Cisco Cloud Web Application and API Protection

Cloud WAF, Bot, API, DDoS, and Client-Side Protection Services



© 2025 Cisco and/or its affiliates. All rights reserved.

Challenges of keeping modern applications secure

Applications drive business competitiveness and success. From sophisticated e-commerce platforms to cloud-based productivity solutions and personal tools on mobile phones, applications do more than generate revenue and drive growth — they are the main platform for attracting and retaining customers.

The application perimeter is expanding and becoming more difficult to define and protect. Whether on-premises or in the cloud, applications are now scattered across different platforms and frameworks. They rely on third-party JavaScript services and the availability of information from other third-party services that they interact with via APIs. As a result, the attack surface grows and risk exposure increases.

As applications constantly change and are updated, security policies must adapt to safeguard them and the data they host while complying with information security policies. In addition, the democratization of generative AI tools in the hands of hackers has brought a new generation of zero-day attacks that are persistent, sophisticated, and aggressive.

It is increasingly difficult to protect against an expanding array of attacks, adapt policies in real time to mitigate automated attacks, and maintain a high level of security with low levels of false positives while ensuring that legitimate traffic is not impacted. This often necessitates manual intervention which increases operational costs and requires expertise that many organizations do not have available.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Cloud WAAP for complete application protection

Cisco, in partnership with Radware,[1] provides an industry-leading web application and API protection (WAAP) suite. Cisco® Cloud Web Application and API Protection (WAAP) and bot management solutions offer a one-stop shop for your application security needs, providing state-of-the-art web application firewall (WAF), API security, bot management, Layer 7 distributed denial-of-service (DDoS) mitigation, and client-side protection. The solution provides comprehensive application protection while enabling business agility and growth.

Comprehensive security

- Extensive protection covers all Open Worldwide Application Security Project (OWASP) key vectors for web application security threats, vulnerabilities, and other sophisticated threats.

AI-powered and automated

- Automation of resource-intensive processes — including security policy refinements, event analytics, API discovery and schema file generation, AI-driven cross-correlation of security events, supply-chain JavaScript services mapping, alerts, and enforcement — provides enhanced security, minimum false positives, and reduced overhead.

Frictionless and adaptive

- Protection quickly and easily adapts to changes made to your applications and the underlying deployment platform — with no interference to your business.

Consistent

- Uniform, state-of-the-art security for all applications — regardless of where they are deployed — enables consistent protection for applications hosted in private data centers and in hybrid and multicloud environments.

Reduced operational cost

- Around-the-clock 24x7x365 support from Radware's[1] highly trained Emergency Response Team (ERT) provides customers with a fully managed service that provides superior protection while reducing operating costs.

In-depth visibility and control

- Advanced security and development dashboards provide actionable analytics, automation, and customized controls that provide full visibility into application threats and enable better decision making for application development teams.

1. Cisco sells industry-leading DDoS protection, application protection, bot management, and application delivery controller solutions through its global OEM partnership with Radware.

© 2025 Cisco and/or its affiliates. All rights reserved.

Comprehensive application protection: Client side, server side, and everything in between

Easily manage and seamlessly scale your application security as you grow your business, evolve your application architecture, and expand your cloud environments and services. Cisco Cloud WAAP and bot protection keeps organizations protected against threat vectors as their business grows and applications evolve. It also helps ensure compliance with new and existing regulations, such as PCI DSS 4.0, NIS2, GDPR, HIPAA, DORA, and more.

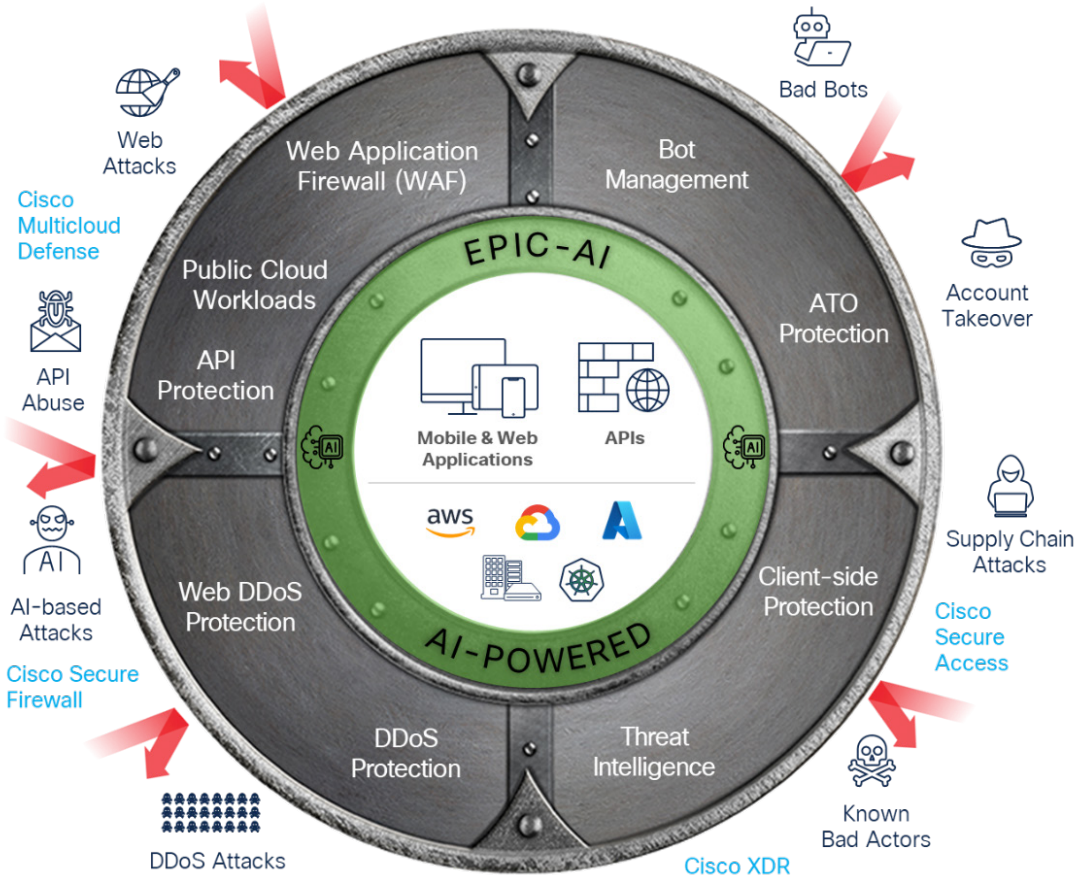


Figure 1. Comprehensive cloud application protection

© 2025 Cisco and/or its affiliates. All rights reserved.

Protect digital assets and data

- Compatible with any application architecture, Cisco Cloud WAAP protects your digital assets and customer data in all environments, whether on-premises or in virtual clouds, private clouds, public clouds, hybrid environments, or Kubernetes.

Detect, manage, and mitigate bots

- Detect and distinguish between “good” bots and “bad” bots to protect websites, mobile apps, and APIs. Easily optimize and customize your bot management policies to provide a better user experience and drive more return on investment (ROI) from your application traffic.

Protect against OWASP vulnerabilities

- Stay protected against 150+ known attack vectors, including the OWASP Top 10 Web Application Security Risks, Top 10 API Security Vulnerabilities, Top 21 Automated Threats to Web Applications, and Top 10 Client-Side Vulnerabilities.

Protect application APIs

- API attacks are a rapidly growing threat to business applications and customer data. Cisco Cloud WAAP combines behavioral analysis and policy automation to protect APIs from increasingly sophisticated API threats and business logic attacks.

Block AI-driven zero-day attacks

- Cisco Cloud WAAP’s unique behavioral-based positive security model stops unknown threats in their tracks. AI-driven, multilayered analysis engines continuously study application traffic and end-user behavior to establish accurate baselines and automatically fine-tune security policies. This allows users to detect and accurately block any anomalous behavior.

Protect your client side from supply chain attacks

- As server-side security improves, attackers increasingly target the less protected and rarely monitored client side. Cloud WAAP’s client-side protection helps ensure that end-user data is protected when interacting with any third-party services in the application supply chain while providing the controls required for PCI DSS 4 compliance.

© 2025 Cisco and/or its affiliates. All rights reserved.

Mitigate application-level DDoS assaults

- Advanced DDoS protection included in the Cloud WAAP solution provides the shortest time to detection and mitigation for HTTP-based DDoS assaults. Using patented behavioral analysis and machine learning-based engines, in conjunction with a robust, global cloud application protection network, Cisco Cloud WAAP stops the most advanced high-volume and high-throughput HTTP DDoS attacks.

Empower your SecOps team with threat intelligence services

- Get real-time, actionable insights from global cyberattack intelligence, enabling your organization to analyze attack traffic, make rapid and educated security decisions, and defend against threats before they escalate. In addition, get reputation alerts on attacks on the web originating from your own network.

AI-powered intelligent cloud application protection as a service

Web application firewall

Cisco Cloud WAAP's adaptive and automated WAF protects against web application attacks, hacking, and other vulnerabilities. Our WAF technology uses an AI-powered positive security model that automatically learns the behavior patterns of legitimate users and continuously refines security policies to avoid false positives while accurately blocking any action that deviates from these patterns of legitimate behavior.

The combination of negative and positive security models provides complete protection against OWASP Top 10 threats and zero-day attacks that WAFs based solely on negative security models cannot stop. Negative security models rely on blocklists of known attack signatures and are not able to detect or stop never-before-seen zero-day attacks.

API protection

The Cloud WAAP solution includes advanced, end-to-end API protection as part of Cisco's comprehensive web application security architecture. This fully automated solution helps ensure the security of applications, APIs, development platforms, and infrastructure. It maps the API attack surface by leveraging an automated deep discovery algorithm to discover API endpoints and their full structure and generates customized security policies to detect and block API-focused attacks in real time. By automatically and continuously learning and mapping the application API business logic, our API protection solution can create alerts and block business logic attacks on APIs. The solution also uses a combination of access controls, data leakage prevention, bot management, and denial-of-service (DoS) mitigation tools to protect against a growing array of API security threats listed in the OWASP API Security Top 10.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bot management

Our industry-leading bot management and mitigation solution, which is included with and integrated into Cisco Cloud WAAP, accurately detects bot activity and intelligently distinguishes between human traffic, beneficial bots, and malicious bots. Bot management provides comprehensive protection of web applications, mobile apps, and APIs from sophisticated AI-driven, automated bots and other security threats.

The solution provides robust and precise bot management across web, mobile, and API traffic by applying proactive, AI-based protection comprising three layers: preemptive protection, behavioral-based detection, and advanced mitigation.

Cisco bot management preemptively blocks unwanted identities, using unique capabilities such as AI-based cross-correlation, JavaScript validation, and mobile attestation for Android and iOS devices. These, along with its proprietary secure identity engine, stop bot attacks on web and mobile apps before they can impact your infrastructure and your business.

The solution employs advanced AI-based technologies such as behavioral modeling (granular intent analysis), behavioral-based detection (discovery of sophisticated bot evasion behavior such as rotating IPs and identities), distributed attack detection, machine learning-based anomaly detection, and browser and device fingerprinting. It is also capable of detecting third-party CAPTCHA-farm services.

It protects against all 21 OWASP Top Automated Threats, including account takeover, credential stuffing, brute force, denial of inventory, DDoS, ad and payment fraud, and web scraping to help organizations safeguard and grow their online operations.

In addition, Cisco bot management provides the widest choice of mitigation options, including a blockchain-based cryptographic challenge that exhausts the malicious bot resources while making for a seamless and CAPTCHA-free user experience.

Web DDoS protection

Cisco Cloud WAAP also includes industry-leading application-layer (Layer 7) protection against DDoS attacks using unique machine learning-based behavioral detection that accurately distinguishes between legitimate and malicious traffic and automatically generates granular signatures in real time to protect against zero-day attacks.

The Cloud Web DDoS Protection Service provides best-in-class security against a wide variety of threats, including HTTP floods, HTTP bombs, low-and-slow assaults, brute force attacks, and disruptive web DDoS tsunami attacks, and can be deployed as a cloud always-on service, a cloud on-demand service, or a hybrid deployment (on-premises with diversion to the cloud).

Contact your Cisco sales representative for more information about deployment options.

© 2025 Cisco and/or its affiliates. All rights reserved.

Client-side protection

Client-side protection is security designed to safeguard data, applications, and processes on the user's device, also known as the client side. Client-side protection prevents data breaches, unauthorized access, malware injection, and code tampering. Client-side protection is required for compliance with PCI DSS 4.0 and the protection of end-user data when interacting with third-party services in the application supply chain.

Client-side protection in Cisco Cloud WAAP provides the following:

- Blocks requests to suspicious third-party services in the supply chain, enhancing compliance with data security standards.
- Protects against client-side attacks coming from third-party JavaScript services (such as formjacking, skimming, and magecart).
- Automatically and continuously discovers all third-party services in your supply chain while providing detailed activity tracking, alerting, and threat-level assessment based on multiple indicators, including script source and destination domain.
- Prevents data leakage by blocking unknown destinations and legitimate destinations with illegitimate parameters, as well as DOM-based cross-site scripting (XSS).
- Uses surgical enforcement capabilities that allow client-side protection to block only nefarious scripts without interfering with vital JavaScript services.

Emergency Response Team Active Attackers Feed

The ERT[2] Active Attackers Feed (EAAF) serves as your own network intelligence agency. It enhances the protection of applications and data centers by introducing a preemptive protective layer on top of the Cloud WAAP attack mitigation solution. The EAAF feed propagates a list of attackers that have been involved in recent security incidents, such as DDoS attacks, application attacks, intrusions, or scanning attacks. This enables the platform or service to preemptively block known attackers before they can threaten your assets and initiate an attack.

2. Emergency Response Team support, Threat Intelligence Service, SecurePath, and other industry-leading security solutions are provided by Radware through its OEM partnership with Cisco.

© 2025 Cisco and/or its affiliates. All rights reserved.

Threat Intelligence Service

The Threat Intelligence Service[2] provides visibility into why certain IPs are flagged, providing invaluable insights and context in real time. The actionable intelligence allows you to confidently assess threats, facilitates informed decision making, and enables organizations to proactively defend against threats before they escalate. Whether it's blocking a suspicious IP, fine-tuning your defenses, or identifying compromised systems, the Threat Intelligence Service will enhance your organization's security.

Key features of the Threat Intelligence Service include:

- Actionable data from real cyberattacks
- Research into any suspicious IP address with IP insights, open proxies, and malware data
- Reputation alerts that enhance network security and integrity by sending proactive, timely alerts of potential cyberattacks originating from the organization's own network
- Seamless REST API integration to any environment, existing security workflows, and systems

AI-based cross-module correlation

AI-driven threat analysis algorithms preemptively and automatically block malicious sources across all applications within an account.

By cross-correlating security events in real time from all active protection modules (WAF, API protection, and bot management) across your organization's chosen applications, the AI-based Correlation Engine assigns each source a penalty score based on the number, type, and severity of the source IP's security events. Once a penalty score crosses a threshold, the malicious source IP is instantly and automatically blocked in all enabled apps for a set duration, whether it attacked one or more applications. This unique way of analyzing the source IPs' malicious behavior and blocking them as needed adds a highly accurate proactive protection layer to your security strategy. It prevents incoming bad traffic from overloading your application server and reduces overhead to your application infrastructure and security management costs.

Global cloud application protection network

Cisco Cloud Application and API Protection leverages Radware's global network of distributed application security points of presence (PoPs) and DDoS mitigation scrubbing centers.

With locations at major traffic hubs connecting to Tier 1 ISPs, and a global mitigation capacity of 15 Tbps, our cloud network provides protection close to your origin server to help ensure low latency and minimal impact on web application performance.

2. Emergency Response Team support, Threat Intelligence Service, SecurePath, and other industry-leading security solutions are provided by Radware through its OEM partnership with Cisco.

© 2025 Cisco and/or its affiliates. All rights reserved.

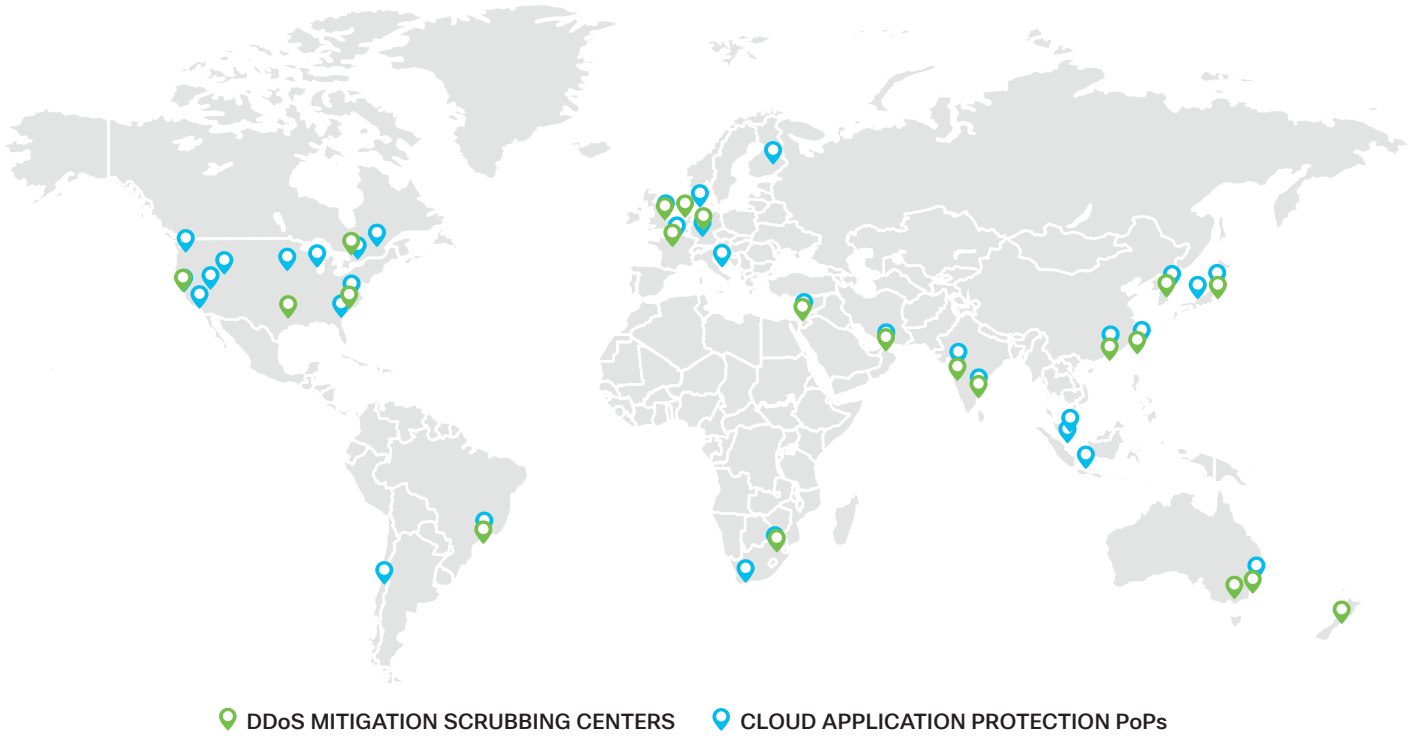


Figure 2. Locations of DDoS mitigation scrubbing centers and cloud application protection PoPs

Application protection for any cloud with Radware SecurePath

SecurePath[2] is an innovative, API-based cloud application security architecture designed for optimal protection of applications deployed across any cloud or data center — on-premises or in private or public cloud environments — while maintaining consistent, high-grade, and comprehensive protection.

SecurePath allows application protection services to be deployed inline, where they serve as a "middleman," or an API-based, out-of-path service. This deployment enables application requests to go directly from the client to the application server without interruption. This innovative approach provides many advantages, including:

- Reduced latency: A consistent, high level of security is provided without the inline latency.
- No key sharing: With no SSL certificate sharing, certificates are managed solely at the origin, making them more private, more efficient, faster to deploy, and easier to maintain.
- No traffic redirection: There is no need for DNS or Border Gateway Protocol (BGP) routing changes to ensure protection. Requests go from the client directly to the application server. Only copies of important transaction parameters are sent to the application protection cloud for inspection.
- Increased uptime: Since traffic is not inspected inline, customers are not impacted by overloads or outages.
- No bottlenecks: Latency thresholds can be set to avoid congestion.

© 2025 Cisco and/or its affiliates. All rights reserved.

Application protection and the content delivery network: The best of both worlds

For customers who wish to combine their web application security with their website delivery, Cisco's partner Radware offers an integrated content delivery network (CDN) solution integrated directly into the Cloud WAAP application security stack and management portal. The CDN solution is based on the Amazon CloudFront CDN and provides a massive, globally distributed footprint, enhanced performance, and DevOps-friendly usability. The integrated CDN offering is built directly into the Cloud WAAP portal for unified management and reporting — all from a single dashboard.



Figure 3. Locations of Amazon CloudFront CDN PoPs

Key features include:

- Massive capacity, based on the AWS network
- Global footprint with over 600 points of presence in more than 100 cities across more than 50 countries
- Unified management within the Cloud WAAP portal
- Single SSL key (the same as the one used for WAF)
- Advanced metrics and reporting
- Cost-effectiveness
- Super-fast operation (faster than most CDN providers; see www.cdnperf.com/)
- Managed services for peace of mind with lower total cost of ownership (TCO)

© 2025 Cisco and/or its affiliates. All rights reserved.

Managed application protection

The ERT[2] members are highly trained security experts who provide proactive security support services 24x7x365 for customers facing an array of application-layer (Layer 7) and network-layer (Layers 3 and 4) attacks. Powered by Radware's Threat Research Center, ERT engineers identify and mitigate security threats, providing industry-leading security expertise and intelligence that allows customers to realize the full benefit of Cisco Cloud WAAP, even when lacking in-house application protection expertise.

Load Balancer as a Service

Integrated into the Cloud WAAP service, Load Balancer as a Service (LBaaS) addresses the evolving needs of modern IT infrastructures. With a range of features aimed at simplifying configuration and boosting efficiency, all load balancer configurations are consolidated in one central place. This gives users a seamless, convenient management experience and empowers them with more control over their load-balancing requirements.

LBaaS complements Cloud WAAP by offering improved service-level agreements (SLAs) and scalability while maintaining high availability and protecting all origin sites. It provides continuous automatic origin-server status health checks, active/active traffic, user load balancing between origin sites, and URL-based server load balancing to optimize resource access and server performance. It delivers advanced persistency capabilities, including IP persistency, to help ensure consistent network connectivity by maintaining a constant IP address for the device or user and cookie-based persistency to help ensure a personalized and consistent user experience across visits by retaining cookies in the user's web browser.

DNS as a Service

Cisco DNS as a Service (DNSaaS) provides comprehensive DNS management, which is crucial for the seamless functioning of any online application. By leveraging DNSaaS, Cisco Cloud WAAP customers can be assured that their applications remain protected, available, and performant.

Fully integrated into the Cloud WAAP portal, the DNSaaS centralized management console provides an easy-to-use interface for managing all DNS hosts, records, and health check configurations in one place. With control over traffic distribution to specific resources and endpoints in addition to real-time analytics and monitoring, Cisco DNSaaS improves latency and helps ensure that end users enjoy a seamless experience.

2. Emergency Response Team support, Threat Intelligence Service, SecurePath, and other industry-leading security solutions are provided by Radware through its OEM partnership with Cisco.

© 2025 Cisco and/or its affiliates. All rights reserved.

Summary

Cisco Cloud Application and API Protection allows organizations to manage and scale application security as the business grows, evolve application architectures, and expand cloud environments and services. It provides:

Comprehensive protection

- A one-stop shop for application protection solutions: WAF, bot management, API, client-side protection, and web DDoS protection.

AI-powered intelligent security

- Comprehensive coverage against known threats and zero-day attacks using advanced, patented AI and machine learning-based behavioral analysis technology.

Reduced overhead and lowered mean time to resolution (MTTR)

- AI-powered adaptive protection with automatic analytics and policy optimization, managed services, and 24x7 support through Radware's ERT.

Centralized management and reporting

- One location to manage and monitor the security of your applications, no matter where they are deployed.

Flexible deployment and compatibility

- Ability to maintain the same level of protection across any environment: on-premises, virtual clouds, private clouds, public clouds, multiclouds, hybrid environments, or Kubernetes.

Compliance with privacy and security standards

- Holistic application protection solution with specific controls, visibility, and reports to comply with security standards such as PCI DSS 4, GDPR, HIPAA, NIS2, and DORA.

Support for informed decisions with real-time threat intelligence

- Ability to research any IP address to shed light on its origin and legitimacy and transform uncertainty into clarity.

SecurePath® is a registered trademark of Radware.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. 3/25