

Application Security Market Trends for Service Providers: Security Approaches for Business-Critical Applications and Data in Today's Evolving Threat Landscape

Abstract

The protection of the applications and data that drive business processes and transactions is critical for ensuring business availability, employee productivity, revenue loss avoidance, and brand and corporate reputation protection. As the miscreant economy spreads across all sectors of the economy and threats increase in sophistication and complexity, the protection of mission-critical business assets, applications, data, and processes has become ever more essential.

To help service provider security-portfolio managers address these requirements within their customer base, this paper presents an overview of the current trends in the application security market, important drivers and inhibitors of application security, the evolving market landscape, and service provider delivery models for application security solutions. Additionally, the paper examines the relevance of the network for these solutions, and offers considerations for security professionals involved in solution implementations.

General Approach and Framework Definition

There are many definitions of what constitutes application security. Many industry sources utilize the application lifecycle approach that emphasizes application fortification throughout the design, development, deployment, upgrade, and maintenance phases. Because providers of managed services are primarily involved at the front end of the application lifecycle (deployment and upgrade), this paper focuses on these stages. Within this scope, the definition of application security will be regarded as encompassing the use of software, hardware, policies, and procedural methods to protect business applications and data, either in static or dynamic form, from internal and external threats.

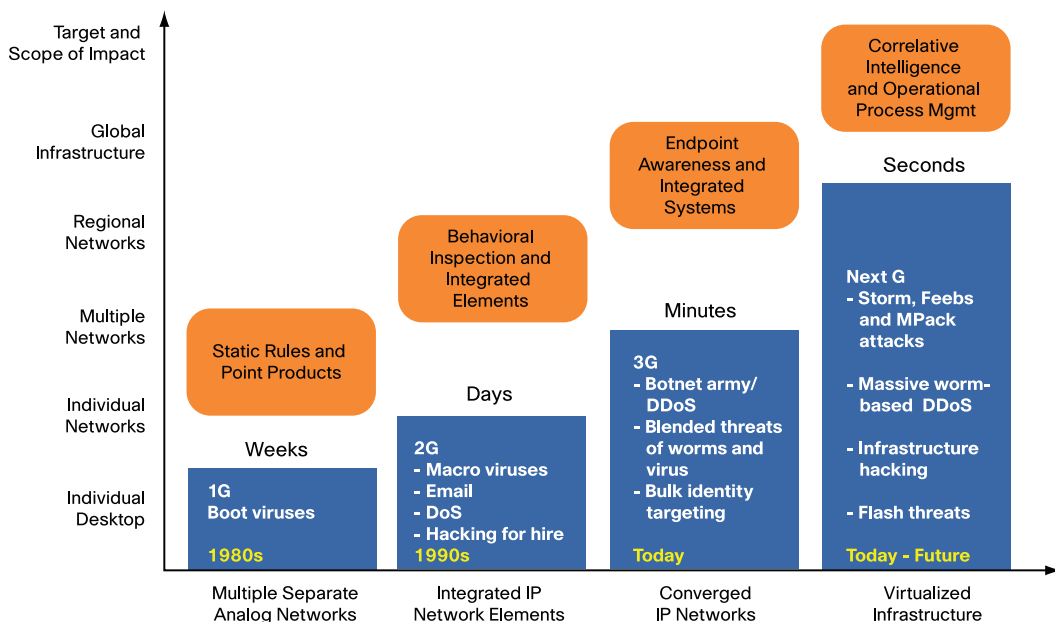
Applications are regarded as data or software programs running within and over business networks to enable business processes and services. This includes both systems software (for managing IT operating systems and IT resources) and applications software (for managing end-user requirements and business processes). As such, the protection of systems, end-user applications, and other business-related data, whether stored or in transit, is critical for business availability, employee productivity, revenue protection, and brand and reputation protection.

This requires that IT managers tasked with deploying application security should define clear business objectives, as well as identify business-critical applications, assets, and processes to be secured before proceeding. In addition, points of protection and their capabilities should also be defined and taken into consideration when evaluating the various security solutions to be deployed. As such, application security is ultimately concerned with the mitigation of business risk and enablement of internal and external compliance requirements by assuring the integrity and availability of applications that support business operations.

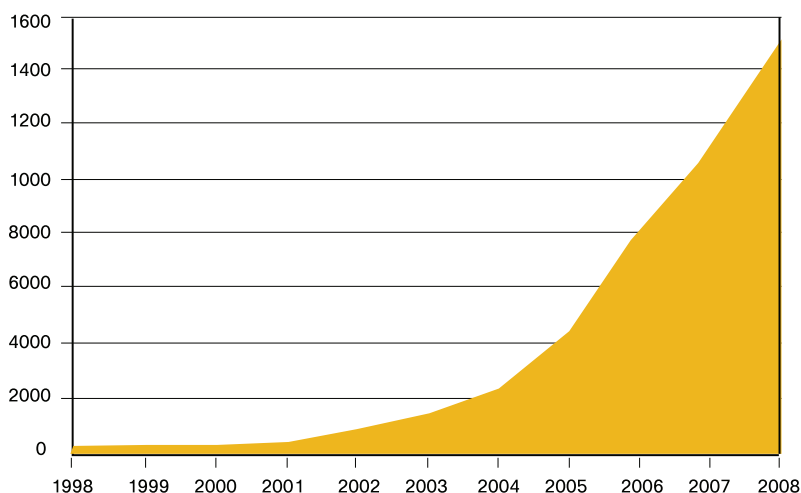
The Evolving Threat Landscape

As many companies are still struggling to introduce basic security such as firewalls and antivirus solutions, the threat landscape has evolved into much more sophisticated and dangerous threats. According to Yankee Group's 2005 Small and Medium Business IT Infrastructure Survey, the leading threats to small businesses were primarily viruses, spam, and spyware, and the vast majority of respondents cited the nuisance factor as the biggest impact from these threats. Today, both small businesses and enterprises face threats that include data and identity theft, blended web and email threats, and targeted botnet attacks. Simultaneously, the window for protecting assets from these threats has shrunk from weeks to minutes or even seconds. (See Figure 1.)

Figure 1. The Evolution of Security Threats



Over the last few years, new threats have continued to emerge (see Figure 2), taking advantage of the significant increase in system vulnerabilities. The two largest vulnerability categories are web applications and PC software. Web application vulnerabilities, which are typically remotely exploitable in nature, constitute the fastest growing and largest segment of the overall vulnerability count. In 2008, remotely exploitable vulnerabilities represented 90.2 percent of all vulnerabilities, up from about 85 percent in 2005. The most common attack techniques were SQL injection, cross-site scripting, and file-include.

Figure 2. Web Application Vulnerabilities – Cumulative Count, 1998 – 2008

Source: IBM Internet Security Systems X-Force 2008 Trend & Risk Report

Primary Drivers and Inhibitors

There are many forces at work that both encourage and discourage the adoption of application security solutions. Forces driving the need for application security include:

- **Aggressive cyber criminals.** Hackers continually change strategies to exploit security loopholes. Although businesses have invested in network security, they are not well equipped to identify or block threats that target application-based vulnerabilities.
- **Permeation of web services, Web 2.0, and applications.** The numbers and types of non-IT-controlled applications continue to grow on corporate networks. The number of endpoints, including mobile workers' laptops and smart devices, has also skyrocketed. Applications are more exposed than ever, particularly where public and private networks interface.
- **Outsourced IT models.** As businesses rely on service providers to manage or host some or all of their critical assets (such as data centers, storage servers, and networks), both customers and service providers must share security responsibilities. Outsourcing must not compromise the security of enterprise resource planning (ERP), customer relationship management (CRM), collaboration, video, and other applications.
- **Cost pressures.** Consolidation, virtualization, and standardization initiatives are being employed to strip down infrastructures and operating costs. Ensuring application security becomes a top priority within a virtualized environment, since applications are no longer tied to a specific server and can be shared across groups and teams.
- **Compliance and regulatory requirements.** Governance and compliance requirements have put additional burdens on the IT groups within retailers, healthcare providers, financial services companies, and numerous other vertical industries. These evolving regulations are driving a sub-market relating to application security testing, and this is just the beginning. For example, it is expected that the Federal Information Security Management Act (FISMA) will soon be revised to include stiffer regulations and enforcement.
- **Network-based computing.** Enterprise customers want to be able to take advantage of virtualized, scalable computing and storage resources offered by service providers, but only if they can be assured that their business data and applications are secure within the virtualized environment.

Factors that currently inhibit application security include:

- **Lack of application security expertise.** Service providers and enterprise IT teams are well versed when it comes to basic understanding and relevance of mature network security tools such as premises-based firewalls, VPNs, intrusion prevention and detection solutions, and Network Access Controls (NACs). However, many of these same professionals lack experience and skill sets relating to web application firewalls or application security testing.
- **Inertia and confusion around need for web application security.** Many businesses feel that endpoint solutions are adequate and are not aware of the emerging blended threats that employ a combination of email and web vectors for attack. Analysts such as IDC recommend a hybrid approach for web and email security, which offers a higher degree of protection by layering network-based services with traditional endpoint and perimeter customer-premises solutions.
- **Lack of push from leading security services players.** Symantec, Check Point, IBM ISS, and Microsoft are protecting large installed bases of software-only or premises-based solutions. They also currently enjoy pull-through revenues for integration services surrounding these products. Application security, in comparison to endpoint security, calls for a more flexible arsenal of solutions and delivery models.

Market Landscape

Because the driving forces are greater than the inhibitors, demand is growing for application security services. Even so, the market remains embryonic and fragmented with a prevalence of niche providers. Current solution providers fall into six broad categories, in terms of the products and services they provide:

- **Application security vendors.** Include a mix of small private players such as F5, Check Point, startups, and a few more-established solution providers such as Symantec and Microsoft that give weight to this category.
- **Systems and network integrators.** Include providers such as HP and IBM, with extensive application development, integration, network aggregation, and data center capabilities, as well as extensive reach into enterprise data centers.
- **Hosting and data center-centric providers.** These providers, such as Savvis, leverage their existing data center infrastructure to offer hosted and virtual security solutions.
- **Network service providers.** This category is dominated by large traditional network providers like Verizon and BT that are looking to extend the value of their network to businesses, in part by offering security solutions.
- **Emerging virtual infrastructure providers.** Companies such as Google and Amazon offer a combination of virtual development platforms and network-based solutions for end users, and are increasingly targeting enterprise customers with enterprise-grade solutions and service-level agreements.
- **Application security testing providers.** This category is essentially a sub-market of the larger application security market. Services include static and dynamic application security testing, and providers range from small specialist providers like Cigital to large software providers like Oracle that bundle security testing solutions alongside other application services.

Target customers in this market include both enterprises and small and medium-sized businesses (SMBs) although they have different security requirements. Enterprises want to gain efficiencies for meeting compliance and audit requirements, and need to lower the total cost of ownership while simultaneously securing business assets. SMBs are struggling to keep up with the rapidly evolving security threats, because they operate with much smaller in-house IT resources and budgets but still face the same threats as much-larger enterprises. However, SMB solutions pose additional challenges for security vendors because they must defend against the same threats types but provide simplified interfaces for ease of use and management.

Adopters of application security include customers in the following vertical markets, each with unique pain points and requirements that are accelerating demand for services:

Markets	Pain Points and Requirements
Financial services	Compliance; critical real-time data flows; identity data; fraud issues
Retail	Transaction data flows; identity data; compliance; budgets
Manufacturing	Intellectual property; collaboration and transaction data flows; brand/trade secrets
Healthcare	Compliance; patient records; fraud; telemedicine
Government	Compliance standards; national security; individual records

Service Delivery Models

Service delivery models greatly impact the overall value and effectiveness of the application security solution. Like many other business solutions, application security is currently delivered using one or a combination of the following models:

- Customer-premises-based, customer-managed
- Hosted service
- Managed service
- Software-as-a-Service (SaaS)

Network-based services and managed services in general introduce more stringent requirements for application security, thereby creating an internal demand for the customer-facing service. For securing data and applications in a virtualized or multi-tenant environment, service providers must rely on federated identity capabilities. Consider the following services, capabilities, and deployment models that require application security built into the service delivery model itself:

- Collaboration services are often purchased by businesses that need to provide access to partners, suppliers, customers, and other external parties (for example, an ecosystem).
- Document sharing, ERP/CRM/BI access, and hosted content introduce additional application and related content security requirements for the broader user community.
- New rich media applications such as high-definition (HD) video, TelePresence, and 2D and 3D computer aided design (CAD) are increasingly used to support business collaboration and are delivered over IP networks. Shared with customers and partners, these applications introduce additional security concerns regarding access, media application encryption, white lists/black lists, user groups, and inter-provider security policies.
- SaaS application models, in which the service provider may host or store application content in disparate geographies, exposes business data to local regulatory environments. This imposes the need for greater service flexibility and policy options for hosted or virtualized resources.

Traditional service delivery models have been based on either software licenses only, or a combination of on-premises equipment (leased or purchased) and software licenses. Both of these

models typically include monthly recurring charges for updates and/or maintenance. Today, providers of all types, from pure software providers to network service providers and virtual infrastructure providers, are optimizing their infrastructures and assets for volume-based multi-tenanted capability and service delivery.

SaaS and on-demand are emerging as the preferred delivery and consumption models in many cases. For SMBs, network-based service models are affordable and can help them overcome skill gaps and operate with limited backup and storage resources. Enterprises, while not as resource-constrained as SMBs, have security requirements around large distributed knowledge workers accessing the corporate network anywhere, anytime, in any format (multiple endpoint types). They also have multiple security and IT compliance requirements around data leakage, and must often secure extended supply chains into, and on top of, their networks – mandating hardened, private WAN-public network interfaces.

Nexus Markets and Service Packaging

At a vertical level, application security is emerging as a standalone service category in its own right. It can be bundled with other security services, particularly alongside data loss prevention and access control. For customers that do not have dedicated in-house security experts, this type of bundling is preferred. Another vertical option is to sell it as part of an enhanced unified threat management (UTM) service.

At a horizontal level, application security is also offered with other managed services that are commonly required within a particular market. Some providers also offer bundles that enrich broader service portfolios by combining application security with collaboration, unified communications, data center, virtualized servers, or other managed services. In doing so, the application-security-embedded service bundle enables service providers to offer a more complete service portfolio, increasing their value and relevance to their target customers.

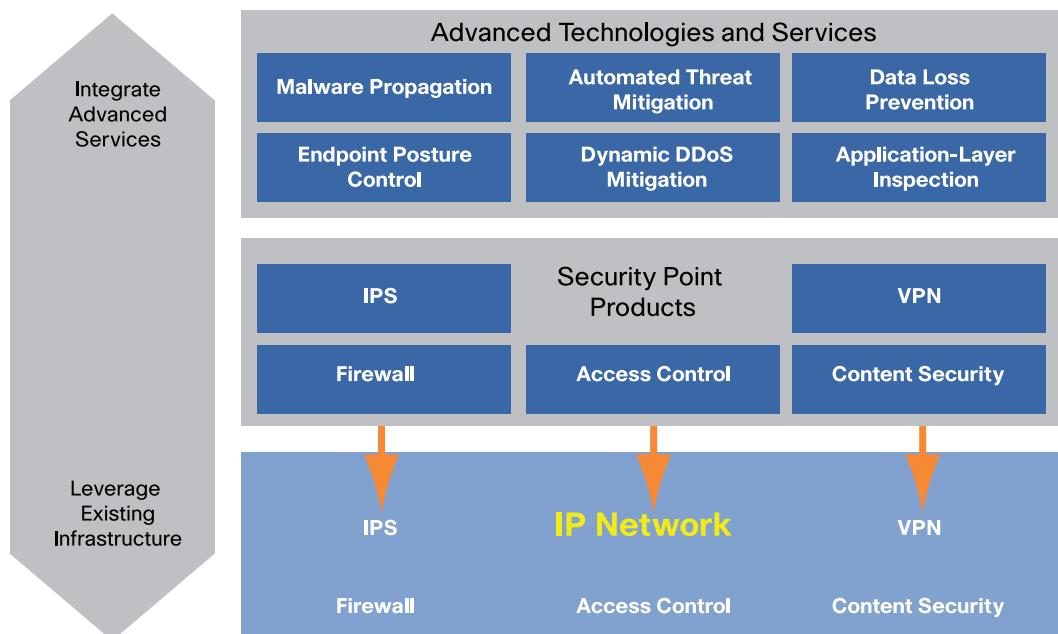
Increasing demand for application security is also driving the emerging Secure Web Gateway market. Secure Web Gateway solutions provide URL filtering, malware blocking, and controls for web-based applications such as voice-over-IP services or instant messaging content. These capabilities give users the ability to safely use the Internet. Businesses can use Secure Web Gateways to enforce company and compliance policies. An increasing number of service providers are offering Secure Web Gateways alongside other security services.

Network Relevance for Application Security Services

A minority of the overall security market still exhibits limited understanding of the need for dedicated application security solutions. However, widespread acceptance is driving security origination, operations, and delivery further back into the network. The network has become a critical platform on which to deliver, manage, and monetize security services. This creates an opportunity for value-added service (VAS) offerings from different market players, while posing challenges too. Many service provider networks are not adequately configured to block next-generation web threats.

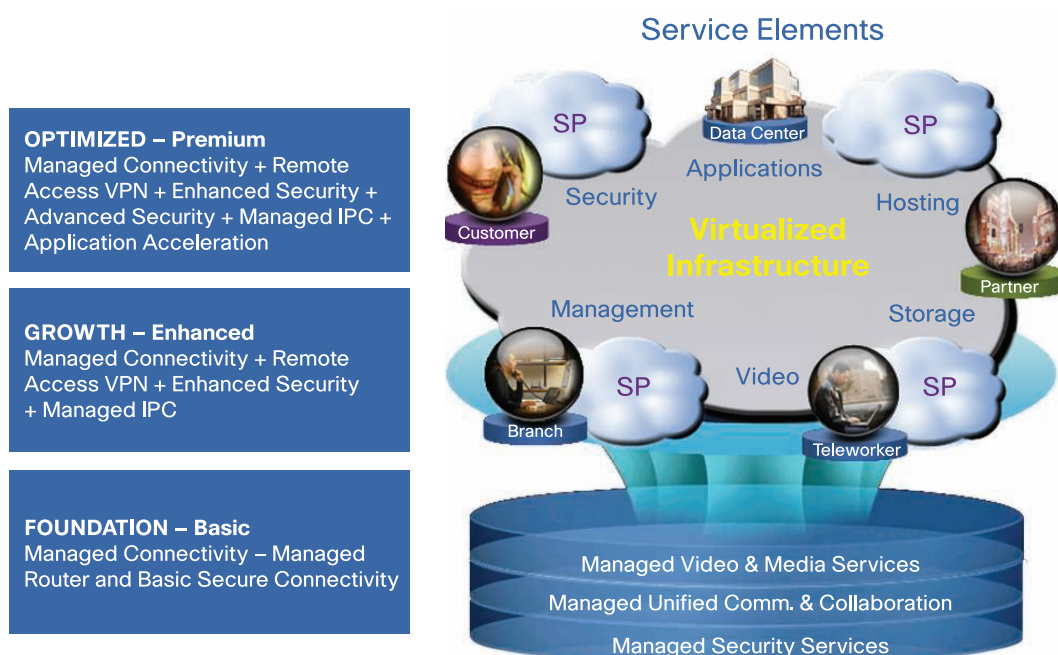
Migration to a flexible network-based service delivery model can help service providers overcome these limitations. Cisco is uniquely positioned to help service providers evolve existing infrastructures and build security into every layer of their service delivery infrastructure (see Figure 3).

Figure 3. Virtualized Network-Based Security as the Platform for Application Security



Cisco® solutions enable service providers to deliver relevant application security solutions in the short term, and also evolve to a new Web 2.0 service model for the medium to long term. The Cisco network-based approach for application security takes advantage of the emerging virtualized, service-oriented model where applications are run and delivered from virtual machines rather than standalone, dedicated systems. As earlier stated, this allows the service provider to extend and cross-sell the benefits of virtualized network security across other managed services such as data center solutions, application performance management solutions, fixed-mobile convergence, and unified collaboration and communication solutions.

Figure 4. Extending the Benefits of a Flexible Architecture to Horizontal Bundling



Cisco Managed Hosted Security Services address application security within the broader overall security context, and include both a robust architectural approach as well as a range of service delivery solutions. The Cisco offering spans a continuum of cost-effective and flexible Cisco security solutions built on virtualized infrastructure that can be delivered dynamically in a “mix-and-match” approach to meet evolving threats and hybrid customer needs. Cisco Managed Hosted Security Services help service providers transform their Service Delivery Data Center, or Service Delivery Center (SDC), into a dynamic, scalable, resilient environment. The SDC encompasses the service provider’s complete virtualized infrastructure: the network, data center, IT, storage, application, and compute resources. Service providers can leverage this investment to deliver a complete portfolio of monetizable security and non-security managed services.

The SDC model helps service providers move up the customer value stack: from foundation security, to transport-aware security, right through to application-aware security. Service providers can adopt service delivery models – premises-based, network-based, data-center-based, or hybrid – that suit their target markets and customers.

Conclusions

Application security has become a pervasive requirement across many markets, and the increasing trend and adoption of web services and business process collaboration are behind its growing relevance. Also accelerating demand is the rapidly evolving, highly sophisticated miscreant economy, which poses a direct threat to business availability and profitability.

Application security is not a standalone security requirement. Rather, it must be addressed across business networks and, more importantly, across business processes. It should be regarded as part of the broader set of business requirements for minimizing business risk, maximizing employee productivity, and protecting company brands and corporate reputations.

Consideration must also be made for application security, in terms of the multiplicity of service delivery models available. These include software only, premises-based, hosted, fully managed, hybrid, and Software-as-a-Service delivery options. The delivery of services over virtualized network-based infrastructures is also gaining momentum. Cisco is well positioned to provide flexible architectures and cost-effective solutions that support variable service provider requirements, and can support providers regardless of their existing infrastructure or delivery models.

The above market trends underscore the need for service providers to address application security. However, the growing revenue opportunity provides the most compelling reason to pay attention. Service providers can increase and diversify revenues with application security services, add value to their portfolios by bundling in application security solutions, and create a foundation for other security-sensitive managed services such as unified communications, collaboration, and rich media services. The direct and indirect revenue opportunities now place application security in the category of a fundamental offering for forward-looking service providers.

For More Information

For more information about Cisco service provider security solutions please visit:

http://cisco.com/en/US/netsol/ns341/ns121/ns310/networking_solutions_solution.html

To learn more about application security in general, service providers can refer to many industry publications and market analyst reports, including:

- Yankee Group’s 2005 Small and Medium Business IT Infrastructure Survey

- IBM Global Technology Services, January 2009, “IBM Internet Security Systems X-Force 2008 Trend & Risk Report”
- “Top 10 Info Security Predictions for 2009” in the Computer Security Institute’s January 2009 Computer Security Alert (http://i.cmpnet.com/v2.gocsi.com/pdf/CSIALERT_2009-Preview.pdf)



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.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)