



**ПОЛИКОМ** ПРФ

Созвездие высоких технологий

## **Снижение затрат на сопровождение систем антивирусной безопасности.**

**Антон Рафаэлович Миносьян**  
**Инженер отдела системной интеграции**

## Зачем нужен Control Manager?

- Можно управлять всем комплексом антивирусного ПО
- Управление любым числом серверов, рассредоточенных по разным площадкам
- Делегирование функций управления и аудит
- Outbreak Prevention Services – упреждающая защита при эпидемиях
- Сбор логов, статистика и отчетность (только в версии Advanced)

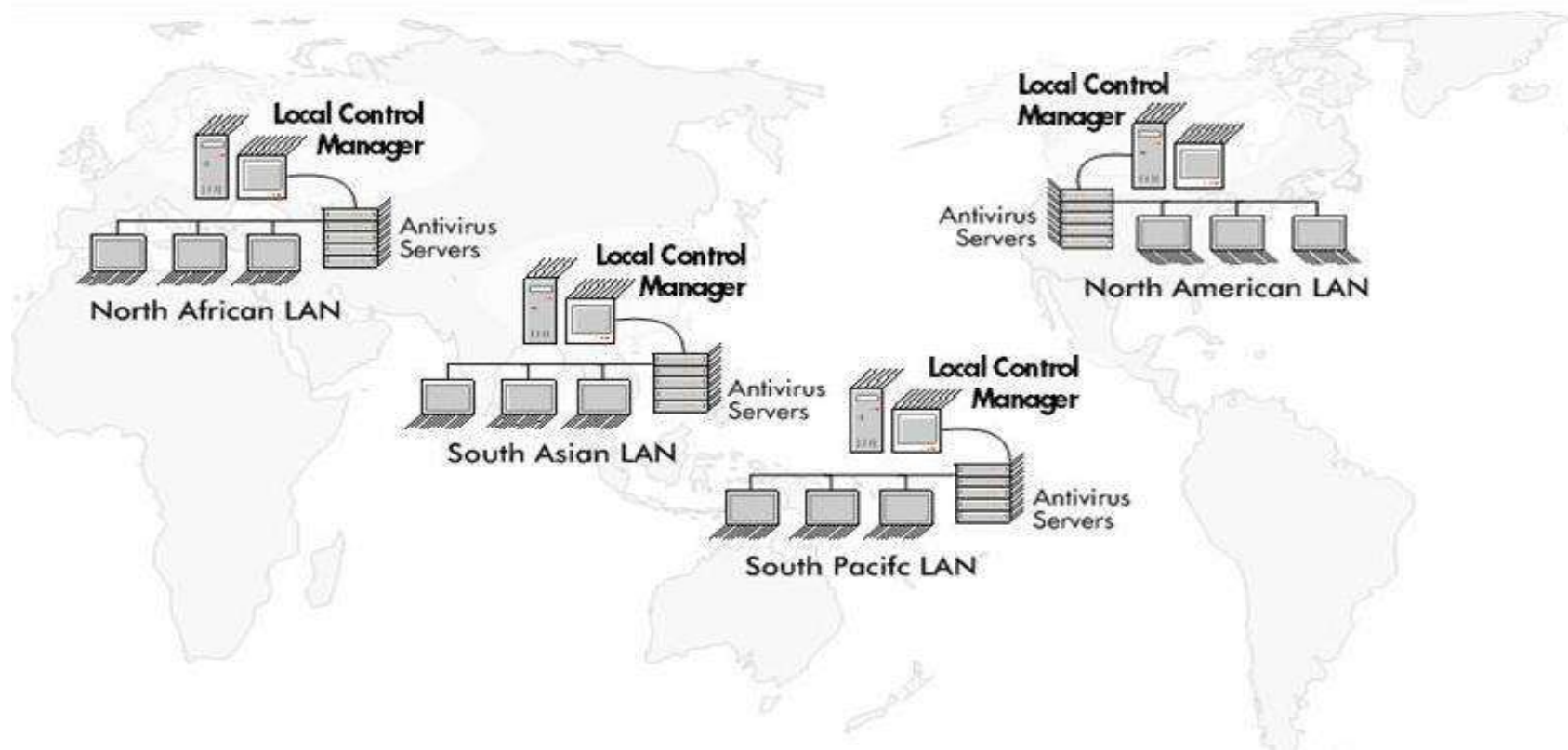


# Система централизованного управления антивирусным комплексом



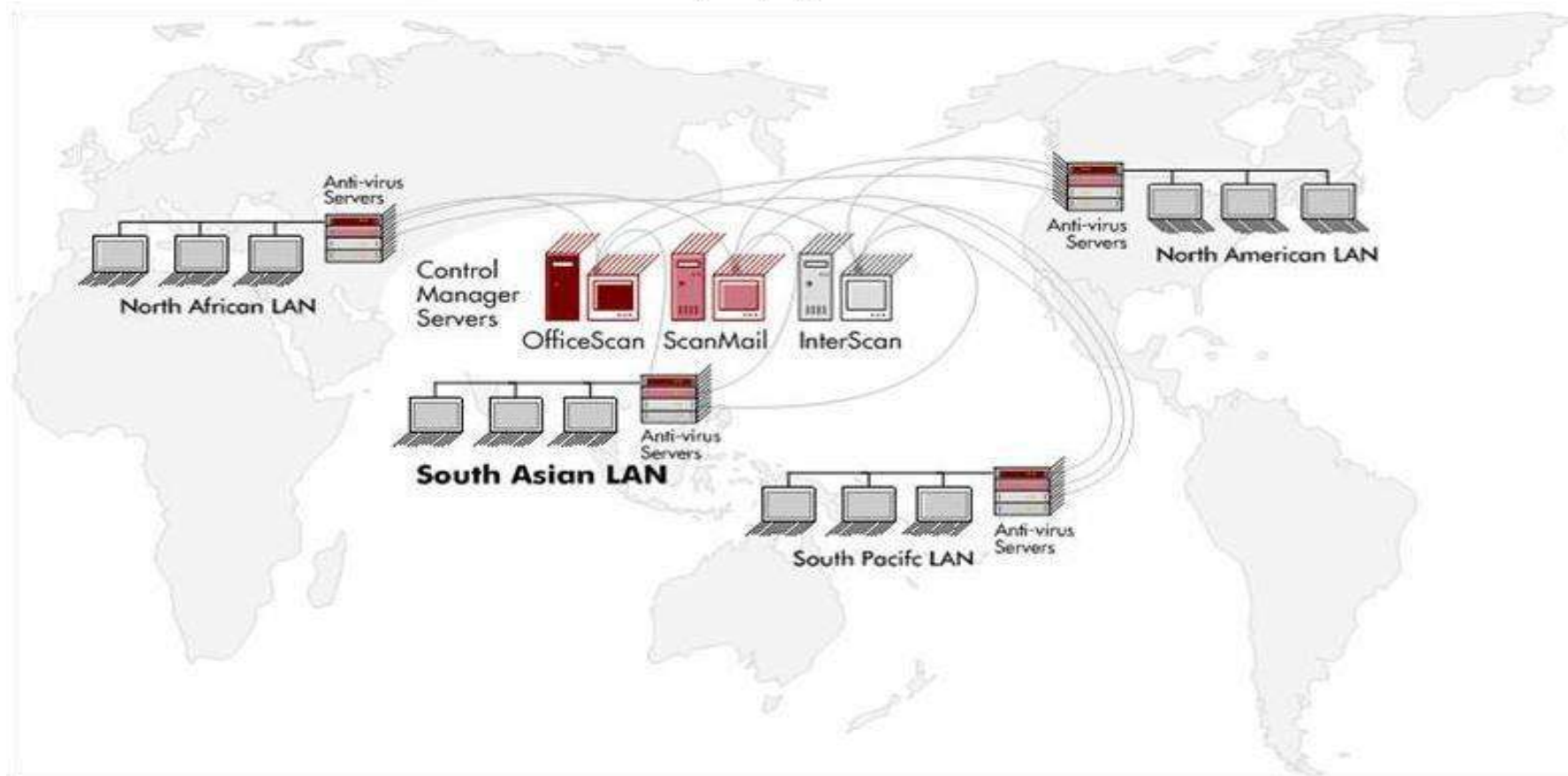
# Варианты внедрения - 1

## Децентрализованная топология



# Варианты внедрения - 2

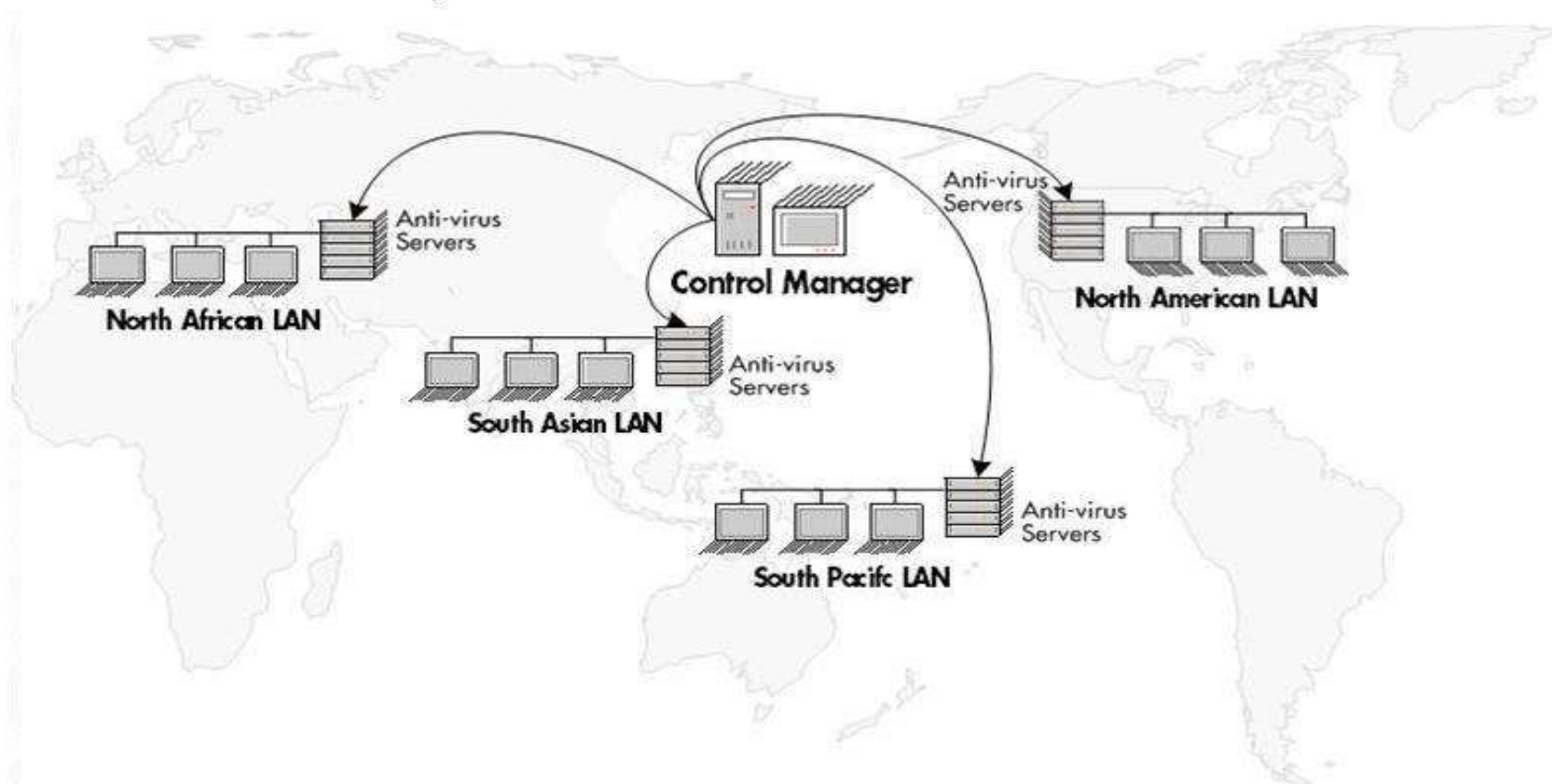
## Топология "по продуктам"



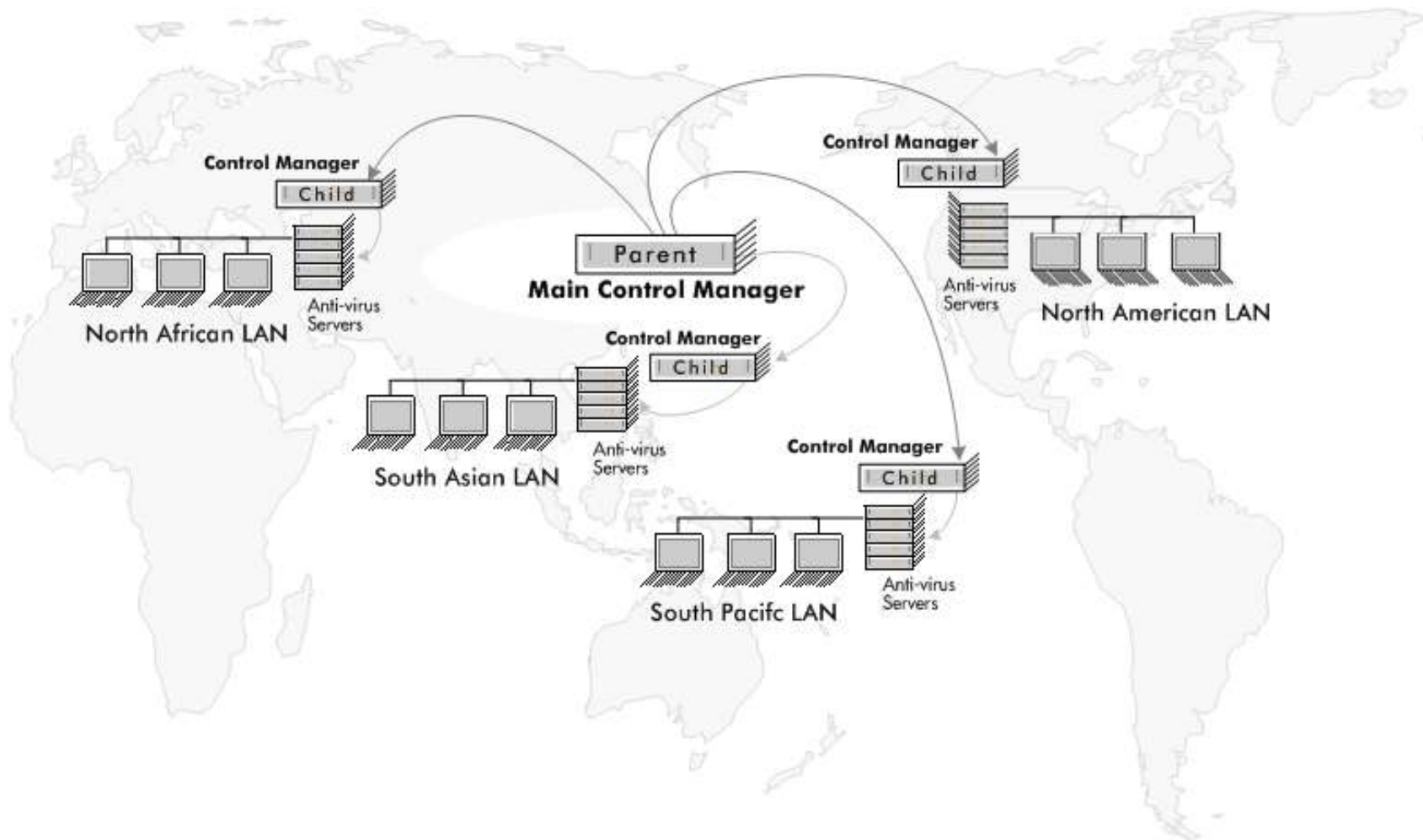


# Варианты внедрения - 3

## Централизованная топология



# Двухуровневое каскадирование в версии Advanced



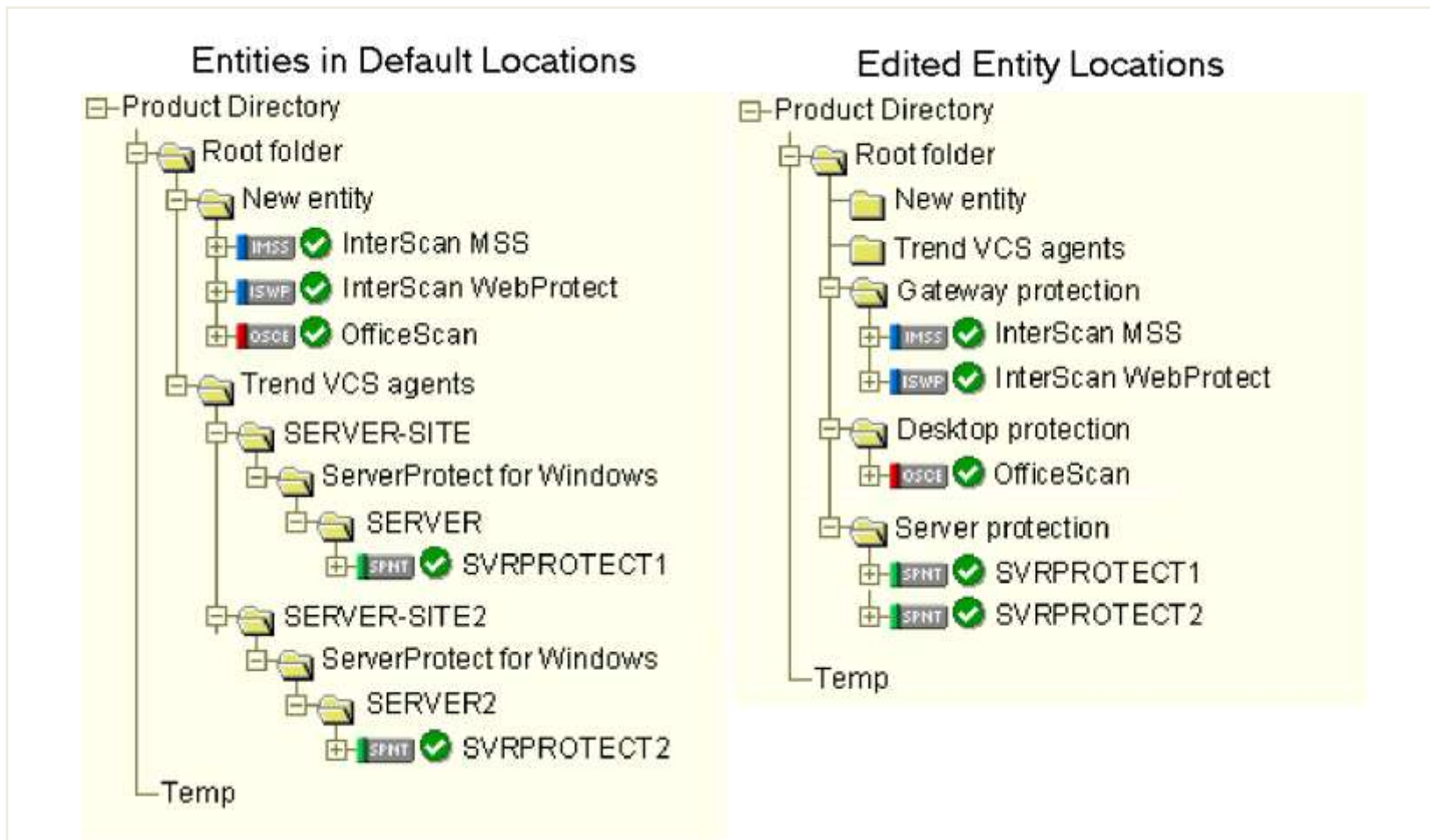
# Product Directory

- Представление всего антивирусного комплекса в виде дерева
- Возможность отправлять команды нескольким узлам одновременно
- Делегирование полномочий





# Product Directory. Демо



# Пользователи и группы

- Корневой администратор (Root)
- Четыре уровня доступа
  - Root
  - Administrator
  - Power User
  - Operator
- Аудит действий пользователей
- Группы используются для рассылки уведомлений и оповещения



# Пользователи и группы. Демо

## User Accounts



Add new users and assign them access rights and privileges depending on their role in the company. This flexibility permits delegation of certain management tasks without compromising security.

Add New User

Add New Active Directory User

User ID	Full Name	Account Type	Domain	Status	Edit	Delete
Nick	Nick Local Administrator	Power User			<a href="#">Edit</a>	<a href="#">Delete</a>
Rosa	Rosa Local Product Admin	Power User			<a href="#">Edit</a>	<a href="#">Delete</a>
Yoshi	Yoshi Regional Administrator	Administrator			<a href="#">Edit</a>	<a href="#">Delete</a>

Add New User

Add New Active Directory User



# Уведомления и оповещения

- Оповещения на основе комплексного анализа событий
- Предопределенные категории с настраиваемыми параметрами
- Можно рассылать пользователям и группам TMSM
- Методы оповещения
  - Почта SMTP
  - Протоколирование в Windows Application Log
  - Пейджер
  - SNMP
  - MSN Messenger
  - Запуск пользовательского приложения



# Уведомления и оповещения. Демо

The screenshot displays the Trend Micro Control Manager web interface. At the top, there is a red header with the logo and navigation tabs: Home, Products, Services, Logs / Reports, Updates, Administration, and Help. The user is logged in as 'root'. The main content area is titled 'Event Category' and lists various event types with checkboxes for selection and links for 'Settings' and 'Recipients'.

Event Category		
<input type="checkbox"/> Alert		
<input type="checkbox"/> Event	<a href="#">Settings</a>	<a href="#">Recipients</a>
<input checked="" type="checkbox"/> Virus outbreak alert	<a href="#">Settings</a>	<a href="#">Recipients</a>
<input checked="" type="checkbox"/> Special virus alert	<a href="#">Settings</a>	<a href="#">Recipients</a>
<input checked="" type="checkbox"/> Special spyware/grayware alert	<a href="#">Settings</a>	<a href="#">Recipients</a>
<input type="checkbox"/> Virus found - first action unsuccessful and second action unavailable		<a href="#">Recipients</a>
<input checked="" type="checkbox"/> Virus found - first and second actions unsuccessful		<a href="#">Recipients</a>
<input type="checkbox"/> Virus found - first action successful		<a href="#">Recipients</a>
<input type="checkbox"/> Virus found - second action successful		<a href="#">Recipients</a>
<input type="checkbox"/> Network virus alert	<a href="#">Settings</a>	<a href="#">Recipients</a>
<input type="checkbox"/> Potential vulnerability attack detected	<a href="#">Settings</a>	<a href="#">Recipients</a>
<input type="checkbox"/> Spyware/Grayware found - action successful		<a href="#">Recipients</a>
<input type="checkbox"/> Spyware/Grayware found - further action required		<a href="#">Recipients</a>
<input type="checkbox"/> Outbreak Prevention Services		
<input checked="" type="checkbox"/> Event	<a href="#">Settings</a>	<a href="#">Recipients</a>
<input checked="" type="checkbox"/> Active Outbreak Prevention Policy received		<a href="#">Recipients</a>
<input checked="" type="checkbox"/> Outbreak Prevention Mode started		<a href="#">Recipients</a>
<input checked="" type="checkbox"/> Outbreak Prevention Mode stopped		<a href="#">Recipients</a>
<input checked="" type="checkbox"/> Outbreak Prevention Policy update unsuccessful		<a href="#">Recipients</a>
<input checked="" type="checkbox"/> Outbreak Prevention Policy update successful		<a href="#">Recipients</a>
<input type="checkbox"/> Vulnerability Assessment		
<input type="checkbox"/> Event	<a href="#">Settings</a>	<a href="#">Recipients</a>
<input type="checkbox"/> Vulnerability Assessment task completed		<a href="#">Recipients</a>



# Обновление

- Точный выбор обновляемых компонент
- Альтернативные источники обновлений
- Обновление по графику и вручную
- Возможность установки отдельного графика для разных компонент
- Создание планов распространения (Deployment Plans)



# Обновление. Демо

## Add New Schedule

---

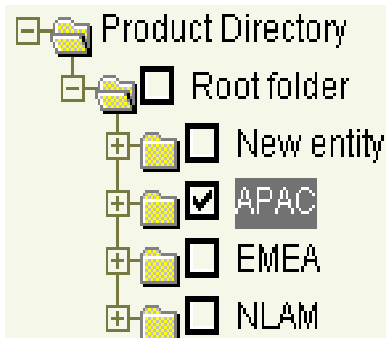
**Plan name:** Regional Updates

**Deployment time:**  Delay  hour(s)  minute(s)

Start at:  :  (hh:mm)

### Select a folder:

In each schedule, select one folder to apply the deployment. For multiple-folder deployment, create multiple schedules. The folders you see depend on the folder access rights you have been given.



# Мониторинг и управление

- Просмотр статусной информации о продукте
- Доступ к веб-интерфейсу продукта из консоли Control Manager
- Отправка команд серверу или группе серверов
- Доступ к журналам событий



# Мониторинг. Демо

Home Services Products Reports Administration

Search Refresh

Managed Products Go

Add/Remove Product Agents

Product Directory

- Root folder
  - New entity
  - APAC
  - EMEA
    - Gateway
      - IMSS MAUI\_IMSS
    - Mail
    - Server
    - NLAM
  - Temp

Product Status Configuration Tasks Logs

### Security Logs Query

Choose the type of security information to display for all child Control Manager servers.

Query	Action
All virus/spyware/grayware log incidents (email, files and http download traffic.)	<a href="#">Query</a>
Viruses/Spywares/Graywares found in HTTP or FTP download traffic	<a href="#">Query</a>
Viruses/Spywares/Graywares found in email	<a href="#">Query</a>
Viruses/Spywares/Graywares found in files	<a href="#">Query</a>
Network viruses found in endpoints	<a href="#">Query</a>
Network viruses found in packets	<a href="#">Query</a>
Content security violations	<a href="#">Query</a>
Web security violations	<a href="#">Query</a>
Security violations	<a href="#">Query</a>
Security compliance	<a href="#">Query</a>

<<Back

Product Status Configuration Tasks Logs

### Query Result (Event Logs)

1-20 of 27 log(s) [Next>>](#) | Page:  [Go](#)

#	Received	Generated at entity	Severity	Event	Product	Computer/Device Name	Description
1	2/15/2006 11:26:13 AM	2/15/2006 11:25:19 AM	Information	Product service stopped	InterScan Messaging Security Suite for Windows	MAUI	InterScan SMTP main service stop running
2	2/15/2006 11:26:12 AM	2/15/2006 11:25:19 AM	Information	Configuration changed	InterScan Messaging Security Suite for Windows	MAUI	IMSS configuration reloaded

# Outbreak Prevention

- Упредительные политики против вредоносного ПО, для которого еще не выпущен паттерн
- Комплексная защита - распространяется на все управляемые продукты, а не только на OfficeScan
- Можно настроить на автоматическую загрузку и применение политики
- Можно написать свою собственную политику на основе существующей





# Outbreak Prevention. Шаблоны

Home Services Products Reports Administration

Start Outbreak Prevention Mode

Services

- Outbreak Prevention
- History
- Settings
- Vulnerability Assessment
- Security Summary
- Current Task
- Tasks
- History
- Global Settings

Top Threats Around the World

[Refresh](#) 1-20 of 128 policies [Next>>](#) | Page:  [Go](#)

	Virus name	Last updated	Alert type	Risk	Delivery method	Required scan engine	Required virus pattern file	Required damage cleanup engine	Required damage cleanup template	More info
<input type="radio"/>	WORM_MYTOB.MX	11/24/2005 10:36:52 AM	Yellow	High	Email, Shared Drives	7.000.0000	2.967.00	3.900.0000	682	<a href="#">View</a>
<input type="radio"/>	CICS_TEST_FILE	8/22/2005 10:47:35 AM	Yellow	Medium	test packet	6.810.0000	2.794.01	3.900.0000	639	<a href="#">View</a>
<input checked="" type="radio"/>	CUSTOM_POLICY	11/5/2003 3:00:46 PM	Yellow	Low	n/a	5.200.0000	n/a	n/a	n/a	<a href="#">View</a>
<input type="radio"/>	EICAR_TEST_FILE	1/12/2004 8:39:39 PM	Yellow	Medium	Email	5.200.0000	1.414.01	n/a	n/a	<a href="#">View</a>
<input type="radio"/>	PE_BAGLE.N	3/14/2004 6:13:31 AM	Yellow	Medium	Email, Shared Drives	5.200.0000	1.815.00	n/a	n/a	<a href="#">View</a>
<input type="radio"/>	PE_BAGLE.P	3/15/2004 7:52:11 AM	Yellow	Medium	Email, Shared Drives	5.600.0000	1.819.00	3.500.0000	290	<a href="#">View</a>

# Outbreak Prevention. Пример политики

Home Services Products Reports Administration

Services

- Outbreak Prevention
  - History
  - Settings
- Vulnerability Assessment
  - Security Summary
  - Current Task
  - Tasks
  - History
  - Global Settings

### Outbreak Prevention Mode - WORM\_MYTOB.MX

**Threat Information**  
This memory-resident worm propagates by sending a copy of itself as an attachment to an email message, which it sends to target recipients, using its own Simple Mail Transfer Protocol (SMTP) engine.

**Outbreak Prevention Policy**  
Policy in effect for: 2 days  
Deployment plan: Deploy to All Managed Products Now (Default)

**Outbreak Prevention Policy Details**  
 Do not block permitted port numbers specified in the Outbreak Prevention settings (n/a).

**Gateway**

- InterScan eManager
- InterScan WebProtect for ICAP
- InterScan Messaging Security Suite for Windows
- InterScan Messaging Security Suite for UNIX
- InterScan Web Security Suite for Windows / Solaris / Linux
- Network Virus Wall
- Portal Protect

**Message**

- ScanMail for Microsoft Exchange
- ScanMail for Lotus Notes / ScanMail for Domino
- ScanMail eManager
- IM Security for Microsoft Live Communications Server

**Desktop/Servers**

- ServerProtect for Windows
- ServerProtect for Linux
- OfficeScan Corporate Edition
- Damage Cleanup Services 3.0

**Remote Office/Third Party**

- Firewall Management-NetScreen

Activate Cancel < Recommended Settings



# Отчетность

- Только в версии Advanced
- Поддерживается генерация отчетов как по запросу, так и по графику
- Наличие готовых шаблонов
- Отчеты по всему комплексу или по выбранным его частям, консолидированные отчеты
- Поддержка различных форматов
  - HTML
  - PDF
  - RTF
  - Crystal Reports
- Автоматическая доставка по e-mail



# Полезные ресурсы

Trend Micro

Поддержка

<http://esupport.trendmicro.com>

База знаний

<http://esupport.trendmicro.com/enterprise/default.aspx?locale=ro> EM

Вирусная энциклопедия

<http://www.trendmicro.com/vinfo/virusencyclo/default.asp>

Beta Community – бета-версии

[www.trendbeta.com](http://www.trendbeta.com)

Поликом Про, техподдержка ПО Trend Micro

[TM\\_Support@polikom.ru](mailto:TM_Support@polikom.ru)



# Благодарим за внимание!



**ПОЛИКОМ ПРОВО**

Созвездие высоких технологий

Москва	+7 (495) 660 3291
Санкт-Петербург	+7 (812) 325 8400

[www.polikom.ru](http://www.polikom.ru)