



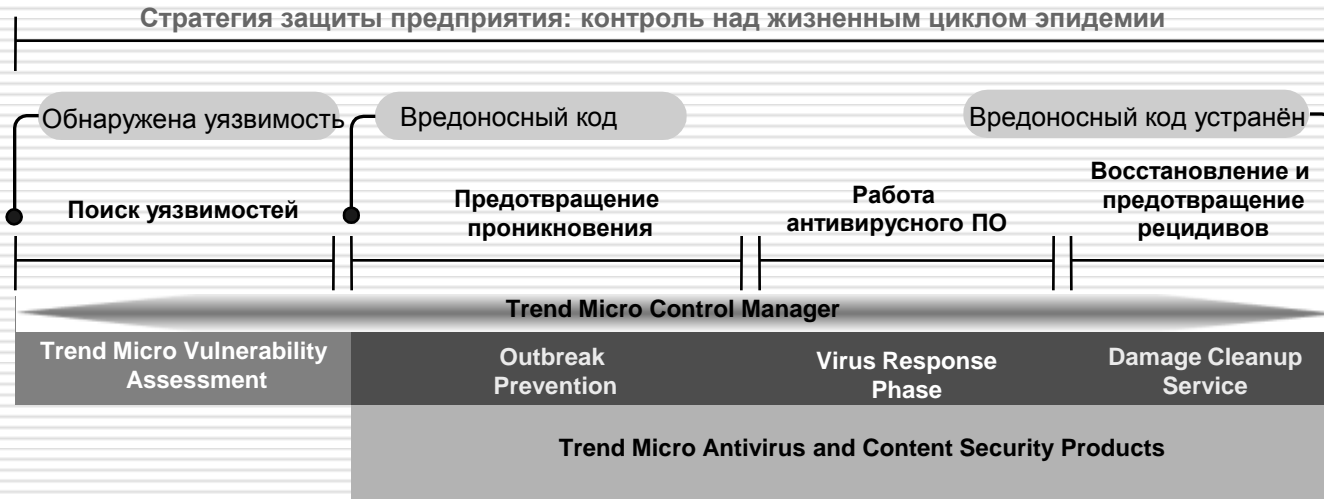
Координация действий по защите и управление продуктами
и службами Trend Micro. Trend Micro Control Manager

Антон Миносьян
Поликом Про

Что на повестке

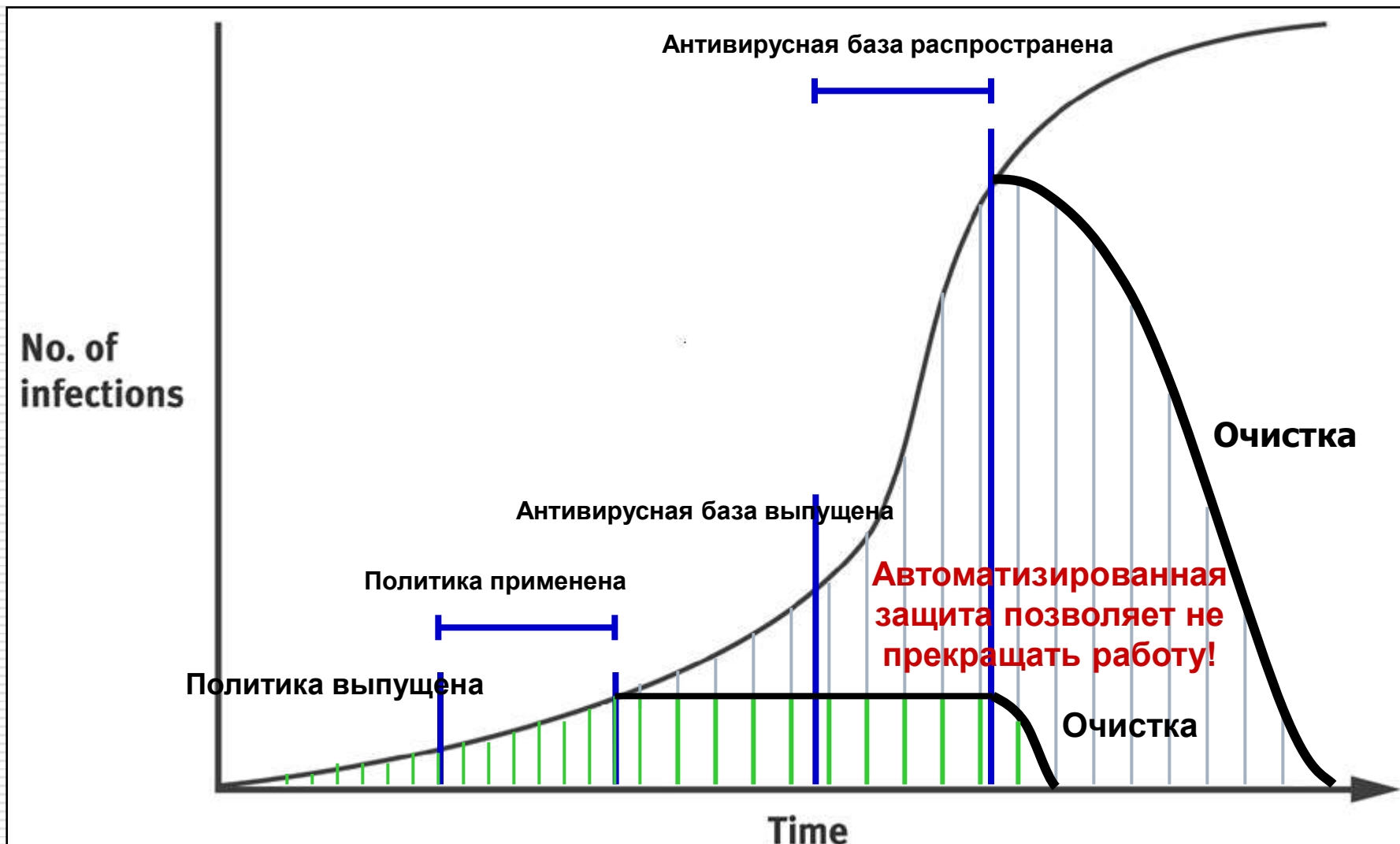
- Стратегия защиты предприятия
- Система централизованного управления антивирусным комплексом

Стратегия защиты предприятия



- Vulnerability Assessment
- Outbreak Prevention
- Damage Cleanup Service

Стратегия защиты предприятия



01.12.2008

Защита с централизованным управлением

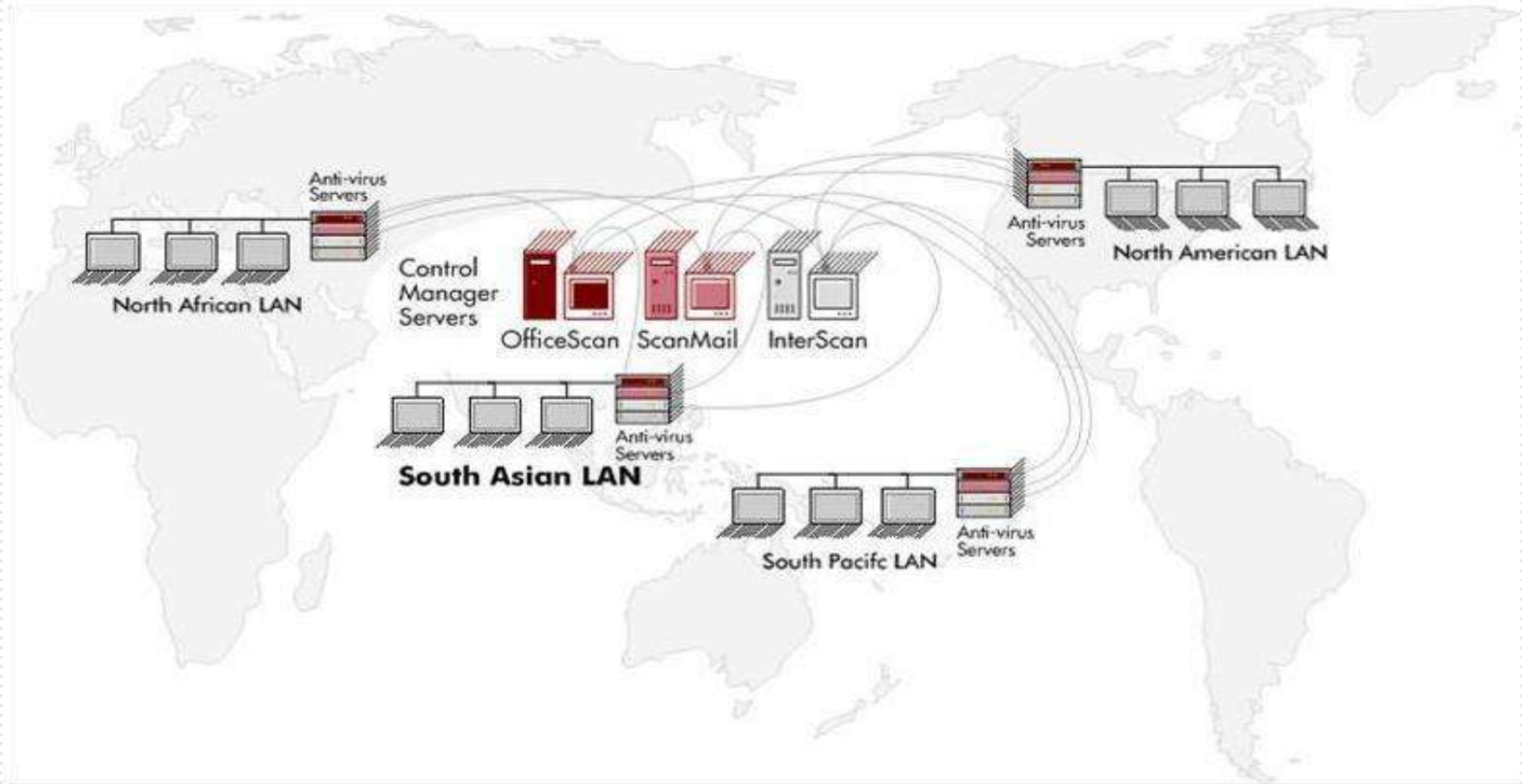


Зачем нужен Control Manager?

- ❑ 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)

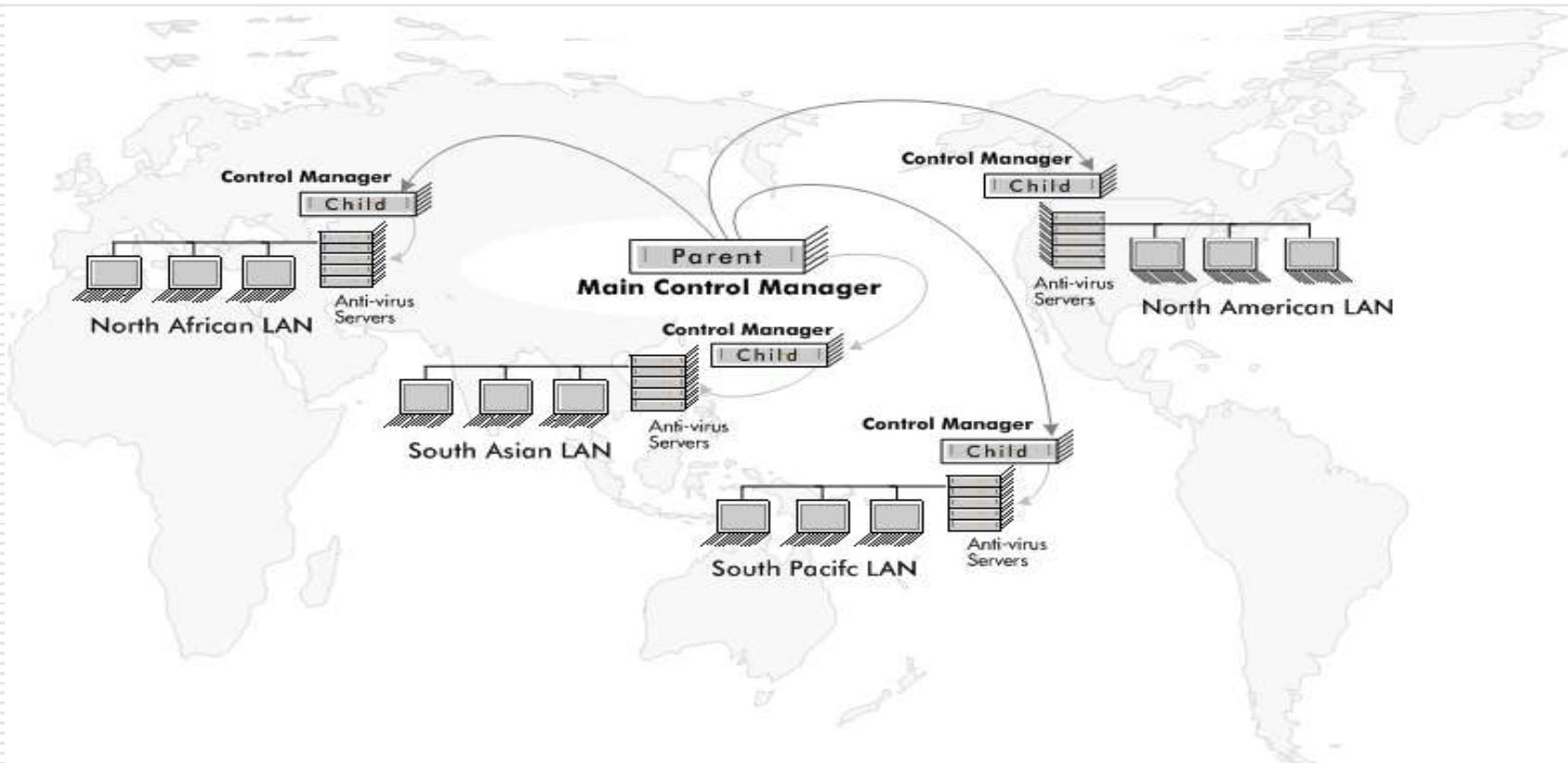
Варианты внедрения

Топология "по продуктам"



Возможности версии Advanced

- Двухуровневое каскадирование
- Комбинированная модель



Новое в версии Control Manager 5

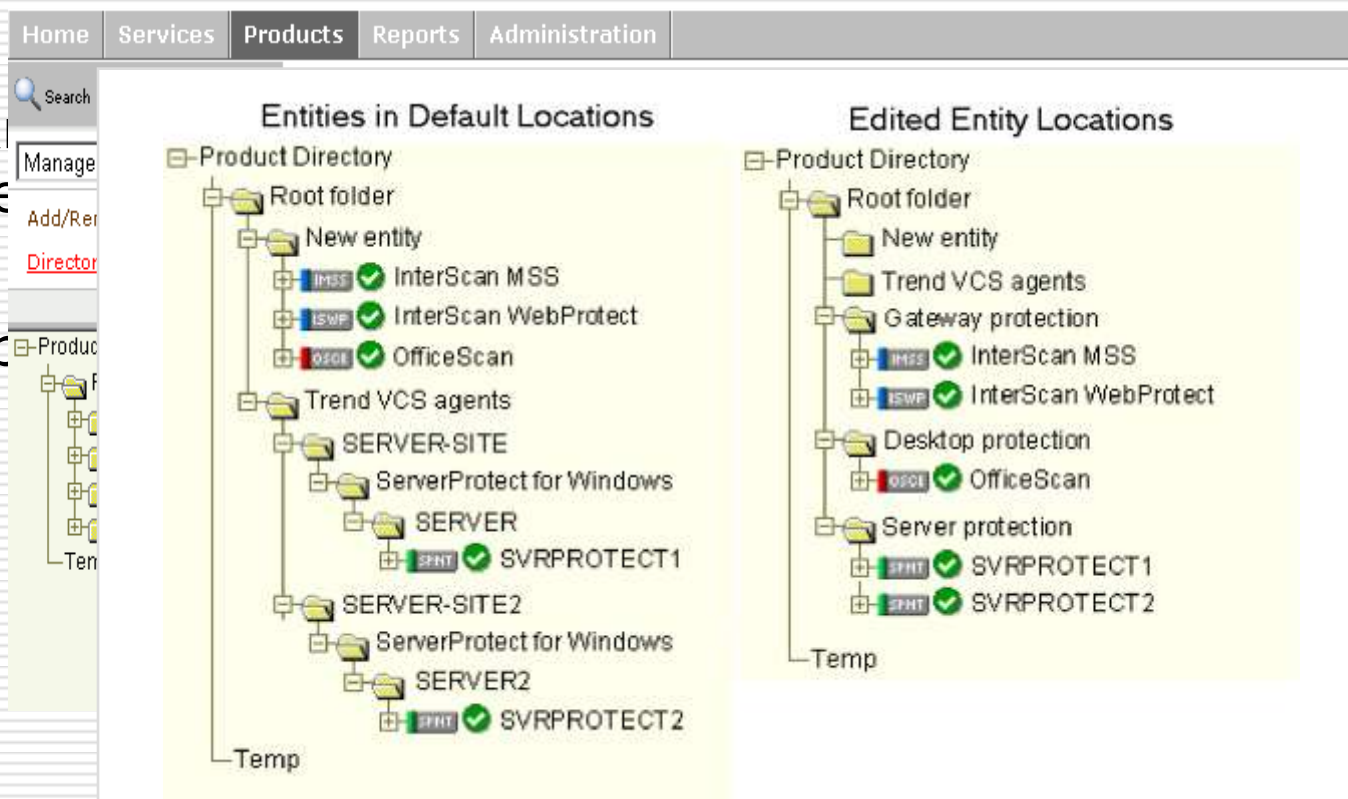
- Возможность просмотра отдельных файловых (OSCE) клиентов в консоли Control Manager
- Конструктор отчетов
- Распространение лицензионных ключей
- Дочерние Control Manager'ы в каскаде видны в дереве продуктов
- SSO в каскаде. Требования по версиям

Product Directory

- Представление антивирусного комплекса в виде дерева

- Возможность одновременного редактирования

- Децентрализация



Пользователи и группы

□ Корневой администратор

□ Четыре уровня доступа

■ Root

■ Administrator

■ Pow

■ Op

□ Аудит д

□ Группы оповещения



Уведомления и оповещения

Virus Outbreak Alert Settings

Alert Settings

Detections: instances

Computer or Users: computers or users

Period: hour(s)

dc1.polikom.com - Trend Micro Control Manager 5.0 - Windows Internet Explorer

https://dc1.polikom.com/WebApp/index.html

File Edit View Favorites Tools Help

dc1.polikom.com - Trend Micro Control Manager 5.0

TREND MICRO Control Manager™

Home Products Services Logs / Reports Updates Administration

Edit Recipients

Recipients

Select Users and Groups:

Available Users and Groups: --- Group List --- Unexpected_Event Update_Event --- User List --- 880_User root

Selected Users and Groups: --- Group List --- Virus_Event --- User List ---

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

TREND MICRO Control Manager™

Log off TREND MICRO

Home Products Services Logs / Reports Updates Administration Help Logged on as: root

Event Category

Alert

Event	Settings	Recipients
<input checked="" type="checkbox"/> Virus outbreak alert	Settings	Recipients
<input checked="" type="checkbox"/> Special virus alert	Settings	Recipients
spyware/grayware alert	Settings	Recipients
und - first action unsuccessful and second action unavailable		Recipients
und - first and second actions unsuccessful		Recipients
und - first action successful		Recipients
und - second action successful		Recipients
virus alert	Settings	Recipients
vulnerability attack detected	Settings	Recipients
√Grayware found - action successful		Recipients
√Grayware found - further action required		Recipients
Malware Prevention Services	Settings	Recipients
outbreak Prevention Policy received		Recipients
Malware Prevention Mode started		Recipients
Malware Prevention Mode stopped		Recipients
Malware Prevention Policy update unsuccessful		Recipients
Malware Prevention Policy update successful		Recipients
System Health Assessment	Settings	Recipients
System Health Assessment task completed		Recipients

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:

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:

Schedule(s):

#	Destination	Deployment Time	Edit	Delete
1	APAC	Start at 19 : 00	Edit	Delete
2	EMEA	Start at 00 : 00	Edit	Delete
3	NLAM	Start at 05 : 00	Edit	Delete

Add New Schedule

Save Cancel

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

Мониторинг и управление

The screenshot displays a web-based management interface with a top navigation bar containing 'Home', 'Services', 'Products', 'Reports', and 'Administration'. Below this, there are three overlapping panels illustrating the workflow:

- Top Panel:** Shows the 'Logs' tab selected. A message states: 'Click the name of the log to view information about the managed product.' Below this, there are links for 'Event Logs' and 'Security Logs'.
- Middle Panel:** Shows the 'Event Logs Query' form. It includes a 'Severity' section with checkboxes for Critical, Warning, Information, Error, and Unknown. The 'Incidents' dropdown is set to 'All events'. There are date pickers for 'From' (9/2006) and 'To' (15/2006).
- Bottom Panel:** Shows the 'Security Logs Query' form with a list of query options and a 'Query' button. The 'Query Result (Event Logs)' table is also visible, showing two log entries.

Product Directory (Left Panel):

- Root folder
 - New entity
 - APAC
 - EMEA
 - Gateway
 - IMSS MAUI_IMSS_AGENT
 - Mail
 - Server
 - NLAM

Security Logs Query Options:

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

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 eManager interface. On the left, a navigation menu shows 'Outbreak Prevention' selected. The main area is divided into two panes. The left pane, titled 'Start Outbreak Prevention Mode', shows a table of 'Top Threats Around the World'. The right pane, titled 'Outbreak Prevention Mode - WORM_MYTOB.MX', shows the configuration for this specific threat.

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

The configuration panel for WORM_MYTOB.MX includes the following sections:

- 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:** Includes 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 VirusWall, and Portal Protect.
- Message:** Includes ScanMail for Microsoft Exchange, ScanMail for Lotus Notes / ScanMail for Domino, ScanMail eManager, and IM Security for Microsoft Live Communications Server.
- Desktop/Servers:** Includes ServerProtect for Windows, ServerProtect for Linux, OfficeScan Corporate Edition, and Damage Cleanup Services 3.0.
- Remote Office/Third Party:** Includes Firewall Management: NetScreen.

- 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

Trend Micro

www.antivirus.com

www.trendbeta.com

www.apl.ru

Прикладная логистика

Support@polikom.ru

Техподдержка
Поликом Про

Контактная информация

190000, Санкт-Петербург
наб. реки Мойки, 86
тел. 812|325-8400 факс : 812|110-6431

103064, Москва
ул. Старая Басманная, 10, строение 5, офис 8
тел. 495|744-1117 факс : 495|737-8975

Антон Миносьян

aminosjan@polikom.ru