



Координация действий по защите и управление продуктами  
и службами Trend Micro. Trend Micro Control Manager

Антон Миносьян  
Поликом Про

# Контактная информация

---

195197, Санкт-Петербург,  
Полюстровский пр., дом 59, литер Э  
тел. 812 325-8400 факс : 812 320-5686

127018, Москва, Сущевский Вал ул., 16,  
строение 3, офис 12  
тел. 495 660-3291 факс : 495 660-3293

АНТОН МИНОСЬЯН

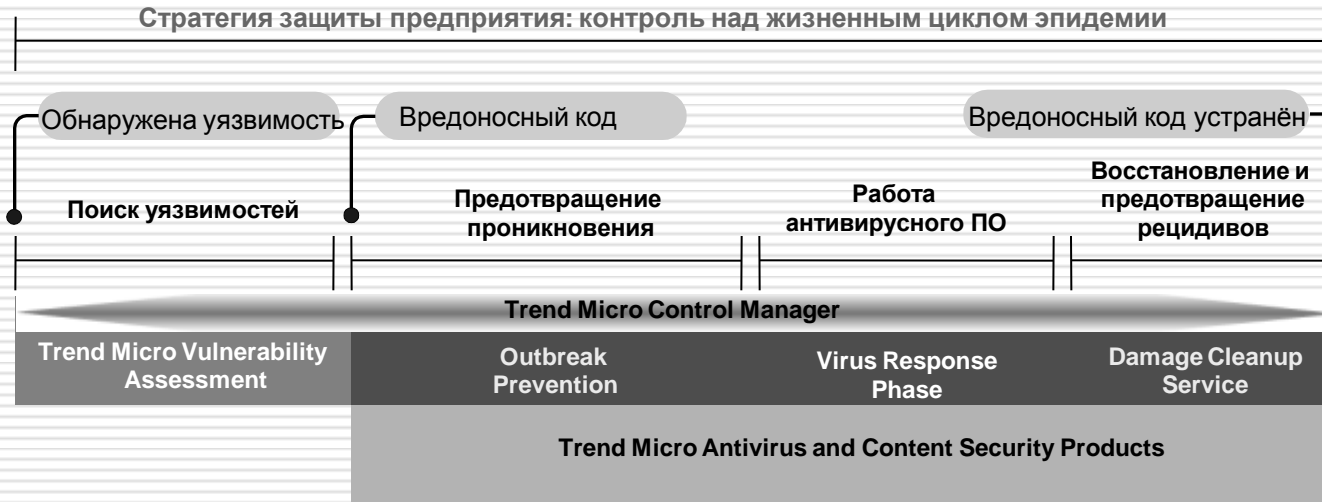
[aminosjan@polikom.ru](mailto:aminosjan@polikom.ru)

# Что на повестке

---

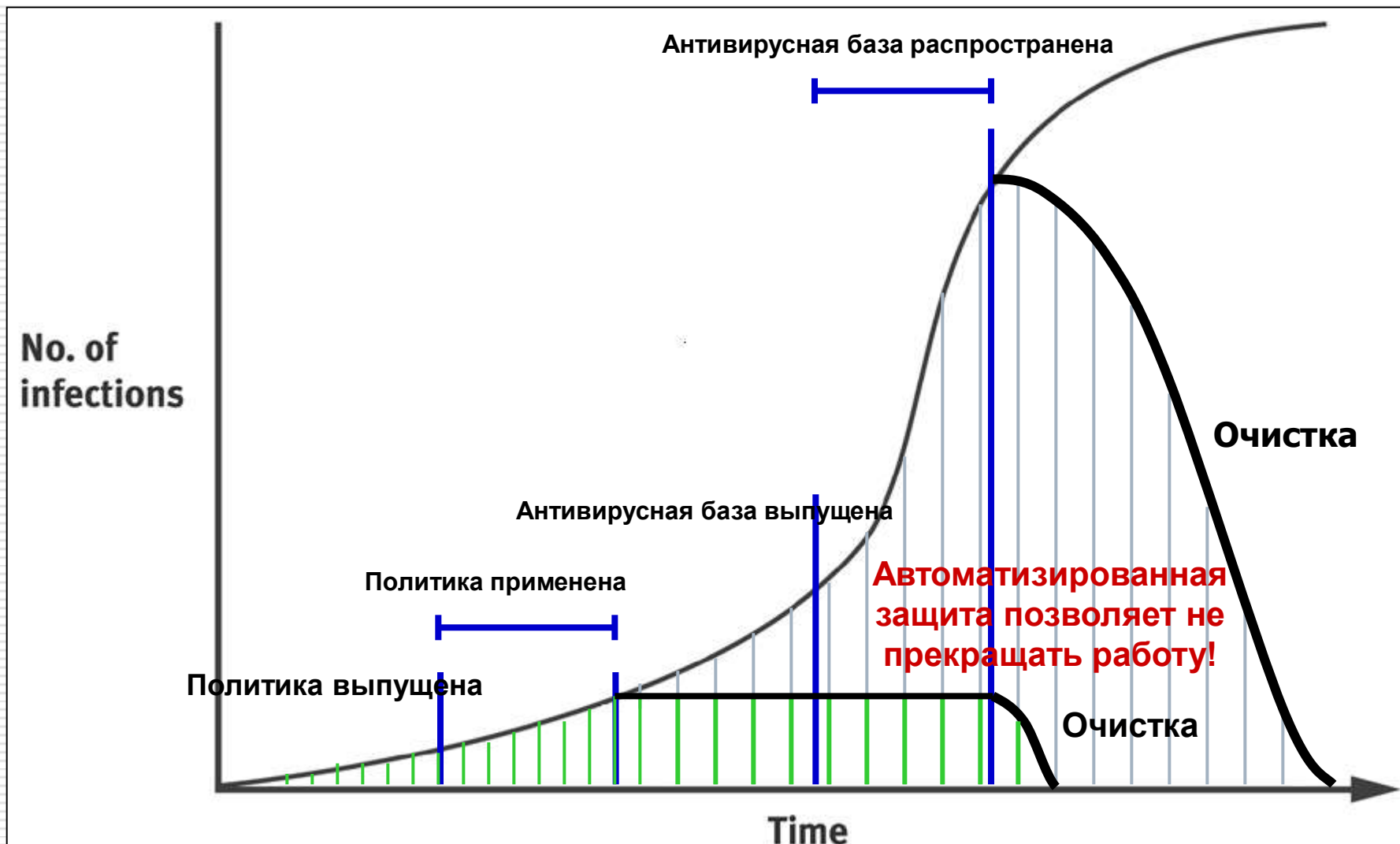
- Стратегия защиты предприятия
- Система централизованного управления антивирусным комплексом

# Стратегия защиты предприятия



- Vulnerability Assessment
- Outbreak Prevention
- Damage Cleanup Service

# Стратегия защиты предприятия



# Защита с централизованным управлением



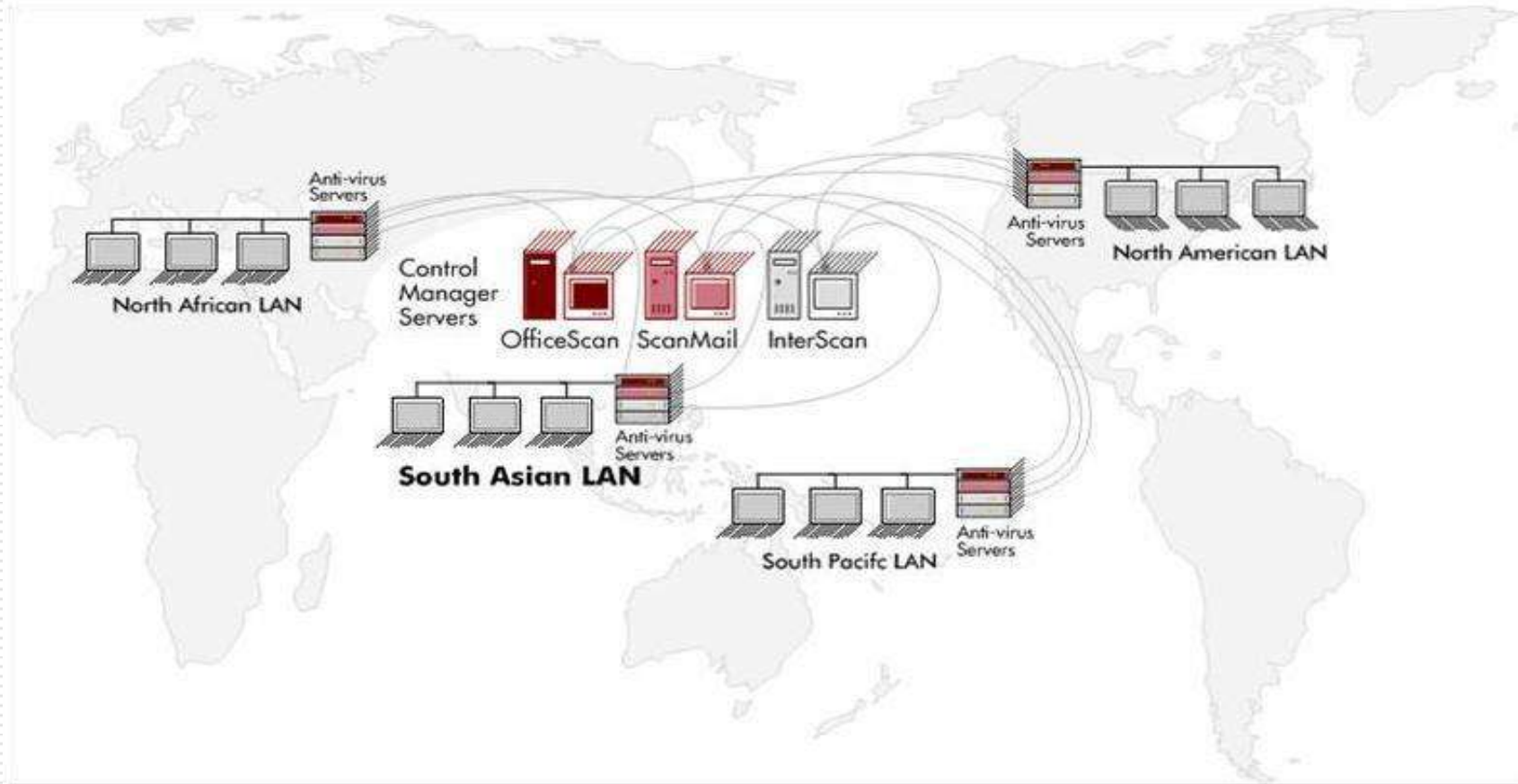
# Зачем нужен Control Manager?

---

- ❑ Можно управлять всем комплексом антивирусного ПО, а не только OfficeScan
- ❑ Управление любым числом серверов, рассредоточенных по разным площадкам
- ❑ Делегирование функций управления и аудит
- ❑ Outbreak Prevention Services – защита от эпидемий (2 фаза EPS)
- ❑ Сбор логов, статистика и отчетность (только в версии Advanced)

# Варианты внедрения

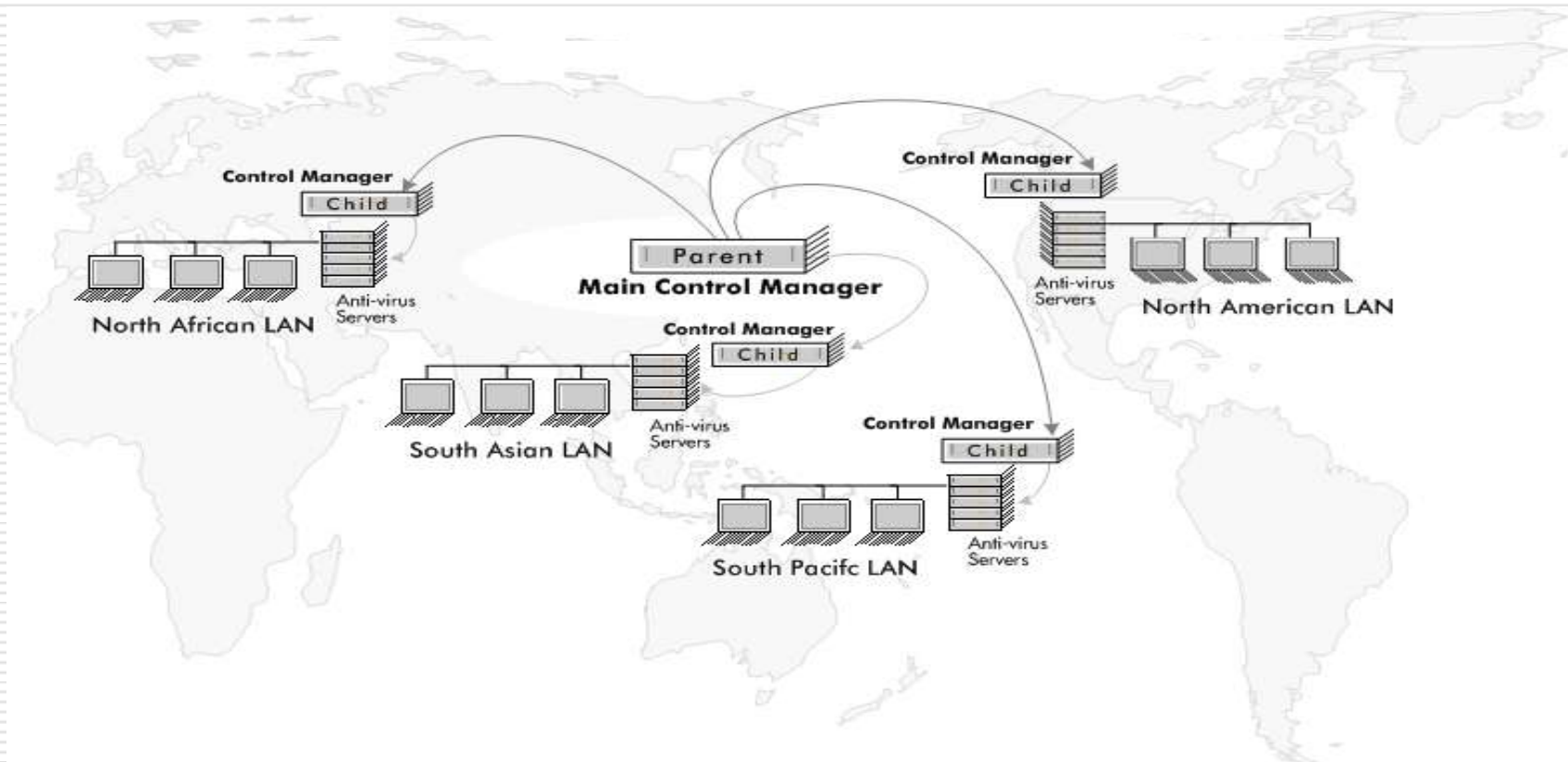
## Топология "по продуктам"





# Возможности версии Advanced

- Двухуровневое каскадирование
- Комбинированная модель



# Новое в версии Control Manager 5

---

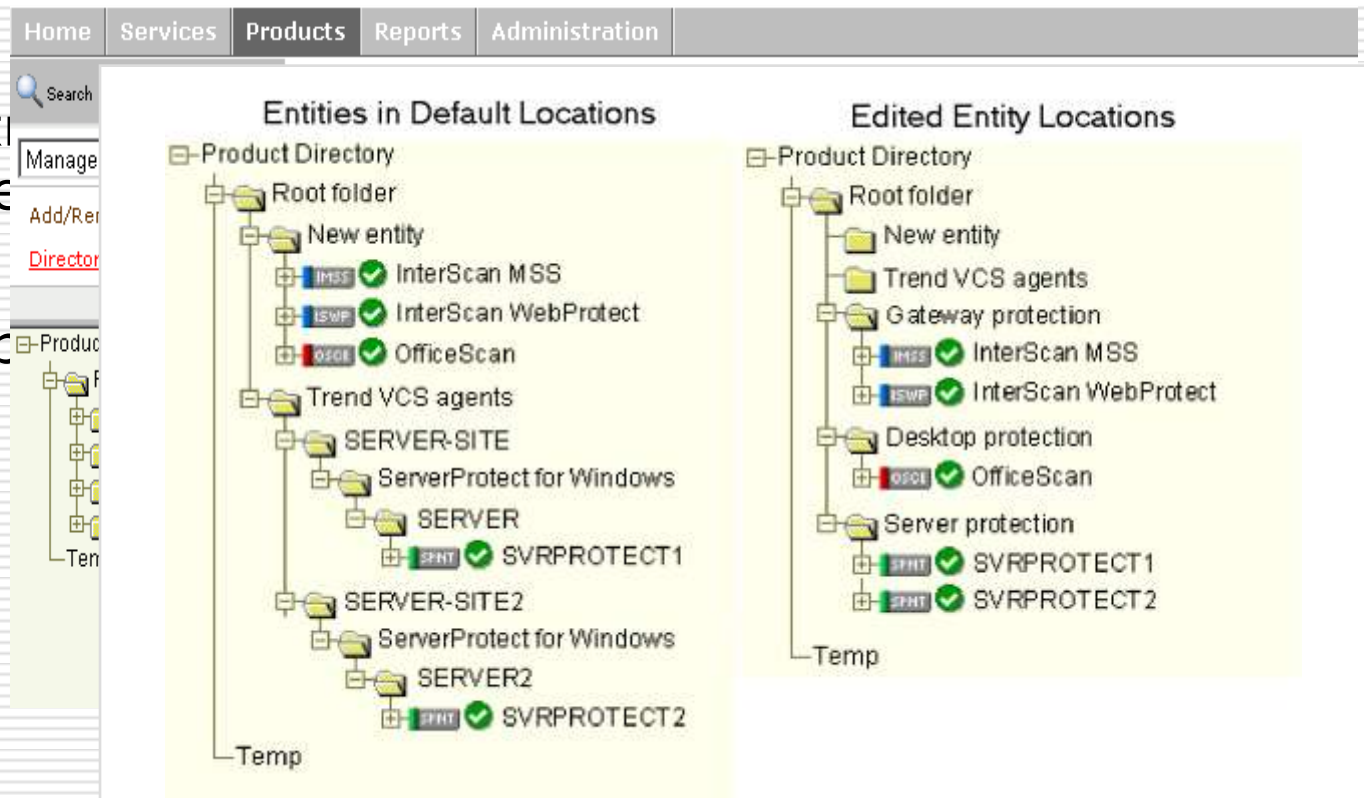
- ❑ Возможность просмотра отдельных файловых (OSCE) клиентов в консоли Control Manager
- ❑ Конструктор отчетов
- ❑ Распространение лицензионных ключей
- ❑ Дочерние Control Manager'ы в каскаде видны в дереве продуктов
- ❑ SSO в каскаде. Требования по версиям

# Product Directory

- Представление антивирусного комплекса в виде дерева

- Возможность одновременного редактирования

- Делегирование



# Пользователи и группы

□ Корневой администратор

□ Четыре уровня доступа

■ Root

■ Administrator

■ Pow

■ Oper

□ Аудит д

□ Группы оповещения



# Уведомления и оповещения

The image displays the Trend Micro Control Manager web interface. It is divided into several sections:

- Virus Outbreak Alert Settings:** A configuration panel with the following settings:
  - Alert Settings
  - Detections: 100 instances
  - Computer or Users: 5 computers or users
  - Period: 1 hour(s)
  - Buttons: Save, Cancel
- Edit Recipients:** A panel for managing notification recipients:
  - Section: Recipients
  - Select Users and Groups: Available Users and Groups (Unexpected\_Event, Update\_Event, User List, SSO\_User, root) and Selected Users and Groups (Virus\_Event, User List).
  - Section: Notification methods
    - Email Notification: . Subject: Control Manager Notification: Virus Outbreak Alert. Message: Control Manager (%cmserver%) notification: %event%. A predefined number of a particular virus has been detected. Virus: %sname%. Alert trigger number: %vent%. Scan engine: %agnver%.
    - Windows Event Log Notification:
- Event Category List:** A table listing various event categories with links for Settings and Recipients:

Event Category	Settings	Recipients
Alert		
Event		
<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>
spyware/grayware alert	<a href="#">Settings</a>	<a href="#">Recipients</a>
und - first action unsuccessful and second action unavailable		<a href="#">Recipients</a>
und - first and second actions unsuccessful		<a href="#">Recipients</a>
und - first action successful		<a href="#">Recipients</a>
und - second action successful		<a href="#">Recipients</a>
virus alert	<a href="#">Settings</a>	<a href="#">Recipients</a>
al vulnerability attack detected	<a href="#">Settings</a>	<a href="#">Recipients</a>
y/Grayware found - action successful		<a href="#">Recipients</a>
y/Grayware found - further action required		<a href="#">Recipients</a>
ak Prevention Services	<a href="#">Settings</a>	<a href="#">Recipients</a>
utbreak Prevention Policy received		<a href="#">Recipients</a>
ak Prevention Mode started		<a href="#">Recipients</a>
ak Prevention Mode stopped		<a href="#">Recipients</a>
ak Prevention Policy update unsuccessful		<a href="#">Recipients</a>
ak Prevention Policy update successful		<a href="#">Recipients</a>
ability Assessment	<a href="#">Settings</a>	<a href="#">Recipients</a>
ability Assessment task completed		<a href="#">Recipients</a>

09.11.2009

# Обновление

## Add New Plan

If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Plan name:

Regional Updates

Schedule(s):

#	Deployment Time	Edit	Delete
---	-----------------	------	--------

Add New Schedule

Save Cancel

Note: After you have added at least one schedule, click Save

## 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.

- Product Directory
- Root folder
- New entity
- APAC

## Add New Plan

If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Plan name:

Regional Updates

Schedule(s):

#	Destination	Deployment Time	Edit	Delete
1	APAC	Start at 19 : 00	<a href="#">Edit</a>	<a href="#">Delete</a>
2	EMEA	Start at 00 : 00	<a href="#">Edit</a>	<a href="#">Delete</a>
3	NLAM	Start at 05 : 00	<a href="#">Edit</a>	<a href="#">Delete</a>

Add New Schedule

Save Cancel

Note: After you have added at least one schedule, click Save to save the new plan and schedule(s).

ENT

ent Plans)

# Мониторинг и управление

The screenshot displays a web-based management interface with the following components:

- Navigation:** Home, Services, Products, Reports, Administration.
- Product Directory:** A tree view showing folders like Root folder, New entity, APAC, EMEA, Gateway, Mail, Server, and NLAM. A specific product, MAUI\_IMSS\_AGENT, is highlighted.
- Event Logs Query Panel:**
  - Instructions: "Click the name of the log to view information about the managed product."
  - Options: [Event Logs](#), [Security Logs](#).
  - Search Parameters:
    - Severity:  Critical,  Warning,  Information,  Error,  Unknown
    - Incidents: All events
    - Product: MAUI\_IMSS\_AGENT
    - Time Range: 9/15/2006 to 9/15/2006
- Security Logs Query Panel:**
  - Instruction: "Choose the type of security information to display for all child Control Manager servers."
  - Table of Query Types:
 

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>
- Query Result (Event Logs) Table:**

#	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 выведен паттерн

The screenshot displays the InterScan Outbreak Prevention web interface. On the left, a navigation menu includes 'Outbreak Prevention', 'Vulnerability Assessment', 'Security Summary', 'Current Task', 'Tasks', 'History', and 'Global Settings'. The main area shows a table titled 'Top Threats Around the World' with columns for Virus name, Last updated, Alert type, Risk, Delivery method, and Required scan engine. The 'CUSTOM\_POLICY' entry is selected. On the right, the configuration panel for 'Outbreak Prevention Mode - WORM\_MYTOB.MX' is shown, including sections for Threat Information, Outbreak Prevention Policy (with a 2-day policy in effect), Outbreak Prevention Policy Details, Gateway (with various InterScan products checked), Message (with ScanMail products checked), Desktop/Servers (with OfficeScan and Damage Cleanup checked), and Remote Office/Third Party (with Firewall Management checked).

Virus name	Last updated	Alert type	Risk	Delivery method	Required scan engine
WORM_MYTOB.MX	11/24/2005 10:36:52 AM	Yellow	High	Email, Shared Drives	7.000
CICS_TEST_FILE	8/22/2005 10:47:35 AM	Yellow	Medium	test packet	6.810
CUSTOM_POLICY	11/5/2003 3:00:46 PM	Yellow	Low	n/a	5.200
EICAR_TEST_FILE	1/12/2004 8:39:39 PM	Yellow	Medium	Email	5.200
PE_BAGLE.N	3/14/2004 6:13:31 AM	Yellow	Medium	Email, Shared Drives	5.200
PE_BAGLE.P	3/15/2004 7:52:11 AM	Yellow	Medium	Email, Shared Drives	5.600

- Можно написать свою основе существующей



# 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

# Control Manager Demo

---



# Полезные ресурсы

---

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

Trend Micro

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

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

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

Прикладная логистика

[Support@polikom.ru](mailto:Support@polikom.ru)

Техподдержка  
Поликом Про