

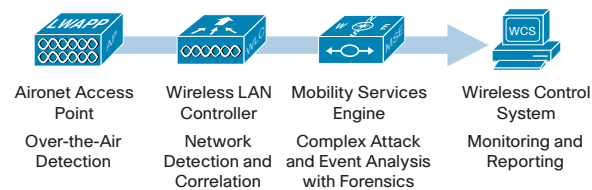
The Cisco Adaptive Wireless Intrusion Prevention Solution

The Cisco® Adaptive Wireless IPS (wIPS) solution 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.

The Value of the Cisco Adaptive Wireless Intrusion Prevention System

The Cisco® Adaptive Wireless IPS (wIPS) is integrated into the infrastructure of the Cisco Unified Wireless Network. Using the WLAN infrastructure to detect, mitigate and report on malicious attacks, security vulnerabilities, and sources of performance disruption increases the accuracy and thoroughness of the solution. At the same time, the solution simplifies network deployment and operations by taking advantage of standard Cisco Aironet® Access Points, Cisco WLAN Controllers, the Cisco Mobility Services Engine, and the Cisco Wireless Control System (Figure 1)

Figure 1 Components of the Adaptive Wireless Intrusion Prevention System



Cisco's infrastructure-integrated 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. 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.

The Challenges of Securing a Wireless Network

The growth of wireless networking and the sheer number of new mobile computing devices have blurred the traditional boundaries between trusted and untrusted networks, and shifted security priorities from the network perimeter to information protection and user security. The need to secure information in motion and control the wireless environment to prevent unauthorized access must be a priority for maintaining the integrity of corporate information and systems. The need to secure the airwaves applies to both companies with wireless networking installed and to companies that want to ensure no unauthorized wireless is in use. These threats include:

- Rogue wireless access points or a variety of Wi-Fi-enabled clients can be innocently introduced by well-meaning staff or by outsiders with malicious intent, but in either case these clients create backdoor access to the company's network.
- Hacker access points that try to lure users into connecting to them for purposes of network profiling or stealing proprietary information.
- Denial-of-service attacks that disrupt or disable your wireless network.
- Over-the-air network reconnaissance, eavesdropping, and traffic cracking.

Recently, there have been highly publicized cases in which companies that neglected to secure their RF environment have found their customer financial data

exploited by hackers; these companies were publicly criticized and forced to pay large fines. While there is a lot to consider in wireless security, the good news is that all of these concerns are addressed by security technologies built into the Unified Wireless Network.

There have also been notable changes to regulatory compliance requirements with regard to Wi-Fi and security, and organizations will need to demonstrate compliance to certified auditing consultants. The security data gathered by both the Cisco Adaptive Wireless Intrusion Prevention System and the Cisco Unified Wireless Network can help not only secure the wireless network to meet regulations but also provide the information needed for auditors to certify compliance.

The Benefits of the Cisco Adaptive Wireless Intrusion Prevention System

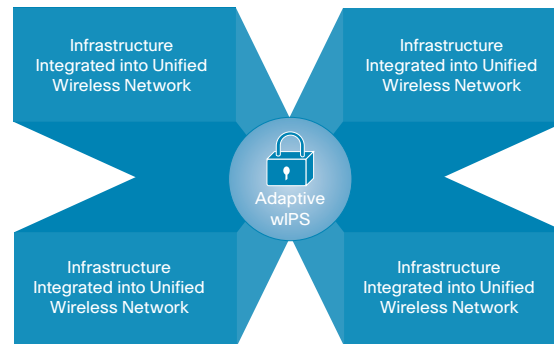
- **Comprehensive protection against wireless threats:** Identifies wireless attacks against your network, including rogues, network reconnaissance, authentication and encryption cracking, denial of service, man-in-the-middle, impersonation attempts, and zero-day or new, unknown attacks to provide comprehensive protection throughout the RF environment.
- **Streamlined threat response:** Multiple detection approaches and advanced classification techniques deliver highly accurate threat detection, minimizing time spent by staff investigating false alarms. Plain English descriptions of events and the threat they represent, flexible staff notification, and customizable rules with administrator-defined policies decrease the time to identify and manage threats.
- **Ongoing, up-to-date protection:** The automated vulnerability assessment and threat research library provide a wireless administrator with the knowledge needed to protect the wireless network without

being a security expert, and detection updates let Cisco stay on top of the threat environment for you.

- **No one-off equipment or management:** Cisco Adaptive wIPS uses the same Cisco Unified Wireless Network hardware and software to reduce training, administration requirements, and eliminate the costs of separate, single-purpose hardware.
- **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.
- **Integrated with Cisco Unified Wireless Network features:** A mobility services suite, including Context-Aware Mobility Service location tracking, Mobile Intelligent Roaming software, and client management provides unified workflows by integrating general wireless network configuration with wireless security policy definition.
- **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 to support the needs of any sized office or campus.
- **Designed for enterprise scale and management:** The Cisco Unified Wireless Network solution provides the scalability necessary to manage hundreds of Cisco Wireless LAN Controllers, which in turn can manage up to 30,000 Cisco Aironet Lightweight Access Points from a single management console. Adaptive wIPS utilizes the extensible Cisco Mobility Services Engine platform to achieve

the highest levels of security that will scale with the growing demands of your wireless network while providing a platform for performing advanced forensics and reporting that simplifies workflows and helps companies meet their compliance goals.

Figure 2 Feature summaries of the Cisco Adaptive wIPS



The Cisco Adaptive Wireless IPS Solution delivers the following key features and benefits:

- Detects and uses customizable rules to auto-classify rogue access points, rogue clients, spoofed clients, and client ad hoc connections. Uses administrator-defined mitigation policies that decrease the time to identify and manage rogue threats.
- Protects against over-the-air attack types including network reconnaissance, authentication and encryption cracking, denial of service, man-in-the-middle, impersonation attempts, and new/unknown attack techniques to provide comprehensive protection throughout the RF environment.
- Assesses wireless security vulnerabilities throughout the network by constantly monitoring the security posture of the wireless network in real time to prevent attacks before they can happen.

- Provides an extensive attack, vulnerability, and performance detection library provides a wireless administrator with the knowledge needed to protect the wireless network without being a security expert.
- Shields wired and wireless networks against wireless threats to enables businesses to meet compliance requirements as set forth by the Payment Card Industry (PCI), the Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA), and other regulations.

Why Cisco?

The Cisco Adaptive Wireless Intrusion Prevention System is a wireless security solution integrated into the network infrastructure to provide superior detection and attack prevention capabilities that protects both the wired and wireless network from wireless threats and attacks. Only Cisco can unify disparate networks and enable the delivery of secure wireless application access across networks to the right user with the right device while protecting the integrity of confidential information. Existing Wi-Fi architectures, while optimized for WLAN performance fall short of delivering the breadth of services required for an easy-to-manage, centralized approach to secure mobility applications deployment. With the Cisco Adaptive Wireless Intrusion Prevention Software, Cisco empowers IT to meet and exceed business mobility demands of their employees by delivering a secure open platform for the development of mobility applications.