



FITI 2016 Konferencia

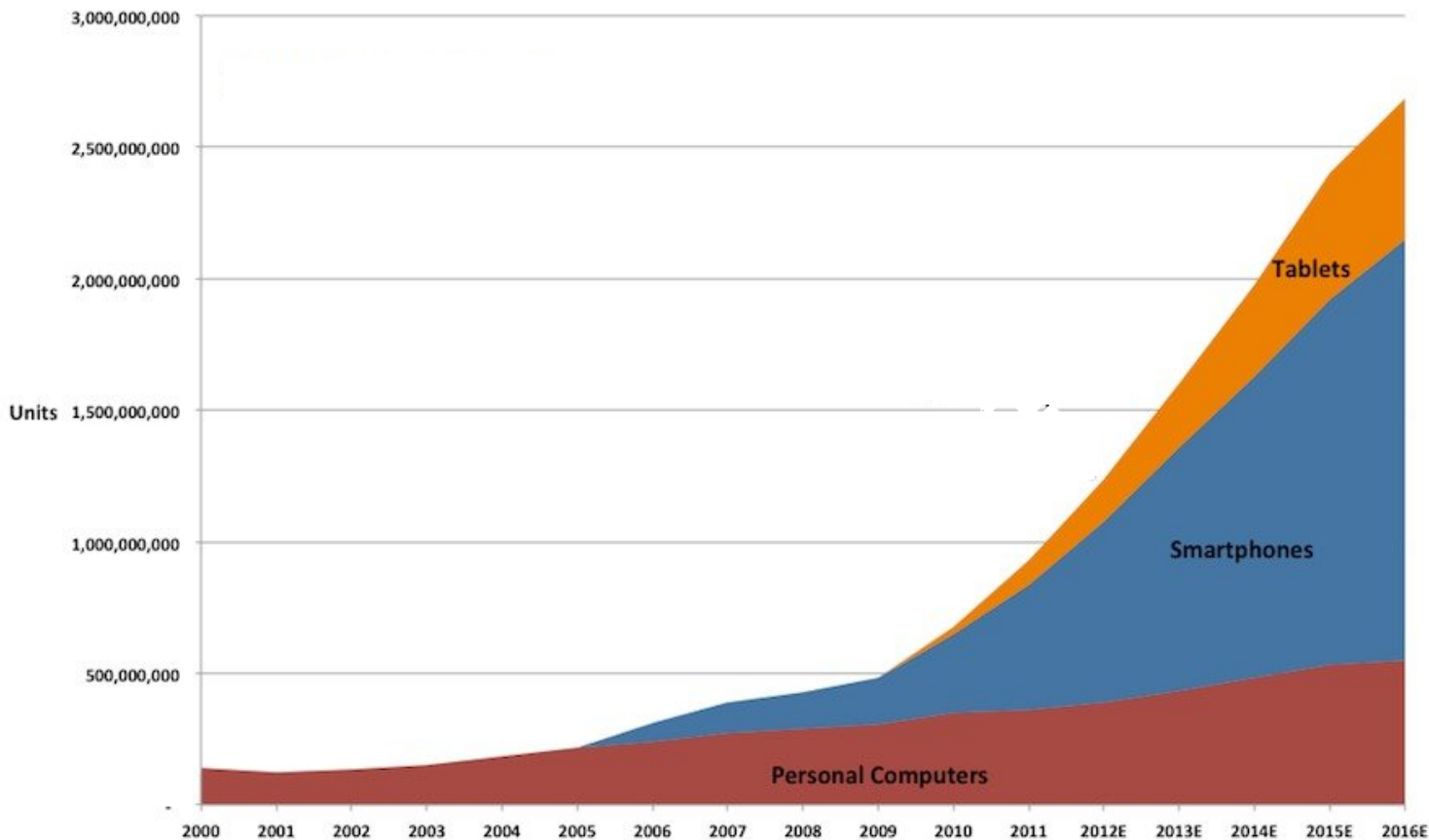
Jövőbiztos adatközpontok – A sebességnövekedés kihívásai és hatásai

7/24 WiFi monitorozás a teljesítmény és biztonság garanciája

Kritikus IT infrastruktúrák esetében fontos tudni, hogy vannak-e jelen hordozható eszközök, ha igen, ezek engedélyezettek-e, ki és milyen célra használja őket. Kordában kell tartani ezeket az eszközöket, hogy a vállalati, intézményi szabályrendszerek se sérüljenek, az adatok biztonságban legyenek, és a felhasználói élményindex se csökkenjen. Ezt garantálni csak és kizárólag folyamatos felügyelet megvalósításával lehetséges.

Internetes eszközök száma

Smartphone és Tablet



Source: Gartner, IDC, Strategy Analytics, company filings, BI Intelligence estimates



Adatforgalom növekedése

Mobil és WiFi

Figure 4

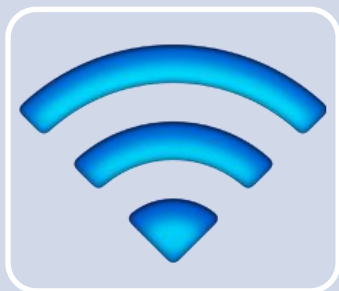
Attribute	Mobile/ Cellular	Wi-Fi	No Difference	N*
Lowest Cost	20%	56%	24%	746
Speed of Network	18%	58%	24%	800
Best Reliability	31%	46%	23%	794
Best Performance for My Applications	27%	46%	27%	759
Best Coverage	46%	35%	19%	792
Most Secure	34%	35%	31%	753
Easier to Use	29%	40%	31%	821

* Don't Knows removed from sample.

Q38. Thinking about Wi-Fi and mobile/cellular networks, which type of wireless network do you think offers the most desirable performance or features in each of the following areas?

Forrás: Cisco IBSG 2012

WiFi piaci trendek



WiFi
mindenhol



BYOD



Carrier
Wi-Fi



Technológia
(802.11n és
ac)



Small Cell
(mobil &
Wi-Fi
integráció)

WiFi hálózatok előretörése

WiFi mindenhol

- Kevesebb Ethernet port
- 100% WLAN “iroda” mára realitássá vált
- Kockázatok növekednek
- A biztonság és megfelelés igénye megnő
- Elvárás a stabil kapcsolat és megbízható teljesítmény



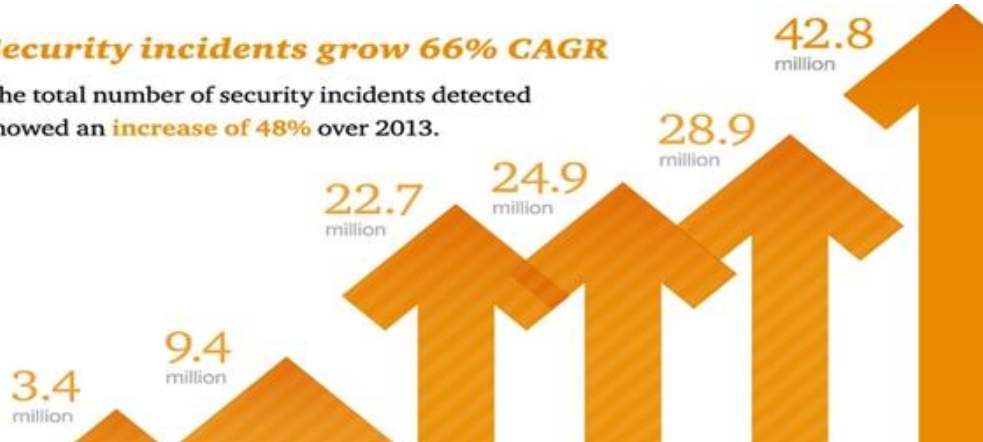
**Mindenki csak
WiFi-n akar
kapcsolódni!!!**

Növekvő biztonsági fenyegetettség

... a költségek is növekednek

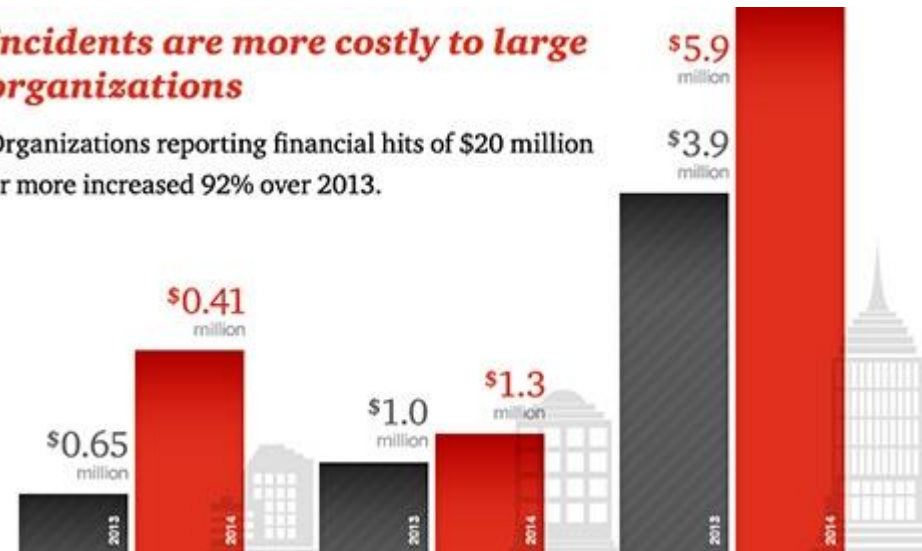
Security incidents grow 66% CAGR

The total number of security incidents detected showed an **increase of 48%** over 2013.



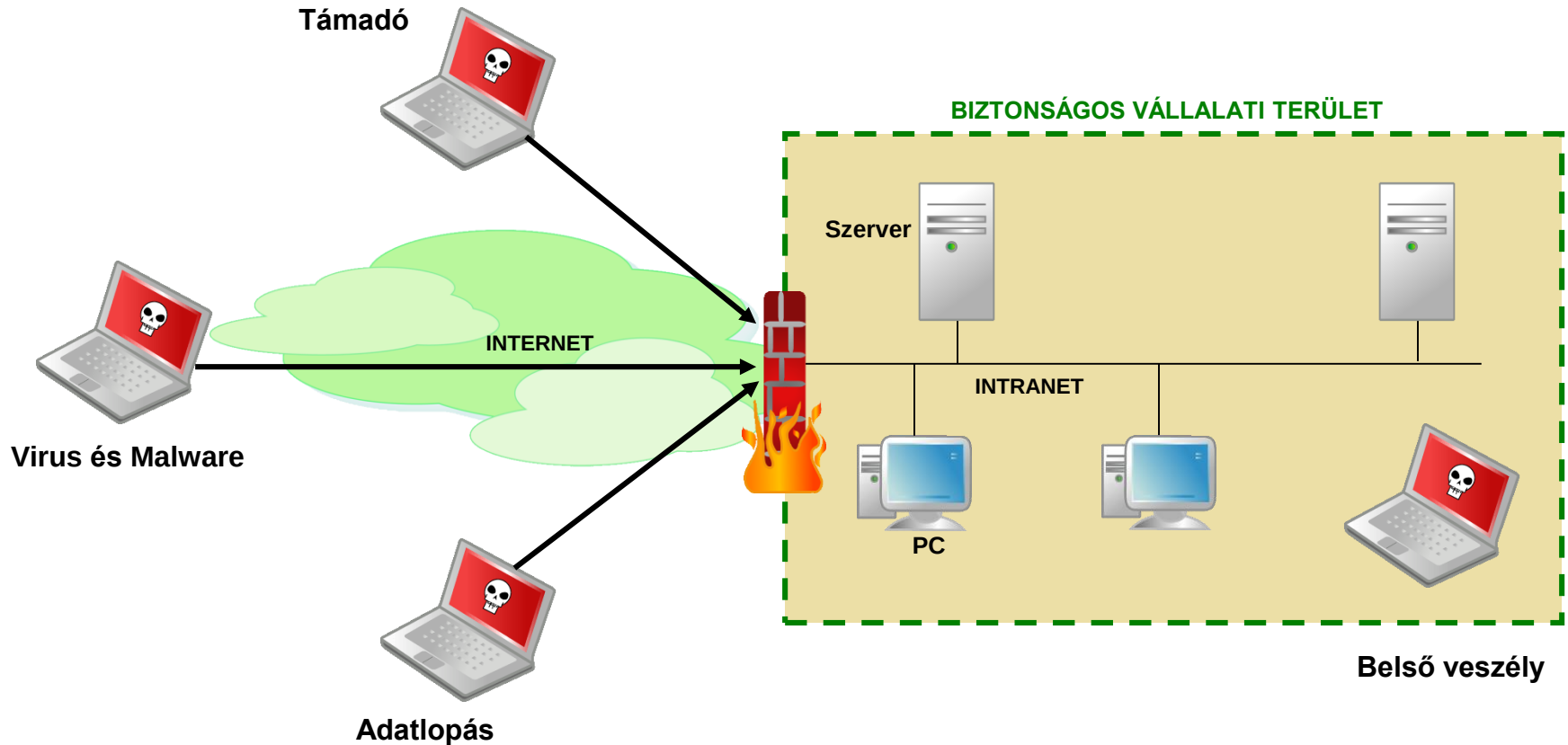
Incidents are more costly to large organizations

Organizations reporting financial hits of \$20 million or more increased 92% over 2013.



Vállalati vezetékes hálózat biztonsága

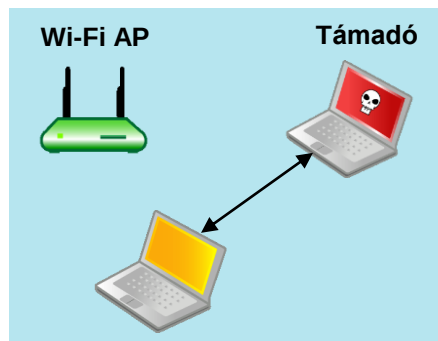
jól körülhatárolható és védhető



Vállalati vezeték nélküli hálózat biztonsága

nehezen körülhatárolható és sérülékeny

6 Wi-Fi Phishing



Mobil felhasználó

Külső Wi-Fi növeli a vállalati hálózat fenyegetettségét

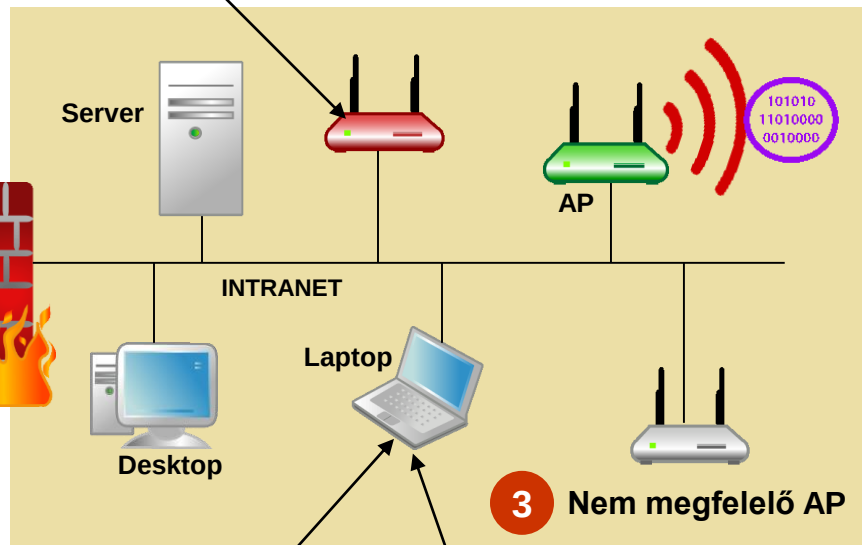
Már bent is van

1 Kópé AP a belső hálózaton



Hacker

2 Biztonsági rés és adatküldés



3 Nem megfelelő AP

4 Szomszéd AP

5 Belső szabályok megkerülése



Városi Wi-Fi

WiFi biztonsági fenyegetettség

Kifinomult támadási eljárások

Egyszerű használat
Egyszerű hozzájutás



reaver-wps

Brute force attack against Wifi Protected Setup



metasploit

Airpwn



Mi az igazi kihívás?

Engedély nélküli
mobil eszközök
és forgalom
detektálása

Diszkrét
biztonsági
megoldásra van
szükség

Engedély nélküli
RF Jammer
detektálása

Diszkrét biztonsági
megoldásra van
szükség

Layer 1&2
biztonságossá
tétele

Igény könnyen
használható
megoldás igénye

Biztosítani a
“no-wireless”
területeket

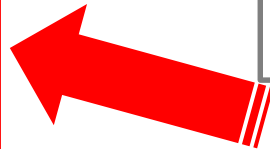
Lementeni és
tárolni a
bizonyítékokat

Engedély nélküli
mobil eszközök
és forgalom
detektálása

Megfizethető
eszközök igénye

Authentication &
Encryption nem
elegendő

A mobil kliens a
gyenge láncszem



RF spektrum vizsgálata

megfelelő biztonság és teljesítmény érdekében



Nem engedélyezett eszközök és forgalom



Tiltott WiFi zóna biztosítása



Események nyomkövetése



RF interferencia források észlelése



Zárt hálózatok monitorozása

Egyéb interferencia források

jelentősen ronthatják a teljesítményt

- Bluetooth
- Mikrosütők
- Cordless telefonok
- Analóg kamerák
- Játék kontrollerek
- Bébimonitorok
- Digitális video berendezések
- RF jammers
- stb...



WiFi teljesítmény

növekvő igények

Elvárások növekednek

- Wi-Fi még akkor is, ha nem annyira jó
- Egyre több alkalmazás WiFi-n

Több kliens+ több BYOD = WLAN stressz nő

- Egyre több a szűk keresztmetszet: torlódás, lefedettség hiánya, stb.
- Túl sok paraméter, komplex alkalmazási infrastruktúra, időszakosan jelentkező problémák, nehéz felderítés

IT feladatvégzés optimalizálást igényel

- Kliens bejelentések általánosak, későn érkeznek
- Kollégák túlfeszítettek
- Eltérő megoldásokkal nehéz a probléma feltárása



Inkább Wi-Fi
mint kábel!



“A felhasználók keresnek más megoldást , ha nem kapják meg a megfelelő támogatást”

AirMagnet Enterprise - AME

24x7 WIDS/WIPS rendszer a biztonságos WiFi hálózatért

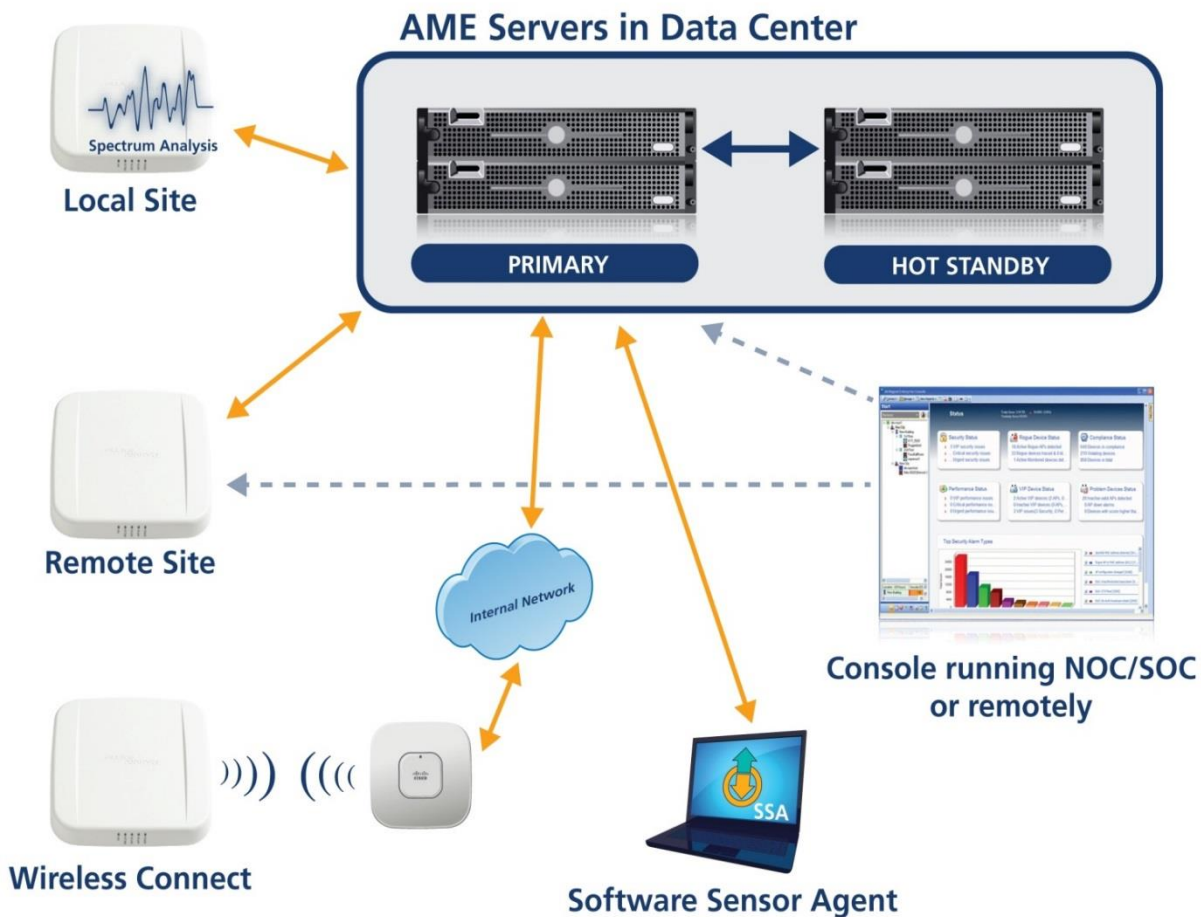
Rugalmas és skálázható

Szerverek

- Virtuális vagy dedikált Windows alapú platform
- A tartalék szerver akár másik adatközpontban
- Akár 1000 szenzor támogatása / szerver

Szenzorok

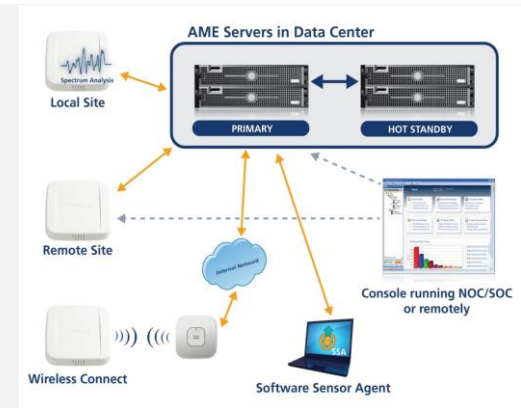
- Földrajzilag bárhol, biztonságos SSL kapcsolattal
- Hardver és Szoftver szenzorok kombinációja optimális monitorozáshoz



AirMagnet Enterprise - AME

24x7 WIDS/WIPS rendszer a biztonságos WiFi hálózatért

- Egy további védvonal – IDS/IPS
- DTU frissítések (Dynamic Threat Update)
- Aktív blokkolás
- Kifinomult capture
- Fenyegetés korreláció
- Smart eszközök észlelése, osztályozása
- 3rd party integráció (SIM/NMS)
- Proaktív analízis és hibakeresés
- Aktív tesztek (Automatic Health Check - AHC)
- Spektrum analízis és osztályozás WiFi/2G/3G/4G
(GSM/UMTS/LTE/PCS/AWS/SMR900/CDMA, Tetra (800 MHz), 900 Mhz ISM)
698 MHz és 2690 MHz

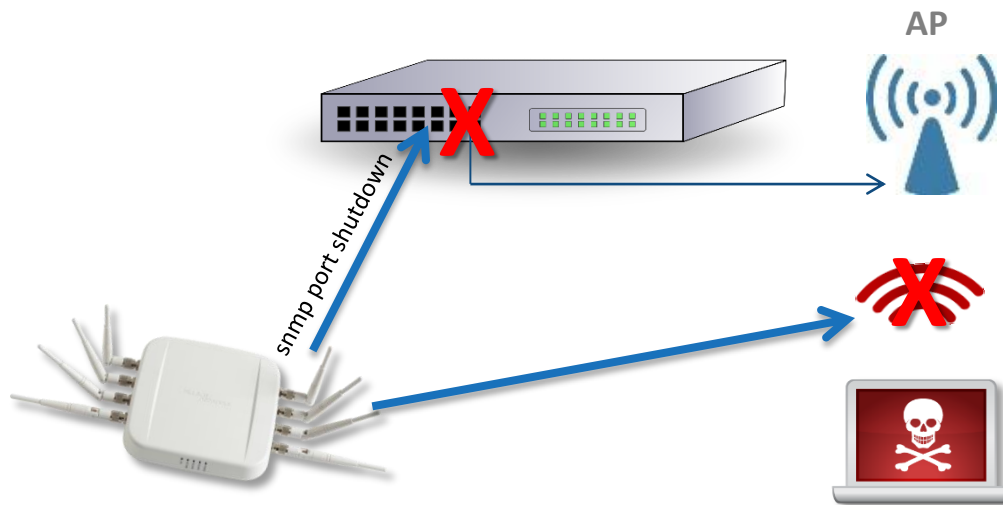


AirMagnet Enterprise - AME

a biztonságos hálózatért

SECURITY

Wireless/Wired Blocking



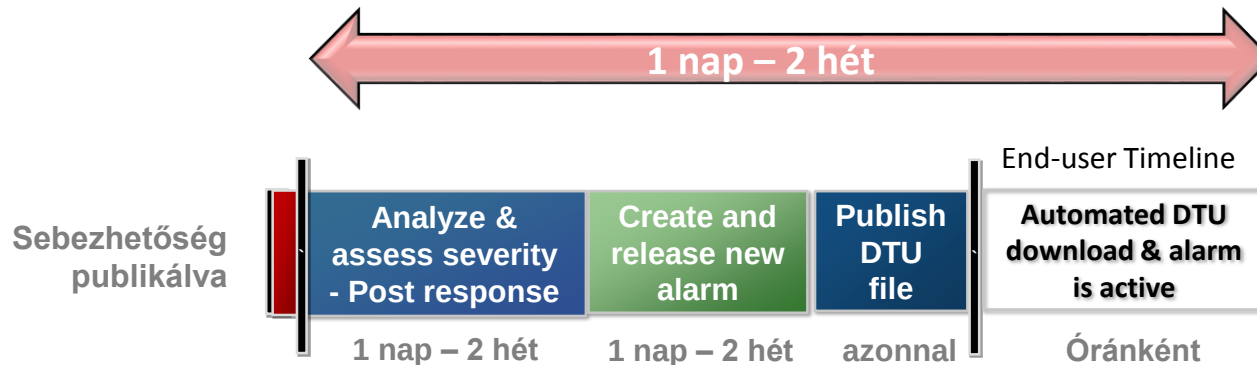
Rendkívül alacsony csatorna terhelés blokkoláskor.
Akár 10 eszköz 10 csatornán történő blokkolása egyetlen szenzorral.

AirMagnet Enterprise - AME

a biztonságos hálózatért

SECURITY

Dinamikus sérülékenység adatbázis frissítés (DTU)



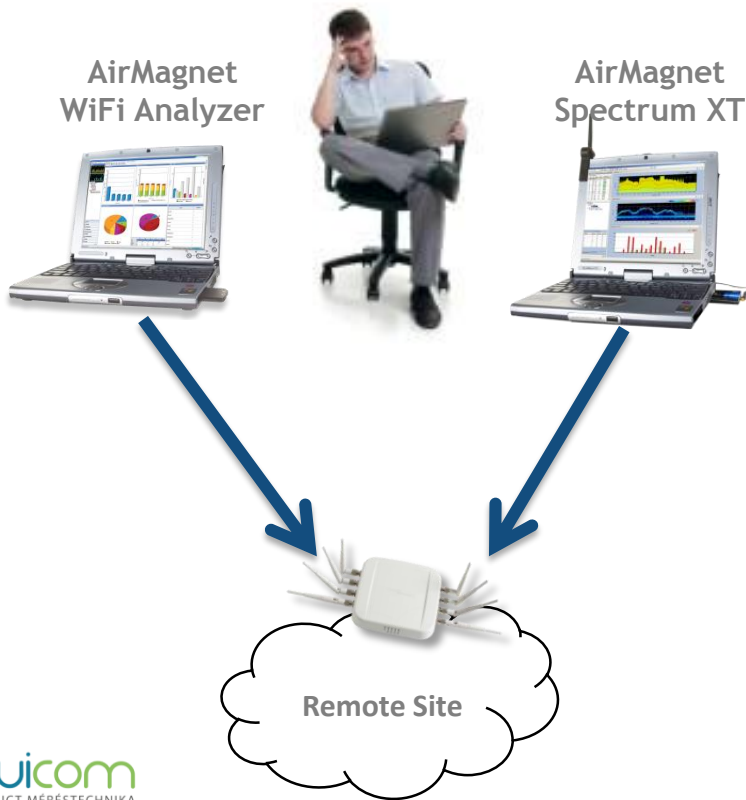
Az új fenyegetések szignatúrái automatikusan beépülnek a meglévő szabályrendszerbe, a szenzorokba töltődnek, leállítás és beavatkozás nélkül!

AirMagnet Enterprise - AME

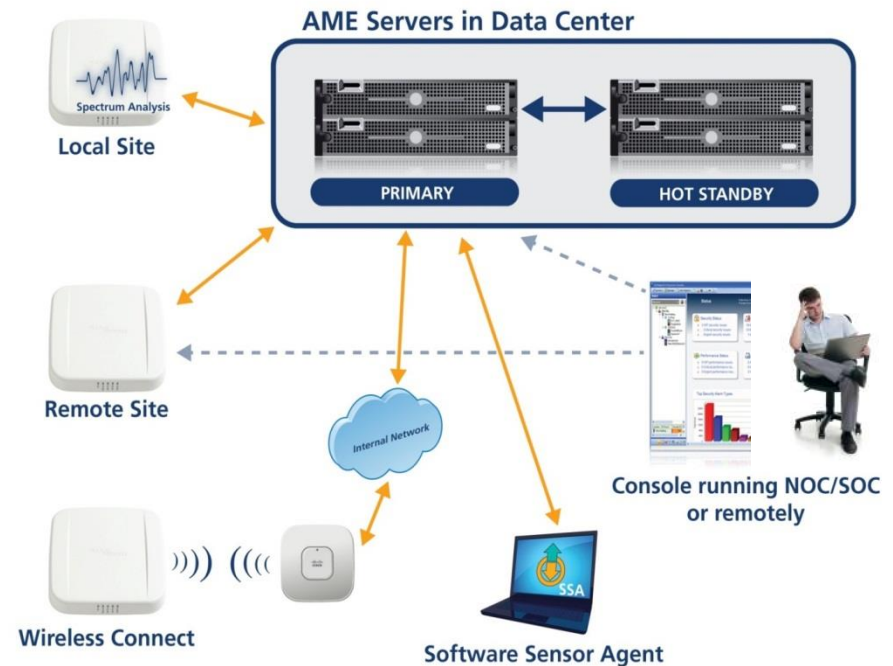
hatékony és kényelmes üzemeltetés



Remote Analyzer



AirMagnet Enterprise (Remote Test Kit)



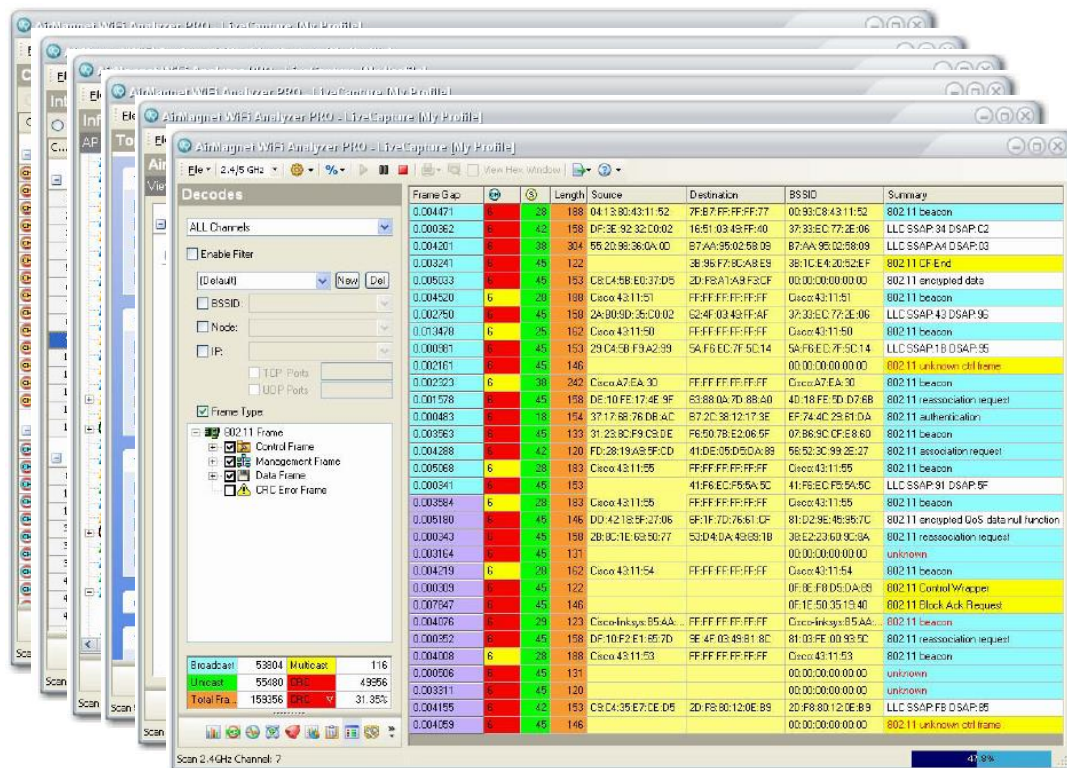
AirMagnet Enterprise - AME

hatékony és kényelmes üzemeltetés



WiFi analízis

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



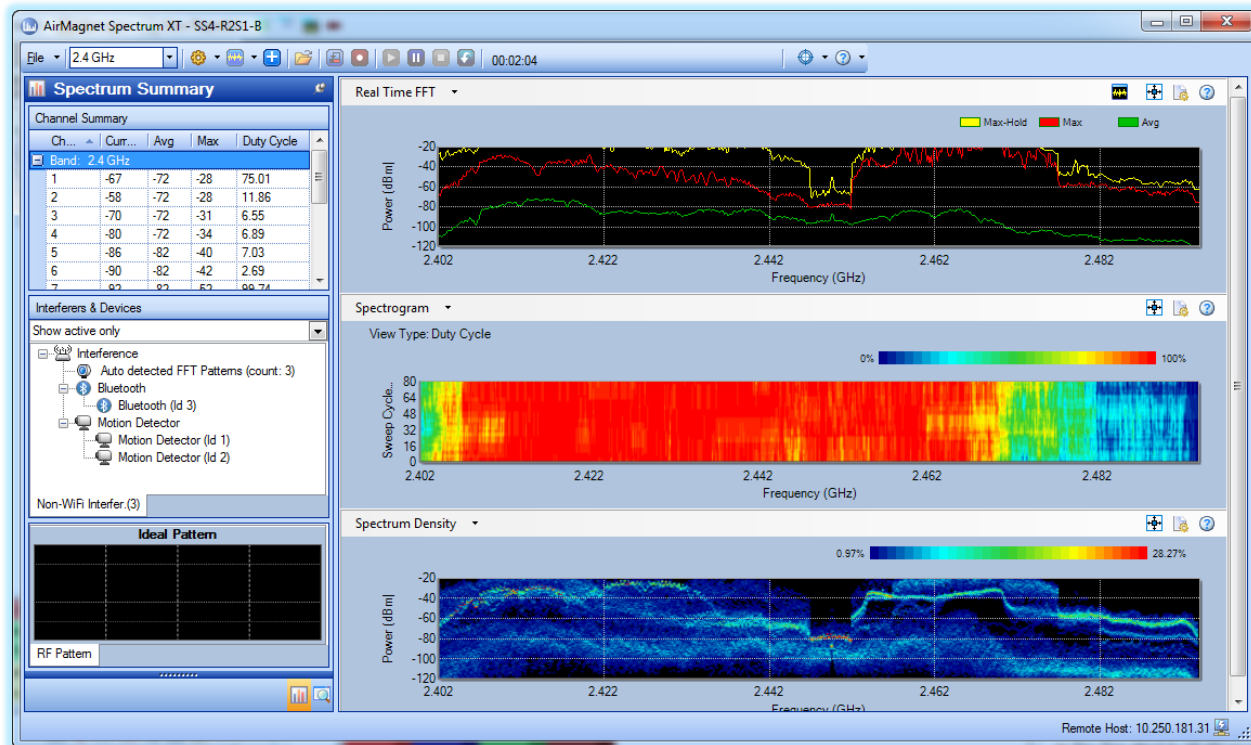
AirMagnet Enterprise - AME

hatékony és kényelmes üzemeltetés



RF spektrum analízis

- Spektrum intelligencia
- Eszköz felismerés
- Bluetooth tesztek
- Riasztások

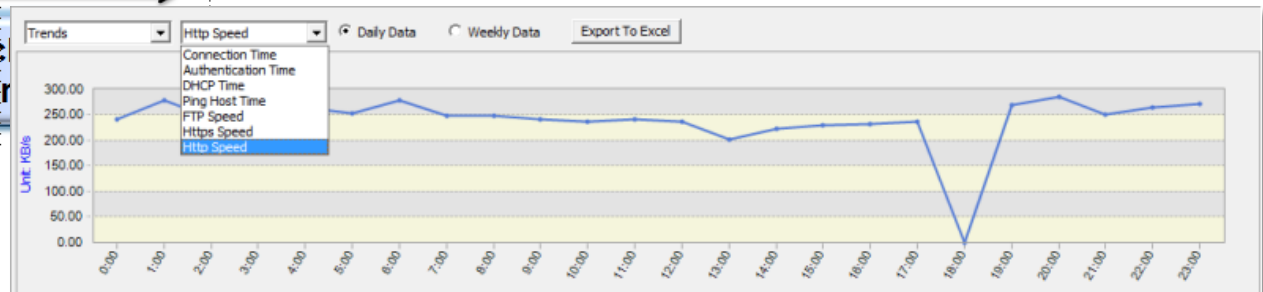
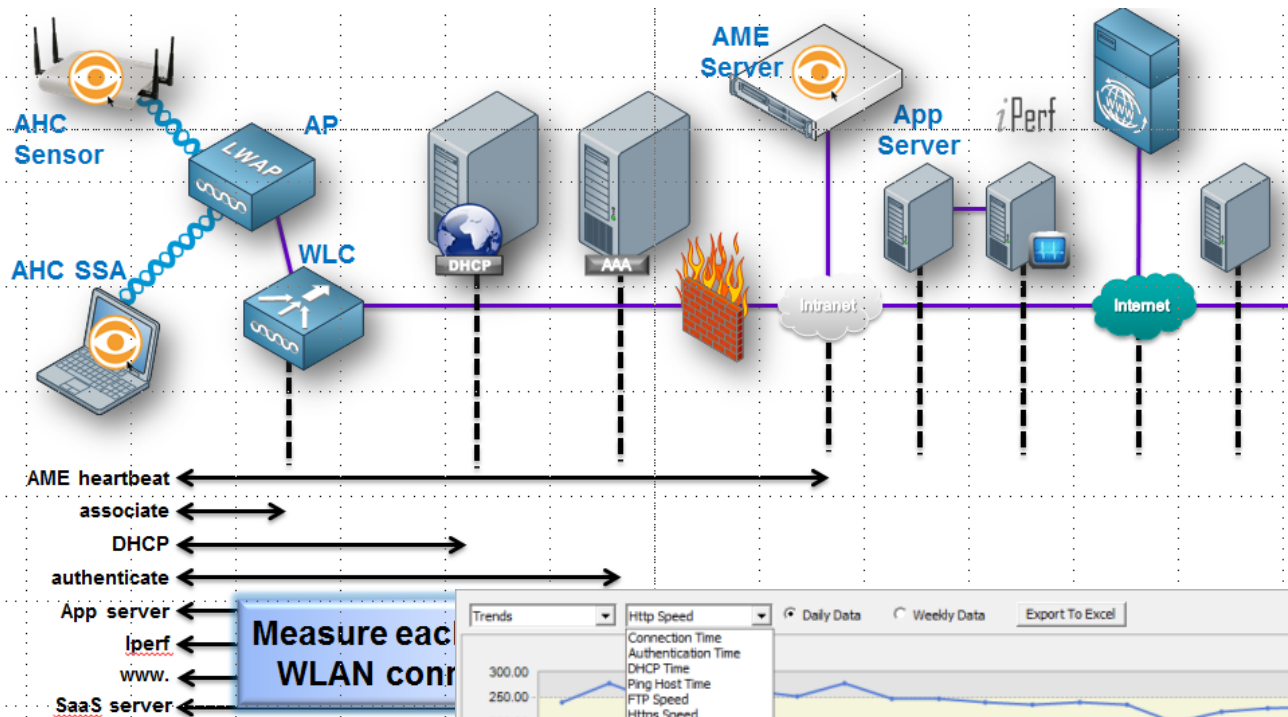


AirMagnet Enterprise - AME

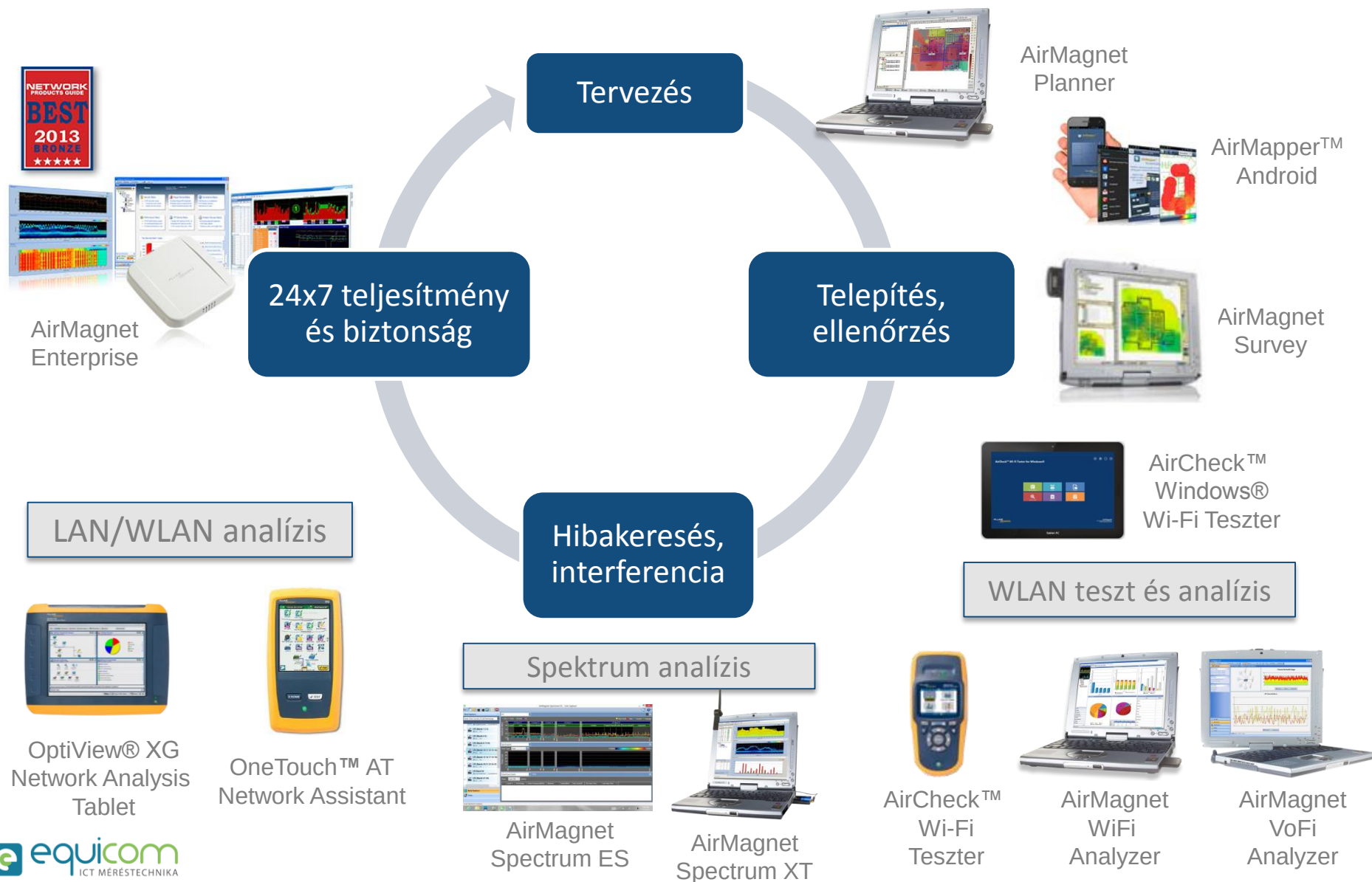
hatékony és kényelmes üzemeltetés



Automatic Health Check (AHC)



WLAN élelciklus



Tesztelje saját hálózatán!

- Kérje személyes konzultációnkat

AirMagnet Enterprise

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

Köszönöm a figyelmet!

Liskai János

liszkai.janos@equicom.hu

