

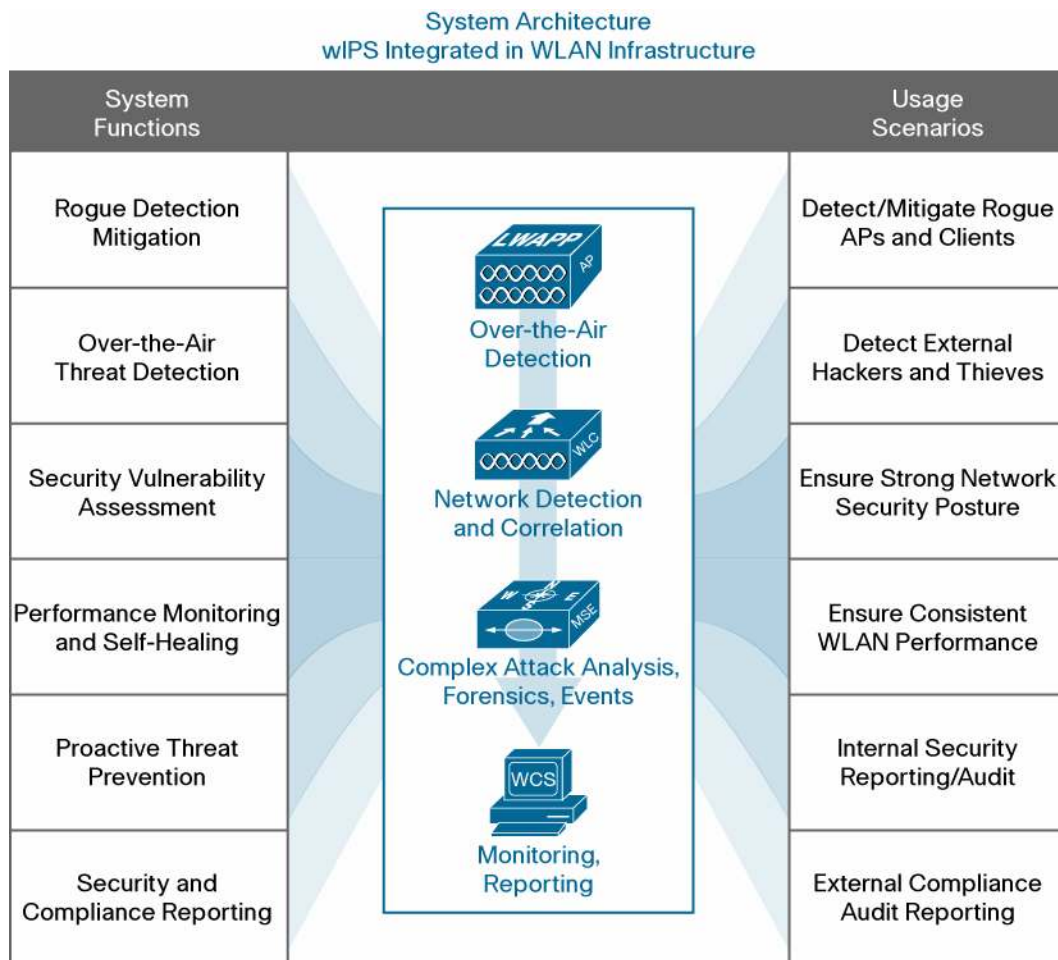
Cisco Adaptive Wireless Intrusion Prevention System

Product Overview

The wireless spectrum is a new frontier for many IT organizations. Like any other networking medium, the wireless spectrum must be properly secured, even if wireless networking is not deployed on site.

The Cisco® Adaptive Wireless IPS (wIPS) is integrated in the Cisco Unified Wireless Network infrastructure and provides wireless-specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption. Cisco Adaptive wIPS (Figure 1) provides the ability to detect, analyze, and identify wireless threats, and centrally manages mitigation and resolution of security and performance issues. Cisco Adaptive wIPS also delivers proactive threat prevention capabilities for a hardened wireless network core that is impenetrable by most wireless attacks, as well as the ability to collaborate with the Cisco Self-Defending Network security portfolio to provide a superset of layered threat protection for both the wired and wireless network.

Figure 1. Cisco Adaptive Wireless IPS: System Overview



Feature Overview

Cisco Adaptive wIPS embeds complete wireless threat detection and mitigation into the wireless network infrastructure to deliver the industry's most comprehensive, accurate, and operationally cost-effective wireless security solution. Adaptive wIPS performs: rogue access point and client and ad hoc connection detection and mitigation, over-the-air wireless hacking and threat detection, security vulnerability monitoring, performance monitoring and self-optimization, network hardening for proactive prevention of threats, and complete wireless security management and reporting. Built on the Cisco Unified Wireless Network and taking advantage of the efficiencies of Cisco Motion, Adaptive wIPS is deployment-hardened and enterprise-ready.

The Power of Integration in the Wireless Network Infrastructure

Cisco Adaptive Wireless IPS is integrated directly into infrastructure components of the Cisco Unified Wireless Network, including Cisco wireless LAN controllers, Cisco access points, the Cisco Mobility Services Engine, and the Cisco Wireless Control System. This integrated wireless threat detection and prevention reduces costs, streamlines operations, and provides comprehensive protection.

Integration of wireless IPS into the WLAN infrastructure offers more than just the cost and operational efficiencies delivered by using a single infrastructure for both wireless IPS and WLAN services. Integration into the infrastructure enables a superset of functionality not architecturally possible with standalone, overlay wireless IPS systems. New functionality delivered by the infrastructure-integrated architecture of Cisco Adaptive wIPS allows network administrators to:

- **See the whole picture:** Typical wIPS solutions rely solely on RF air monitoring for detection. Adaptive wIPS builds on RF air monitoring by employing network traffic and anomaly analysis within the access points and WLAN controllers, as well as real-time device inventory analysis and network configuration analysis to detect threats and monitor performance. This approach delivers more accurate and thorough detection.
- **Take corrective action:** Cisco Adaptive wIPS doesn't just detect threats, vulnerabilities and performance issues; it makes it possible to take corrective action. Integration in the WLAN infrastructure enables Adaptive wIPS to go beyond passive monitoring and reach into the infrastructure to fix security threats and performance issues, and to do so in real time.
- **Take advantage of the entire WLAN footprint:** Adaptive wIPS can use all the access points in the network for location and mitigation of rogue devices. This increases location accuracy and mitigation scalability.
- **Benefit from flexible deployment architectures:** Cisco Adaptive wIPS can use access points dedicated to full-time air-monitoring or access points serving WLAN users. This deployment flexibility enables right-sized security models on a site-specific basis.

Comprehensive Protection, Accurate Detection

Cisco's advanced approach to detection, combining air monitoring, network traffic and anomaly analysis, real-time network device and topology information, and network configuration analysis, delivers a comprehensive view of the event to the Cisco Adaptive wIPS analysis engine. With that breadth of information, Adaptive wIPS detects events not traceable with over-the-air signatures alone and makes more accurate detection decisions, thus increasing effectiveness while reducing false positives.

Building upon the core detection capabilities, Cisco Adaptive wIPS delivers rich attack classification, providing users with flexible rules for automatically classifying and mitigating security events. Automatic classification, coupled with the system's inherent accuracy, greatly reduces the operational expenses associated with manual investigation of potential threats detected by the system.

Cisco couples these advanced detection and classification techniques with an extensive attack, vulnerability, and performance detection library. Examples of event classes detected include: rogue access points/clients, ad hoc connections, hacker access points such as honeypots and evil twins, network reconnaissance, authentication and encryption cracking, man-in-the-middle attacks such as address/identity spoofing and replay attacks, protocol attacks, denial-of-service (DoS) attacks, over-the-air and network security vulnerabilities, and performance issues such as co-channel interference and coverage holes.

Complementing Adaptive wIPS with Proactive Threat Prevention

The best way to secure your network is to design a system that prevents an attack before damage can be done. Network security hardening features embedded in the Cisco Unified Wireless Network complement the Adaptive wIPS solution to provide the following proactive threat prevention techniques:

- **Remove security offenders from the network:** Client exclusion policies can automatically respond to high levels of user authentication failures and IP address spoofing.
- **Defuse network reconnaissance, spoofing, and man-in-the-middle attack:** Cisco Management Frame Protection, the basis for IEEE 802.11w, encrypts and authenticates WLAN management frames to defend against many common over-the-air attacks.
- **Protect against data theft:** Strong user authentication and Wi-Fi Protected Access 2 (WPA2) and 802.11i encryption standards protect access to your network and data traversing the WLAN.
- **Lock out rogue access points:** Using 802.1X wired port authentication on Cisco access points virtually eliminates the possibility that a rogue access point will join the wired network.

Features and Benefits: Technical Overview

The sections below outline each functional area of the Cisco Adaptive Wireless IPS solution and the associated benefits.

Rogue Detection, Classification, and Mitigation

Cisco Adaptive Wireless IPS features rogue detection and mitigation functionality as shown in Table 1. Rogue access points and clients can create backdoor access to your network and can be used for data theft from your wireless clients. Adaptive wIPS detects, auto-classifies based on customizable rules, and mitigates rogue access points, rogue clients, spoofed clients, and client ad hoc connections.

Table 1. Features and Benefits: Rogue Detection, Classification, and Mitigation

Feature	Benefit
Detection	
On/Off-Channel Scanning	Detects rogue access points, rogue clients, spoofed clients, and client ad hoc connections on all channels in 802.11-related spectrum
Signature-Based and Network	Increases breadth and accuracy of rogue, ad hoc, and spoofing detection, thus

Feature	Benefit
Analysis-Based Detection	decreasing manual threat investigation by staff
Spectrum Intelligence	Detects rogue devices and denial of service in non-802.11 frequencies, such as Bluetooth, radar, and microwave
Event Classification	
Customizable Rogue Event Auto-Classification	Auto-classifies the threat level of rogue events-based user-defined classification rules, thus reducing staff intervention
Rogue Switch-Port Tracing	Establishes if a detected rogue access point is on the customer network, thus reducing manual staff investigation to assess the threat
Physical Location of Rogue	Plots rogue access points and clients on a floor map, thus helping assess the rogue threat and facilitate removal
Mitigation	
Rogue Switch-Port Disable	Remotely disables Ethernet port to which a rogue access point is connected, thus speeding mitigation
Over-the-Air Mitigation	Mitigates rogue access points, clients, and ad hoc over-the-air connections using any Cisco access point deployed, thus speeding and scaling mitigation
Automatic or Manual Mitigation	Flexible mitigation actions enable tailoring to customer risk environment and operational model

Over-the-Air Attack Detection

Cisco Adaptive wIPS features over-the-air attack detection functionality as shown in Table 2. Over-the-air attacks are spawned by hackers adjacent to your RF environment. Since RF signals penetrate walls, an attacker could be someone sitting in the parking lot in front of your office. Attack types include network reconnaissance, authentication and encryption cracking, denial of service, man-in-the-middle, impersonation attempts, and new/unknown attack techniques.

Table 2. Features and Benefits: Over-the-Air Attack Detection

Feature	Benefit
Breadth of Attack Detection	
Network Reconnaissance and Profiling Detection	Analyzes traffic behavior and performs pattern matching to detect tools and techniques such as Netstumbler, Wellenreiter, Kismet, honeypot access points, and other methods, providing an early alert that a hacker is looking for avenues of attack
Authentication and Encryption Cracking Detection	Analyzes traffic behavior and performs pattern matching to detect tools and techniques such as AirSnarf, AirCrack, ASLEAP, Chop-Chop, and other methods, providing an alert of potential or attempted data theft
Malicious or Inadvertent Denial of Service Detection	Analyzes traffic behavior and performs pattern matching to detect tools and techniques such as 802.11 protocol abuse, AirJack, RF jamming, resource starvation, and other methods, providing an alert of potential or attempted network service disruption
Man-in-the-Middle Attack Detection	Analyzes traffic behavior, performs pattern matching and authentication methods to detect tools and techniques such as replay attacks, fake access points, 802.11 protocol manipulation, and other methods, providing an alert of potential data theft or unauthorized network access
Impersonation and Spoofing Detection	Analyzes traffic behavior, performs pattern matching and authentication methods to detect tools and techniques such as MAC/IP spoofing, fake access points, evil-twin access points, Dynamic Host Configuration Protocol (DHCP) spoofing, and other methods, providing an alert of potential data theft or unauthorized network access
Zero-Day Attack Detection	Analyzes traffic behavior to detect newly introduced or previously uncategorized attack methods, providing an alert of a potential threat
Ongoing Threat and Vulnerability Research and Detection Development	Cisco has a wireless threat and vulnerability research team dedicated to finding out about new attack techniques, as well as proactively analyzing the network for vulnerabilities that could be exploited; the research team helps ensure that Cisco Adaptive wIPS detection capabilities stay ahead of the threat horizon
Event Classification and Tuning	
Default Detection Profiles	Default detection tuning profiles, customized by customer type, enable effective operation minutes after system startup and provide a head start in system tuning
Knowledge Base-Driven Tuning	Detection tuning is tied to a threat knowledge base in WCS, giving operators plain-language descriptions of attack types and detection methods as well as tuning guidance, thus making tuning easier even for novice security operators

Security Vulnerability Monitoring

Cisco Adaptive wPS features security vulnerability monitoring functionality (Table 3).

Understanding the security posture of the wireless network in real time is the most important aspect of attack prevention. Cisco WCS management system automatically performs automated 24/7 wireless vulnerability monitoring and assessment by proactively and persistently scanning the wireless network for weak security or out-of-policy configurations.

Table 3. Features and Benefits: Security Vulnerability Monitoring

Feature	Benefit
Automated, 24/7 Configuration Analysis	Analyzes all wireless controller, access point, and management interface security configurations; by analyzing actual configurations rather than relying solely on over-the-air vulnerability sniffing, the WCS delivers greater accuracy and depth of vulnerability analysis, such as analysis of management protocol security and analysis of security services operating on the network
Analyze Against Industry Best Practices or Customer-Specific Security Policies	WCS is prepopulated with industry best practices for wireless security vulnerability assessment; using the WCS Config Audit functionality, customers can also analyze configurations against their own specific security policies; this dual approach enables the greatest flexibility and breadth of vulnerability analysis
Broad Vulnerability Identification	Identifies vulnerabilities that can result in unauthorized management and network access, data theft, man-in-the-middle attacks, DoS attacks, and protocol attacks, and also advises on security services to run on the wireless network

Performance Monitoring and Auto-Optimization

Cisco Adaptive wPS features performance monitoring functionality as shown in Table 4. A poor performing network affects network and application availability and can be a result of malicious or accidental means. Utilizing radio resource management (RRM), the system provides unmatched performance and network self-healing. Information about noise and interference, as well as client signal strength and other data, is used to dynamically assign channels and adjust access point transmit power in real time to avoid co-channel interference, to route around failed devices, and to minimize coverage holes.

Table 4. Features and Benefits: Performance Monitoring and Auto-Optimization

Feature	Benefit
Continuous Real-Time Monitoring of Network Health and Performance	Defends against over-the-air interference, malicious or accidental
Automatically Fixes Problems in the RF Domain	Remedies issues, such as RF-based denial of service, without administrator intervention, thus increasing network uptime with minimal operational overhead
Complete RF Management without Specialized RF Skills	RF management expertise built into the system, thus reducing the burden on operational staff

Management, Monitoring, and Reporting

Cisco Adaptive wPS features complete security management, monitoring, and reporting functionality as shown Table 5. wPS management is fully integrated into the Cisco WCS, providing a single, unified tool for both wireless network and wireless security operations.

Unification of wireless network and wireless security management reduce challenges by keeping access point and client device inventories and security policies aligned, as well as by simplifying event management and reporting.

Table 5. Features and Benefits: Management, Monitoring, and Reporting

Feature	Benefit
Single Management Platform for Wireless Network and Security	
Real-Time Device Inventories	Access point and client device inventory is always up-to-date, with no double-entry or cross-vendor management integration issues, thus enabling high accuracy in rogue detection while minimizing administrative overhead
Virtualized Management Domains	wIPS enables split wireless security management and monitoring from other wireless management roles or geographies
No One-Off Management Platforms	All wIPS and general wireless management is performed from WCS, thus minimizing staff training and support on disparate platforms
Integrated with Cisco Unified Wireless Network Features	wIPS provides unified workflows integrating general wireless network configuration, wireless security policy definition, and location service operation
Command Authorization and Audit Trails	All management commands can be authorized by authentication, authorization, and accounting (AAA); configuration, investigation, and mitigation actions logged can be traced back to the administrator, enabling accountability
Designed for Enterprise Scalability	WCS is designed for the highest-scale environments: up to 3000 user-serving or wIPS access points per WCS instance
WCS Security Dashboard	
Single, At-a-Glance View	Single screen summary of all security events and vulnerabilities presented in a streamlined, at-a-glance format; ability to drill-down on classes of events and individual events with a mouse click; eases day-to-day monitoring
Wired Security Integration	Malware and hacking events associated with wireless users can be monitored from WCS Security Dashboard, thus providing a network-wide view of wireless user activity
WCS Performance (RRM) Dashboard	
Single, At-a-Glance View	Single screen summary of all performance-related events presented in a streamlined, at-a-glance format; ability to drill-down on classes of events and individual events with a mouse click; eases day-to-day monitoring
WCS Event Management and Reporting	
Complete Event Forensics	Captures all traffic associated with an attack for ease of attack investigation
Event Escalation to Staff	Automatically alerts staff regarding critical events, thus decreasing response time; fully customizable by event type
Per-Admin Reports	Historical reports can be customized for individual administrators based on their preferences and area of responsibility, thus streamlining event analysis
Report Auto-Scheduling	Historical reports can be scheduled to run automatically at specific times, thus streamlining workflows
Payment Card Industry (PCI) Reporting	Historical reports may be customized for events pertinent to Payment Card Industry (PCI) compliance, thus streamlining audit-related activities
Event Storage and Archiving	Security attack events are stored in the Cisco Mobility Services Engine for long-term archiving, thus streamlining historical analysis

Deployment Components, Scalability and Platform Support

Standard components of a Cisco Adaptive wIPS are:

- Cisco LWAPP access points for wIPS monitoring
 - Cisco Aironet® 1130 AG, 1140, 1240 AG, and 1250 Series Access Points support Cisco Unified Wireless Network Version 5.2 and later and the Adaptive wIPS feature set
- Cisco Wireless LAN Controllers to serve wIPS monitoring access points
 - Cisco 2100 Series Wireless LAN Controller, Cisco 4400 Series Wireless LAN Controller, Cisco 5500 Series Wireless LAN Controller, Cisco Wireless Services Module for Cisco Catalyst® 6500 Series, Cisco Catalyst 3750G Integrated WLAN Controller, WLAN Controller Network Module for Cisco 2800 and 3800 Series Routers
 - Cisco Unified Wireless Network Version 5.2 and later supports the Adaptive wIPS feature set

- Cisco Mobility Services Engine 3310 Series and Cisco Adaptive wIPS software license using Cisco Unified Wireless Network Version 5.2 or later for support of the Adaptive wIPS feature set. Multiple mobility services can coexist with Cisco Adaptive wIPS on the same MSE 3310 when using the Cisco Unified Wireless Network Version 6.0 or later.
 - Up to 2000 wIPS access points can be served by a single Mobility Services Engine
- Cisco Mobility Services Engine 3350 Series and Cisco Adaptive wIPS software license using Cisco Unified Wireless Network Version 6.0 or later for support of the Adaptive wIPS feature set. Multiple mobility services can coexist with Cisco Adaptive wIPS on the same MSE 3350.
 - Up to 3000 wIPS access points can be served by a single Mobility Services Engine
- Cisco WCS Version 5.2 or later for management, configuration, and reporting
 - Up to 3000 wIPS or user-serving access points can be served by a single WCS instance
 - A Mobility Services Engine is managed by only one WCS instance at a time; this should be considered in overall network scalability design
 - A single WCS instance can manage multiple Mobility Services Engines at a time

Licensing and Ordering Information

Cisco Adaptive wIPS in Cisco Unified Wireless Network Version 5.2 or later is a licensed software feature set on the Cisco Mobility Services Engine. Table 6 shows the license levels available for Adaptive wIPS. These license levels may be combined in any permutation to arrive at the count of access points you need to run Adaptive wIPS. For example, combining a five access point and a 25 access point license yields a license to run Adaptive wIPS on 30 access points.

Table 6. Cisco Adaptive Wireless IPS Software Licenses

Part Number	Description
AIR-WIPS-AP-5	Adaptive wIPS Software License: Supports 5 Cisco Monitor-Mode Access Points
AIR-WIPS-AP-25	Adaptive wIPS Software License: Supports 25 Cisco Monitor-Mode Access Points
AIR-WIPS-AP-100	Adaptive wIPS Software License: Supports 100 Cisco Monitor-Mode Access Points
AIR-WIPS-AP-500	Adaptive wIPS Software License: Supports 500 Cisco Monitor-Mode Access Points
AIR-WIPS-AP-2000	Adaptive wIPS Software License: Supports 2000 Cisco Monitor-Mode Access Points

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, visit [Cisco Technical Support Services](#) or [Cisco Advanced Services](#).

For More Information

For more information about Cisco Adaptive wIPS, visit <http://www.cisco.com/go/WIPS>.

For more information about the Cisco Self-Defending Network, visit <http://www.cisco.com/go/SDN>.

For more information about the Cisco Mobility Services Engine, visit <http://www.cisco.com/go/MSE>.

For more information about the Cisco Unified Wireless Network, visit <http://www.cisco.com/go/wireless>.



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, COBNT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumina, 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, CCDE, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco ICS, 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, FrameShare, GigaDrive, HomeLink, Internet Quotient, IOS, IPPhone, IQDisk Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanel, ProConnect, SmartShore, 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. (081216)

