

AIRDEFENSE WEP CLOAKING : Protection For Legacy Encryption Protocols

AirDefense WEP Cloaking™ provides protection for wireless infrastructure secured by legacy encryption protocols. This is an add-on module to AirDefense Enterprise, the market leading Wireless Intrusion Prevention System.

Protect WEP from being cracked

AirDefense WEP Cloaking is the first and only patented technology to protect retailers and other organizations using the Wired Equivalent Privacy (WEP) security standard to protect networks from common attempts used to crack encryption keys. Leveraging the AirDefense Enterprise platform, the WEP Cloaking module uses the same Enterprise sensors to continuously protect access points, laptops and portable data terminals, in use by many retailers, from passive and active attempts to crack WEP encryption keys. There are several freeware WEP cracking tools available and 23 known attacks against the original 802.11 encryption standard; even 128-bit WEP keys take only minutes to crack. AirDefense's WEP Cloaking module enables organizations to operate WEP encrypted networks securely and to preserve their existing investment in mobile devices. By placing AirDefense sensors in the vicinity of retailers' devices, AirDefense's patented WEP Cloaking technology renders popular cracking tools useless.

Ensure secure wireless and PCI compliance

Retailers and other companies handling credit card processing must comply with the security requirements adopted by the Payment Card Industry (PCI) to protect card holders from identity theft. Today, the majority of retailers across the United States continue to use the WEP standard to protect data on portable data terminals and other wireless devices. The Payment Card Industry's data security standard requires that WEP encrypted networks either be upgraded or supplemented with additional security. AirDefense's WEP Cloaking solution offers a new, cost-effective avenue for compliance. The AirDefense Enterprise solution already plays an important role verifying compliance of wireless security by providing compliance reports, forensic records of wireless activity and real-time notification of wireless intrusions. The addition of WEP Cloaking provides an entirely new dimension of protection that can act as the security supplement for WEP encryption.



WEP Cloaking

Avoid costly and time-consuming wireless infrastructure upgrades

The AirDefense WEP Cloaking module extends the shelf-life of existing and future WLAN infrastructure deployments. There are tens of thousands of legacy WEP devices already deployed, such as wireless scanners, portable data terminals, wireless POS, VoWLAN phones, and embedded Wi-Fi clients and many may not be firmware upgradeable to stronger encryption protocols. Although wireless security professionals have long known of the need to use technologies stronger than WEP, organizations may require months or years before such a change can be fully implemented. The cost of such upgrades can be in the millions. AirDefense's WEP Cloaking technology enables companies to preserve their existing and often considerable investment in wireless devices even after their security life-span has seemingly expired.

Benefits

- Tremendous cost savings by avoiding expensive hardware upgrades of existing WEP devices
- Meet PCI requirement for supplementing WEP encryption (PCI DSS 4.1.1)
- Enhance shelf-life of legacy and future wireless LAN infrastructure deployments