



## Cisco AON Security

### Enabling and Enforcing Application-to-Application Security through the Network

#### TODAY'S APPLICATION SECURITY CHALLENGES

Today's CIOs and CXOs must manage and mitigate security- and privacy-related risks that dramatically affect their profitability and corporate governance and compliance imperatives. From simple yet insidious to complex and pervasive, these security challenges threaten to overwhelm business boundaries and protection mechanisms, thus requiring an increasing share of management attention and IT resources. Today's top security concerns include:

- **Insider threats from employees and trading partners**—In fact, most security breaches emanate from internal business networks.
- **Interconnected networks with no clear boundaries**—As boundaries between networks disappear in order to connect partners and suppliers, multiple new threat vulnerability points are introduced.
- **Distributed systems based on service-oriented architectures**—Security for Web services has been problematic and difficult to standardize and enforce across organizational boundaries, leaving enterprise network boundaries porous and permeable.
- **Attacks that are growing in complexity**—New massive and blended attacks threaten to overwhelm point-based security systems.
- **Growing use of personal applications**—Web-based e-mail, instant messaging, and peer-to-peer applications provide multiple points of entry for viruses, worms, and other attacks and provide a readily accessible means of disseminating proprietary and confidential information.
- **Ever more pervasive attacks**—Nearly, two-thirds of companies have been attacked by worms or viruses. Computer worms such as CodeRed compel enterprises to improve patch management and network segmentation.
- **Phishing and pharming attacks**—New schemes for Internet-based fraud are difficult to stop, and they pose the risk of identity theft to unsuspecting customers and employees.
- **Spyware on the rise**—Two-thirds of computers have spyware residing on them.
- **Spam and spim**—Unsolicited e-mail (spam) accounts for more than half of e-mail messages, costing businesses billions per year. Instant messaging spam (spim) totaled more than 1.2 billion messages in 2004.
- **Uncertain effect of risk management**—Although many companies measure security performance, two-thirds do not measure return on investment (ROI) for risk management.

Clearly, security has emerged as a top business priority. In addition, ever-increasing global requirements for compliance and corporate governance make network security and privacy imperative, and enterprises are seeking ways to mitigate security risks in a way that also enables them to balance costs against business requirements. Today's security landscape is permeated by fear that hacker attacks will overwhelm perimeter security systems, uncertainties about how to control insider abuse, and doubt that point-based security systems can effectively sustain and protect the network. What is needed is a comprehensive security fabric that overlays and permeates existing networks to provide end-to-end security that transcends organizational and domain boundaries.

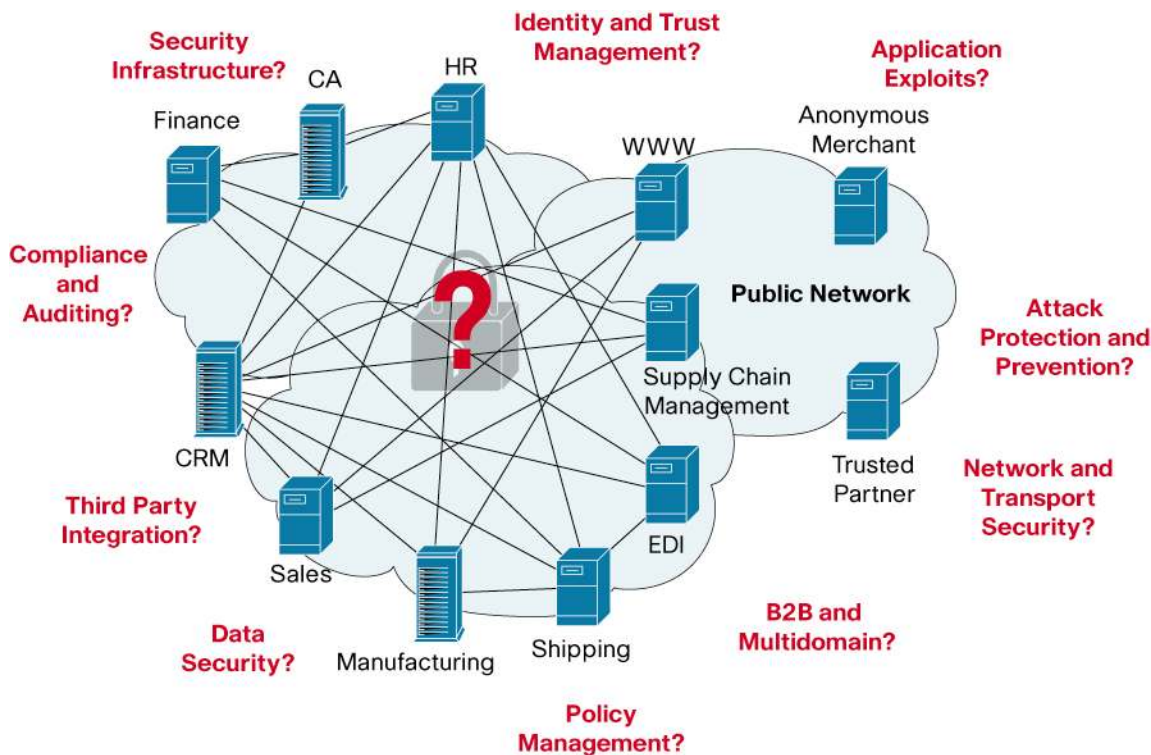
## TODAY'S APPLICATION-TO-APPLICATION SECURITY LANDSCAPE

The primary challenge in inter-application communications is how to transparently and cost-effectively enable and enforce security on the massive scale required by today's distributed and service-oriented architectures. Even in a simple security scenario requiring two applications to exchange information, concerns of trust, confidentiality, and integrity must be considered. In real-world enterprise deployments that can consist of hundreds of interdependent applications, the ability of the network to deal with complex security challenges becomes the primary determining factor in the success of the implementation. The network must be equipped to enable and enforce complex security that spans enterprise and partner boundaries with consideration to:

- Compliance and auditing requirements that provide stiff penalties and fines for violators.
- Identity and trust management concerns that are increasingly difficult to manage across partner ecosystems.
- Security infrastructure requirements that require a balance of performance and protection.
- Data security that protects confidentiality and integrity of information in transit.
- Attack protection and prevention to foil massive and complex assaults.
- Security policy management to invoke and enforce business rules across organizational boundaries.
- Business-to-business (B2B) and multi-domain security to enable e-commerce relationships among trading partners.
- Network and transport security to provide fundamental and ubiquitous protection.
- Third-party integration to enable application, network, and specialized systems from multiple providers.

These and other considerations give rise to CXOs' fundamental awareness that security is imperative for business growth and expansion.

**Figure 1.** Complex Application-to-Application Security Challenge



CIOs and CSOs realize that traditional perimeter and point security approaches are not sufficient to deal with today's complex multi-domain and inter-application security challenges. In addition, implementing security mechanisms in the applications themselves becomes monolithic and resistant to change, and implementing security using a collection of point systems introduces unwarranted costs and complexities. The Cisco® Application-Oriented Networking (AON) solution and its inherent AON security fabric offers enterprises a significant advantage when it comes to realizing end-to-end security in today's complex, distributed, and service-oriented environments. Cisco Systems® can combine and integrate the necessary trust enablement, policy enforcement, and threat protection mechanisms required for this application-oriented network security embedded and delivered within the network fabric. Attributes of Cisco AON security include:

- Pervasive application-to-application security throughout and across networks, particularly in extended business ecosystems.
- Offloading of security services from applications to ensure consistent security enforcement across multiple threat vulnerability points.
- Transparent overlay of security in the network fabric to ensure that operations of users, systems, and services are unchanged while secured.
- Holistic security implementations that operate at multiple layers across application internetworking topologies.
- Adaptive solutions that flex and expand as perimeter boundaries disappear, new business relationships are formed, and business needs grow.

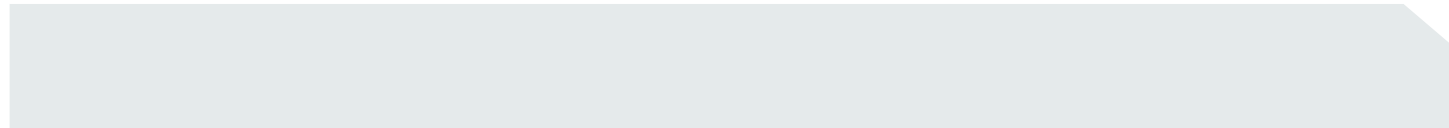
With regard to the profit line, the inherent Cisco AON security helps enable the lowest total cost of security that can be realized only when an inherent security fabric offloads security functions from applications to networks to ensure consistent security policy administration and enforcement across users and applications throughout the service network.

## **CISCO AON SECURITY OVERVIEW**

Cisco Application-Oriented Networking represents a significant advance and new paradigm in application internetworking: inherent networking intelligence can be infused directly into applications, enhancing the enterprise's end-to-end and machine-to-machine security, real-time awareness, visibility, and flexibility, while reducing the costs and complexities of integrating and provisioning distributed, services-oriented and older applications. Cisco AON helps enable the "new physics" and the "new economics" of application communications through non-intrusive and shared network intelligence that selectively enforces business-aware policies and provides actionable knowledge based on real-time context and dynamic content. The solution frees applications and middleware to deliver essential and specialized business functions, extends the network to take advantage of its inherent and pervasive functions, helps enable the move beyond monolithic architectures, and allows the realization of the full promise of the adaptive enterprise and distributed and service-oriented computing. The secure application communications of Cisco AON helps ensure that security is an inherent element of all inter-application messaging.

Cisco AON network integrated modules and appliances provide a set of intelligent services that operate either transparently to applications or in an explicit manner that virtualizes application services at the network level. These services are delivered according to the in-transit content and inherent context of application communications, with security services including:

- Identity-aware routing of application messages with built-in translation and transformation of message protocols.
- Reliable delivery of application messages with application-level security, including encryption, authentication, authorization, signing, and public and private keys.
- Hardware-based acceleration, caching, load balancing, and compression with secure message logging and monitoring of business-related events related to compliance, privacy, and corporate governance.
- Enterprise-class support for service-oriented architectures and Web services with extensible security services for custom protocols, formats, and application logic.
- Extensible and programmable security enforcement framework to easily integrate with the existing security infrastructure fabric of client companies.



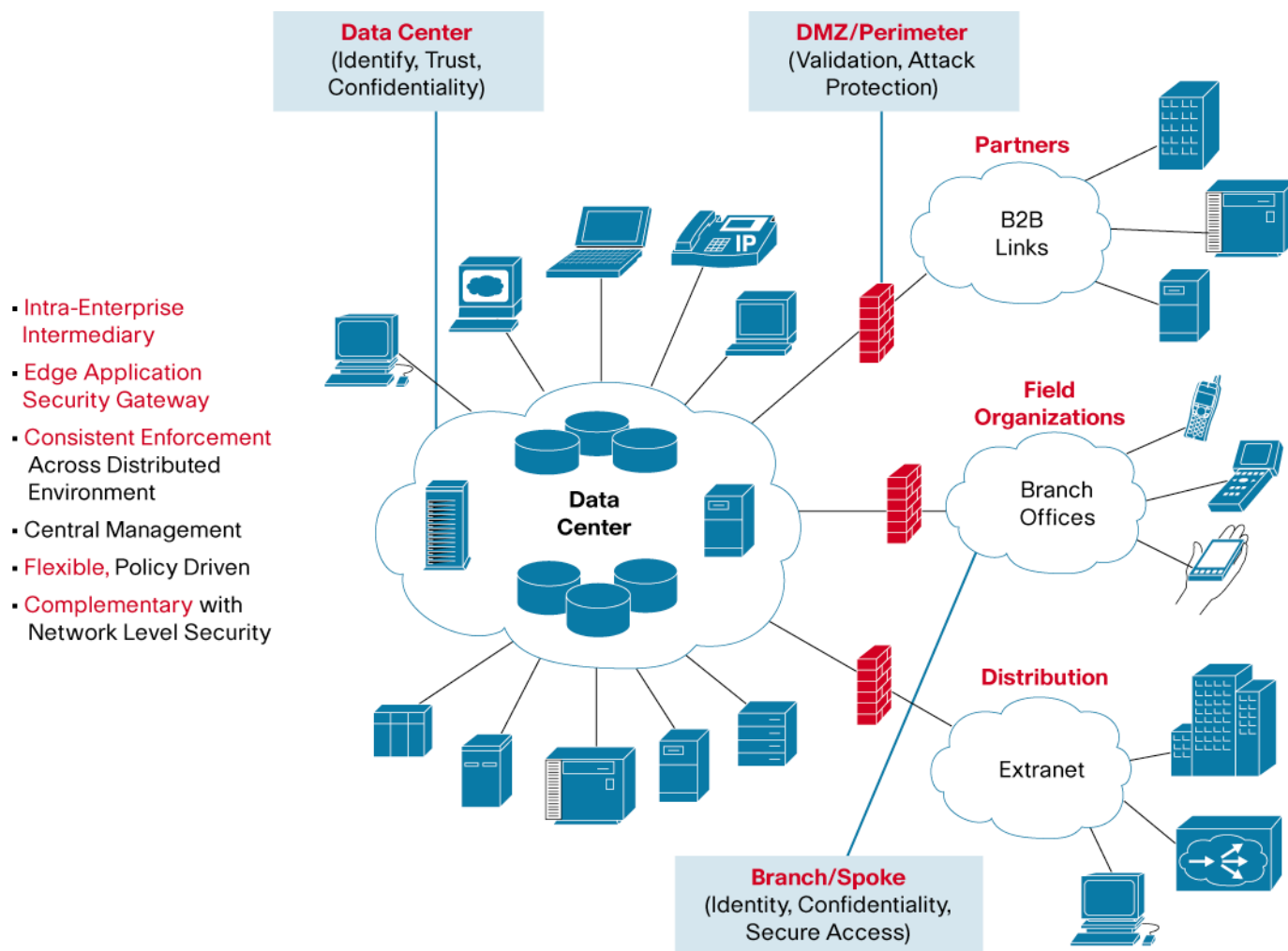
Security integrated at the message level is an important attribute of the Cisco AON security fabric. Today's message security is implemented primarily within the application or in intermediary software or gateways. The message-based approach of Cisco AON provides a security umbrella to business applications such as order processing, business intelligence, and other transactional and management systems to operate in a loosely coupled service-oriented manner while securely exchanging data. Importantly, service-oriented infrastructures and message schemas such as Extensible Markup Language (XML) enable machine-to-machine communications that benefit significantly from the network fabric-based approach to application security. This approach allows for lower cost of ownership and maintenance, flexibility, and effective and pervasive policy enforcement.

An important attribute of Cisco AON is ease of integration with enterprise-wide applications and spanning external B2B and multi-domain application environments. Cisco AON security capabilities are delivered in this environment—partly through the core AON platform, partly through integration with existing security infrastructures, and partly through services provided by third-party security applications integrated with AON. The total set of security features provided by Cisco AON includes:

- Trust enablement and threat protection for XML and Web services as well as older applications
- Identity- and content-based authentication, authorization, and access control
- Data security and confidentiality in the form of digital signatures and message field-level encryption
- Integration with enterprise security services such as public key infrastructures and certificate authorities
- Business requirement-directed security policy management and enforcement
- Application logging enabling compliance and security audit logging
- Protection against threats to applications and underlying networks
- Network and transport security through Secure Sockets Layer (SSL), HTTP, and HTTPS

Cisco realizes that a requirement of total enterprise security integration is that the Cisco AON application internetworking security solution must work in combination with application security capabilities provided by other Cisco partners.

**Figure 2.** Cisco AON Security Deployment Landscape



Cisco AON security can be deployed intra-data center between applications, at the data center edge, in the branch office, or at perimeter-connecting enterprises with numerous partners and suppliers.

### Application-to-Application Security at the Enterprise Core

In application-to-application deployments, Cisco AON is deployed in the data center core behind the Web tier and between application servers and database servers. In such deployments, which typically rely on XML-based service-oriented or Web services infrastructures or traditional middleware, Cisco AON establishes trust between applications through identity verification, message integrity, and data confidentiality with encryption and decryption. In the enterprise core, many diverse applications with various messaging protocols and security systems require that Cisco AON enable transparent security integration between applications; provide a secure, manageable, and scalable messaging infrastructure; and integrate with existing security infrastructure and services.

## **B2B Application Security at the Data Center Edge**

At the data center edge, Cisco AON is deployed as a B2B security gateway to virtualize back-end infrastructures and establish trust with partner applications through identity verification and message integrity, authorization for access to appropriate applications, and data confidentiality with encryption and decryption. As a gateway to the external world, Cisco AON is exposed to all types of traffic; therefore, the solution must enable and enforce security policies at application level and ensure a balance of security and performance under varying load conditions.

For perimeter application security in B2B environments, Cisco AON augments and sits behind firewalls to validate and conform content through schema and field validation and provides attack protection against external assaults such as man-in-the-middle attacks, distributed denial-of-service (DDoS) attacks, and other XML payload attacks. Cisco AON at the perimeter must secure large-scale enterprise hubs connecting hundreds of suppliers, logistics providers, and trading partners—a scenario that requires a heterogeneous security infrastructure, pervasive visibility into spokes, security functions for multiple protocols, and support for performance- and security-oriented service-level agreement (SLA) commitments.

## **Branch and Spoke Security in the Branch Office**

In enterprise branch office environments, Cisco AON is deployed at the branch office edge or at a B2B partner site as a security gateway to establish trust with data center hubs through digital signing, ensure data confidentiality using encryption, and enable secure access with support for SSL and Transport Layer Security (TLS) protocols. Branch offices are typically connected to central offices through VPNs, are not supported by a dedicated IT staff, and they typically focus on consolidation of servers and shared infrastructure to lower cost of operations. Cisco AON provides end-to-end application-level security, prioritization, and traffic shaping based on application context, and centralized visibility and management to ensure compliance, privacy, and confidentiality.

## **CISCO AON SECURITY FOR APPLICATION INTERNETWORKING**

Cisco AON provides transparent integration between message-level application security and network-oriented packet-level security. At the application level, it provides:

- Authentication.
- Authorization.
- Secure control of XML content with policy-based schema validation and protection against multiple XML vulnerabilities.
- Policy-based content inspection and filtering.
- Prevention of complex and blended application layer threats.
- Enforcement of business policies for auditing and regulatory compliance.
- Heterogeneous integration of disparate application security infrastructure.

At the network level, Cisco AON offers the following benefits:

- Extends network firewall and intrusion prevention solutions.
- Detects traffic anomalies and protects against DDOS attacks and other oversized payloads at application layer.
- Integrates with Cisco network security services for complete, end-to-end security definition and enforcement.

## Cisco AON Security in Action

In a typical service-oriented security enforcement scenario, Cisco AON may be asked to enforce a security policy requiring identity validation and entitlement authorization, signing and verifying of XML content for enforcement of data integrity and non-repudiation, encryption and decryption of sensitive content for message-level privacy, and schema validation to detect anomalies within the application messages. In this scenario, Cisco AON security works by first determining identity by extracting claims from a message, verifying identity by extracting proof of possessions, authenticating any or all extracted claims, and finally authorizing access to the endpoint application or service multiple elements or contents, verifying all or none of the XML signatures and encrypting or decrypting selective elements of contents. Next, Cisco AON validates content against a schema or Document Type Definition (DTD) to detect any anomalies with the message content.

Cisco AON can be deployed as modules in Cisco switches and routers as well as network integrated appliances in transparent mode in which a Cisco switch or router can transparently redirect application traffic to an AON module where policies are applied to application messages before forwarding them to the destination applications. In transparent mode, the sending and receiving applications are unaware of the presence of the AON solution in the data path. Alternatively, Cisco AON can be configured in explicit or proxy mode, in which application traffic is explicitly redirected to AON modules for processing. In this mode, at least the sending consumer application is aware of the AON module in the data path. The explicit mode is often used to have Cisco AON act as a service virtualization network element hiding or proxying for endpoint application services.

For configuration and management, the Cisco AON Development Studio creates Policy Execution plans (PEPs), which represent a set of operations or “bladelets” applied to application messages. The Cisco AON Management Console provides centralized control for configuration, certificate management, and lifecycle management of a distributed Cisco AON network.

Cisco AON enhances message-handling performance and provides superior levels of application security and availability. Typically, it attends to only a fraction of network traffic flow, so that the vast majority of network traffic passes through as usual. To minimize processing overhead and achieve enterprise-ready levels of throughput and reliability for this specific traffic, Cisco AON provides hardware acceleration and built-in load-balancing and high-availability services to scale in terms of adding either multiple blades to perform as a single virtual node or a single blade performing multiple functions, including security, message routing, protocol bridging, transformation, etc. To reduce application-to-application response time and conserve network bandwidth usage, request and response caching can also be performed for entire messages or for certain message elements. Cisco AON can cache XML and non-XML response messages or elements of a message—and it can compress messages between nodes.

### Example 1: Cisco AON Security in a Business-to-Business Environment

In a B2B environment, an enterprise doing business with diverse trading partners—each with different status and privileges—enables one partner to order any item from its product catalog in any quantity, while authorizing yet another partner to order only select items in limited quantities. The enterprise exposes its ordering system as an XML-based Web service with associated business policies that:

- Authorize access to only qualified partners.
- Enable orders up to entitlement levels.
- Require that all orders come as attachments with predefined XML schemas.
- Ensure orders are digitally signed.
- Log any violations and upon a specified number of violations, temporarily revoke trading privileges.

Without Cisco AON, it is far more difficult and complex to embed security policies into multiple applications, implement visibility of compromised systems or violation of schemas, or modify these policies when changes occur.

With Cisco AON security, trading partner ABC’s order is placed in the right format and is delivered reliably, while returning an exception for trading partner XYZ’s unauthorized order. Meanwhile, an unknown entity attempts to place an order, which is rejected without human intervention.



Then, trading partner ABC's systems have compromised an external entity, which can attack the enterprise's trading system with multiple messages with malicious attachments. Cisco AON does schema validation resulting in a failure, refuses the order, and triggers a security exception notification. After a specified number of exceptions, Cisco AON revokes trading privileges and sends a notification to appropriate parties. Cisco AON also can block the compromised trading partner's access by shutting down the necessary ports through the network firewall—and it can conduct all these complex operations expediently without human intervention or the potential for operator error.

Another unique advantage of Cisco AON is that business partners can be quickly enabled to enforce security policies at their end simply by adding AON modules to the routers and switches that provide network connectivity. They do not need to incur the heavy costs of building additional security into their back-end applications.

### **Example 2: Cisco AON Security in the Enterprise**

In an enterprise core environment, Cisco AON serves as an application-to-application security fabric or gateway. For example, an insurance company deals with claims containing sensitive customer information, such as patient records, credit card information, and social security numbers. Business flows include:

- The customer submits data security through the Web for a variety of claims.
- The Web server decrypts the data and, depending on the type of claim, encrypts and directs it to back-end applications.
- Back-end applications process the claim, interact with financial systems for reimbursement, and log information into a reporting system.

Now, new privacy and confidentiality laws dictate that:

- All credit card and social security numbers must be encrypted when sent from one application to another.
- Only authorized applications can access customer information.
- Processing agents can access records for only their respective departments.
- Only select information can be sent to reporting applications.

Without Cisco AON, the company would need to modify all applications based on the new privacy laws.

With Cisco AON security, an AON module is configured to encrypt credit card and social security numbers and route to appropriate servers, helping ensure that financial applications can access customer records but other applications cannot. Additionally, Cisco AON rejects access requests from a spurious application, and after a specified number of violations, locks down related ports to deny access attempts from the spurious application.

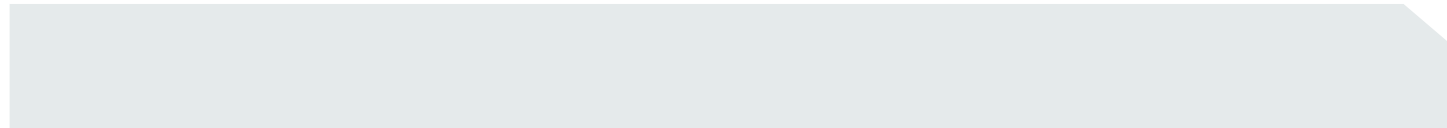
### **Advantages of Cisco AON Security**

Cisco AON provides a security fabric that integrates with the underlying AON application internetworking fabric to provide more robust, consistent, and easy-to-manage security for applications across the enterprise and its extended boundaries. Cisco AON security is transparent and pervasive, offloading the burden of security from applications in a way that is difficult to tamper with or bypass, and is distributed across the enterprise from the data center to the branch office for scalable and highly available application and network services.

To enable consolidation of application security infrastructure, Cisco AON security is holistic with integrated application threat protection and trust enablement capabilities, supporting a wide range of security features at the application message level, including authentication and authorization, content validation, and attack protection.

Cisco AON minimizes the total cost of security, through distributed enforcement of security policies with centralized management; the solution can enforce security policies where they make the most sense without additional management complexity. For example, documents can be digitally signed at the branch office, with credentials authenticated at the data center edge, and content validated at the application server tier.





Cisco AON security is adaptive through its readily extensible framework and broad compliance with standards. The Cisco AON Software Development Kit allows creation of custom protocol adapters and custom bladelets, with support for all major Service-Oriented Architecture, Web service, and security standards. The AON security solution is easy to integrate with third-party identity, policy, and public key infrastructures.

## **SUMMARY**

As the flagship for a new technology paradigm, Cisco AON provides the foundation for a new class of Cisco products; it provides an essential point of convergence between networks and applications based on today's highly distributed, service-oriented and older architectures. And it embeds a new class of application intelligence into the network to better meet the underlying needs of applications for security, visibility, event-oriented messaging, optimized delivery, and other core integration and deployment services.

Cisco AON complements existing networking technologies by providing a greater degree of awareness about the information flowing through the network, helping customers to route information between disparate applications, enforce security policies, optimize the flow of application traffic, and provide improved visibility of information. This solution provides this enhanced level of application intelligence within the network by understanding more about the content and context of information flow at the application communications level rather than the packet level.

Cisco AON is an important component of the Cisco Intelligent Information Network (IIN) vision and strategy. The Cisco IIN provides the foundation for building network infrastructure that meets a company's most strategic business objectives aligned with industry trends such as virtualized computing and service-oriented architectures. At the point where networks and applications converge, this solution points the way to a new era of business relevance for the network—as a strategic enabler and accelerator of today's distributed, service-oriented and traditional business applications and processes. The results—rapid time to market, readily extensible collaboration, and on-demand computing—produce sustainable competitive advantage.

## **FOR MORE INFORMATION**

For more information about the Cisco AON products and services, visit <http://www.cisco.com/go/AON> or contact your local Cisco account representative.

**Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

**European Headquarters**

Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

**Asia Pacific Headquarters**

Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel  
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal  
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan  
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0601R)

