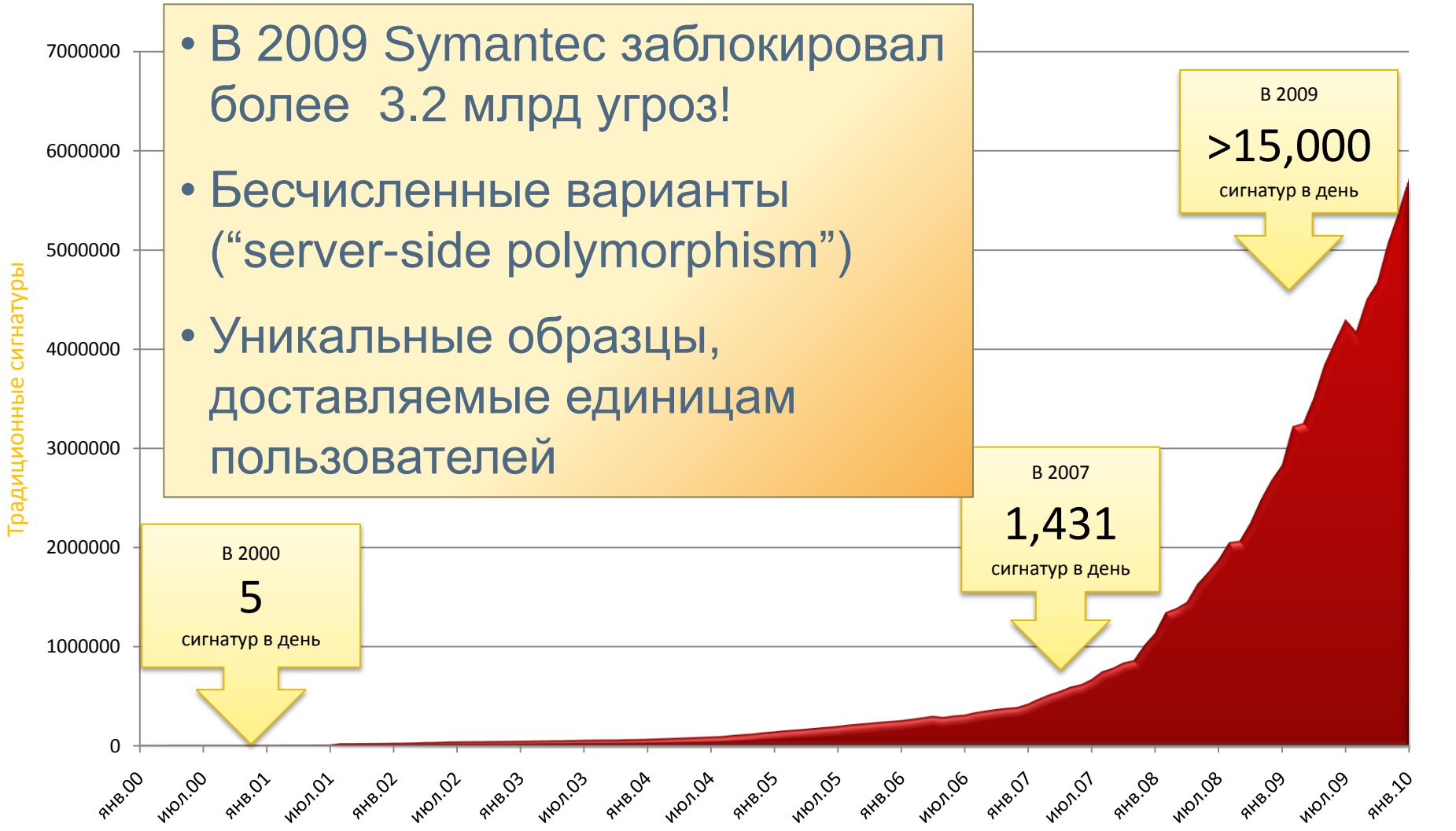
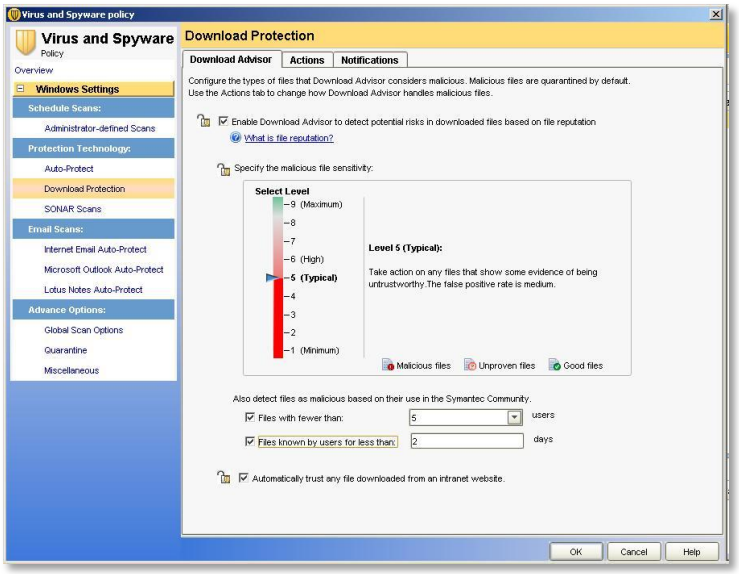
Symantec Endpoint Protection, Symantec Protection Center

Олег Шабуров

Картина угроз – двигатель появления Amber

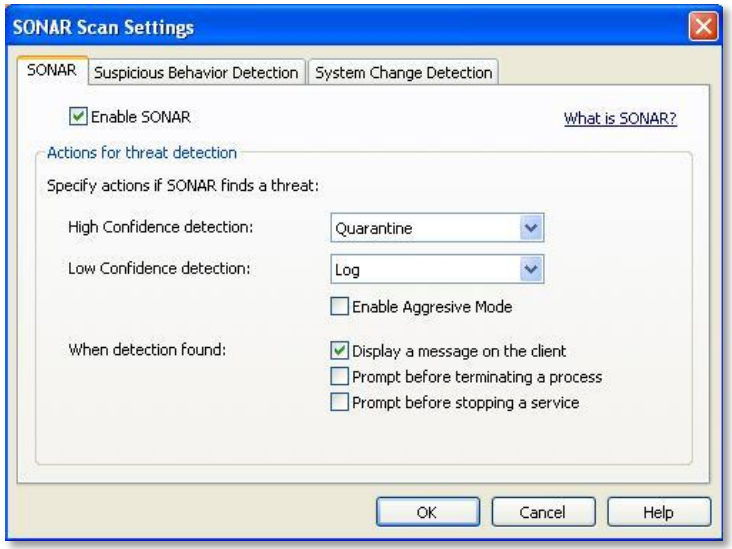


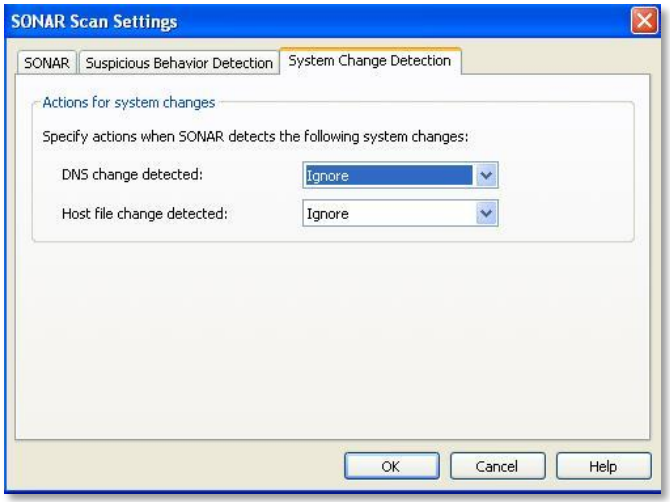
Reputation Protection – Download Advisor



- Проблема: пользователи часто сталкиваются с образцами злонамеренного ПО, доставляемого единицам пользователей. Стандартные сигнатуры выходят с задержкой
- Решение: технологии защиты, не зависящие от наличия образца злонамеренного ПО у Symantec
- Функции:
  - Репутация для обнаружения угроз
  - Возможность кастомизации политик
  - «Порог» по времени и распространенности
  - Логи и отчеты по источнику заражений
  - Защита для браузеров, P2P-приложений, почты…

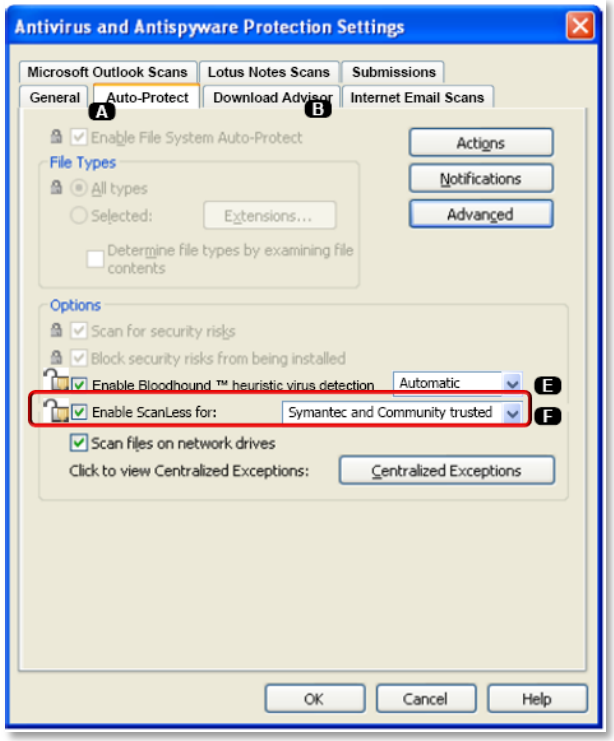
Reputation Protection – SONAR

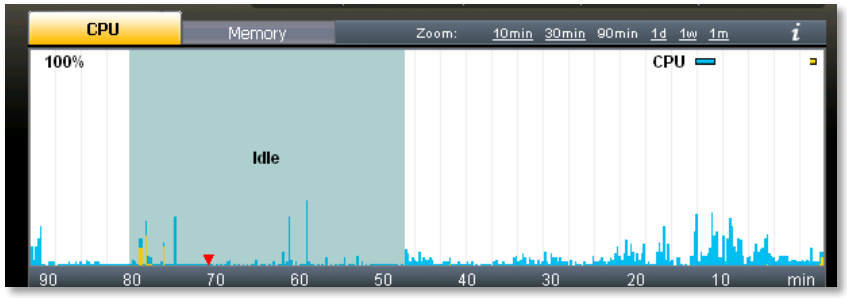




- Проблема: эффективность TruScan зависит от обновлений продукта, которые происходят по умолчанию раз в час
- Решение: обновить TruScan, чтобы она работал в режиме реального времени и использовал репутацию для избавления от ложных срабатываний
- Функции:
  - Защита рабочих станций и серверов
  - Работает на 32/64 битных системах
  - Анализ файлов и сетевого поведения
  - Защита от изменения hosts-файла и DNS
  - Защита собственных модулей
  - Репутация для защиты от ложных срабатываний

Новая технология ScanLess





- Проблема: Сканирования загружают систему. Ресурсы тратятся на сканирование одних и тех же файлов
- Решение: технология, пропускающая «доверенные» файлы, а также сканирование во времена простоев
- Функции:
  - Репутация для исключения файлов, которым доверяет Symantec и сообщество
  - Администратор может выбирать либо пользоваться информацией, либо все блокировать
  - Сканирование во время простоев
  - Применимо к сканированиям по запросу/по расписанию

Protection Center 1.0, 2.0

Сложность управления безопасностью возрастает

Организация

- Operations Team
- Security Team
- Compliance & Audit
- Executive Team
- Data Owners

Цели

Уменьшение TCO

Стандартизация

Повышение эффективности

Централизованная информация

Технологии

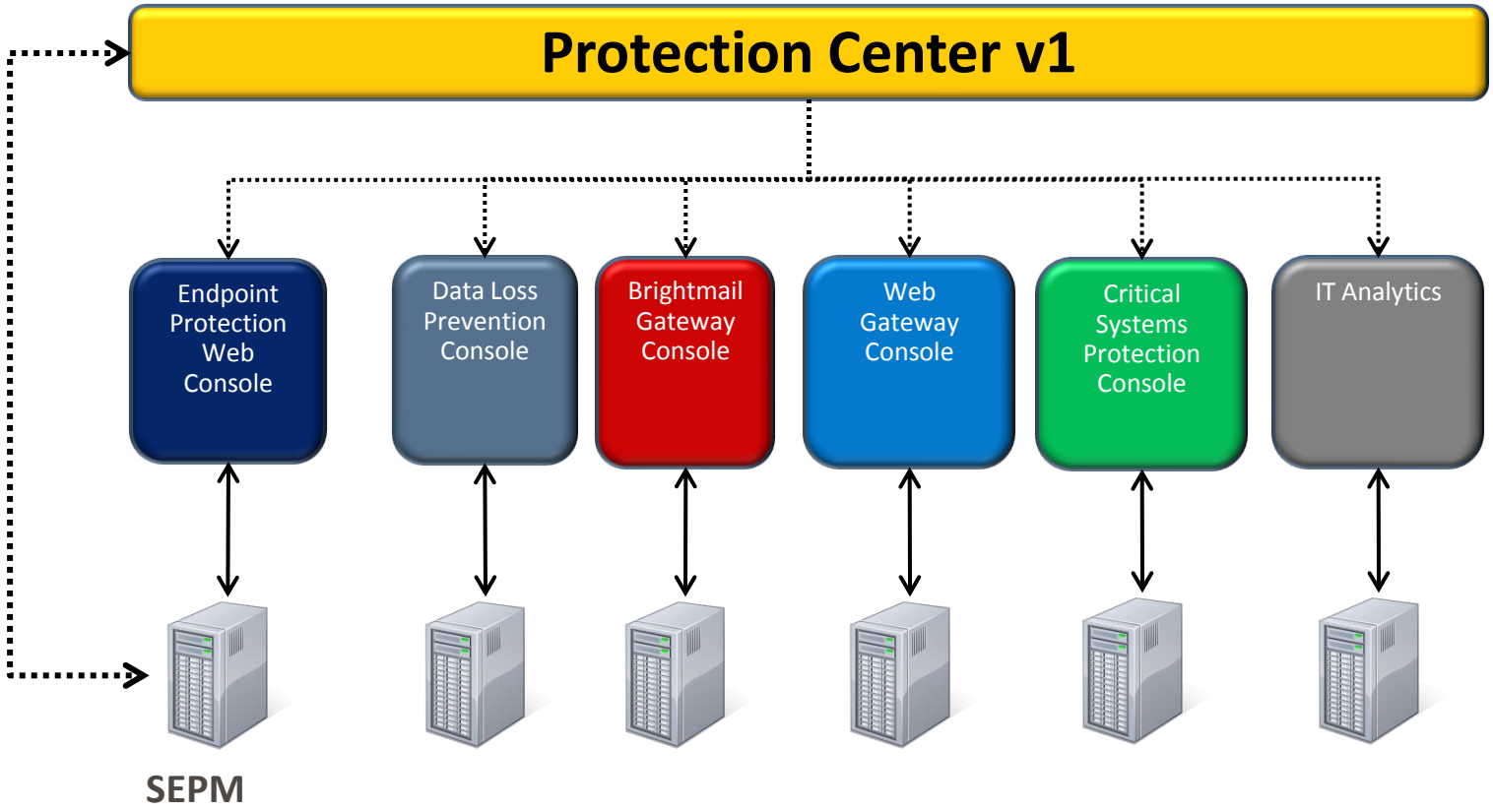
- Client Security
- Server Security
- Messaging Security
- Network Security
- Compliance
- Data Loss Prevention
- Helpdesk Tools
- Management Software

Protection Center 1.0

Первый шаг к централизации управления

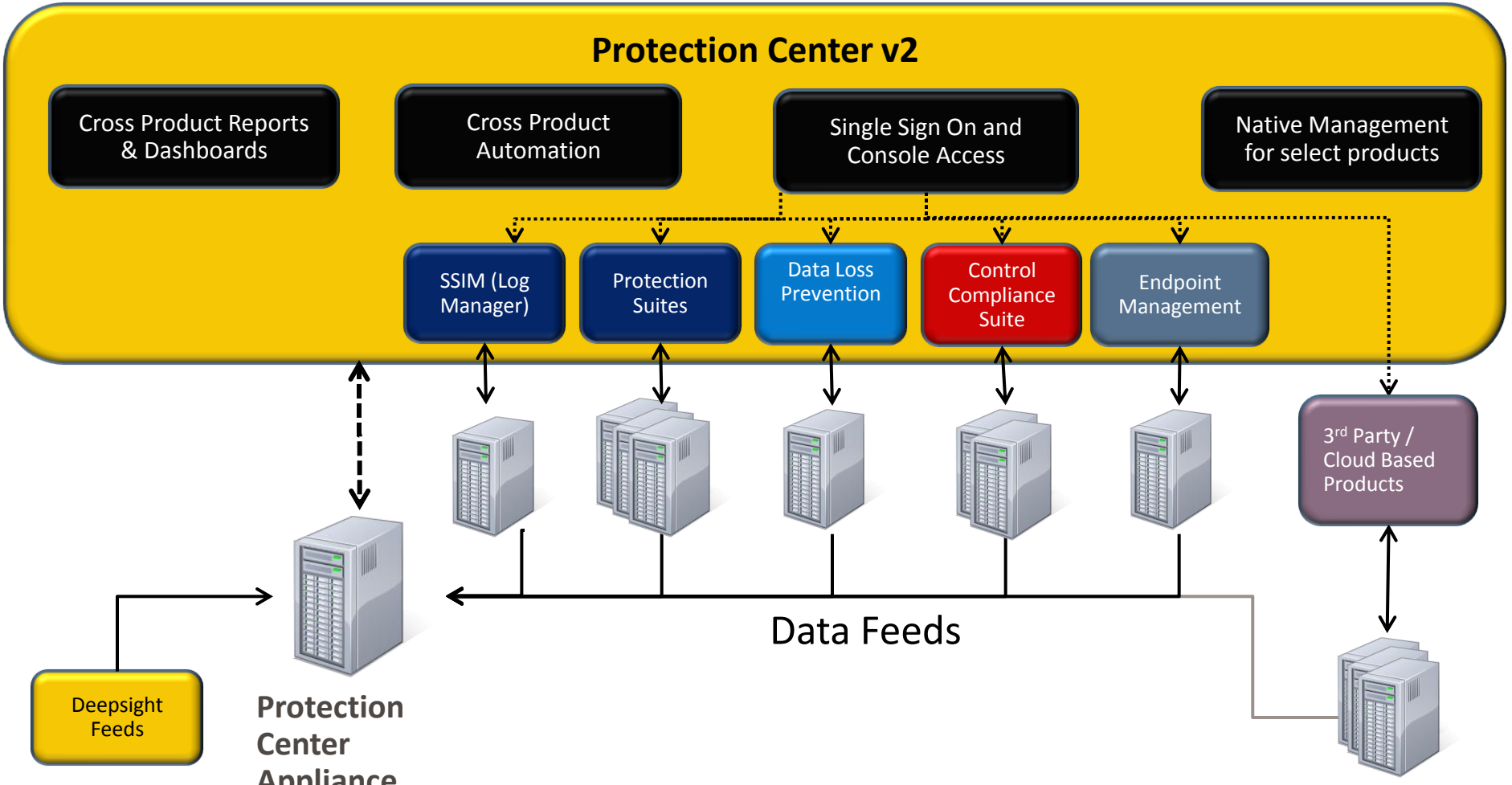
Protection Center 1.0

SSO и централизованное управление



Protection Center 2.0

Кросс-продуктовая отчетность и автоматизация



Protection Center 2.0

Унифицированная консоль управления

Общий вид и управление

Прозрачный Single Sign On

Кросс-продуктовые отчеты, дашборды

Простота управления

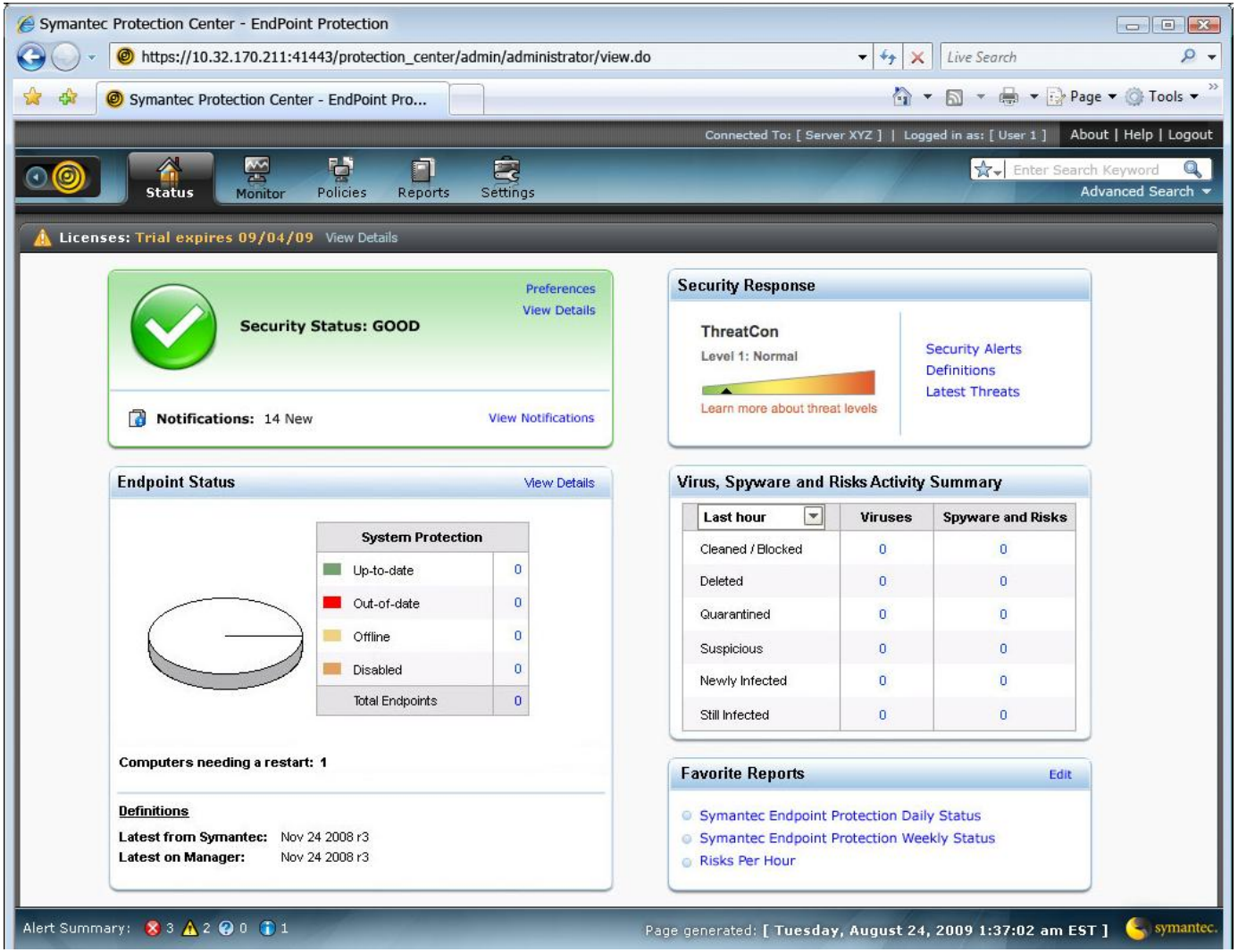
Protection Center 2.0
Интерфейс нового поколения

Основан на исследовании поведения пользователей

Новый стандарт Symantec

Оптимизирован под произво-дительность

Более интерактивный



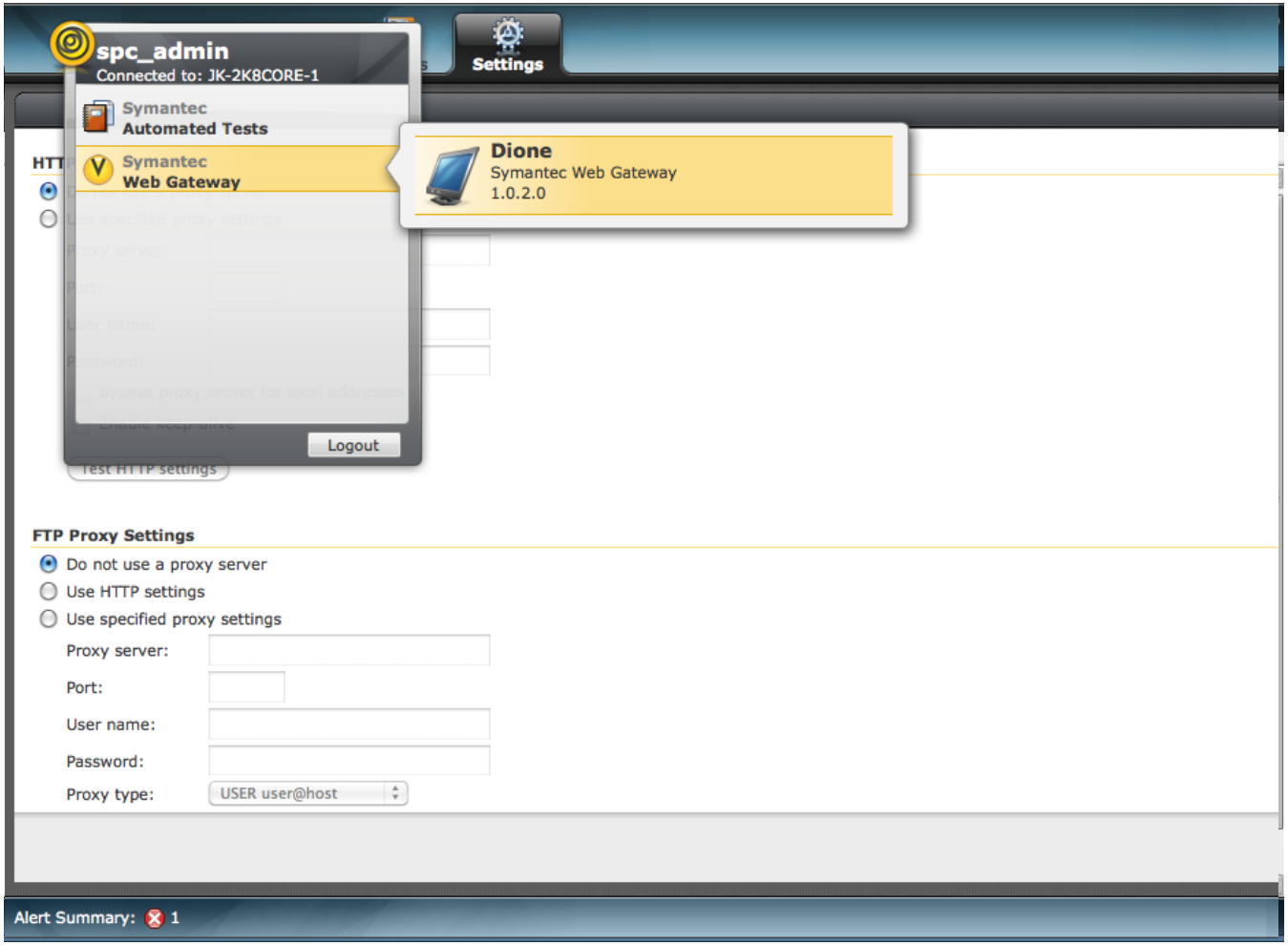
Protection Center 2.0
Интеграция и управление

Автоматическое обнаружение

Работа с имеющимися инфраструктурами

Централизованное управление пользователями

Ролевое администри-рование



Protection Center 2.0

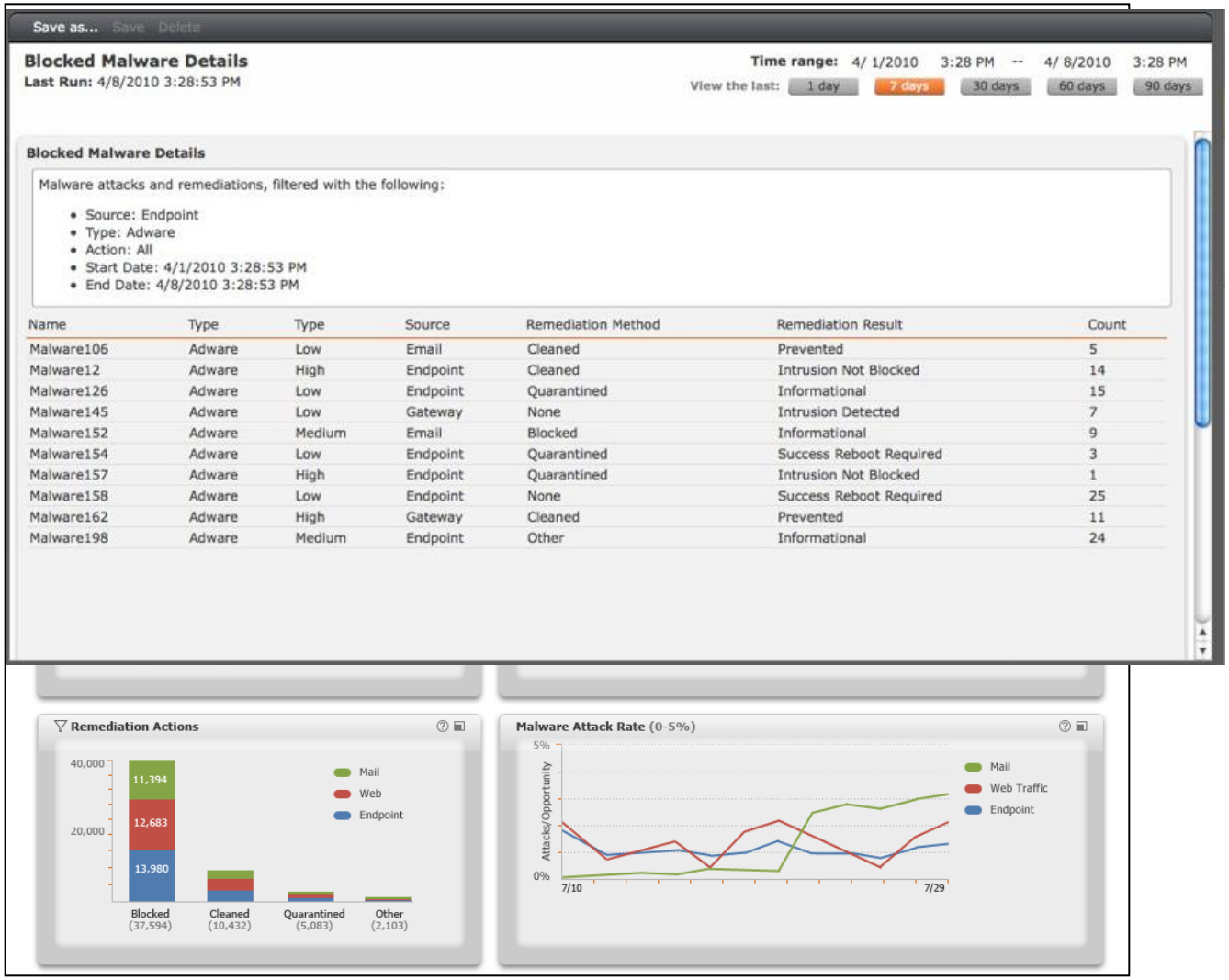
Кросс-продуктовая отчетность

Единая отчетность по продуктам

Встроенные действия

Возможность Drill-Down

По запросу / по расписанию



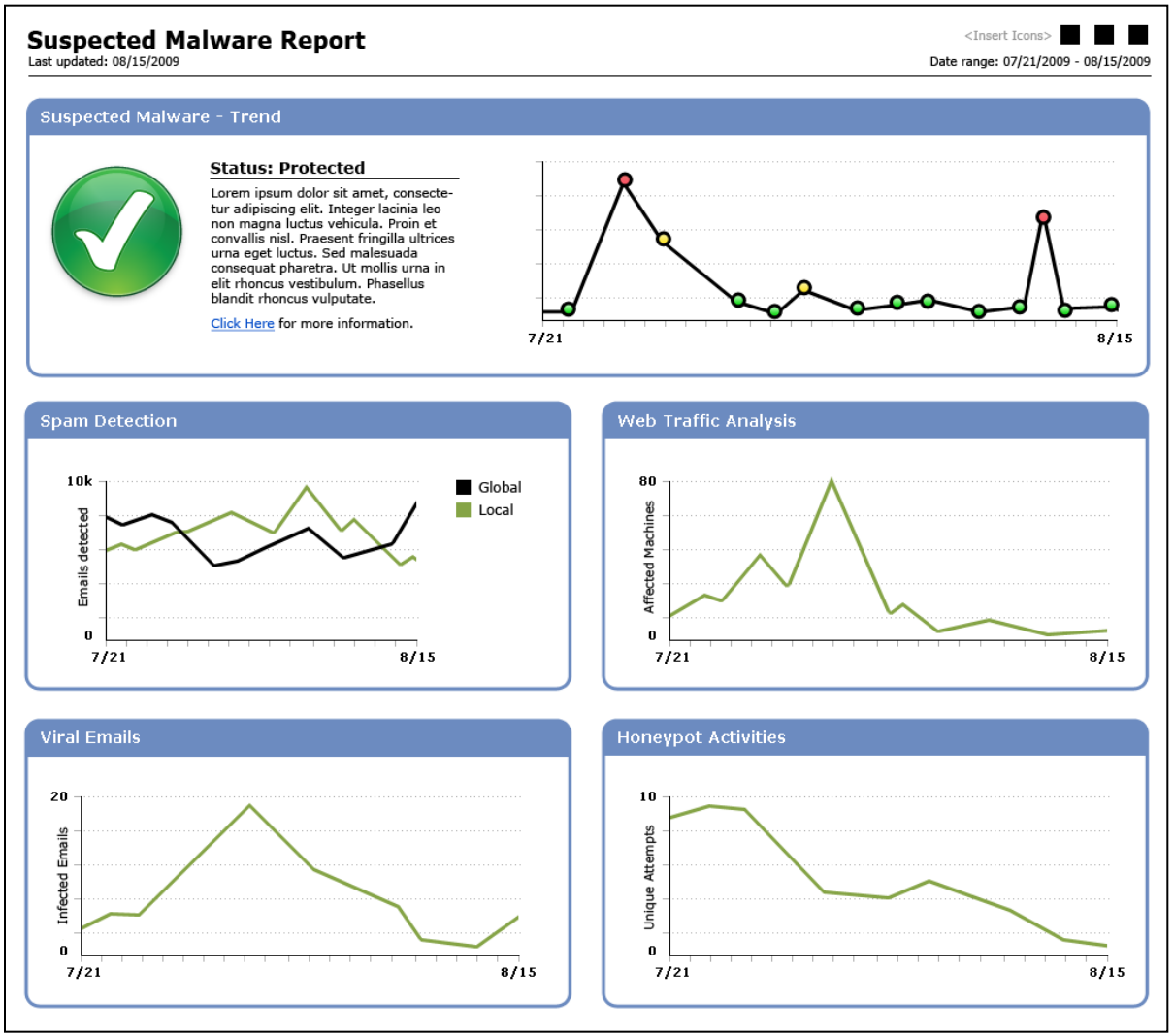
Protection Center 2.0
Кросс-продуктовый анализ

Подозрительное ПО

Отчеты по активам

Отчеты по аудиту

Отправка отчетов



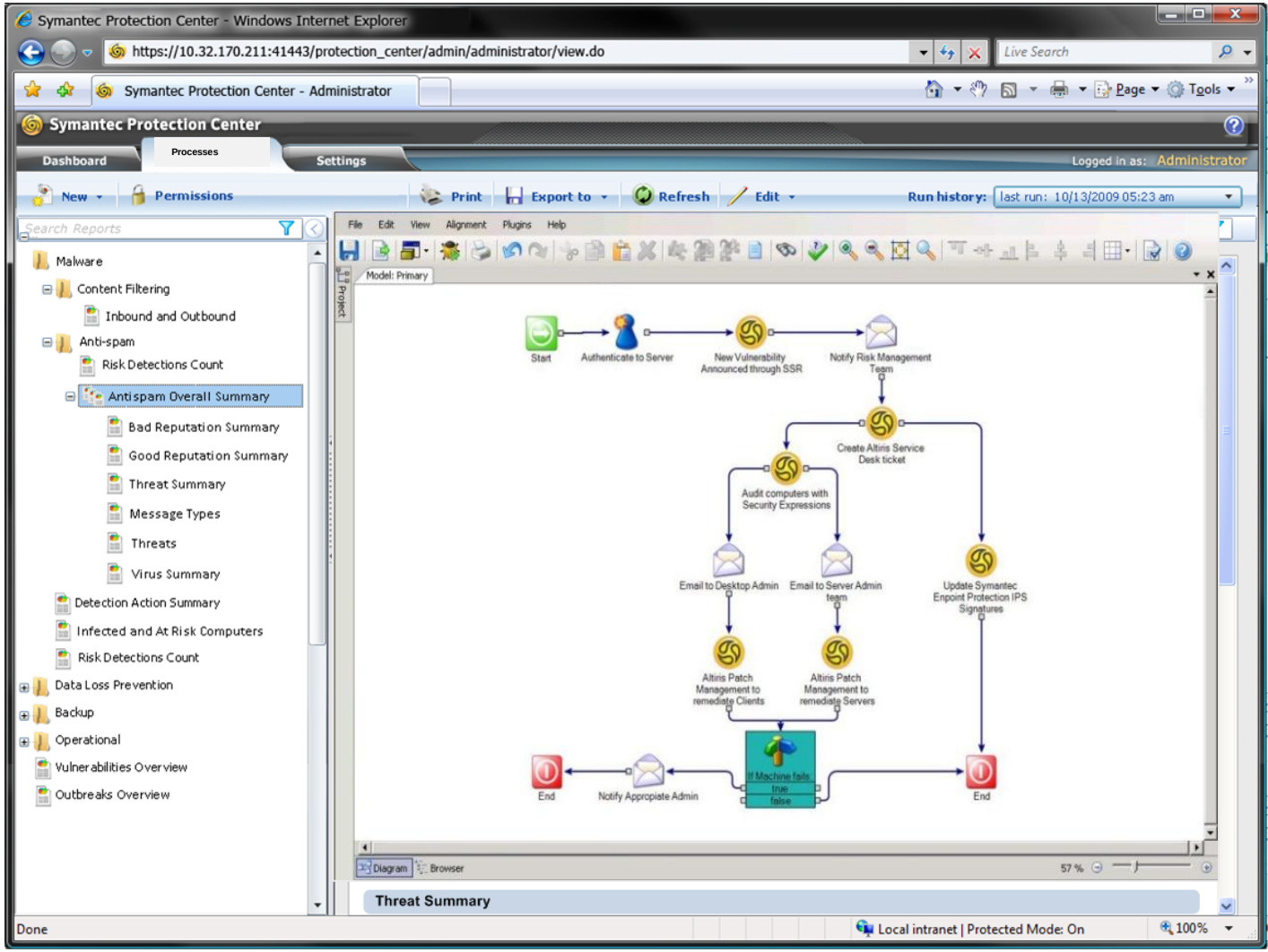
Protection Center 2.0:
Автоматизация кросс-продуктового процесса

Управление любыми продуктами

Автомнатизиро-ванное и ручное управление

Конструктор рабочего процесса

Symantec и продукты 3-х сторон



Спасибо за внимание!

Олег Шабуров

oleg_shaburov@symantec.com

+7-916-924-8006

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.