



Vezeték nélküli hálózatok biztonsága

2014. október 8.

Czirák Zoltán
ügyvezető igazgató
vállalati hálózatok

Vezeték nélküli hálózatok biztonsága

A mobil adatforgalom rohamos növekedése egyre magasabb szintre helyezi a vezeték nélküli hálózatok teljesítmény és biztonság követelményeit. A vezetékes megoldásokkal ellentétben a Wi-Fi esetében a fizikai hozzáférés lényegesen egyszerűbb, ami tovább növeli a kockázatot. Nem feledkezhetünk meg továbbá azokról a kritikus területekről sem (pl. bankok, nemzetbiztonsági intézmények, büntetés végrehajtás, stb.), ahol semmiféle mobil kommunikáció nem megengedett, de mindössze táblákkal tiltják a mobiltelefon vagy Wi-Fi képes eszközök használatát. Előadásunkban erre mutatunk egy hatékony megoldást.

Az EQUICOM-ról dióhéjban

@equicom

az Ön ICT mérés technikai szakértője

- Kizárólag ICT mérés technikai megoldásokra szakosodva
- Több mint 15 éves szakmai múlt
- Világviszonylatban vezető beszállítók kizárólagos magyarországi képviselője

EXFO
EXPERTISE REACHING OUT

FLUKE
networks

AIRMAGNET

FITEL
FURUKAWA ELECTRIC

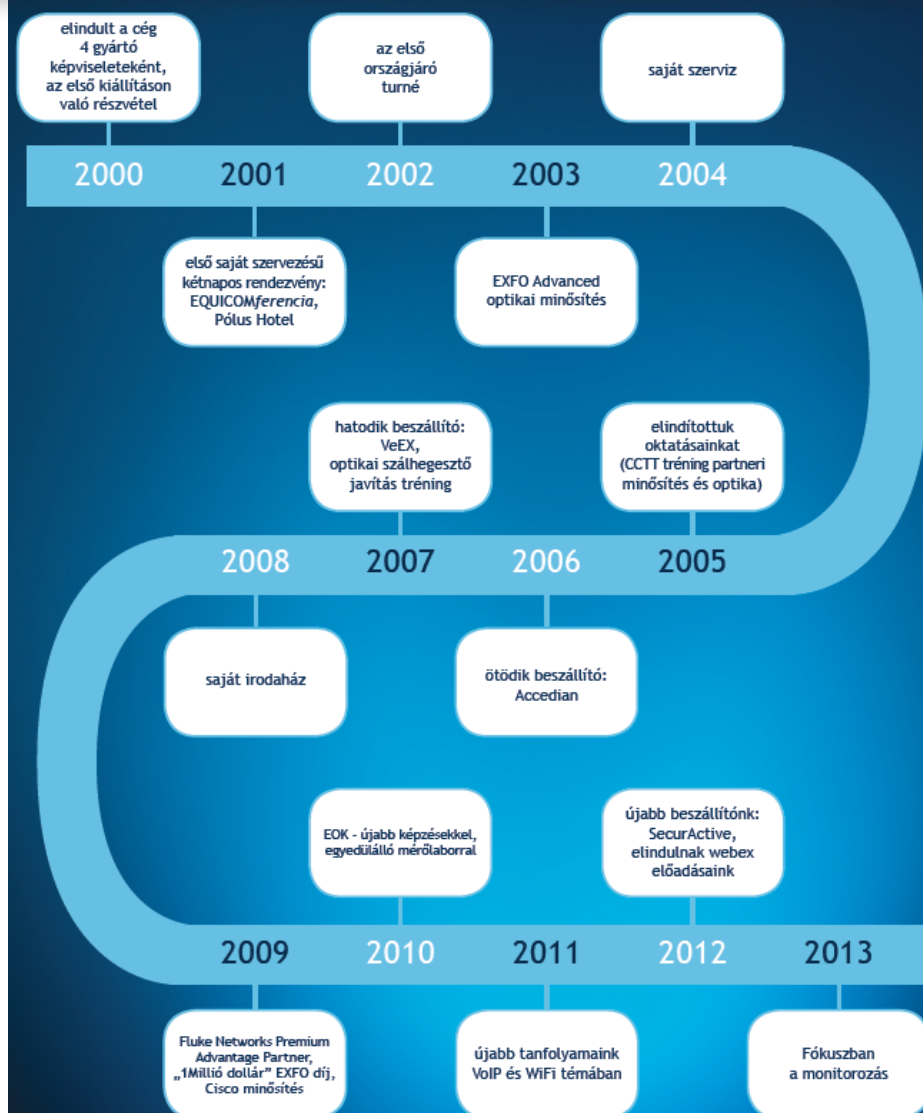
SUNRISE TELECOM

VeEX

ACCEDIAN
NETWORKS

SecurActive
Performance Vision

- Piaci jelenlét: szolgáltatók és vállalati szegmens
- Közvetlen kapcsolat a felhasználó és a gyártó között
- Szakértelem, tanácsadás, támogatás, szakmai oktatások (9 tematikus EOK tanfolyam)



Wi-Fi evolúció

#1 eszközök és adatmennyiség



#2 sebesség és technológia

2Mbps 11Mbps 54Mbps 150Mbps 433Mbps 866Mbps

>8Mrd
90PB/óra
6.75Gbps

consumer IoT
okostelefon
laptop



b

a

g

n

a
c

a
d

a
h

1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014



#3 Felhasználási területek



BRING YOUR OWN DEVICE
Straight Ahead ↑↑

TSUNAMI HAZARD ZONE
3G
IN CASE OF IP DATA FLOOD
OFFLOAD TO WI-FI

a biztonság *kritikus*

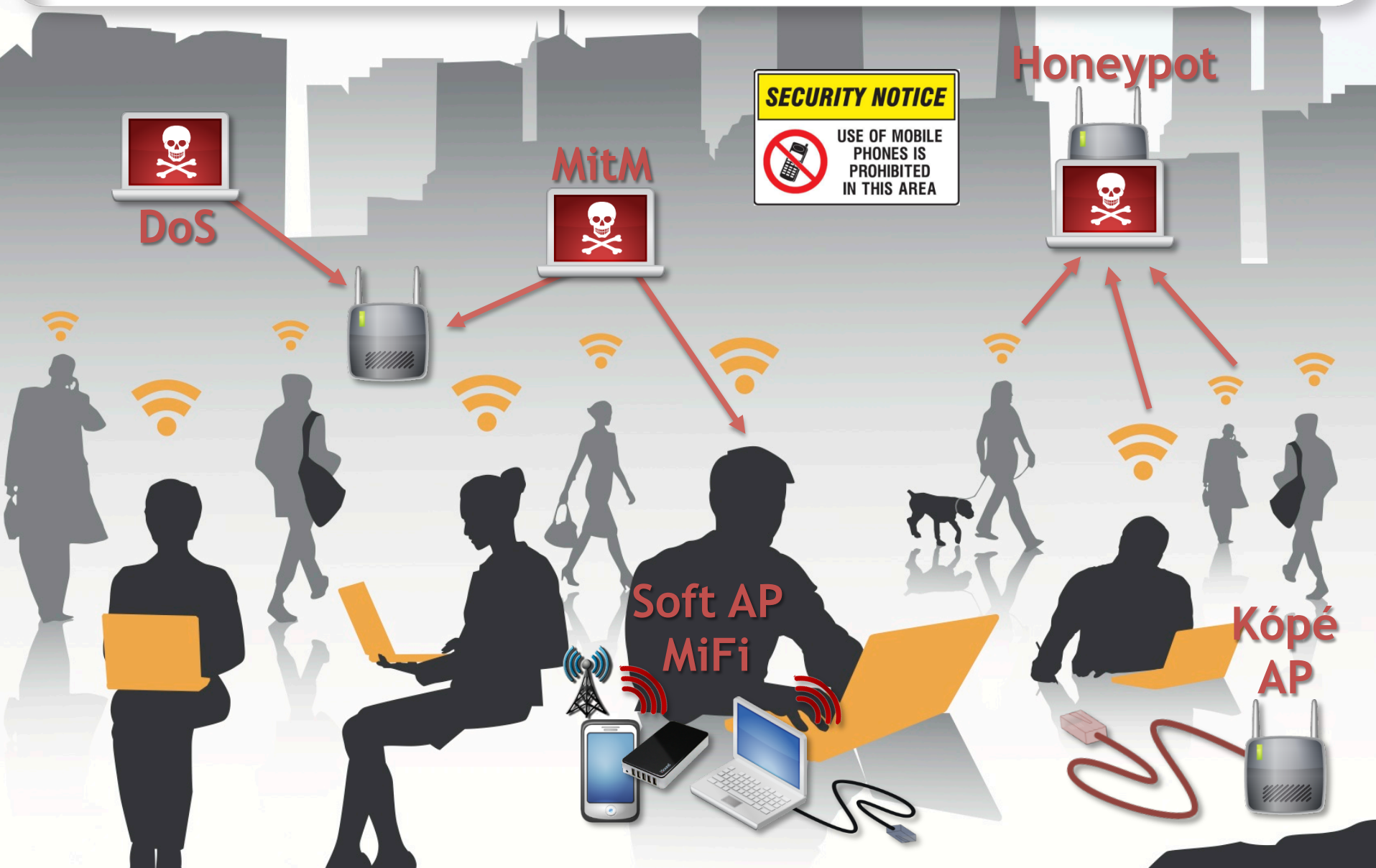


Wi-Fi veszélyek/támadások

...és a mobil is itt van

@equicom

a GSM mérés technikai szakértője



AirMagnet Enterprise - architektúra

@equicom

az Ön ICT mérés technikai szakértője



100% passzív*

72 óra

WiFi és spektrum

konzol

3x3 MIMO

- WIPS/WIDS
- Spektrum
- AHC
- mesh



Automatic Health Check

AME

>1000 szenzor

DTU

Dynamic Threat Update

airmagnet.com

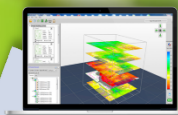
WLAN életciklus

@equicom

az Ön ICT mérés-technikai szakértője

AirMagnet Enterprise

WLAN/Cell monitorozás



AirMagnet
Planner

OptiView XG
és OneTouch AT
LAN/WLAN analízátorok



AirMagnet
Survey

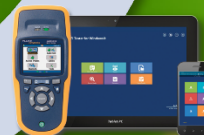
AirMagnet
WiFi Analyzer



Airmapper
Android



AirMagnet
VoFi Analyzer



AirCheck™
WiFi teszter család

AirMagnet
Spectrum XT
és Spectrum ES



Köszönöm a figyelmet!

Tesztelje saját hálózatán! ➡ info@equicom.hu

- Kérje személyes konzultációnkat

Fluke Networks WLAN megoldások

- www.equicom.hu/wlan

Szakmai cikkeink ➡ info@equicom.hu

- BYOD - a jelenség
- WLAN hálózatbiztonság és megfelelőségi irányelvek
- Lefedő vs. Integrált vezeték nélküli hálózatvédelem

Webex előadásaink

- <http://www.equicom.hu/webex>

Monitorozó megoldásaink

- <http://www.equicom.hu/monitoring>

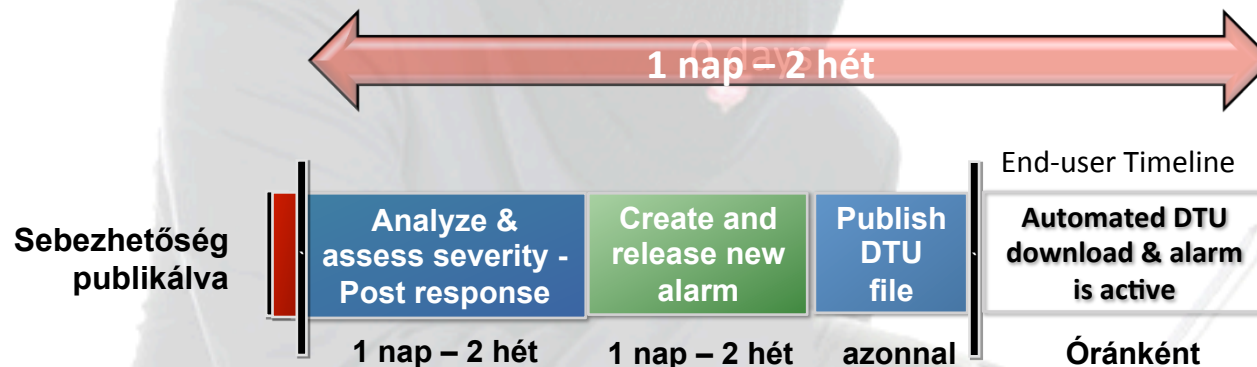


Háttér diák



SECURITY

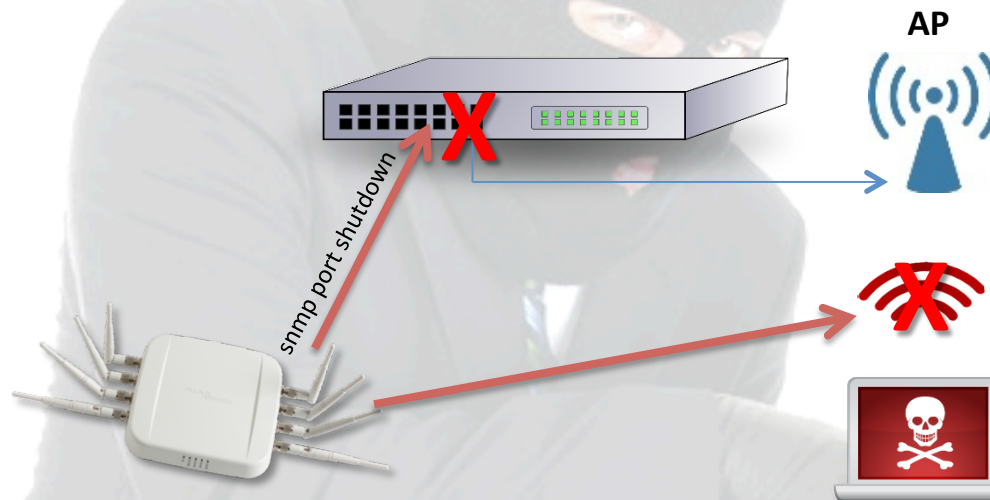
Dinamikus Sérülékenység adatbázis Frissítés (DTU)



Az új fenyegetések szignatúrái automatikusan beépülnek a meglévő szabályrendszerbe, a szenzorokba töltődnek, leállítás és beavatkozás nélkül!

SECURITY

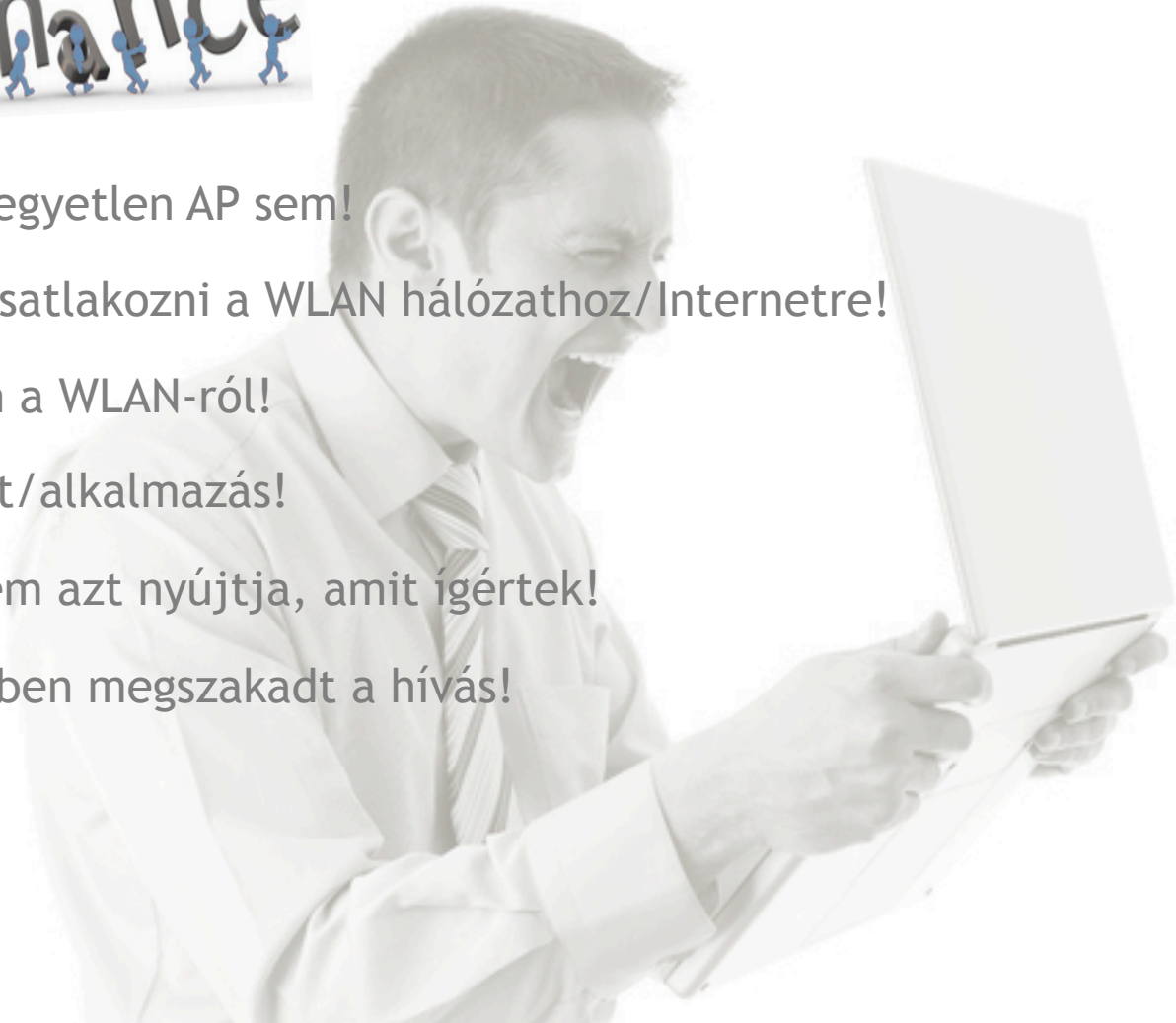
Wireless/Wired Blocking



Rendkívül alacsony csatorna terhelés blokkoláskor.
Akár 10 eszköz 10 csatornán történő blokkolása egyetlen szenzorral.

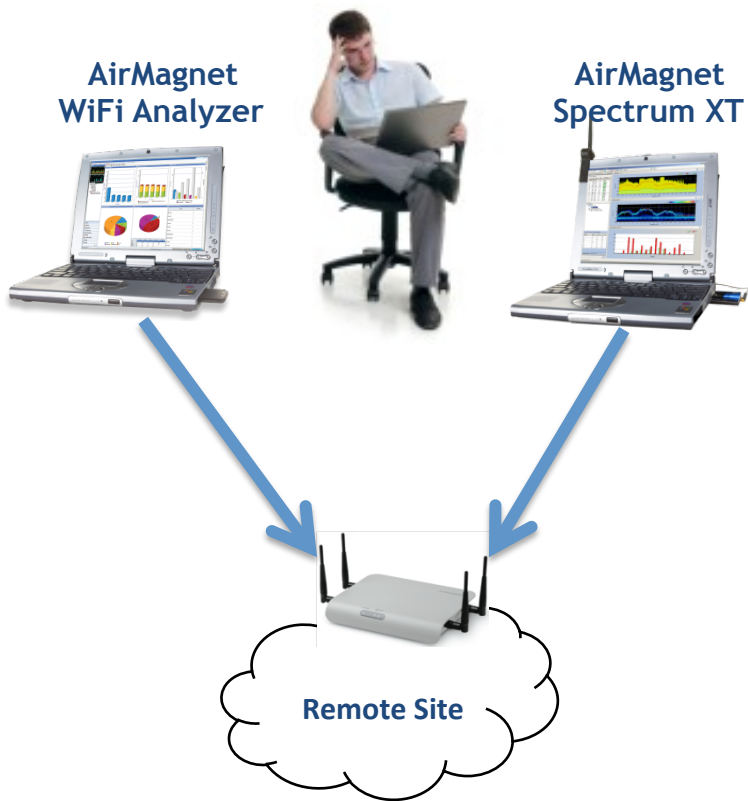
Performance



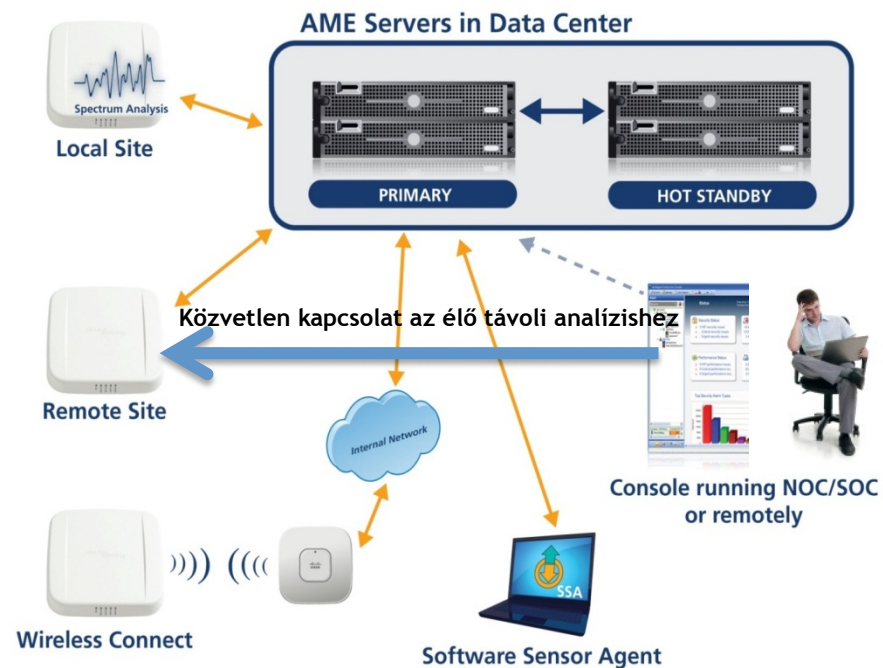
- Nem látszik egyetlen AP sem!
 - Nem tudok csatlakozni a WLAN hálózathoz/Internetre!
 - Leszakadtam a WLAN-ról!
 - Lassú hálózat/alkalmazás!
 - A 802.11n nem azt nyújtja, amit ígérték!
 - Roaming közben megszakadt a hívás!
 - stb. stb. stb.
- 



Remote Analyzer



AirMagnet Enterprise (Remote Test Kit)





WiFi analízis

- Csatornák
- Interferenciák
- Infrastruktúra felépítése
- Top Traffic tesztek
- AirWise policy
- Decode
- Riportok

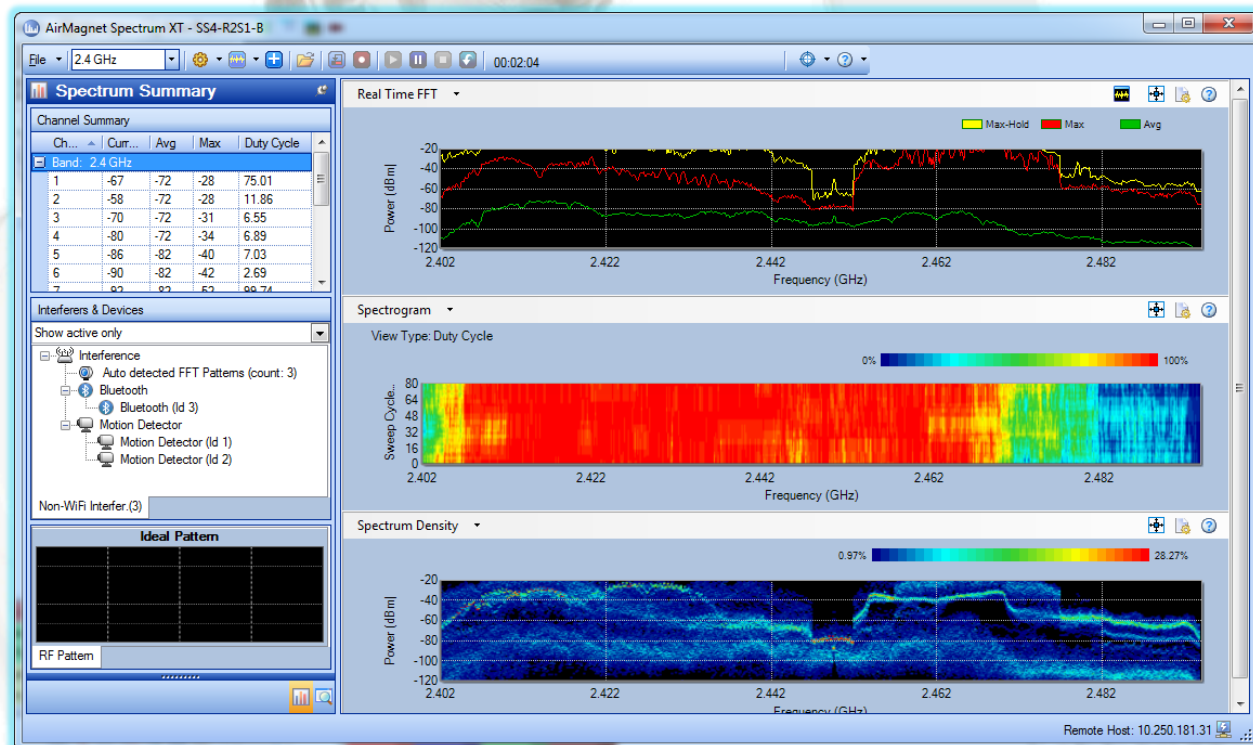
Frame Gap	Length	Source	Destination	BSSID	Summary
0.004471	188	04:13:80:43:11:52	7F:B7:FF:FF:FF:77	00:93:C8:43:11:52	802.11 beacon
0.000362	198	DF:3E:92:32:C0:02	16:51:03:49:FF:00	37:33:EC:77:2E:06	LLC SSAP:34 DSAP:C2
0.004201	304	95:20:98:36:0A:00	B7:AA:95:02:58:09	B7:AA:95:02:58:09	LLC SSAP:AM DSAP:03
0.003241	122	38:95:F7:0C:A8:E9	38:1C:E4:20:52:EF	802.11 CF End	
0.000533	193	C8:CA:98:ED:37:D5	2D:FB:A1:A9:F3:CF	00:00:00:00:00:00	802.11 encrypted data
0.004520	180	Cisco:43:11:51	FF:FF:FF:FF:FF:FF	Cisco:43:11:51	802.11 beacon
0.002750	190	2A:00:50:35:00:02	62:4F:03:43:FF:AF	37:30:EC:77:2E:06	LLC SSAP:42 DSAP:95
0.013470	162	Cisco:43:11:50	FF:FF:FF:FF:FF:FF	Cisco:43:11:50	802.11 beacon
0.000361	153	29:CA:58:F3:A2:99	5A:F6:EC:7F:5C:14	5A:F6:EC:7F:5C:14	LLC SSAP:1B DSAP:95
0.002161	146			00:00:00:00:00:00	802.11 unknown ctrl frame
0.002223	242	Cisco:A7:EA:30	FF:FF:FF:FF:FF:FF	Cisco:A7:EA:30	802.11 beacon
0.001578	178	DE:10:FE:17:4E:9F	E3:88:0A:7D:88:40	40:18:FE:7D:D7:68	802.11 reassociation request
0.000483	154	37:17:86:76:D8:4C	E7:2C:38:12:17:3E	EF:74:4C:29:61:DA	802.11 authentication
0.003583	133	31:23:8C:F9:C9:DE	F6:50:78:E2:06:5F	07:86:9C:CF:E:8:60	802.11 beacon
0.004288	120	FD:28:19:A2:9F:CD	41:DE:05:05:DA:89	56:52:3C:99:2E:27	802.11 association request
0.003688	183	Cisco:43:11:55	FF:FF:FF:FF:FF:FF	Cisco:43:11:55	802.11 beacon
0.000341	193		41:F6:EC:F5:5A:5C	41:F6:EC:F5:5A:5C	LLC SSAP:91 DSAP:9F
0.003984	193	Cisco:43:11:55	FF:FF:FF:FF:FF:FF	Cisco:43:11:55	802.11 beacon
0.001810	146	DD:42:18:9F:27:06	9F:1F:7D:76:61:CF	81:02:9E:46:36:7C	802.11 encrypted GoS data/rtnl function
0.000343	198	2B:9C:1E:62:90:77	53:04:DA:43:08:1B	38:E2:33:63:9C:9A	802.11 reassociation request
0.001014	121			00:00:00:00:00:00	unknown
0.004219	162	Cisco:43:11:54	FF:FF:FF:FF:FF:FF	Cisco:43:11:54	802.11 beacon
0.000039	122			0F:FE:F8:D5:DA:08	802.11 Control Wrapper
0.000767	146			0F:1E:50:35:19:40	802.11 Block Ack Request
0.004076	123	Cisco:linksys:B5:AA	FF:FF:FF:FF:FF:FF	Cisco:linksys:B5:AA	802.11 beacon
0.000292	158	DF:10:F2:1E:95:7D	9E:4F:03:49:81:8C	81:03:FE:00:93:5C	802.11 reassociation request
0.004008	188	Cisco:43:11:53	FF:FF:FF:FF:FF:FF	Cisco:43:11:53	802.11 beacon
0.000506	131			00:00:00:00:00:00	unknown
0.003311	120			00:00:00:00:00:00	unknown
0.004155	153	C8:CA:35:E7:CE:D5	2D:FB:80:12:0E:89	2D:FB:80:12:0E:89	LLC SSAP:F8 DSAP:95
0.004029	146			00:00:00:00:00:00	802.11 unknown ctrl frame

Broadcast	Unicast	Multicast
53204	116	116
Unicast	55480	49556
Total Fra.	193266	31.35%



RF spektrum analízis

- Spektrum intelligencia
- Eszköz felismerés
- Bluetooth tesztek
- Riasztások



Performance

Automatic Health Check (AHC)

