Cisco Wireless Intrusion Prevention System

The Cisco® Wireless Intrusion Prevention System (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.

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. IT security concerns include rogue wireless access points creating backdoors, distributed denial-of-service (DDoS) attacks, over-the-air network reconnaissance, eavesdropping, traffic cracking, and the need to demonstrate industry compliance.

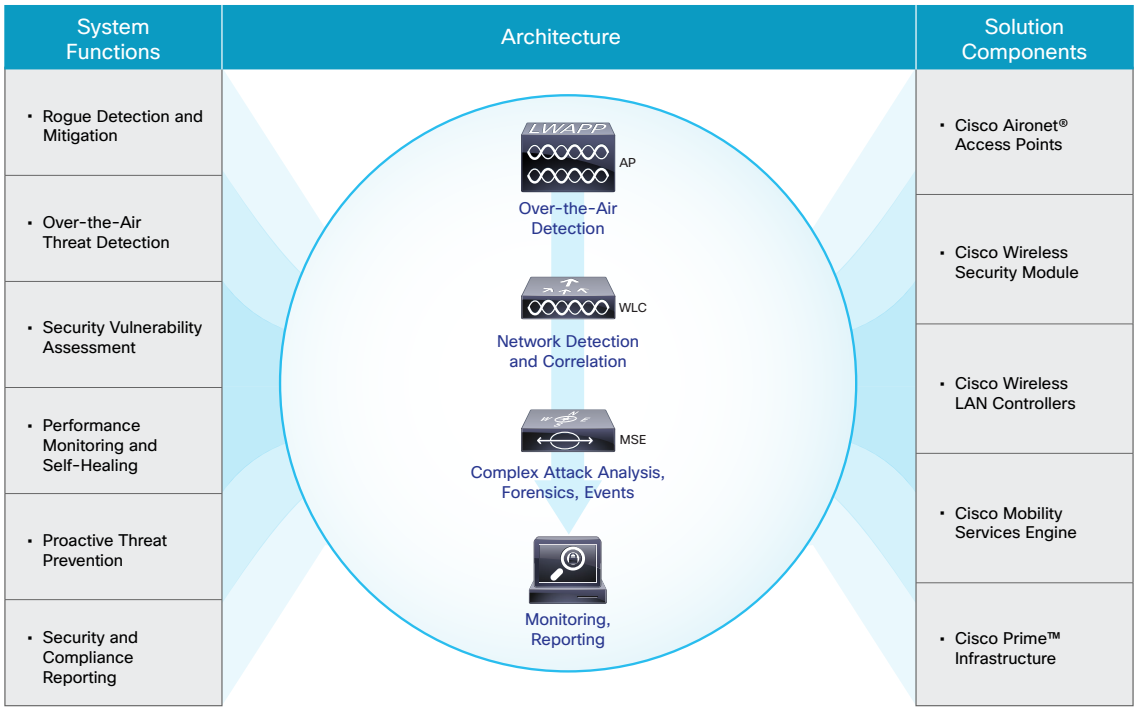
The Value of the Cisco wIPS Solution

The Cisco wIPS solution is a comprehensive wireless security solution that uses the Cisco Unified Access™ infrastructure to detect, locate, mitigate, and contain wired and wireless rogues and threats at Layers 1 and 2. Integration of wireless IPS into the WLAN infrastructure offers cost and operational efficiencies delivered by using a single infrastructure for both wIPS and WLAN services. The solution is made up of standard Cisco Aironet® access points, with the wireless security modules, Cisco wireless LAN controllers, the Cisco Mobility Services Engine, and Cisco Prime™ Infrastructure (Figure 1).

The Benefits of the Cisco wIPS Solution

The Cisco wIPS solution offers a superset of capabilities not architecturally possible with standalone, overlay wireless IPS solutions. The infrastructure-integrated architecture of Cisco wIPS allows network administrators to:

Figure 1. Components of Cisco wIPS



- **Provide comprehensive protection:** Cisco wIPS identifies and locates wireless attacks against your network, including rogues, network reconnaissance, authentication and encryption cracking, denial of service (DoS), man-in-the-middle, impersonation attempts, and zero-day or new, unknown attacks to provide comprehensive protection throughout the RF environment.
- **See the whole picture:** Cisco wIPS analyzes network traffic to detect anomalies and wireless attacks within the access points and WLAN controllers. It also tracks device inventory, audits network configuration, and monitors performance across the network.
- **Take corrective action:** Cisco wIPS doesn't just detect threats, vulnerabilities, and performance issues; it notifies the administrators about ongoing wireless threats, locates the attacker, captures relevant forensic data, and automatically launches countermeasures when possible.
- **Take advantage of the entire WLAN footprint:** Cisco wIPS can use all the access points in the network for detection, location, and mitigation of rogue devices. This increases location accuracy, reduces false positives, and results in faster mitigation.

- **Offer ongoing, up-to-date protection:** The automated vulnerability assessment and up-to-date threat library provide a wireless administrator with the knowledge needed to protect the wireless network without being a security expert.
- **Benefit from flexible deployment architectures:** Cisco wIPS can use access points dedicated to full-time monitoring, access points serving WLAN users while providing on-channel protection, or a dedicated wireless security module that provides security across 2.4 and 5 GHz without compromising data-serving radios.
- **Use a solution designed for enterprise scale and management:** Cisco Prime Infrastructure can manage hundreds of Cisco wireless LAN controllers and up to 15,000 Cisco Aironet access points. wIPS uses the Cisco Mobility Services Engine platform to locate wireless threats and correlates security events such as rogues, interferers, and active intrusions.

Feature Summary

Cisco wIPS delivers the following key features and benefits:

- **Rogue detection, location, classification, and mitigation:** wIPS detects, automatically classifies based on customizable rules, and mitigates rogue access points, rogue clients, spoofed clients, and client ad hoc connections.
- **Over-the-air attack detection:** wIPS identifies and locates wireless attacks against the network, including rogues, DoS attacks against valid clients and the network, man-in-the-middle attacks, impersonation attempts, and zero-day or new, unknown attacks.
- **Monitoring for security vulnerabilities:** wIPS automatically performs automated 24x7 wireless vulnerability monitoring and assessment by proactively and persistently scanning the wireless network for weak security or out-of-policy configurations.
- **Management, monitoring, and reporting:** wIPS is fully integrated into the Cisco Prime Infrastructure, providing a single, unified view for wired and wireless network management. Cisco Prime Infrastructure offers built-in industry compliance reports, such as those required for compliance with Payment Card Industry (PCI) 2.0 standards.

Why Cisco?

Only Cisco delivers a wireless intrusion prevention system that is deeply integrated into the Unified Access network infrastructure to provide superior detection, including location and attack prevention capabilities that protect both the wired and wireless network from wireless threats and attacks.

For more information, visit www.cisco.com/go/wips and www.cisco.com/go/mse.

C45-504521-01 10/13