



# Check Point Endpoint Security

*- pojedynczy agent ochrony stacji końcowej*

Marek Krauze

*marek.krauze@clico.pl*

# Agenda

## Rozwiązania klasy „Endpoint security”

- Wyzwania dla bezpieczeństwa
- Pojedynczy agent, pojedyncza konsola
- Silne zabezpieczenia
- **POKAZ ZABEZPIECZEŃ CHECK POINT EPS**
- Pytania



# Wyzwania dla bezpieczeństwa

- Zbyt wiele aplikacji zabezpieczeń do utrzymania
- Wiele konsol zarządzających
- Problemy z kompatybilnością poszczególnych agentów

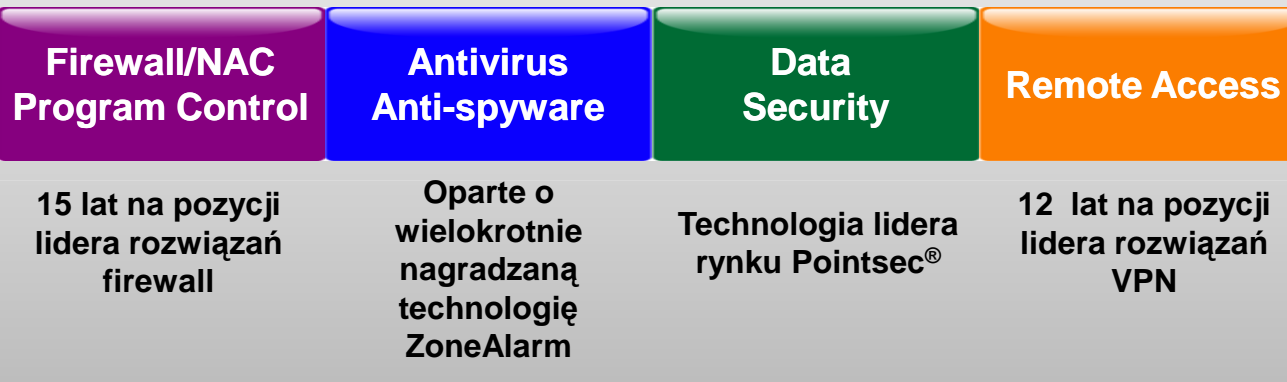
*Dają w wyniku...*

- Niewystarczający poziom zabezpieczeń
- Zwiększenie nakładów i kosztów administracyjnych
- Wiele interakcji testowania – po każdej aktualizacji oprogramowania

# Wprowadzenie: Check Point Endpoint Security

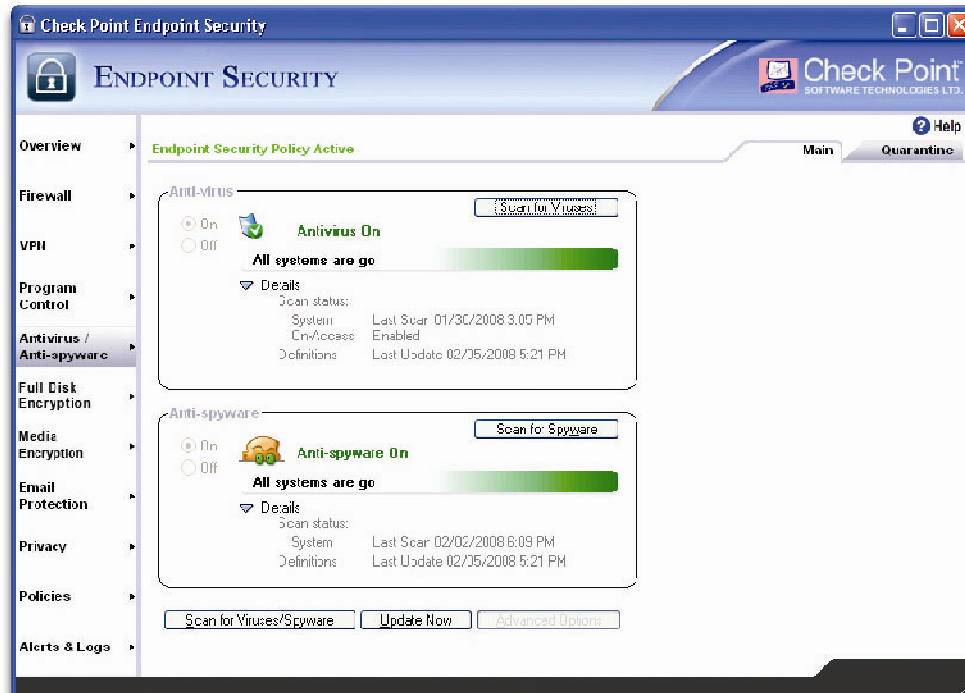


## Pojedynczy agent dla bezpieczeństwa stacji końcowej



- Rozwiązuje problem szerokiego zakresu ryzyka
- Ujednolica wszystkie najważniejsze komponenty ochrony
- Jedyne rozwiązanie zawierające zarówno ochronę danych jak i bezpieczeństwo zdalnego dostępu

# Pojedynczy agent ochrony stacji końcowej



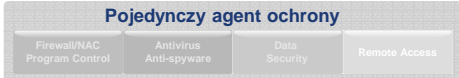
## Łatwy do wdrożenia i zarządzania

- Jedyne wszechstronne rozwiązanie ochrony:
  - Firewall, NAC & Program Control
  - Antivirus & anti-spyware
  - Bezpieczeństwo danych
  - Zdalny dostęp
- Jedna instalacja
- Jeden intuicyjny interfejs

Unikalne

Jedyne rozwiązanie zawierające **zarówno** zabezpieczenie danych jak i VPN

# Uproszczona instalacja i wdrożenie



**Client Configuration** Manage Installer Versions

**Client Packages**  
Configure the installation packages that are available for installing and updating the client software.

[New Package](#)

Package	Client Type	Installer File	Date Modified
<a href="#">Agent Client, v7.0.843.000 [English]</a> <a href="#">Edit</a>   <a href="#">Duplicate</a>   <a href="#">Export</a>   <a href="#">Delete</a>	Agent	Agent Client, v7.0.843.000 [English]	2008-01-31 21:07:35
<a href="#">Auto iFlex Duplicate</a> <a href="#">Edit</a>   <a href="#">Duplicate</a>   <a href="#">Export</a>   <a href="#">Delete</a>	VPN Flex	VPN Flex Client, v7.0.843.000 [English]	2008-01-31 21:21:37
<a href="#">Flex Client, v7.0.843.000 [English]</a> <a href="#">Edit</a>   <a href="#">Duplicate</a>   <a href="#">Export</a>   <a href="#">Delete</a>	Flex	Flex Client, v7.0.843.000 [English]	2008-01-31 21:07:35
<a href="#">VPN Agent Client, v7.0.843.000 [English]</a> <a href="#">Edit</a>   <a href="#">Duplicate</a>   <a href="#">Export</a>   <a href="#">Delete</a>	VPN Agent	VPN Agent Client, v7.0.843.000 [English]	2008-01-31 21:07:35

Rows 1-4 of 5 | Row:  [Last](#)

**Office Awareness**  
In order to use the correct policy, Check Point Endpoint Security clients need to know whether or not they are connected to your network. Use Office Awareness to prevent your Check Point Endpoint Security clients from using the Disconnected policy when they lose contact with the Check Point Endpoint Security Server. [Edit](#)

You have not defined any Office Awareness Servers.

**Client Settings**  
The client settings shared between all clients are shown below. Some settings may require that policies are re-deployed to take effect. [Edit](#)

**Heartbeat**

Interval (secs): **60**  
Protocol: **http**

**Log Upload**

Interval (secs): **3600**  
Retry delay (secs): **900**  
Max Retries: **3**

**Log Upload Size**

Min number of events: **10**  
Max number of events: **50**  
Max age of events (secs): **432000**

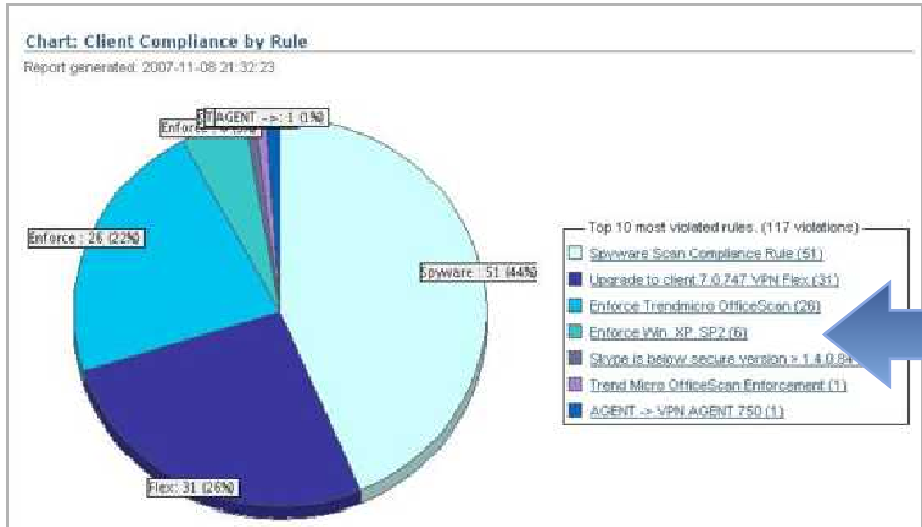
Szybka i łatwa instalacja oraz uaktualnienia

Współdzielone ustawienia

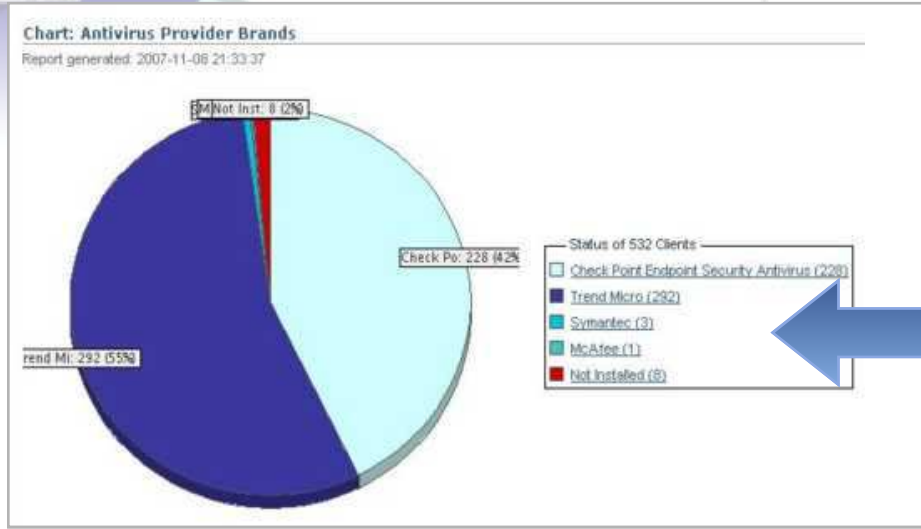
# Wymuszanie polityki zabezpieczeń

Pojedynczy agent ochrony

- Firewall/NAC Program Control
- Antivirus Anti-spyware
- Data Security
- Remote Access



Weryfikacja poziomu bezpieczeństwa stacji



Wymuszanie polityk ochrony AV dla produktów „3rd party”

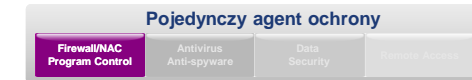
# Lider rynku firewall

The screenshot displays the Check Point Endpoint Security management console. The main window is titled "Add Firewall Rules to Policy" and contains a table of existing rules. A "New Firewall Rule" dialog box is open, showing the configuration for a "New Outgoing Firewall Rule".

Name	Source	Destination	Protocol	Time	Action	Track
Allow Mail	Any	Any	Mail Servers	Always	Allow	None
Allow VWeb	Any	Any	Web Servers	Always	Allow	None
All traffic	Any	Any	Any	Always	Allow	None
All Traffic Out	Client Computer	Any	Any	Always	Allow	None
Block IGMP	Any	Any	IGMP	Always	Block	Alert & Log
Block NetBIOS	Any	Any	NetBIOS	Always	Block	Alert & Log
Block Ping	Any	Any	Ping (ICMP Echo)	Always	Block	Alert & Log

**New Outgoing Firewall Rule Configuration:**

- Rule Details:**
  - Name: [Empty]
  - Description: [Empty]
  - Action: Allow
  - \*Times: Always to 1 AM
  - \*Days: Every Day
  - Track: None
- Destination Locations:**
  - Any Destination Location
  - Select from Destination list
- Affected Ports & Protocols:**
  - Any Port or Protocol
  - Select from Protocol list



## 15 lat na pozycji lidera rynku firewall

- Proaktywna ochrona ruchu wchodzącego i wychodzącego
- Blokowanie niechcianego ruchu
- Tryb „stealth” – stacja niewidoczna dla intruzów
- Szczegółowa kontrola dostępu do sieci

# Rozszerzona ochrona aplikacyjna

The screenshot shows the 'Program Group Permissions' section of the Endpoint Security console. It features a table of program groups with columns for Group Name, Rank, Count, and Description. A pop-up window titled 'Program Permissions' is also visible, showing a list of programs with checkboxes for selection.

Group Name	Rank	Count	Description
PA quarantined programs		12	Programs quarantined by the system (1,054,342)
Critical Services	1	29	These applications are critical to the system and should not be blocked.
Secondary Services & Apps	2	21	These applications are secondary to the system and should be blocked as needed.
ActiveSync	3	114	Applications related to ActiveSync.
Tools	4	8	

Unikalne

Pojedynczy agent ochrony

- Firewall/NAC Program Control
- Antivirus Anti-spyware
- Data Security
- Endpoint Access

## Usługa Program Advisor

- Automatyczne wymuszanie uprawnień aplikacyjnych
  - Natychmiastowe terminowanie znanych złośliwych programów
  - Zezwolenie na uruchamianie wyłącznie zaakceptowanych programów
- Jak to robimy?
  - Usługa uwierzytelnienia dobrych, znanych programów
  - Identyfikacja znanych złych programów
  - Setki tysięcy programów w bazie usługi Program Advisor
  - Oparte o rzeczywiste dane z milionów stacji końcowych (Zone Alarm)

# Kontrola dostępu do sieci - NAC

## Ensure Endpoint Policy Compliance

Gateway Manager

**Success**  
The entity *checkpoint/VPN* was created successfully.

You can identify gateways that should be governed by different security policies below.

Gateway	Description	Assigned Policy
VPN-1//Perimeter (disconnected) <a href="#">Edit</a>   <a href="#">Delete</a>	Check Point VPN-1 POWER/UTM	
VPN-1//Datacenter (disconnected) <a href="#">Edit</a>   <a href="#">Delete</a>	Check Point VPN-1 POWER/UTM	
<input type="checkbox"/> checkpoint//VPN <a href="#">Edit</a>   <a href="#">Delete</a>	Check Point VPN-1	Default Domain Policy

- Check Point VPN-1 POWER/UTM
- Nortel Contivity with TunnelGuard
- Check Point VPN-1 for remote access users
- Check Point InterSpect
- 802.1x Compatible Network Access Server
- Cisco VPN Gateways

Pojedynczy agent ochrony

- NAC dla połączeń lokalnych oraz VPN
- Zapewnienie, że tylko zaufane stacje uzyskają dostęp do sieci

Współpraca w zakresie wymuszania polityk z modułami CP Firewall oraz modułami firm trzecich

Wsparcie dla standardu 802.1x/EAP

# Antivirus / Anti-spyware

Edit Policy Save Cancel

Name & Notes | Access Zones | Firewall Settings | Program Rules | **Anti-Virus Anti-Spyware** | Smart-Defense | Messaging Settings | Enforcement Settings | Client Settings

### General Settings

Protect against spyware  
 Protect against viruses

### Spyware Scan Settings

Spyware scans are quick scans that should be run on a short interval. They add security with minimal impact to endpoint computer performance.

Scheduled Scan Time: Mondays at 12 noon

Restrict clients that don't comply with the Spyware Scan settings  
 Perform Spyware Scan after installation

### Anti-Virus Scan Settings

Anti-Virus scans are a rigorous scan of every file on the selected targets, and as such will have an impact on endpoint performance. These scans are recommended for previously-unprotected endpoints.

Scheduled Scan Time: Never at 12 mid

Perform Deep Scan after installation

### Scan Target

Local

### Chart: Check Point Antivirus Scanned Date

Report generated: 2007-11-09 21:48:52

Status	Count	Percentage
Within 24 Hours	6	1.1%
48 Hours	6	1.1%
4 Days	7	1.3%
Last Week	8	1.5%
2 Weeks	48	9.0%
Older than 2 Weeks	85	15.8%
Never Scanned	10	1.9%
Other Brands	298	55.4%
Not Installed	9	1.7%

Pojedynczy agent ochrony

Firewall/NAC Program Control | **Antivirus Anti-spyware** | Data Security | Remote Access

## Eliminuje wirusy i inne złośliwe oprogramowanie

- Wielokrotnie nagradzany mechanizm ochrony przed złośliwym kodem
- Najwyższe współczynniki wykrywalności
- Uaktualnienia sygnatur co 1 godz.

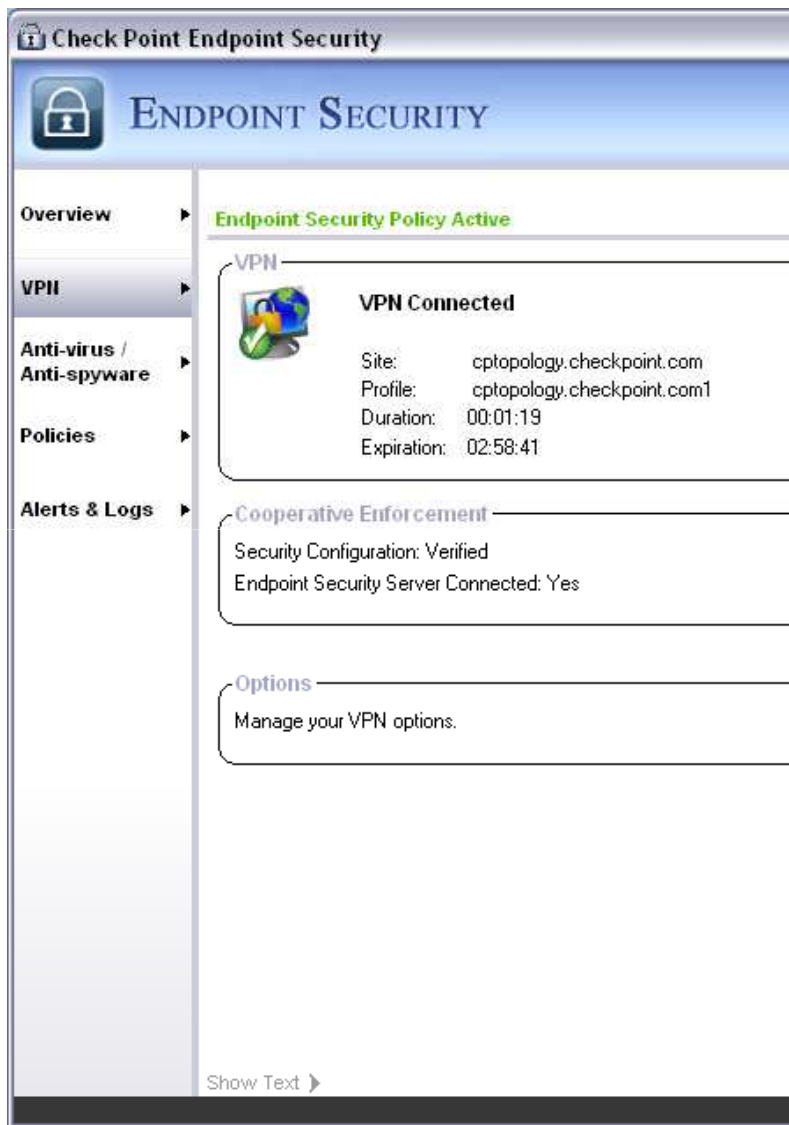
# Bezpieczeństwo danych



## Ochroną przed utratą lub kradzieżą danych

- Najczęściej stosowane rozwiązanie zabezpieczenia danych
  - Ponad 14 milionów instalacji
- Oparte na technologii Pointsec® - lider rynku
  - **Full Disk Encryption** – zapewnia najbardziej wszechstronną ochronę wszystkich danych
  - **Port Protection** – kontroluje wykorzystanie portów i urządzeń zew.
  - **Media Encryption** – szyfruje wrażliwe dane przenoszone przez urządzenia mobilne, np. USB





## Ensure Confidential Remote Communications

- Secure remote VPN access through VPN-1® gateways
- Only endpoint security solution that includes unified remote access
- Applies full security policies to the VPN traffic
- Multiple VPN entry points provides high availability and flexible access

# Najwyższa klasa rozwiązań



15 lat na pozycji lidera rynku firewall



Leader in Gartner Mobile Data Protection Magic Quadrant 7 years in a row



Certyfikat Common Criteria EAL 4



Ponad 100 million zainstalowanych klientów VPN



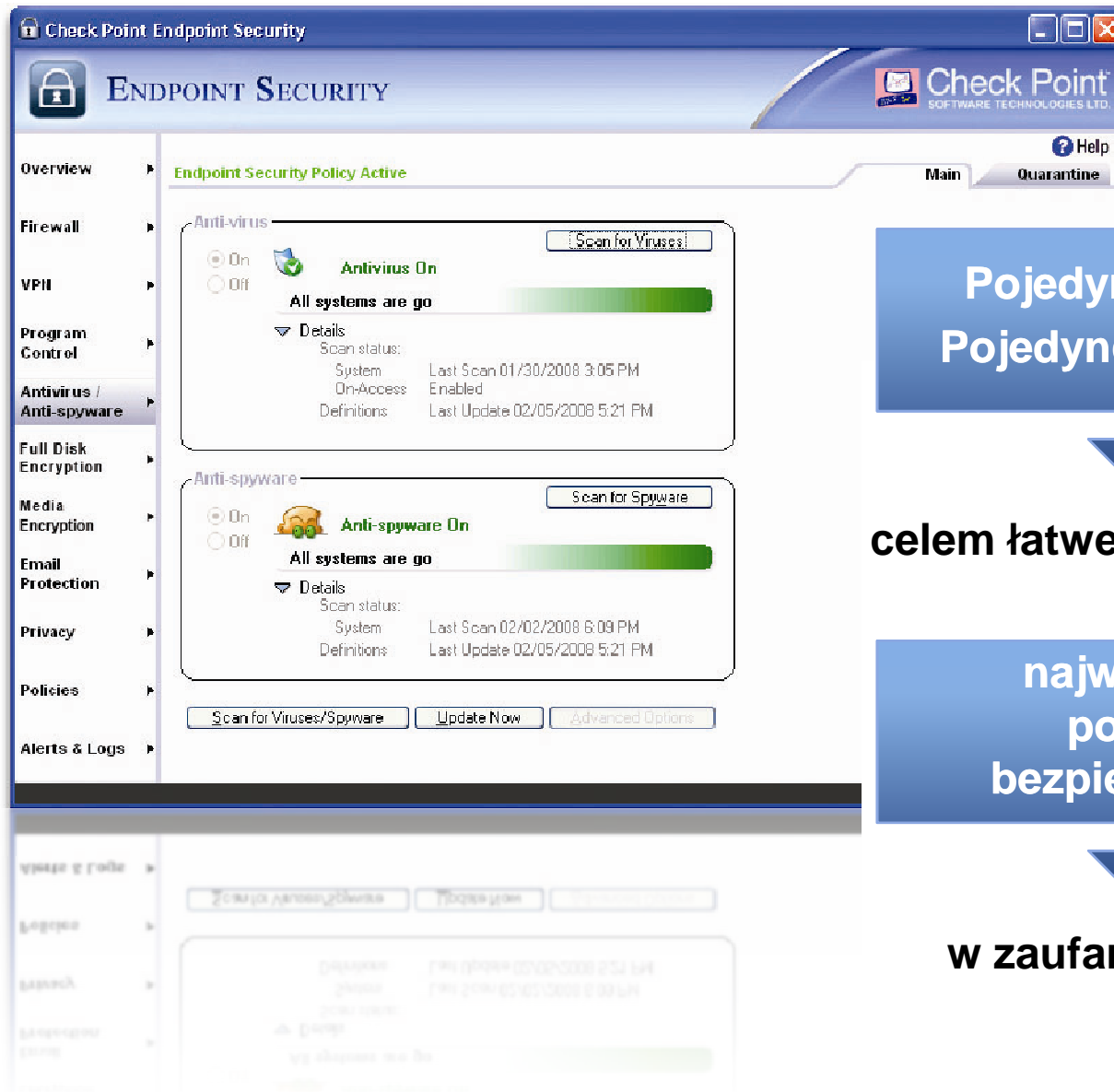
Ponad 80 million chronionych PC



Gartner



# Podsumowanie



Pojedynczy agent  
Pojedyncza konsola

celem łatwego zapewnienia

najwyższego  
poziomu  
bezpieczeństwa

w zaufanej ochronie

# Pytania?

