

Business Case for Independent Security in Modern Wireless Networks

Why is Dedicated Monitoring Required?

Unlike wired networks, wireless LANs (WLANs) do not have singular choke points through which all traffic flows. End-users, rogues and hackers can travel on any channel to most any network location. As a result, today's Wi-Fi security demands that you monitor all channels and all the physical airspace of your environment – "good enough" security is not an acceptable strategy to ensure wireless network integrity.

Furthermore, the vast majority of wireless threats simply can't be identified by simple threat signatures. Instead, they require a correlated analysis of multiple steps of intrusion and identity spoofing. Given that part-time scanning typically sees less than 1 percent of the total traffic in the environment, it is (a) doomed to completely ignore the vast majority of wireless client devices and (b) virtually impossible for this approach to detect real-world attacking behavior. Simply put, no WLAN security solution will be comprehensive if it doesn't observe and evaluate 100 percent of the traffic. Only a dedicated monitoring solution has the focus needed to monitor all channels, devices and behaviors, delivering complete WLAN security.

Wired security solutions inspect all traffic for threats.
How do you get that same level of security for Wi-Fi?

Wi-Fi Security Requirements:

- See all channels
- See all devices

Solution:
Dedicated Wi-Fi Monitoring

Integrated or Independent?

As WLANs have become more and more critical to the enterprise, dedicated Wi-Fi security has become a fundamental requirement. As a result, wireless AP vendors have recognized the importance of dedicated monitoring and rushed to integrate this level of security into their hardware by either using dedicated access points as sensors, or adding additional radios to an AP that can be used for security. This can seem like a convenient solution, but it also violates many of the security best practices that the networking industry has learned (often painfully) over the years. For example, by mixing security modules in the very device and infrastructure it is supposed to protect makes the "layered" security approach as weak as the entity it is supposed to be protecting. In addition, overloading infrastructure devices with security modules may be cost effective, but it compromises the performance of some network applications, such as voice. Let's examine these and others in more detail.

Defense-in-Depth – A fundamental concept of security in any form is to provide multiple layers of protection between the untrusted world and an organization's assets. In our homes we may use a combination of deadbolt locks, a security system and friendly neighbors that look out for one another.

They all approach security in a different way, and one does not obviate the need for the others. The same is true of our enterprise networks where we employ combinations of encryption, firewalls, intrusion detection systems, NAT and a host of other technologies. The key is that we spread these technologies across the infrastructure such that if one component fails in its security task, others are there to provide another layer of protection. An independent, dedicated monitoring system is the most comprehensive approach to delivering a “defense-in-depth” approach by providing layers of full visibility and threat response that sits between the outside world and the actual network infrastructure.

Integrated Security vs. Reliability – Using a single AP to perform both data services and dedicated security is simply a bad idea and violates a host of security best practices. Power and processing issues are already an area of concern for 802.11n access points. Adding an additional full-time radio that will need to scan constantly could considerably spike the power, memory and processing requirements of the AP. This could mean that security functionality would actually rob your network of performance and even run the risk of causing the AP to fail by requiring more power than is available via PoE. Even worse, this effect gets more pronounced as the WLAN gets busier.

Therefore, as the activity in the network goes up, your reliability goes down. Furthermore, consider what happens in the event the WLAN fails. An integrated radio system will be completely blind, whereas an autonomous, independent solution can show you exactly what is happening while continuing to protect your end-users and enforce your policies. Some sources would have you believe an integrated security approach for wireless is “good enough security.” But, don’t be fooled; integrated, time-slicing approaches cannot handle the depth of alarms and/or complex attacks that come in over time.

Vulnerabilities – APs simply must be visible to the network or they can’t do their job. By physically tying the security layer into the infrastructure, you are effectively advertising a weakness to any hacker – they can simply DoS the AP in a way that overloads the AP resources, and they know that the WIDS system is blind. This is a more aggressive illustration of the point above, but it is also a key reason that the security management layer is always separated from the thing it is trying to protect.

Infrastructure Independence - It is increasingly common for a single enterprise to leverage multiple vendors and legacy wireless equipment in their wireless environments. Integrated security systems give multiple silos of information on the environment, but no way of coordinating these mixed environments. Additionally, integrating a component as critical as security into the infrastructure makes it very risky to adopt a new infrastructure or architecture in the future. Given the incredible speed at which the wireless market evolves, retaining the flexibility to adopt new technologies in the future without compromising your security makes good business sense. An independent monitoring solution provides unified and consistent coverage of

all infrastructures, instead of forcing staff to use multiple consoles and system with differing features and capabilities.

Feature Complete and Industry Focus – One of the most important reasons that best-of-breed solutions dominate the enterprise security market is the fact that they are heavily focused on the challenges that are evolving in the space. These solutions provide deeper feature sets, fully developed user experiences, and focused development teams that deliver new solutions to market faster. Infrastructure vendors are traditionally very slow to integrate acquired technologies and slower still to respond when new features may be required, such as responding to a new industry attack or threat. As a result, it is very important to take a good look at what your dedicated monitoring solution will actually provide. Can you investigate threats fully in the interface? Does it have long-term compliance reporting? Does it provide forensic options for threats?

Security Integrated into the Infrastructure (Dedicated Security AP or Radio)		Independent Security Monitoring (Dedicated Sensor)	
<p>PROs</p> <ul style="list-style-type: none"> Single vendor solution Single user interface 	<p>CONs</p> <ul style="list-style-type: none"> Need to deploy additional AP for every 5 to 6 data APs, or purchase more expensive multi-radio AP Single point of failure (multi-radio approach) Self-monitoring Vulnerable to DoS Attacks Potential to affect network performance Single vendor silo of information Limits future migrations Slow to integrate and develop new features 	<p>PROs</p> <ul style="list-style-type: none"> Best-of-breed functionality Defense in depth Consistent layer of defense over all vendors Easy to adopt new hardware No impact on the performance of the network 	<p>CONs</p> <ul style="list-style-type: none"> Need to deploy sensor for every 5 to 6 data APs

