-based network management across their entire corporate WAN, simplifying operations and enhancing security. With Cisco ACI, IT professionals can build a data center network fabric with hundreds of switches automatically, focusing on communication through a single point of network configuration. The solution is designed to optimize and automate network infrastructure deployment, which minimizes downtime and allows for faster innovation.

Figure 1. Cisco APIC is the main architectural component of Cisco ACI

Source: Cisco



Figure 2. ACI Fabric Overview

Source: Cisco



How Cisco ACI Can Help You Realize Cloud's True Power

The true power of the cloud hinges on the underlying network infrastructure it leverages. Cisco ACI occupies a unique position in the cloud ecosystem because it offers teams building cloud infrastructure comprehensive automation through a software-defined approach to physical network infrastructure. As a multicloud solution, ACI puts organizations securely in control of their public and private cloud resources using single-pane-of-glass management. IT teams can easily connect and manage infrastructure anywhere, from core to network edge. This allows Cisco ACI to serve as a unifying platform that bridges the gap between on-premises data centers and the growing adoption of public and private cloud resources.

By providing a consistent, automated, and policy-driven approach to network management across hybrid and multicloud environments, organizations can maximize the benefits of cloud computing while maintaining the necessary visibility, control, and security over their entire infrastructure. Expected outcomes include:

- **Increased value of IT team:**
 - Data center infrastructure and operations teams evolve into service builders and brokers, capable of providing the optimal blend of performance, security, cost, and location tailored to the needs of line-of-business holders.
 - Services can be delivered on-premises within the core data center, at remote sites, or in the public cloud, ensuring flexibility and alignment with business requirements.
 - Developers and application architects benefit from a consistent development and runtime environment, whether operating on-premises or in the cloud, facilitating seamless workflow integration.
- **Accelerate change while protecting the business:**
 - By establishing robust connections, stringent security measures, and efficient processes, Cisco ACI lays the groundwork for swift changes and agile delivery of new services.
- Companies can leverage a reliable infrastructure foundation for rapid adaptation to evolving business needs while safeguarding against potential threats and risks.
- **Multicloud continuity:**
 - Cisco ACI enables seamless management of infrastructure resources at any location and at any scale to support new initiatives in IoT and mobility.
 - The solution removes the technology barrier so that application deployment is driven by business needs and cost considerations, not by AI/ML limitations.

Talk to WEI today

As digital transformation redefines the business landscape, corporate networks and IT architectures must evolve to support change effectively and securely. This requires a modern and adaptable network foundation that seamlessly integrates with cloud environments and keeps pace with evolving business demands - something WEI is very familiar with.

Cisco ACI serves as a catalyst in this transformation. It enables policy-driven automation that accelerates infrastructure deployment and governance, simplifies management to easily move workloads across multifabric and multicloud frameworks, and proactively secures against risk arising from anywhere.

Sources:

1. Cisco Application Centric Infrastructure (Cisco ACI) Solution Overview: <https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-741487.html>
2. Cisco - What is Digital Transformation?: https://www.cisco.com/c/en_uk/solutions/digital-transformation/what-is-digital-transformation.html#~digital-transformation-faqs
3. Cisco Application Centric Infrastructure (ACI) - ebook: <https://ebooks.cisco.com/story/cisco-application-centric-infrastructure-aci/>
4. Cisco Application Centric Infrastructure (ACI) - Move from reactive to proactive multicloud networking: <https://www.cisco.com/site/us/en/products/networking/cloud-networking/application-centric-infrastructure/index.html>

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.