White Paper

Building Secure Wireless LANs

Aerohive Networks, Inc.
3150-C Coronado Avenue
Santa Clara, California 95054
Phone: 408.988.9918
Toll Free: 1.866.918.9918
Fax: 408.492.9918
www.aerohive.com

Table of Contents

Introduction

Security of a wireless network still ranks as one of the largest concerns of IT professionals planning to roll out an enterprise wireless LAN. Many people erroneously believe that a wireless LAN is inherently insecure. This is largely due to security flaws in early Wi-Fi protocols like WEP (Wired Equivalency Protocol), more recent vulnerabilities found in TKIP and lack of awareness as to how to deploy a secure WLAN. Today the security concerns of the legacy protocols have been largely eliminated and best practices for secure deployment have been developed allowing many wireless deployments to be arguably more secure than their wired counterparts.

When people first think of wireless security they typically first think of things like WEP, WPA and rogue detection. While these things are an important part of wireless security, they are only a part of building a secure wireless network.

Wireless security just like wired security has gone through evolutionary improvement over the years. As security evolved, more capabilities were added to improve the security of the network and deal with new threats. Today security is more than just a single feature and instead is a solution and set of practices defined to provide security for a specific network configuration. This whitepaper will help the wireless network administrator or security manager to understand the security capabilities in a modern Wi-Fi solution, where they should be used and how the WLAN integrates with other security devices in the network. Finally this document will describe how Aerohive provides a comprehensive and market leading Wi-Fi security solution for the enterprise.

Holistic Security Approach

Creating a secure wireless network is not only about configuring APs. Many of the most impactful wireless security practices have nothing to do with the access point. Figure 1 highlights the major components of a wireless security solution that must be considered to protect the network and the entire flow of traffic from the client through the network.

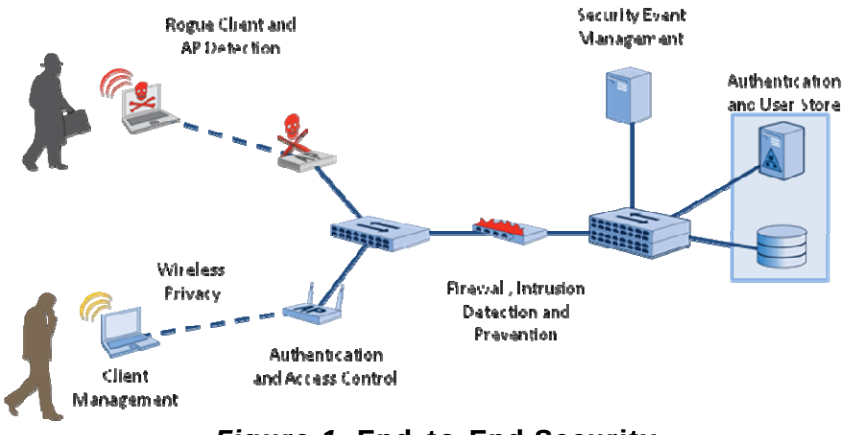

Figure 1. **End-to-End Security**

As an administrator installs wireless they should consider the end to end security implications:

- **Wireless Privacy and Key Management** – using keys to encrypt and secure traffic transmitted across the air.
- **Authentication** – identifying users as they come on the network. This means authenticating employees as well as guests and contractors. Also determining whether RADIUS, Active Directory or LDAP is used for authentication.
- **Client Management and NAC** – managing WiFi clients to ensure that they only connect to the enterprise or safe infrastructure using the correct security settings, system health and credentials.
- **Identity Based Access Control** – using the identity of a client to provide access to the correct VLAN, and allow or deny access to specific applications or resources.
- **Network Firewall and Intrusion Detection and Prevention** – using existing security infrastructure to detect and prevent attacks. Once they are on the network and running applications wireless users pose the same security risks as wired users. So, traffic from both wired and wireless users should be able to be scrubbed by the same best in class security devices, whether they are network firewalls, network antivirus scanners or intrusion detection systems.
- **WIDS and Rogue Detection** – ensuring that Rogue APs, Rogue Users and DoS attacks can be detected, located and mitigated.
- **Security Reporting and Security Event Management (SEM)** – integrating into an existing SEM system such that it can take logs from the wireless system to enable correlation with other systems in the network.
- **Device Physical Security and Data Storage** – ensuring the networking platform itself is securely implemented so that it cannot be compromised – even if stolen.
- **Compliance** – ensuring the products deployed and policies enforced are consistent with the corporate or industry compliance requirements.

Combined correctly, a holistic approach to network security will ensure strong and consistent security for both wired and wireless users.

Deploying a Secure WLAN

This whitepaper provides a holistic view of Wi-Fi security and provides guidelines that will enable an enterprise to deploy a wireless network as secure, or more secure than the wired network. The following components need to be considered in the deployment.

Wireless Privacy

The most commonly discussed aspect of wireless security (and arguably the most important along with authentication) is being able to deliver encrypted access to the user of the network. There have been several incarnations of

wireless privacy and this section will attempt to clear up any remaining questions or doubts about wireless privacy.

At the inception of the 802.11 standard a security mechanism was added to ensure that traffic sent from clients to the Access Points was secure. This was called WEP (Wired Equivalency Protocol). Unfortunately WEP was quickly proven to be easily cracked. In the end the encryption used in WEP (RC4) was fine but the way it handled keys enabled WEP to be cracked in short order. Many tools from security researchers have become available that can crack WEP in shorter and shorter times. With WEP being easy to crack, workarounds emerged to deal with the vulnerability.

Home users that understood the problems with WEP began employing other security techniques such as disabling broadcasting of the SSID or using MAC filters to allow only their computers access to the network. For consumers this was usually good enough, but those security mechanisms are easily bypassed by someone that's determined to gain access, so they are inadequate for the enterprise. MAC filtering has significant limitations because a MAC address can be easily spoofed by an attacker. And while disabling SSID broadcasts does prevent the SSID from being broadcast in the AP's beacons, connected clients still send the SSID name in probe requests so the SSID is easily detected using wireless packet capture or sniffer software. Another problem with using hidden SSIDs is that they can cause some devices to have difficulty in roaming and lead to unpredictable client behavior on the network..

Enterprise customers needed a more secure solution. Companies began treating the wireless network in the same way they treated the Internet, as an inherently insecure network. Many separated the wireless from the wired network and only allowed people into the network via VPN (Virtual Private Network) tunnels just as if they were traversing the Internet. The controller based Wi-Fi solution also emerged at this time to help deal with this issue. Instead of risking running WiFi traffic across the corporate network, the traffic would be tunneled from the AP to a controller in a DMZ where policy enforcement could be applied. This enabled enterprises to completely separate Wi-Fi traffic into an overlay network. There were drawbacks to this approach in the cost, scaling and complexity of deploying controllers, but at that time it was a way to deliver a more secure wireless network. The concept of using an overlay network for security purposes is now a dated one due to advances in wireless encryption protocols, but the details of that comes later.

The IEEE set up the 802.11i task group to develop a secure alternative to WEP but did not move fast enough to meet the demand for secure WiFi. So the Wi-Fi Alliance (an industry consortium) created WPA which was a snapshot of the work being done in the 802.11i. The benefit of WPA was that it could use the same encryption standards as the original WEP but with a more secure key management protocol called TKIP. It also enabled the use of AES[1] encryption which is considered to be more secure than RC4. Since WPA TKIP could still use the existing WEP RC4 encryption engine most devices that

[1] A common myth is that AES is only supported with WPA2 but that is incorrect; AES can also be implemented with WPA, however many older clients do not support WPA with AES

supported WEP could support WPA via a software update. Since the creation of TKIP, one major vulnerability has been found (called the Michael MIC Vulnerability), where TKIP can be cracked in short order if there is no PTK (Pairwise Temporary Key) rekey. It is recommended that the PTK rekey is set to between 2 and 10 minutes, if the AP supports it, if not TKIP should not be used. Aerohive does support PTK rekey, and therefore can offer a reasonable degree of security with TKIP. Even so, using TKIP is only recommended with legacy clients and only with short rekey intervals. WPA using AES is considered to be a vetted and secure standard but it has several major drawbacks - the most notable of which is that it does not support fast roaming.

In order to address the shortcomings of WPA, WPA2 was created. WPA2 was based upon a later snapshot of 802.11i . WPA2 added a few minor security optimizations but most importantly it added roaming features to WPA. Because WPA and WPA2 sufficiently resolved the privacy issues with wireless access the use of VPNs were no longer required and were slowly phased out of most deployments once WPA and WPA2 were proven to be secure. In addition one of the key security benefits of tunnels employed by controller based architectures disappeared due to the strong security now available at the AP.

The WPA and WPA2 security standard comes in two flavors for Wireless: WPA Personal and WPA Enterprise. WPA Personal uses pre-shared keys where the keys are manually defined on the client as well as the access point. This is often referred to as WPA Pre-Shared Keys or WPA-PSK for short. WPA Enterprise utilizes unique keys per client provided automatically through 802.1X, RADIUS and EAP. In most cases it is best to use WPA Enterprise mode for businesses because it is easier to manage the individual user access and is viewed as being more secure because the keys are dynamically generated for the client and AP at the time of login. Personal mode is usually only used in the enterprise for specific applications where the client may not support 802.1x; for example, legacy barcode scanners.

If pre-shared keys must be used there are a couple of things to be aware of when using them. The reality of security is that every security mechanism is breakable given enough time. Luckily WPA2 AES is very secure and would take many lifetimes to crack effectively using modern technology. But, if an overly simple key is defined it can be vulnerable to a dictionary attack which uses software with a large database of words to try one word at a time until it finds the right one. A strong password with numbers, letters, and special characters is extremely difficult to guess and usually renders dictionary attacks useless. Another big drawback to using pre-shared keys is that they must be stored on the user's notebook computer. Since the notebook is often out of the office it becomes vulnerable to having the keys stolen. There are several programs that will strip the pre-shared keys from Microsoft Windows and save them to a USB memory stick enabling an attacker to easily breach the network. The other significant issue with pre-shared keys is that terminated employees' authentication cannot be easily revoked from the network. Updating keys every time there is a potential leak of the key is very burdensome and in larger enterprises is unmanageable.

For network administrators that can't move to a proper 802.1X solution, Aerohive has implemented a solution called Private PSK that enables each user to have a unique PSK, which can be individually assigned and revoked which significantly improves the security and manageability of a PSK deployment.

Authentication

Once privacy through the air is ensured the next step in ensuring security is authenticating the user. Far and away the most common form of authentication in enterprise wireless is 802.1X. 802.1X relies upon RADIUS Extensible Authentication Protocol or EAP to mutually authenticate users to the infrastructure at a port/MAC address level and provide unique keys to each authenticated user that can be leveraged by WPA or WPA2 to encrypt the traffic. A few WiFi solutions provide the ability to also leverage Active Directory and OpenLDAP databases for authentication which can avoid installing an intermediary RADIUS server however when this is done 801.2X is still employed for the client.

If 802.1X is not used, some organizations just rely on the secrecy of their pre-shared key to hope that the right users are on the network. Given the flaws in this approach, security can be enhanced by forcing users to a Captive Web Portal (CWP) where their authentication credentials are entered and they are authenticated against RADIUS, LDAP or Active Directory before they are allowed access. MAC-based authentication can also be used to authenticate the machine, but as discussed previously, the ability to spoof MAC addresses limits the security of this approach.

Client Management and NAC

While the focus of WiFi security is usually on the AP, the single largest cause of undetected wireless vulnerabilities is clients. Because clients can be controlled by less technically sophisticated employees those employees often blunder into unsecure situations. Controlling client behavior is critical to ensuring a secure network. Fortunately there are simple solutions to this problem. The two available technologies that are employed to control client behavior are Client Management and NAC. Even though these are separate they are often implemented in a single solution (e.g. Juniper's (formerly Funk) Odyssey Client within their Unified Access Control solution).

Client management provides central configuration and control of the WiFi client software (and sometimes wired client). This makes it easier to centrally manage and configure end users access to the WiFi network, and it enables the IT department to control which networks clients can connect to. This solves a whole raft of security issues like users connecting to unsecured networks, fake APs, and ad-hoc networks.

Network Access Control (NAC) is used for both wired and wireless to determine the security stance of a client before providing access to the network. This allows control of what the client can access, how they are connecting, where they are connecting from and if their system has proper and updated security such as an updated antivirus signature. It is important that any wireless solution properly integrate into these systems so clients are

managed as part of an entire network for wired, wireless and remote clients. This allows a greater control of client access well beyond just what in-line security platforms currently provide.

Identity Based Access Control

Once a client has connected to a network, the next thing to consider is what they are allowed to do on the network. Providing access to only the resources that an employee needs to do their job is always a good practice. A strong identity-based security capability enables the enterprise to granularly define who can access what resources (VLANs, Applications, Servers), at what time and at what QoS level. In general users are put into a role via returned RADIUS attributes or Active Directory group policy, but this also may be done via ESS association, security stance or MAC OUI. Features like stateful inspection firewall, time-of-day/day-of-week controls, traffic segmentation, MAC address filters and MAC address firewall enable an enterprise to tightly define user access based upon application, destination IP, source or destination MAC Address, time of day, and VLAN or Tunnel.

Other identity based policy such as QoS policy are important, but that is out of scope of this whitepaper.

Network Firewall and Intrusion Detection and Protection

So far we have mainly discussed the security issues with getting users onto the network and to the right resources, but it is also important to be able to monitor and control the client traffic as it traverses the wired network. Segmentation is clearly one of the most basic of best practices to keep one type of user traffic separate from other traffic or applications. This must be done while providing user access to the needed resources. Between segments often there is a policy enforcement device that defines what users can and can't access on other segments. This can be as simple as a router running a few ACLs or as sophisticated as a full blown stateful inspection firewall and IPS solution. The practice of segmenting and enforcing traffic not only improves security, it also makes it easier to manage a large network of users and simplifies the application of firewall rules.

A properly configured firewall will segment users, control access and traffic, and provide detailed reporting. The best firewalls that do this for wireless clients are the same as the best firewalls for a wired network. By leveraging best in class firewalls from companies like Juniper and Checkpoint you can protect the entire network, wired and wireless, with a single system that offers more features, is simpler to manage and easier to troubleshoot than separate firewalls for the wired and wireless networks. The same is also true for IPS systems, AV gateways and spyware gateways. This typically allows the use of an existing system without the need for new equipment and additional training for existing IT staff. This also has the added benefit of reducing the cost of the wireless deployment.

Some WiFi vendors, including Aerohive, include firewalls embedded in the Wi-Fi gear. These firewalls are great for providing an additional level of security for wireless users, or if the Wi-Fi traffic is locally bridged at the AP, enabling

access controls to be enforced before putting the traffic on the switched network.

There are two common ways to segment traffic from a wireless network and one uncommon way. The most common is clearly VLANs. Trusted and capable, VLANs leverage the existing switches in the network to provide line-speed performance while maintaining traffic separation. The beauty of VLANs is that they segment without obscuring the traffic on the wire. This enables the existing firewall, IPS, and other policy enforcement systems in place to do their job unhindered. For employee access VLANs are certainly the most flexible and simplest to deploy. The other common way to segment is through tunnels. Many AP vendors only support tunneling to enable segmentation. This approach has some benefits but also some major drawbacks. The biggest drawbacks are:

1. Client traffic must traverse the network to get to a tunnel terminator of some kind (usually a controller in a wireless network) before going to its destination. This can introduce latency and jitter.

2. Client traffic is obfuscated as it crosses the network. Tunneled traffic will have a new IP header applied that changes the port, protocol, source and destination IP addresses of the packet. Most policy enforcement devices currently in the network leverage this information to apply policy. This renders many of the existing security measures already in the network useless. In addition, many AP tunnels have an encrypted payload, which totally obfuscates the data within making it impossible to check packets for viruses and attacks.

3. The final problem is performance. A tunneled network is only as fast as the tunnel terminator (or controller). Invariably the tunnel gateway is a bottleneck of some sort, and the move to 802.11n amplifies this problem. One would often apply some level of oversubscription to a controller just like you would have in a switched network, however in a wired network over subscription is often 2-1 or 4-1 with a controller in a 802.11n network 20-1 oversubscription is not uncommon. Also if MTUs are not set low enough packets may need to be fragmented further reducing performance.

Clearly tunneling has some significant disadvantages for employee networks, however tunneling does have its place. A “dirty net” or traffic that is always destined for the Internet and is treated as an outside network may be tunneled if VLANs are not feasible. A common example of a dirty net is a guest network. Where the clients do not adhere to company policy and should not have access to the corporate network. A VLAN or a tunnel that leads to the Internet is a great way of taking that traffic out of the network. A guest network is often restricted by the performance of the Internet gateway so the tunnel terminator is rarely the bottleneck. In addition, because it is a guest network and does not have access to the rest of the network, policy enforcement is not as important as it would be for employee traffic.

Finally, there is one far less common, but sometimes useful, method of segmenting traffic; MAC firewall. A MAC firewall is like a MAC filter but instead

of enforcing a client MAC or "source MAC" it can also filter on "destination MAC". This means that at the Ethernet frame level traffic can be restricted to be sent to only a specific destination MAC addresses, like the default gateway. This does not keep the traffic off the network, but it does restrict where it can go. This can be useful for providing wired and wireless client isolation or can be used to isolate traffic without using VLANs or tunnels. This is often the only way to segment in environments that do not have VLAN capable switches and where tunneling is infeasible.

Rogue Detection and WIDS

Wireless Intrusion Detection Systems or WIDS for short is probably one of the least understood security capabilities in wireless. Part of the confusion arises because wireless IDS capability is fundamentally different than a traditional wired IDS system. A classic wired IDS looks for over-the-wire attacks at a choke point in the network (between subnets, in front of servers, or at the Internet gateway). Often this means looking into the packet payload for application layer attacks but it can also include pattern recognition, honeypots and a host of other security measures. A wireless IDS solution does not look deeply into the content of the data traversing the network. Instead it observes the WiFi messages that clients and access points are sending in the air, even if they are not connected to the enterprise wireless network. This enables a WIDS solution to observe the behavior of malicious APs and clients as well as more benign (but still vulnerable) misconfigured or misbehaving clients and APS.

The most common vulnerabilities enterprises are concerned about are:

- **Rogue APs** – Rogue AP is a generic term that can be used to describe any out-of-compliance AP but in general people think of a rogue as an unsecured AP put on the network either by an unknowing employee trying to get wireless access or more frighteningly by an attacker trying to gain access to the corporate network via wireless.

- **Ad-Hoc Clients** - Ad-hoc mode is a capability of all wireless clients to connect directly with any other client without accessing the access point infrastructure. By themselves ad-hoc clients are not much of a threat, but in an enterprise they create multiple risks. The most concerning is that a computer could be connected to another computer over the ad-hoc connection at the same time as they are on the wired network, giving an outside attacker access to the corporate network via the ad-hoc connection.
- **Compliance** – Ensuring that the APs that IT has installed fall within the company standard of configuration. While this sort of misconfiguration is unlikely with a modern Wi-Fi solution with central management, companies that have left over autonomous APs will often have inconsistency in configuration that can reduce performance or implement weak security that creates vulnerabilities for the corporate network. Also there may be regulatory compliance that requires regular checking of the infrastructure, whether there is a real risk or not.

- **Attacks on Client** – There are many attacks that try to gain access to a client laptop through their wireless interface, most of which involve luring clients to connect to a malicious AP. There are ways of detecting these attacks with WIDS but the best way to prevent this is through a good client management strategy.

- **DoS Detection and Prevention** – Dealing with layer 1 and 2 denial of service attacks on the AP infrastructure is often considered a WIDS function. Common attacks are things like disassociation floods, ARP floods and other such attacks that can bring down the wired or wireless infrastructure. In some cases the attacker is not actually on the network which limits what the AP can do, except send an alarm, but in other cases a user needs to be connected in order to initiate an attack. In those cases the user can be banned from the network. DoS attacks from malicious users are rare and often not that effective. More frequently detecting DoS attacks from a client is an indicator that a authorized user has a virus or is running an unauthorized application.

Security Reporting and Security Event Management (SEM)

Monitoring and reporting is a critical piece of security overall. The ability to track, report and respond to issues and violations to the security policy is critical to good security. This provides assurance that your current policy is working and that the network is secure.

1st party support should include:

- **Client Data** – IP Address, Policy set, host name, user name
- **Client Behavior** - association times, applications accessed, roaming history and disassociation.
- **Rogue APs and Clients**
- **Compliance**
- **DoS Attacks**
- **Firewall logs** (if firewall is available)

3rd party Security Event Management systems such as Arcsight and Network Forensics enable threat correlation and analysis by leveraging the wireless logs and logs from other equipment in the network. This will often provide much more insight into what is happening on the network than any 1st party solution.

Device Physical Security and Data Storage

There's been a debate as to the merits of thin versus fat APs when it comes to the storage of secret information like RADIUS keys, pre-shared keys and other network credentials. The traditional assumption is that because thin-APs don't store anything locally, the AP cannot be hacked to retrieve secure information. This is based out-of-date assumption that thin APs don't store secure information. Historically, thin APs were not able to operate in a mesh, locally forward traffic, work in remote offices, or mutually authenticate with the controller. However, over the years these features have been added and these advancements have forced all vendors, thin and fat, to store keys and

configuration on APs. The belief that thin APs are architecturally more secure because keys are not stored locally is a dated one, and worse can give a false sense of security.

The ability to securely store keys on an AP is critical for any architecture and it is important to work with a company that makes device security and storage security a priority. The AP manufacturer must implement some form of secure key storage in hardware. This usually means that the hardware must have a TPM (Trusted Platform Module) or some similar hardware key storage. In reality very few WLAN manufacturers implement a TPM chip on their APs thus risking critical enterprise security keys during AP theft.

Compliance

The final topic of discussion is Compliance. For many industries there are compliance requirements for data-security. Common examples include PCI (for credit card transactions), HIPAA (for medical data and records), SOX (for corporate financial reporting) and others. Many times the configurations required for compliance go beyond what is required by an enterprise for WLAN security, and requires that the entire system (wired LAN, wireless LAN, WAN, client, etc) is compliant as a whole. When looking at an enterprise WiFi solution it is important that a flexible solution capable of meeting all of the security requirements for compliance is selected.

Regardless of the compliance governing body, there are several universal requirements. They are as follows:

1. Data privacy through strong encryption and authentication
2. Data segmentation and access control in the AP and as it traverses the network
3. Comprehensive reporting and monitoring to ensure ongoing compliance

These requirements are broad in scope and require an end-to-end security solution to fully deliver upon them.

The Aerohive Advantage

Aerohive's unique approach to wireless LAN architectures eliminates controllers and enables customers to forward traffic at the edge to optimize traffic performance as well as network resiliency and load. Aerohive's solution provides these advantages while maintaining a strong security posture because comprehensive security enforcement is performed right at the edge of the network – where the wireless users first get access to LAN. Many companies have segmentation and firewall policies that must be applied when the wireless traffic bridges to the local network. This is especially true for companies with regulatory compliance concerns like PCI. Aerohive's implementation provides full policy enforcement at the edge of the network, enabling secure local forwarding.

Aerohive APs are built to be secure. Every feature within the product goes through a thorough internal examination to help eliminate vulnerabilities

during design, and then during QA is scanned for vulnerabilities. Aerohive also contracts 3rd party security firms to perform penetration tests to ensure device security. When vulnerabilities are found they are fixed with the highest priority. Aerohive has a policy of public disclosure of security vulnerabilities that includes a security alert system to notify customers as quickly as possible of vulnerabilities and steps to eliminate the vulnerability.

In addition to building secure products, Aerohive offers a rich set of security features including:

- **Wireless Privacy** – Full support for 802.11i, WPA and WPA2

- **Authentication** – Strong authentication using 802.1X with RADIUS, Active Directory or OpenLDAP. Captive Web Portal authentication and MAC authentication. In addition Aerohive offers the unique Private PSK feature to add enterprise class security and management to pre-schared keys.

- **Client Management and NAC** – Interoperability with all major client management, NAC and inline security solutions within the enterprise.

- **Identity Based Access Control** – In-line policy enforcement with strong role-based stateful inspection firewall and access control.

- **Network Firewall and Intrusion Detection and Protection** – Segmentation of traffic based upon user role and stance without breaking the existing wired IPS and firewall systems in place. In fact Aerohive recommends leveraging those resources to improve the security of the wireless traffic.

- **Rogue Detection and WIDS** – Wireless DoS detection and prevention and wireless IDS for rogue detection and compliance monitoring.

- **Security Reporting and Security Event Management (SEM)** – complete wireless reporting within HiveManager and support for third party event management.

- **Device Physical Security and Data Storage** – Strong device security including a TPM chip for secure key and configuration storage and physical locking mechanisms to deter theft.

- **Compliance** – Solutions for being deployed in HIPAA, SOX and PCI compliant networks among others.

Aerohive's ability to offer secure wireless access is based on an end-to-end approach that has been built from the beginning rather than as an afterthought. Not only has Aerohive implemented a comprehensive set of security features, but Aerohive's architecture also has been designed to take advantage of other security systems in place within an enterprise to ensure consistent security policy for users whether they are wired or connected wirelessly. Through an end-to-end approach Aerohive has delivered a comprehensive and market leading security solution to deliver a wireless

network that is not only capable of securing wireless access but, itself, is secure.

