



Aerohive and IntelliGO

End-to-End Security for devices on your network



Introduction

Networks have long used a password to authenticate users and devices. Today, many cyber attacks can be used to capture these credentials or crack them using affordable or open source tools giving access to intruders that are undetectable by most network security systems.

Administrators also particularly have a tough time enforcing security on end-user devices because of the number and types of operating systems that need access to the network.

At the same time the security of devices on the network from known to unknown vulnerabilities presents a risk of losing compromising corporate data. This is driving organizations to require greater visibility and control of the users, devices, applications and vulnerabilities on their networks.

Aerohive and IntelliGO

Aerohive and IntelliGO have teamed up to offer the most secure network experience for organizations who require uncompromising encryption for their connections and strong policies around the security state of devices permitted on the network. This includes:

Secure, scalable Wi-Fi from Aerohive

- Security starts with the Aerohive access points at the edge of the Wi-Fi network. With a range of protection services built into every access point, you can safely enable mobility throughout your organization:
- Fully stateful layer 2-7 firewall policies personalized to specific user groups or devices
- On-board RADIUS Server, CA and AD integration to leverage certificate authority and RADIUS capabilities of existing IntelliGO installation
- OS/Device classification engine enables granular policy enforcement
- Scheduled SSID availability
- WIPS policy for rogue detection and mitigation
- TPM chips inside every AP encrypt precious data from physical theft
- GRE and VPN tunneling to DMZ or remote locations
- Comprehensive monitoring and reporting
- Application Visibility and control with Deep Packet Inspection
- Unique Private Pre-shared Key (PPSK) technology brings enterprise grade security with unprecedented ease of use to guest access, BYOD and IoT applications.

Enhanced security with IntelliGO

Secure Network Experience with EAP-TLS

Using the IntelliGO built-in and automated Certificate enrollment engine and RADIUS services EAP-TLS services can be used to offer a the most secure wireless experience for users. This allows role specific attributes during authentication to profiles for app firewall, and avoids MITM attacks because no passwords are sent over the air.

Administratively Approved Guests

Using IntelliGO, guest authentication can be managed by Administrators or Sponsors allowing guests to authenticate or receive credentials through SMS, Email or Captive Portal.

Strong User and Device Policies

Using IntelliGO, authentication can tie the user, device or state of the device to a policy, ensuring only secure devices, and users with certain specified roles can access critical information. IntelliGO works with existing Aerohive profiles and attributes to enhance dynamic membership and roles on the network.

Vulnerability Scanning

IntelliGO can scan devices for known and unknown vulnerabilities by leveraging the in-built vulnerability scanning to provide an indicator of compromise detection.

Deeper Device Visibility

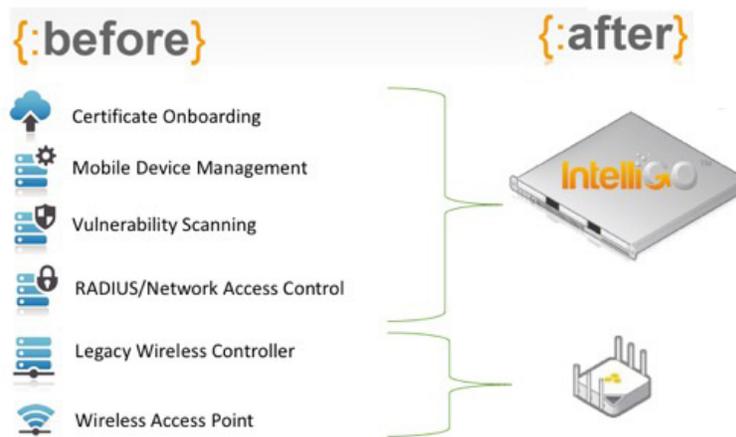
IntelliGO running on thin clients or agentless can discover the applications, processes, services, modified files and security state of devices connected to the network. This provides complete end-to-end visibility of connected devices.

Device Control

Using IntelliGO you can configure mobile devices and send commands such as application install, device profiles for wireless onboarding, and lock or locate a device if lost or stolen.

How It Works

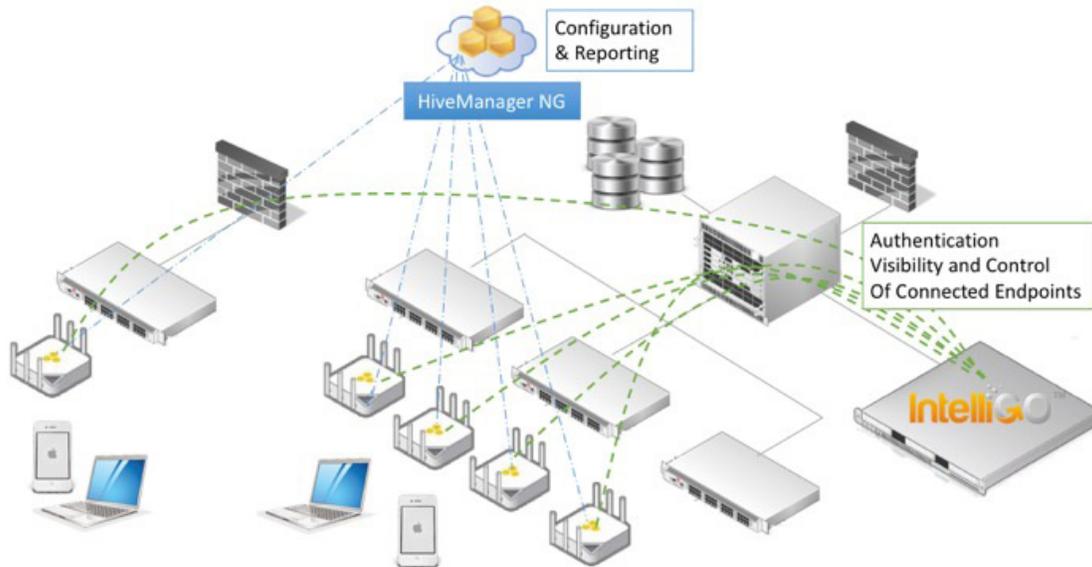
Aerohive and IntelliGO enable the most secure networking experience available by providing a centralized authentication cluster using the IntelliGO appliances or hosted software. Similar to the distributed control plane and cloud management of the Aerohive access points, IntelliGO simplifies the outlay of outdated technology to support secure networking:



Deployment

IntelliGO can be deployed on premises or hosted.

Aerohive and IntelliGO: Easily control Users, Devices, Applications and Security with the fewest tools



Once installed, and running enrollment for IntelliGO secure networking follows a three step process:

1. New devices enroll one time for certificates through the inbuilt-in enrollment portal or transparently through existing device managers.
2. Once enrolled, IntelliGO will scan the machines for vulnerabilities and device information.
3. Policies on IntelliGO can dynamically apply user or device role based on the information collected, all of which is visible from a single dashboard.

Once enrolled, all context - including security, users, devices, applications and runtime information about devices, is stored and available for policy in the IntelliGO Console:



Summary

Together Aerohive and IntelliGO can offer a secure networking experience with the simplest deployment. Using these platforms solutions together helps avoid the risk of data loss, ensuring every connected device is secure and within the organization's control. This unmatched visibility and control is offered with little overhead and no impact to performance or the user's networking experience.

About IntelliGO Networks

IntelliGO offers the next generation of access control. The IntelliGO platform allows organizations of any size to leverage secure networking protocols such as EAP-TLS and audits the security of every network connected device. IntelliGO is used by some of North America's largest and most trusted brands securing tens of thousands of devices every day. IntelliGO is headquartered in Toronto Ontario. For more information call us at 1 888 855 3555 or send an email to info@intelligonetworks.com.

About Aerohive Networks

Aerohive (NYSE: HIVE) enables our customers to simply and confidently connect to the information, applications, and insights they need to thrive. Our simple, scalable, and secure platform delivers mobility without limitations. For our customers worldwide, every access point is a starting point. Aerohive was founded in 2006 and is headquartered in Sunnyvale, CA. For more information, please visit www.aerohive.com, call us at 408-510-6100, follow us on Twitter @Aerohive, subscribe to our blog, join our community or become a fan on our Facebook page.

"Aerohive" and "HiveManager" are registered trademarks of Aerohive Networks, Inc. All product and company names used herein are trademarks or registered trademarks of their respective owners. All rights reserved.

About Aerohive