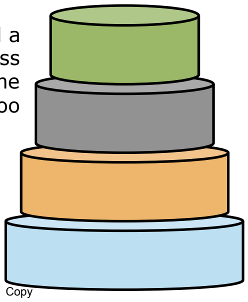
Building a Secure Wireless Network

Joel M Snyder
Senior Partner
Opus One
jms@opus1.com

Agenda: Securing Wireless Networks

- **Using encryption and authentication**
- **Handling unauthenticated users**
- **Managing RF and bandwidth**
- **Using WLAN switch technology**
- **Applying IDS and firewalls to protect wireless**
- **Preparing for hybrid mobile devices**

Creating a Secure Wireless Network Means Looking at the Big Picture



But you can’t build a secure network unless you also spend time up here, too

Most of us spend most of our time down here- which is a really important place to be!

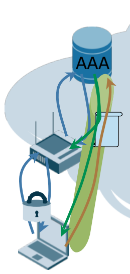
Use 802.11i and WPA to Protect the Channel and Authenticate Users

Always Start With a Secure Base and You Can Build on Top of That

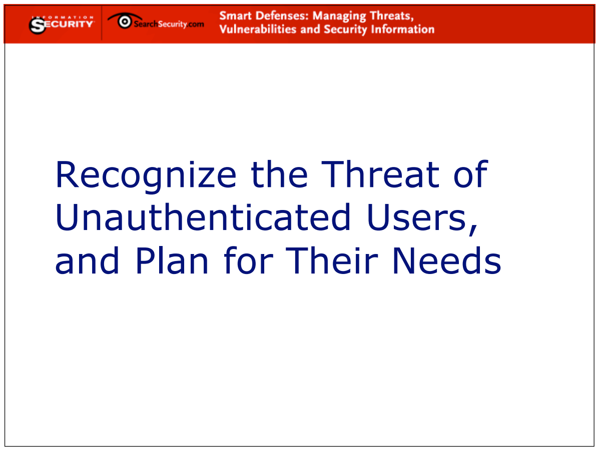
Minimum Enterprise Requirements for Secure Wireless

- Use 802.11i (WPA2) security to
  - Encrypt the communications channel
  - Authenticate each wireless user
  - Ensure per-user, per-session encryption keys
- Fall back to WPA security if hardware requires it
- Root out and salvage hardware that won’t support WPA (802.1X plus dynamic 128-bit RC4 keys)

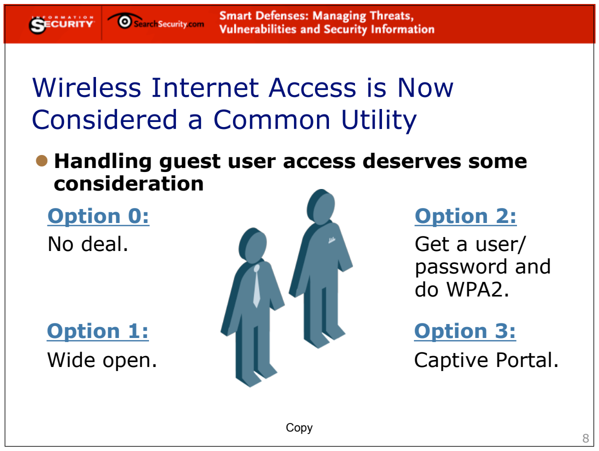
Reviewing 802.11i



a) Conversation between AP and AAA protected by a RADIUS secret (so you should pick a good one!)
b) EAP Tunnel created between user and AAA server protected by TLS (802.1X/RADIUS)
c) TLS certificate proves to user that they are not talking to a “rogue” AP
d) User credentials sent down encrypted tunnel to AAA server
e) Per session encryption / authentication keys created by AAA server (and shared with AP)
f) User’s session protected and authenticated; can’t be sniffed even by other authenticated users



Recognize the Threat of Unauthenticated Users, and Plan for Their Needs



Wireless Internet Access is Now Considered a Common Utility

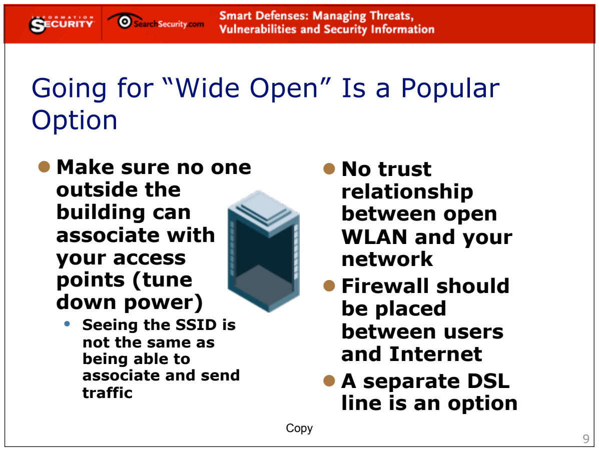
- **Handling guest user access deserves some consideration**

Option 0:
No deal.

Option 1:
Wide open.

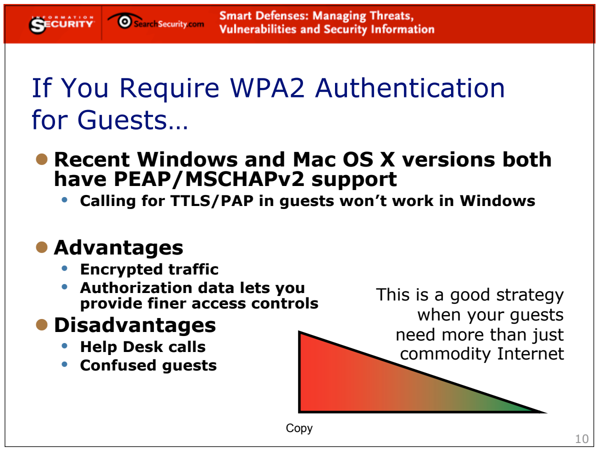
Option 2:
Get a user/ password and do WPA2.

Option 3:
Captive Portal.



Going for "Wide Open" Is a Popular Option

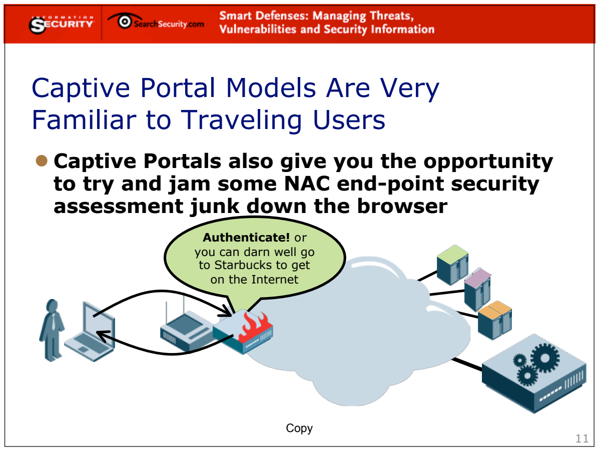
- **Make sure no one outside the building can associate with your access points (tune down power)**
  - **Seeing the SSID is not the same as being able to associate and send traffic**
- **No trust relationship between open WLAN and your network**
- **Firewall should be placed between users and Internet**
- **A separate DSL line is an option**



If You Require WPA2 Authentication for Guests…

- **Recent Windows and Mac OS X versions both have PEAP/MSCHAPv2 support**
  - **Calling for TTLS/PAP in guests won't work in Windows**
- **Advantages**
  - **Encrypted traffic**
  - **Authorization data lets you provide finer access controls**
- **Disadvantages**
  - **Help Desk calls**
  - **Confused guests**

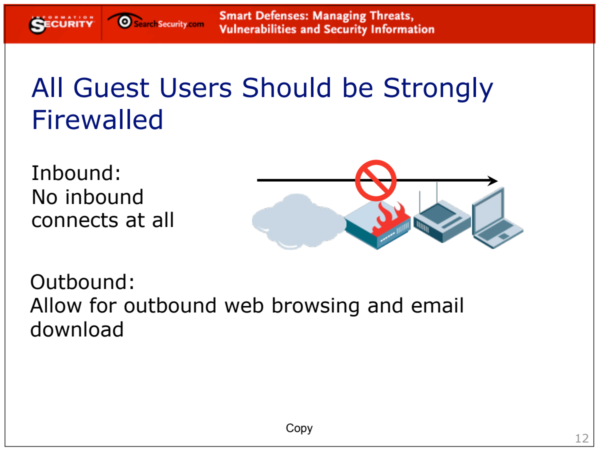
This is a good strategy when your guests need more than just commodity Internet



Captive Portal Models Are Very Familiar to Traveling Users

- **Captive Portals also give you the opportunity to try and jam some NAC end-point security assessment junk down the browser**

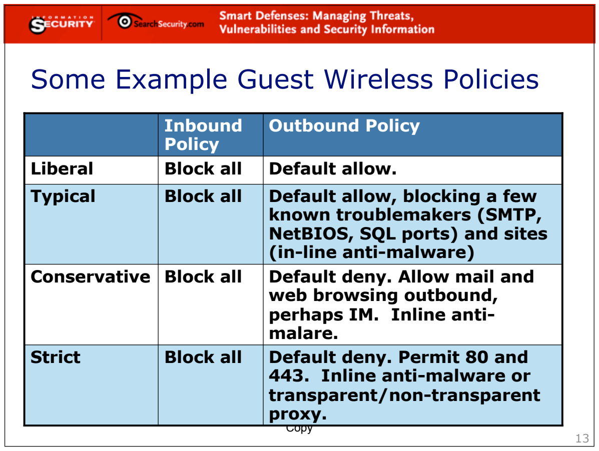
Authenticate! or you can darn well go to Starbucks to get on the Internet



All Guest Users Should be Strongly Firewalled

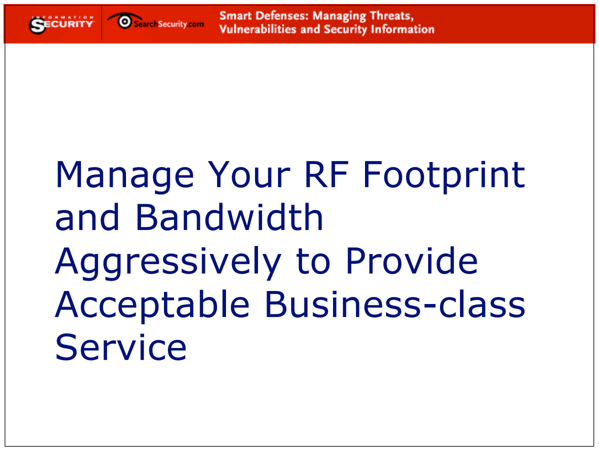
Inbound:
No inbound connects at all

Outbound:
Allow for outbound web browsing and email download

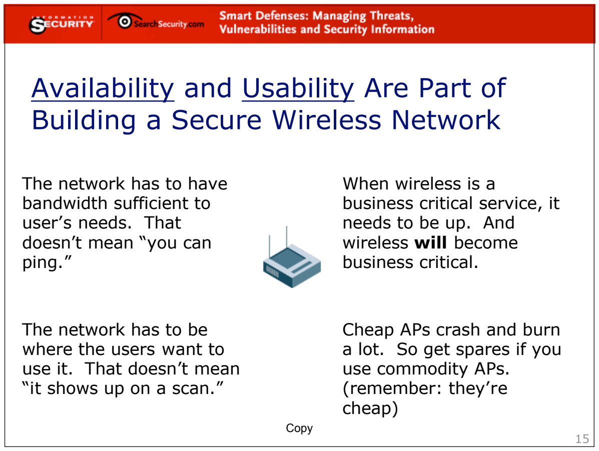


Some Example Guest Wireless Policies

	Inbound Policy	Outbound Policy
Liberal	**Block all**	**Default allow.**
Typical	**Block all**	**Default allow, blocking a few known troublemakers (SMTP, NetBIOS, SQL ports) and sites (in-line anti-malware)**
Conservative	**Block all**	**Default deny. Allow mail and web browsing outbound, perhaps IM. Inline anti-malare.**
Strict	**Block all**	**Default deny. Permit 80 and 443. Inline anti-malware or transparent/non-transparent proxy.**



Manage Your RF Footprint and Bandwidth Aggressively to Provide Acceptable Business-class Service



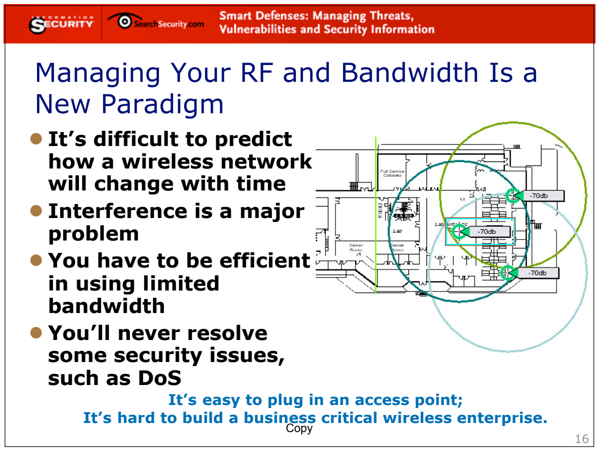
Availability and Usability Are Part of Building a Secure Wireless Network

The network has to have bandwidth sufficient to user's needs. That doesn't mean "you can ping."

When wireless is a business critical service, it needs to be up. And wireless **will** become business critical.

The network has to be where the users want to use it. That doesn't mean "it shows up on a scan."

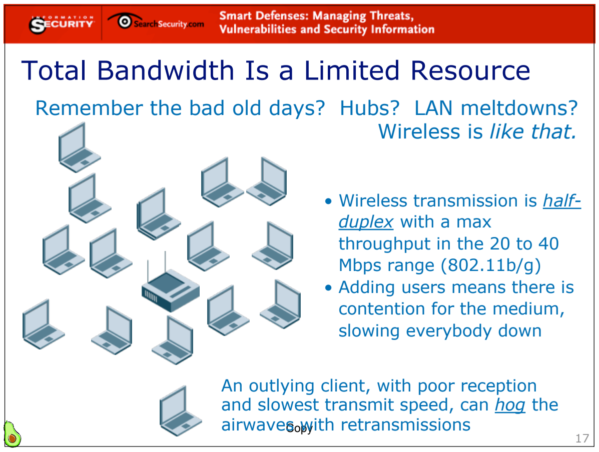
Cheap APs crash and burn a lot. So get spares if you use commodity APs. (remember: they're cheap)



Managing Your RF and Bandwidth Is a New Paradigm

- **It's difficult to predict how a wireless network will change with time**
- **Interference is a major problem**
- **You have to be efficient in using limited bandwidth**
- **You'll never resolve some security issues, such as DoS**

It's easy to plug in an access point;
It's hard to build a business critical wireless enterprise.

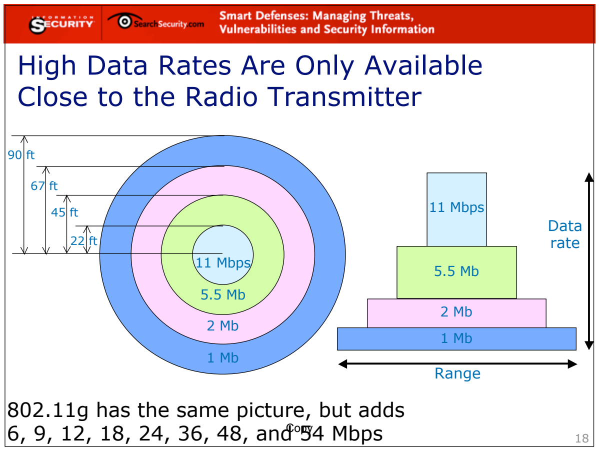


Total Bandwidth Is a Limited Resource

Remember the bad old days? Hubs? LAN meltdowns? Wireless is *like that.*

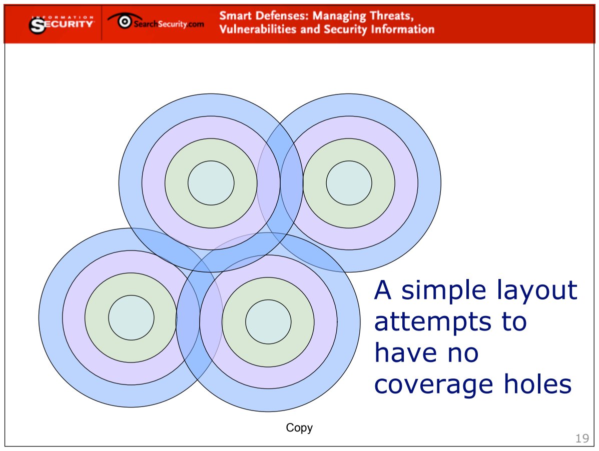
- Wireless transmission is *half-duplex* with a max throughput in the 20 to 40 Mbps range (802.11b/g)
- Adding users means there is contention for the medium, slowing everybody down

An outlying client, with poor reception and slowest transmit speed, can *hog* the airwaves with retransmissions

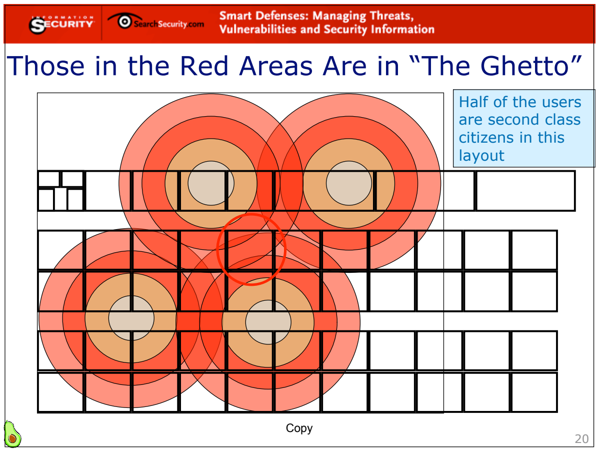


High Data Rates Are Only Available Close to the Radio Transmitter

802.11g has the same picture, but adds 6, 9, 12, 18, 24, 36, 48, and 54 Mbps

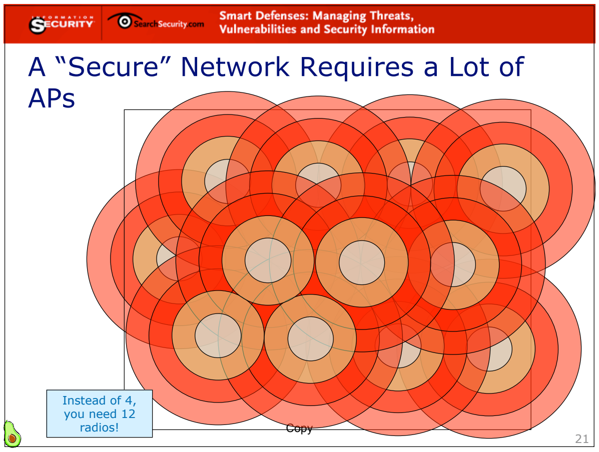


A simple layout attempts to have no coverage holes



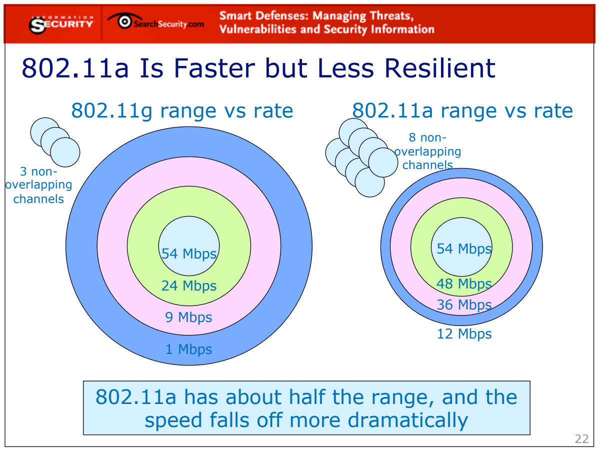
Those in the Red Areas Are in "The Ghetto"

Half of the users are second class citizens in this layout



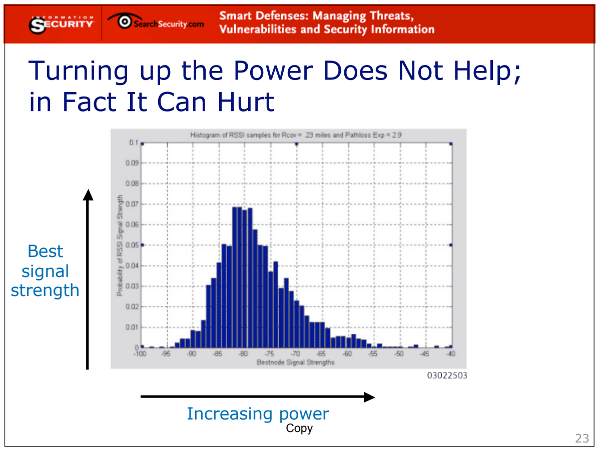
A "Secure" Network Requires a Lot of APs

Instead of 4, you need 12 radios!

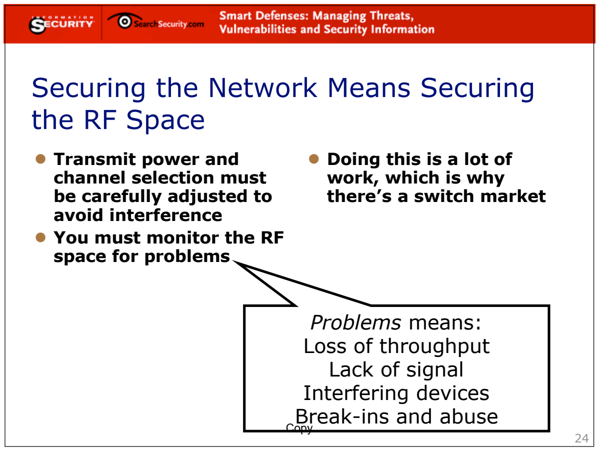


802.11a Is Faster but Less Resilient

802.11a has about half the range, and the speed falls off more dramatically



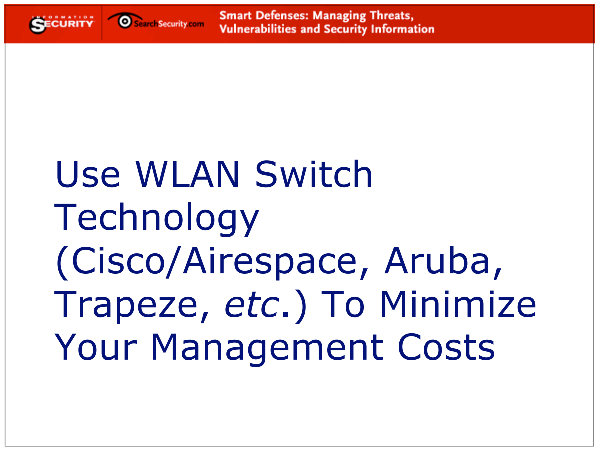
Turning up the Power Does Not Help; in Fact It Can Hurt



Securing the Network Means Securing the RF Space

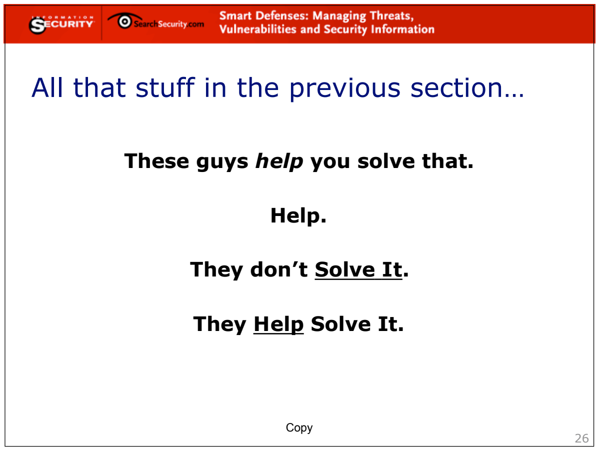
- **Transmit power and channel selection must be carefully adjusted to avoid interference**
- **You must monitor the RF space for problems**
- **Doing this is a lot of work, which is why there's a switch market**

Problems means:
Loss of throughput
Lack of signal
Interfering devices
Break-ins and abuse



Smart Defenses: Managing Threats, Vulnerabilities and Security Information

Use WLAN Switch Technology (Cisco/Airespace, Aruba, Trapeze, *etc*.) To Minimize Your Management Costs



Smart Defenses: Managing Threats, Vulnerabilities and Security Information

All that stuff in the previous section…

These guys *help* you solve that.

Help.

They don't Solve It.

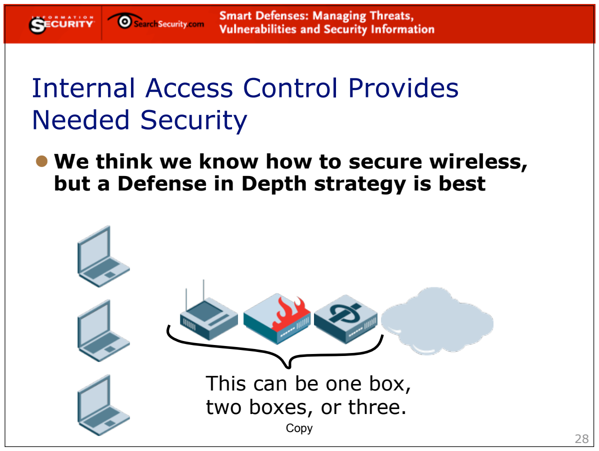
They Help Solve It.

Copy

26

Smart Defenses: Managing Threats, Vulnerabilities and Security Information

Apply IDS and Firewall Technology to the Point Where Wireless Joins Your Network



Smart Defenses: Managing Threats, Vulnerabilities and Security Information

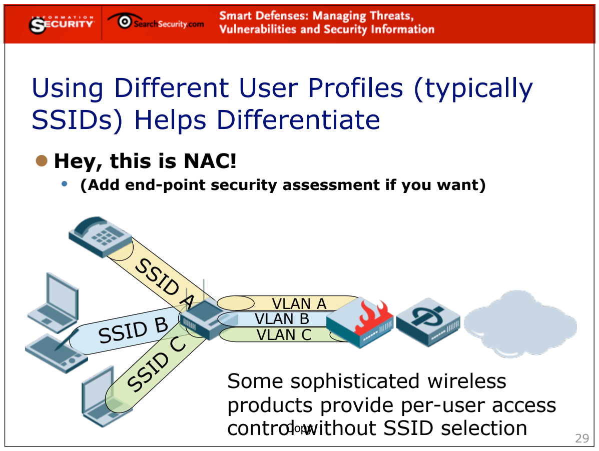
Internal Access Control Provides Needed Security

- **We think we know how to secure wireless, but a Defense in Depth strategy is best**

This can be one box, two boxes, or three.

Copy

28



Smart Defenses: Managing Threats, Vulnerabilities and Security Information

Using Different User Profiles (typically SSIDs) Helps Differentiate

- **Hey, this is NAC!**
  - **(Add end-point security assessment if you want)**

Some sophisticated wireless products provide per-user access control without SSID selection

Copy

29

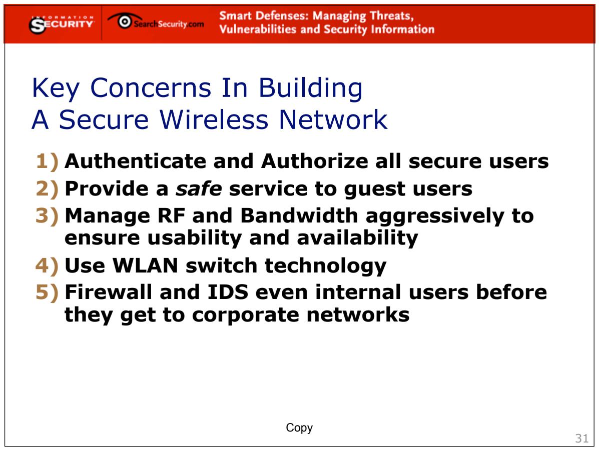
Smart Defenses: Managing Threats, Vulnerabilities and Security Information

Speaking of Mobile Devices…

- **Prepare for Hybrid Mobile Devices (Phones, PDAs) by proactively deploying synchronization and control Tools**
- **Don't be BlackBerry-ed!**

Copy

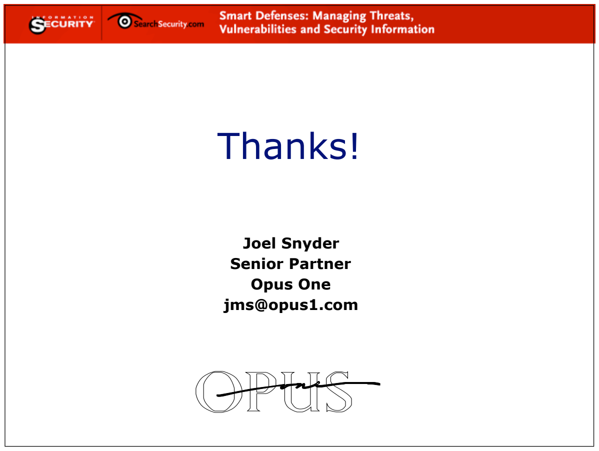
30



Key Concerns In Building A Secure Wireless Network

1) **Authenticate and Authorize all secure users**
2) **Provide a *safe* service to guest users**
3) **Manage RF and Bandwidth aggressively to ensure usability and availability**
4) **Use WLAN switch technology**
5) **Firewall and IDS even internal users before they get to corporate networks**

Copy



Thanks!

Joel Snyder
Senior Partner
Opus One
jms@opus1.com