Cisco ACI and Apprenda: Today's Most Secure and Advanced Enterprise Hybrid Platform-as-a-Service Solution

BENEFITS

- **Faster time to market:** Our best-in-class self-service console and policy engine increases developer productivity, automates networking configurations, and reduces process delays.
- **Ease of security and compliance management:** Our solution allows you easily manage security and compliance at various layers, including data and application layers.
- **Leverage existing investments:** Our platform allows you to enable existing Microsoft .NET and Java applications for the cloud and supports most commercially available OS, virtual machine, database, and middleware software.
- **Optimized resource utilization:** Our solution enables dynamic isolation of distributed applications and isolation of multiple applications on the same infrastructure.
- **Ease of operations and real-time visibility:** Our user-friendly GUI provides easy management and real-time view of your applications, resources, and network.

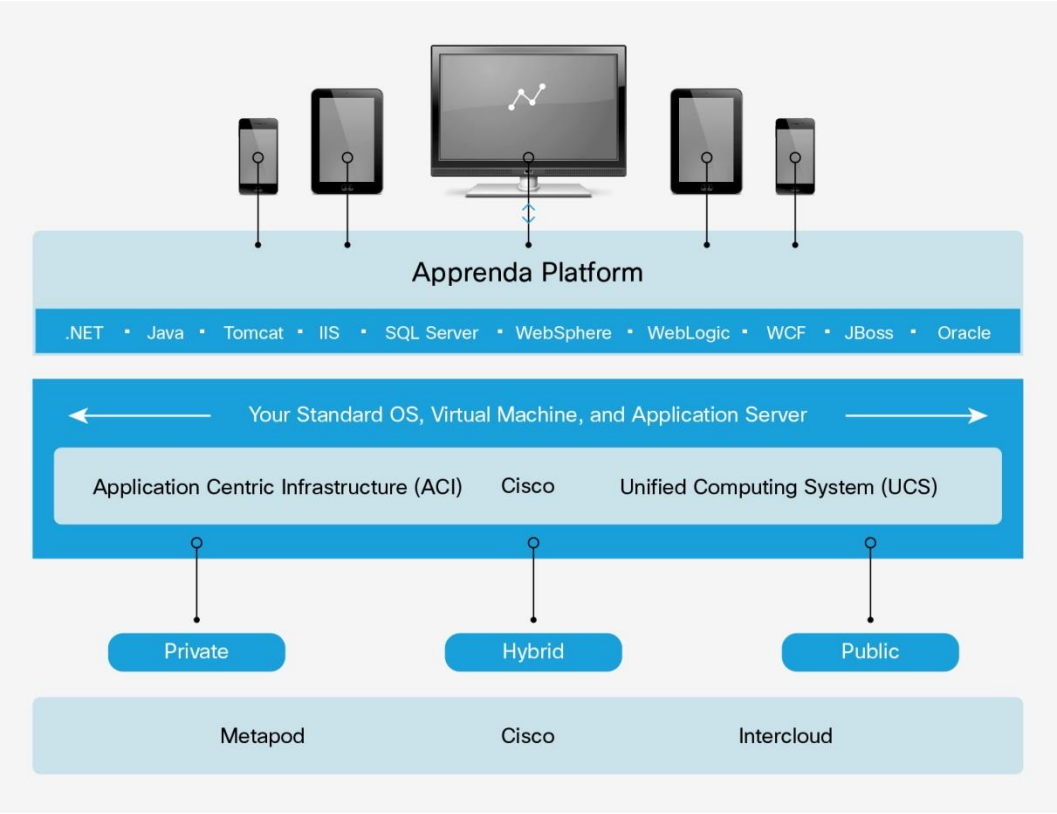
Easily develop, deploy, and manage your application portfolio while dynamically securing the entire data path according to DevOps policies. With the Apprenda and Cisco® Application Centric Infrastructure (Cisco ACI™) solution, you can efficiently enable your existing and new applications for the cloud without sacrificing security or compliance.

Overview

Cisco ACI provides an application-level policy model that abstracts the infrastructure details all the way up to application requirements so that the underlying infrastructure can be automatically configured based on application requirements. Apprenda is an enterprise platform-as-a-service (PaaS) software layer that can be extended to any hybrid cloud infrastructure. Together, Cisco ACI and Apprenda create a policy-based PaaS solution (Figure 1) to provide today's most secure and advanced enterprise-class application development platform for hybrid cloud environments. Using our solution, organizations can achieve much faster application development and cloud migration times without any loss of security or compliance.

Apprenda integrates with Cisco ACI open policy interfaces to free developers and IT from the manual constraints of network configuration and to achieve complete isolation of application tiers and data within shared infrastructure. Moreover, Apprenda's enterprise PaaS offering provides an optimal operating model for Cisco ACI that requires no changes in organizational structure, processes, or skills and allows organizations achieve the full potential of policy-based management for cloud networking. Together, Cisco ACI and Apprenda provide an outstanding solution for achieving both compliance and rapid development through self-service IT resources.

Figure 1. Apprenda PaaS and Cisco ACI



Trends and Challenges

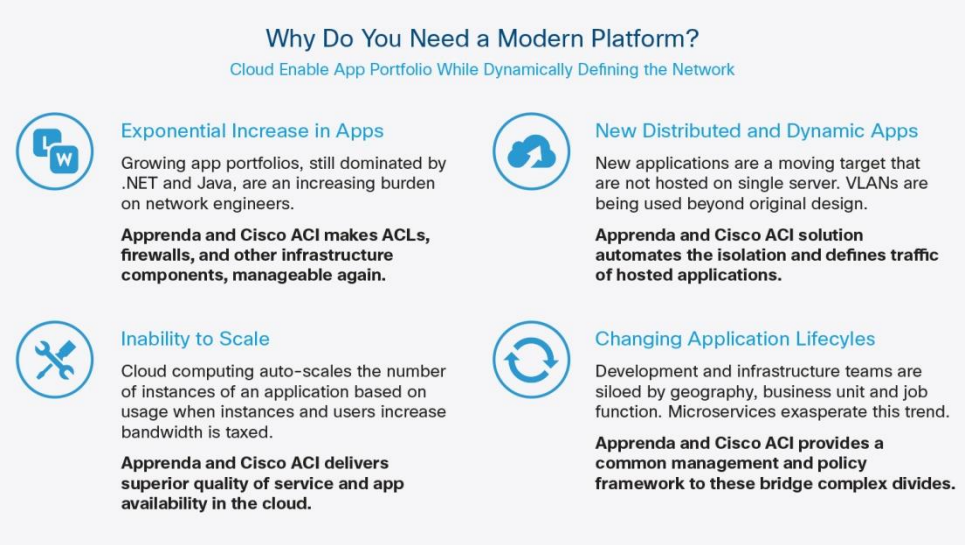
As software becomes the competitive currency of the enterprise, the data center is evolving into a strategic asset. Central IT operations are moving to distributed cloud applications and dynamically provisioned infrastructure to meet demands for more efficient and faster development cycles. However, these changes create challenges for static networks that were never designed for cloud platforms (Figure 2):

- Exponential increase in application portfolio size: The growing portfolio of applications is an increasing burden on IT and network engineers. For example, access control list (ACL) and firewall rules are difficult to maintain as the application portfolio grows. As the number of applications increases, IT spends more time on maintenance tasks rather than innovation. According to Gartner, application development and maintenance consumes 34 percent of IT budgets (Source: http://www.gartner.com/newsroom/id/2711017).
- Distributed and dynamic applications: Although applications may have been hosted in single virtual machines in the past, new applications are distributed and dynamic. VLANs are currently being used beyond their original design: they are used not only for segmentation, but for security and policy compliance.

The result is a tangled set of operations to restrict failure and broadcast domains that is not easily managed between clusters. Management of network segmentation needs to be automated and should be designed within the application itself.

- Changing application lifecycles: Development and infrastructure teams today are isolated by geography, business unit, and job function. Microservices exacerbate this trend. Applications are hosted on very different infrastructures during different stages of development. Organizations need a common management and policy framework to bridge these complex divisions.
- Inability to scale: Cloud computing quickly expands and decreases the number of instances of an application based on the usage demands at a given moment. An increase in instances and users accessing an application can tax bandwidth. This need to scale creates problems for traditionally static networks, which, at the least, need to be overprovisioned. The result is diminished quality of service and application availability—counteracting the benefits the cloud.

Figure 2. Challenges



Main Features

- Policy engine to achieve automated application, data, and network isolation and scaling
- Self-service console for developers to develop, deploy, and management applications
- Support for existing and new applications, whether written in Java or .NET
- Comprehensive support for most of enterprise OS, virtual machine, database, middleware, and public cloud applications
- Full-featured administration console for defining deployment policies, managing resources, and viewing real-time use trends

> “Application development and maintenance eats up 34% of IT budgets.”
> **— Gartner:** http://www.gartner.com/newsroom/id/2711017

How the Solution Works

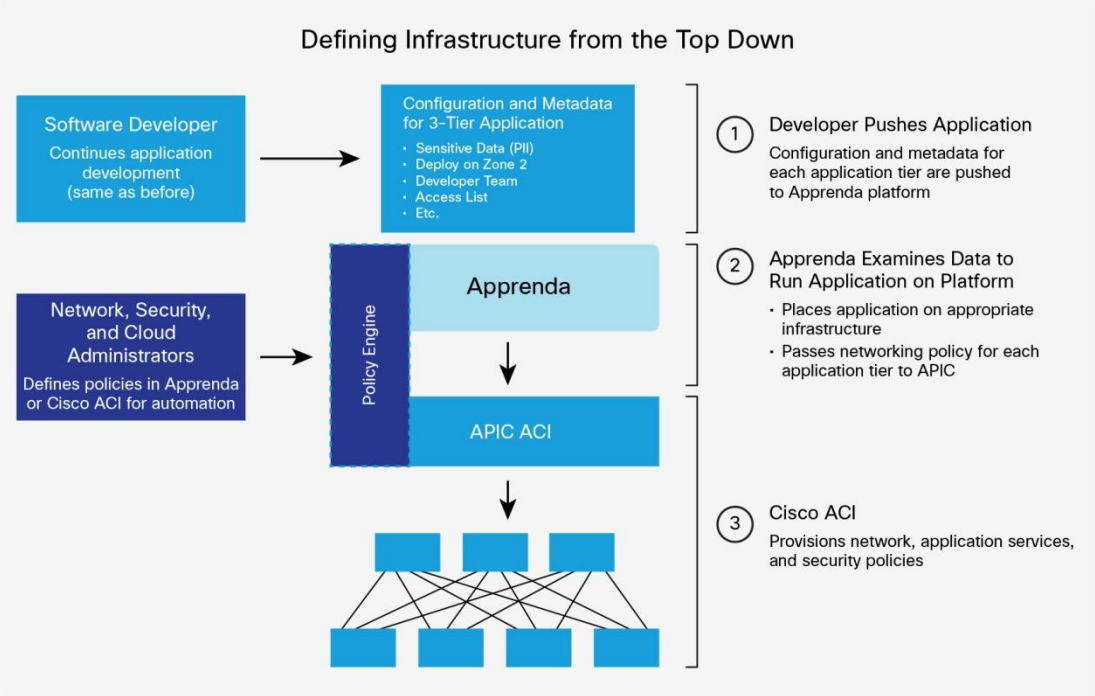
Cisco ACI provides an application-level policy model that abstracts the infrastructure details all the way up to application requirements so that the underlying infrastructure can be automatically configured based on application requirements. Apprenda is an enterprise PaaS software layer that can be extended to any hybrid cloud infrastructure. The Apprenda cloud enables existing and new applications so that developers can focus on their core competency—programming—instead of infrastructure or policy. The abstraction of network policies by Cisco ACI enables the Apprenda platform to incorporate these rules automatically into its own policy model. Conversely, the abstraction of the application and metadata at deployment of the application gives Cisco ACI a completely natural way to reach the developers without imposing new DevOps requirements on them. Together, Apprenda and Cisco ACI provide an outstanding tool for achieving both compliance and rapid development through self-service IT resources.

Using Cisco ACI and Apprenda, administrators can create policies for groups of endpoints requiring similar treatment in the infrastructure for each tier or component of the application. The Apprenda platform is set up as a self-service resource portal for developers in lines-of-business, partner, and system integrations. The Cisco ACI policies are embedded in the Apprenda platform

Figure 3 shows how Apprenda and Cisco ACI work together. Developers are responsible for changing or hosting their applications on Apprenda. They are not aware of the underling network or infrastructure architecture, which is abstracted by the Apprenda platform—the platform takes care of those details. When the developer is ready to host the application on the platform, the developer defines information about the application, such as whether it includes personally identifiable information (PII). This definition creates policy information about the application. The Apprenda platform passes that policy information from the application configuration file and metadata to Cisco ACI.

Cisco ACI then stores that policy in the Cisco Application Policy Infrastructure Controller (APIC), creating the rule book that determines which applications (or tiers or arbitrary groups of endpoints) can talk to each other. The Cisco APIC pushes the policy down to the individual Cisco Nexus® 9000 Series Switches in the fabric, which implement the required networking rules for the application architecture.

Figure 3. Policy-Based Application Isolation by Cisco ACI and Apprenda



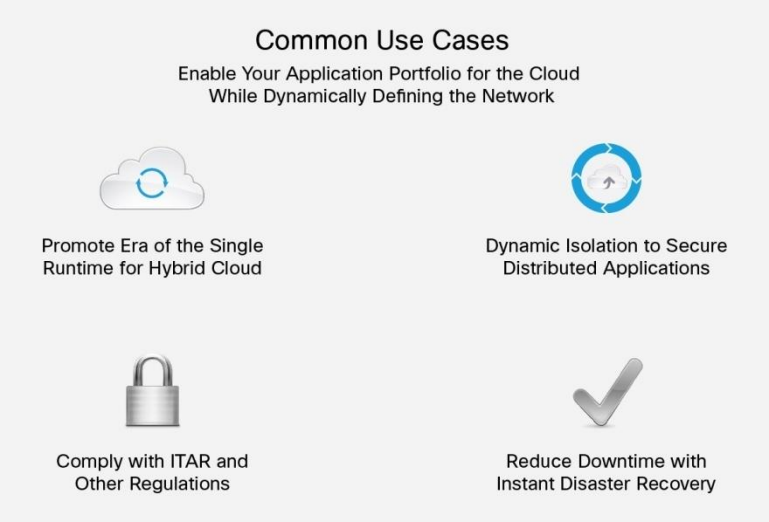
With Cisco ACI, an administrator simply configures the application policy in the APIC. The administrator does not configure the Cisco Nexus 9000 Series Switches individually, significantly reducing the opportunity for human error and the time required to make changes and add applications to the data center.

Additionally, the solution provides high availability for the application and the underlying infrastructure. If a problem occurs in the APIC, the individual policy information is still contained in the networking switches. If the APIC cluster goes down, traffic will be forwarded as usual by the switches. If part of the infrastructure goes down, Apprenda brings up more instances of the application on different infrastructure, which is still governed by Cisco ACI.

Use Cases

Apprenda and Cisco ACI address a vast number of use cases. The top-four use cases are discussed here and summarized in Figure 4.

Figure 4. Top-Four Use Cases

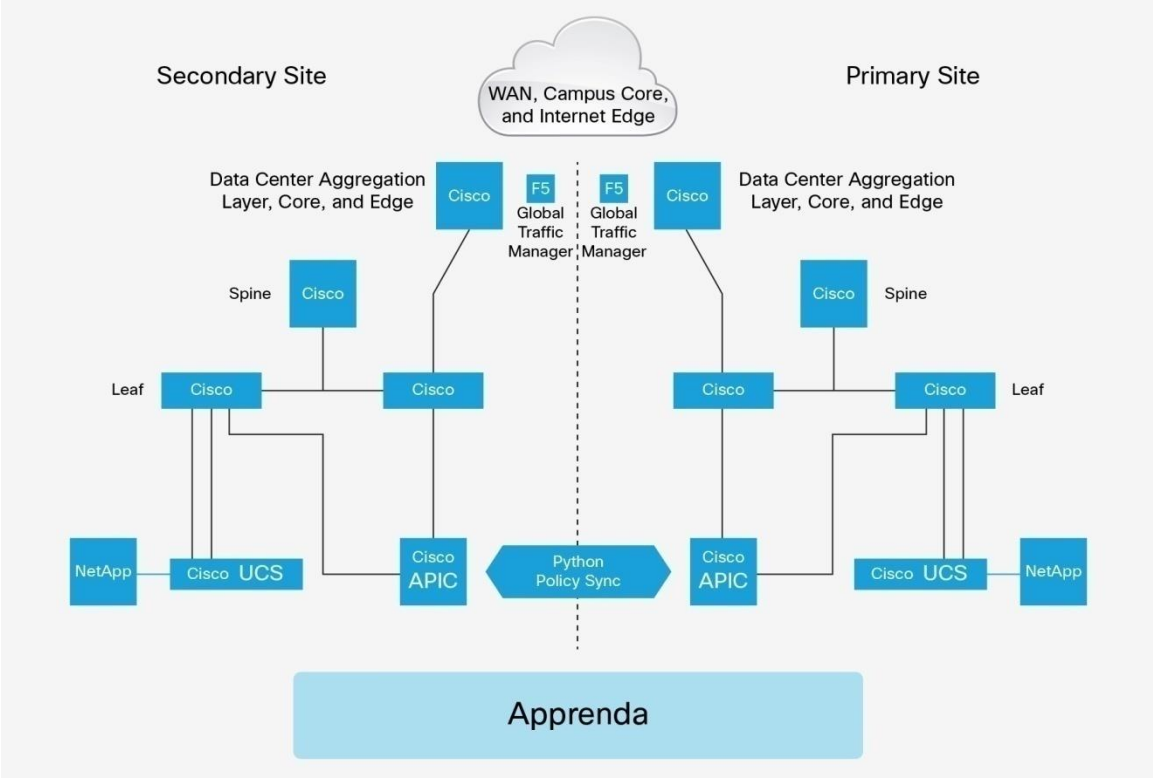


- **Dynamic application isolation for security:** In cloud and microservices architectures, applications and their instances are distributed among many different servers or virtual machines, which makes isolation challenging. In addition, the network in the cloud needs to respond to demand by scaling dynamically. These challenges exist at every tier and component of the application. For example, a public-facing website of an organization needs different levels of security and access than other applications or database tiers, which typically are secured behind a firewall. Apprenda and Cisco ACI can automate the network communication permitted among applications in these modern environments.
- **Hybrid clouds:** Organizations want to host different applications on different infrastructures. Some applications may be hosted in the public cloud while others are not. Some applications may be hosted on traditional infrastructure while others use the power of Cisco ACI. The organization may also have policies that govern whether or not an application is hosted in a bare-metal, private infrastructure cloud, or in a traditional virtualized environment. Apprenda can automate the deployment of these applications.

  Apprenda application deployment policies enable finely detailed mapping of applications and application components to infrastructure based on flexible and configurable properties

- **Governance for International Traffic in Arms Regulations (ITAR) and other compliance requirements:** As in the hybrid cloud use case, some applications need to run on specialized infrastructure. For highly regulated industries, in addition to hosting these applications, data, and services in different locations, all traffic related to ITAR or other regulations to be monitored, audited, and isolated from any other network traffic. Apprenda's policy engine helps ensure that applications are hosted on regulatory-compliant infrastructure, and Cisco ACI provides the tools needed to properly monitor and manage the network segmentation and traffic.
- **Backup and disaster recovery:** Apprenda can be installed in different data centers and still be part of the same logical fabric. If the underlying infrastructure in Apprenda fails, the platform repopulates instances of the application in the affected region on healthy resources. All configuration of the application, for each tier, is handled by Cisco ACI. The Cisco ACI network architecture can be stretched across data centers as two independent fabrics with Layer 3 connectivity between them. Each data center has a unique IP address name-space scheme and connects to the WAN. In the operational model, each APIC cluster is identified as the primary or secondary instance (Figure 5), and changes, additions, and deletions to the application tenants are replicated from the primary controller to the backup controller.

Figure 5. Backup and Disaster Recovery



Why Cisco?

Cisco uniquely delivers the full promise of software-defined networking (SDN): a fully programmable network that connects, secures, and helps ensure the operation of distributed applications and tenants automatically, resulting in extremely low total cost of operations (TCO). Its centralized, declarative policy is implemented through an application-aware switching fabric, which simplifies the interactions of all data center and cloud teams while enabling organizations to incorporate multivendor Layer 4 through 7 services with ease and simplicity. Many other SDN solutions use central configuration of commodity switches, resulting in low capital expenditures (CapEx) but adding much greater complexity, lengthening the time to service, and increasing operating expenses (OpEx).

Cisco Capital Financing to Help You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx, accelerate your growth, and optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital financing is available in more than 100 countries. Learn more.

Next Steps

If you are interested in a joint Cisco ACI and Apprenda solution, please contact a representative:

- Apprenda: PaaS@apprenda.com
- Adam Ozkan at Cisco: adaozkan@cisco.com

For more information about Apprenda, visit http://www.apprenda.com/cisco.

For more information about Cisco ACI, visit http://www.cisco.com/go/aci.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-736553-00 04/16