

# Az IBM megközelítése a végpont védelemhez

## IBM PROFESSIONAL SECURITY SERVICES

### IT SECURITY

#### VÉGPONT VÉDELEM

#### VÉGPONT ADAT VÉDELEM

Sérülékenység centrikus behatolás  
elhárító rendszer (IPS)

Kliens tűzfal

Anti-malware technológia

IBM X-Force® védelem

Szignatúra és viselkedés alapú AV

Puffer Túlcsondolás Elleni Védelem

Futures

Network access control

Adatszivargás védelem

Titkosítás menedzsment

Proventia content analysis

Device Control



#### BIZTONSÁGI KONFIGURÁCIÓ MENEZSMENT

#### VÉGPONT RENDSZER KARBANTARTÁS

Application Control

Security configuration management

Security policy management

Vulnerability assessment

Patch management

Power management

AV and anti-spyware  
client management

Deployment/removal tools

### IT OPERATIONS

# Végpont védelmi megoldás

## Rendszer Védelem

IPS

Tűzfal

Anti-Malware

X-Force



Az IBM megoldás tartalmazza az alábbi összetevőket:

- Megelőző védelem az X-Force® kutató – fejlesztő csapatnak köszönhetően
- Hozt alapú behatolás elhárító rendszer (IPS)
- Anti-malware technológia

### Általános Problémák

- 1.A végpontok nincsenek menedzselve
- 2.A különböző megoldások közötti kommunikáció hiánya gyenge pont lehet
- 3.Magas TCO és támogatási költségek
- 4.A különböző agentek terhelése a végpont erőforrásait felemészti

### Az IBM Proventia ESC Értéke

- 1.Komplett – teljeskörű védelem munkaállomás, szerver és hordozható gépek számára
- 2.Alacsonyabb költség, mint a külön-külön megoldások
- 3.Megoldás az anti-malware megoldások közötti kommunikációra
- 4.Alacsony adminisztráció

# Adat Biztonság

## Adat Biztonság



NAC

DLP

Titkosítás

Tartalom Vizsg.

Az IBM megoldás tartalmazza az alábbi összetevőket:

- Network Access Control
- Data Loss Prevention
  - Verdasys partnerség
- Titkosítás
  - PGP & Verdasys partnerség
- Tartalom Vizsgálat
  - Proventia Content Analyzer segítségével

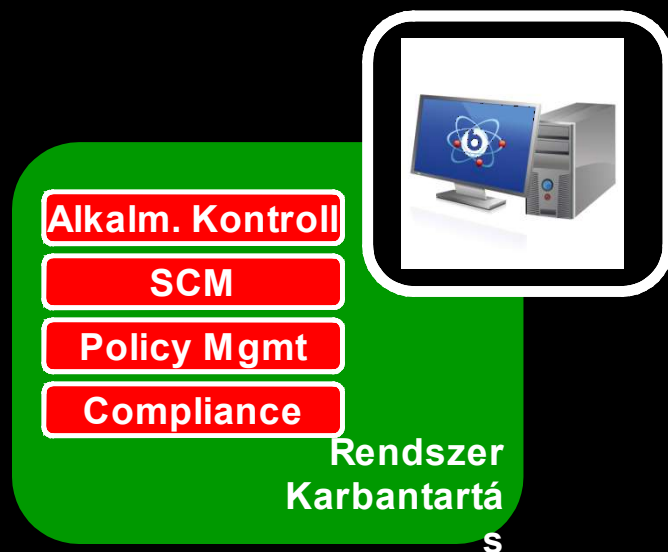
## Általános Problémák

1. Komplex menedzsment megvalósítása különböző agentek és vendorok között
2. Nehéz hálózati hozzáférés kontroll a különböző hálózatokon
3. A teljes körű adatbiztonsági megoldások installálása
4. A megfelelőség mérése a különböző gyártók alkalmazása miatt

## Az IBM Proventia ESC Értéke

1. Egy központi menedzsment felület több gyártó megoldásához
2. Gyors telepítő/eltávolító eszközök
3. A „fixlet” technológiával gyorsan felvértezhetjük védelemmel a megfelelő végpontokat
4. Egyszerű megfelelőségi nézet

# Biztonsági Konfiguráció Menedzsment



Az IBM megoldás tartalmazza az alábbi összetevőket:

- Policy Menedzsment
- Alkalmazás kontroll
- Biztonsági Konfiguráció Menedzsment (SCM)
- Megfelelőségi tulajdonságok

## Általános Problémák

1. Audit / Megfelelőség
2. Komplex / drága „kézi” konfigurációs audit, riportolás és helyreállítási folyamatok
3. Nincs központi nézet a rendszer konfigurációkban
4. Hosszú időbe telik a végpontok megfelelő beállítása

## Az IBM Proventia ESC Értéke

1. Valós idejű konfigurációs nézet
2. Heterogén rendszertámogatás
3. Kézi és automatizált helyreállítás
4. „Valós rendszer” pontos és auditálható riportokhoz
5. Szabvány oldali konfigurációs megközelítés

# Rendszer Karbantartás



Asset Discovery

Software Dist

Power Mgmt

Patch Mgmt

AV Client Mgmt

Konfiguráció  
Menedzsment

Az IBM megoldás tartalmazza az alábbi összetevőket:

- Asset discovery
- Szoftver elosztás
- **Power management**
- AV konfiguráció menedzsment
- Valós idejű, automatizált patch menedzsment

## Általános Problémák

1. A „sérülékenységi ablakok” csökkentése
2. Különböző környezetek
3. Patch-elési ütemezés
4. Patch-elés sikerének visszajelzése

## Az IBM Proventia ESC Értéke

1. Lerövidült patch-elési folyamatok
2. Sikertelen patch-elés észlelése
3. Valós idejű visszajelzés a patch állapotáról
4. Szoftver elosztás (mérettől függetlenül)

# Végpontvédelem és takarékoság?

- Gartner felmérés szerint **\$40K takarítható meg** 1 év alatt 2500 gép esetén
- Ez körülbelül **\$16 / PC** megtakarítás

## Gartner Newsroom

### PRESS RESOURCES

[Event Registration](#)

[Events Calendar](#)

[Gartner Blog Network](#)

[Videos](#)

[Podcasts](#)

[Photographs](#)

[Gartner Books](#)

[Analyst Coverage Areas](#)

[Press Release RSS Feed](#) 

[Attribution Guide](#)

### ABOUT GARTNER

[Products & Services](#)

### Press Releases

CURRENT | [VIEW ALL](#)

#### **Gartner says PC Power Management Activation Can Save a 2,500-PC Organization More Than \$40,000 a Year**

Total Power Consumption per Year for a Well-Managed, 2,500-PC Organization is 43 Percent Lower than for an Unmanaged One

STAMFORD, Conn., February 9, 2009 —

Organizations that are actively employing power management functionality can expect to save \$43,300 per year, compared with an unmanaged 2,500-PC organization, according to Gartner, Inc. In addition, turning off and unplugging machines saves another \$6,500, but this may affect employee productivity because updates will need to be carried out during working hours.

"Much attention on power consumption has focused on the data center, but PC power consumption in an organization can also be significant, especially given steadily rising electricity prices," said Federica Troni, principal analyst at Gartner. "IT organizations should recognize that the greatest savings come from employing power management features. They should investigate the power management capabilities of their PC life cycle management tools and PC power management point solutions to implement these policies and to better support management activities."

Forrás: <http://www.gartner.com/it/page.jsp?id=878912>