

Antigen

HIGH-PERFORMANCE
GROUPWARE SECURITY

Messaging and Collaboration Security

Antigen 6.5 for Exchange

Miguel Canales

Regional Engineering Manager CEUR

miguel_canales@sybari.com

Sybari Software



- Sybari's mission is to deliver superior antivirus and information security solutions for groupware environments.
- We remain ever-vigilant about developing innovative solutions that effectively manage content within the enterprise and protect the integrity of our clients' data and mission-critical systems.
- We strive to provide our customers with unparalleled customer support and service.



Please visit us at www.sybari.com

Sybari



The Antigen Product Family

- For Microsoft Exchange, Lotus Domino, and Microsoft SharePoint Portal Server
- Reliable, high performance server-side antivirus and content management solutions
- Designed to detect and remove viruses *BEFORE* they reach mission critical apps
- Protect the integrity of client's data and mission critical mail systems



Sybari Worldwide

East Northport, New York (World Headquarters / Technical Support)

Madrid (European Headquarters / Technical Support)

Singapore (Asia Pacific Headquarters / Technical Support)

Plantation, Florida (Latin America Headquarters)

San Jose, CA (Technical Support)

London, U.K.

Paris, France

Rome, Italy

Amsterdam, Holland

Dubai, UAE

Sydney, Australia

Munich, Germany

São Paulo, Brazil

Mexico City, Mexico



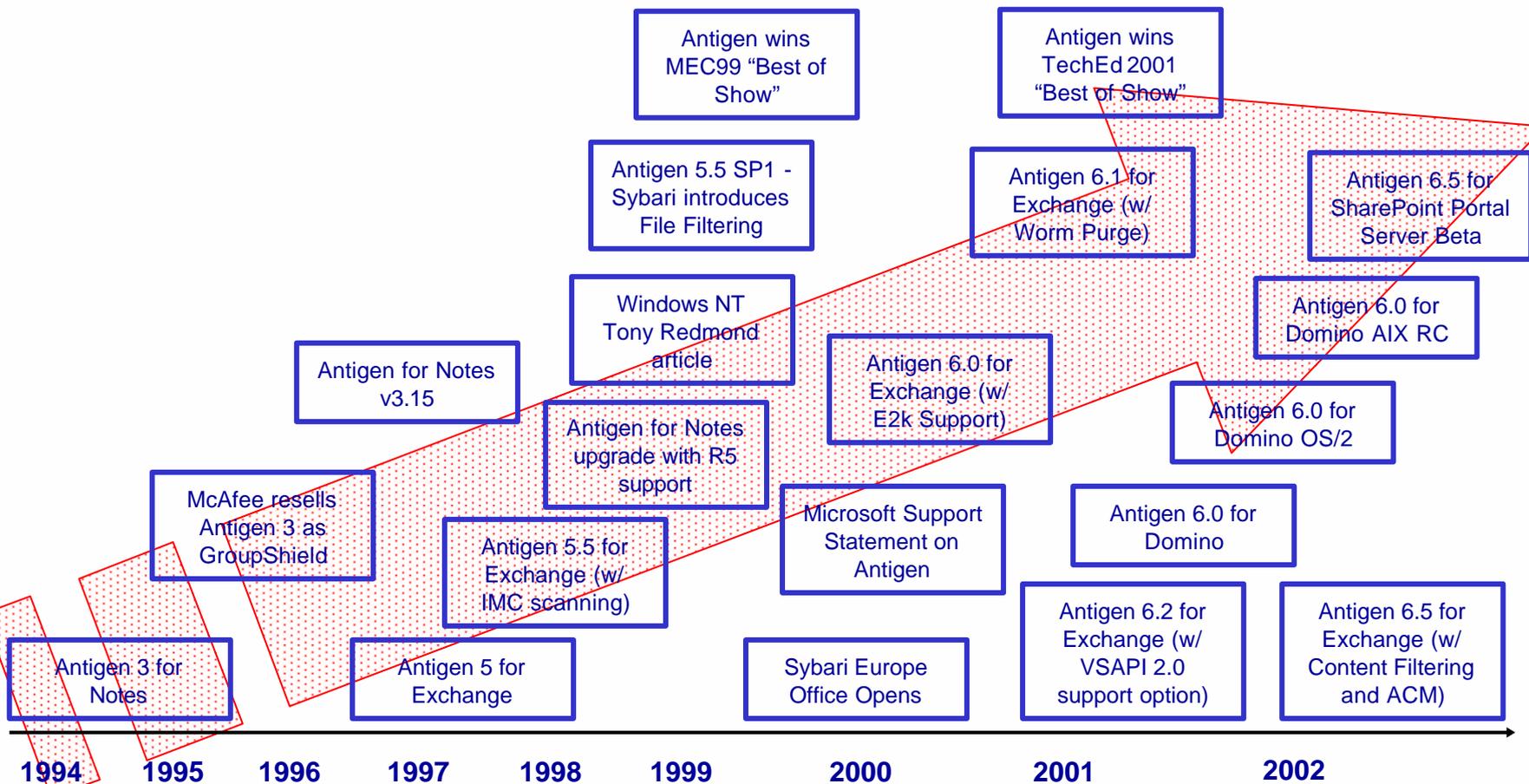
Over 200 employees worldwide

Time Tested

More than **8 million** Groupware seats are virus-free as a result of Sybari technology and products.



Sybari Company History



Sybari
EVER-VIGILANT PROTECTION

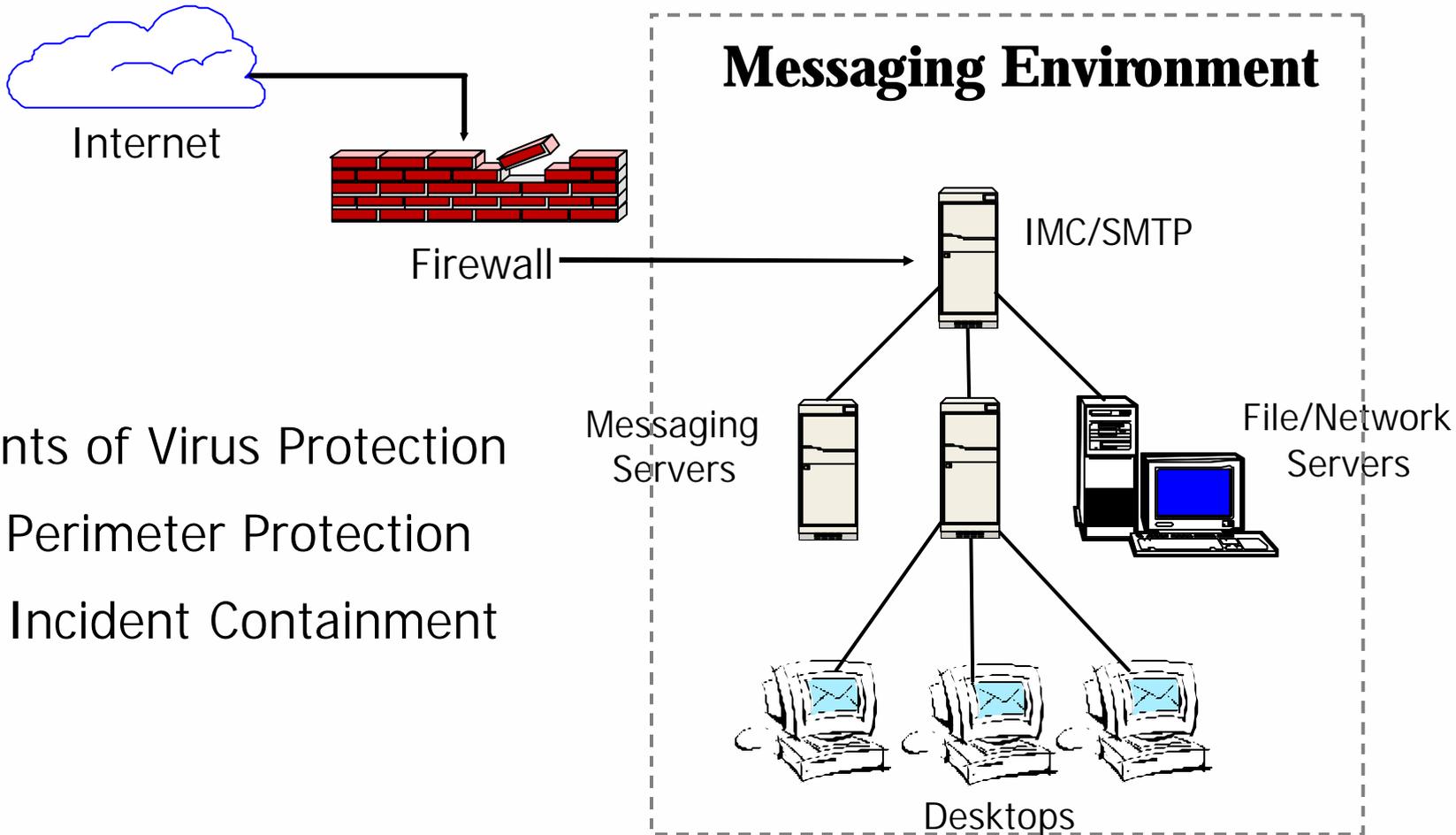


Antigen

HIGH-PERFORMANCE
GROUPWARE SECURITY

*The Need for Antivirus Security
In Exchange Environments*

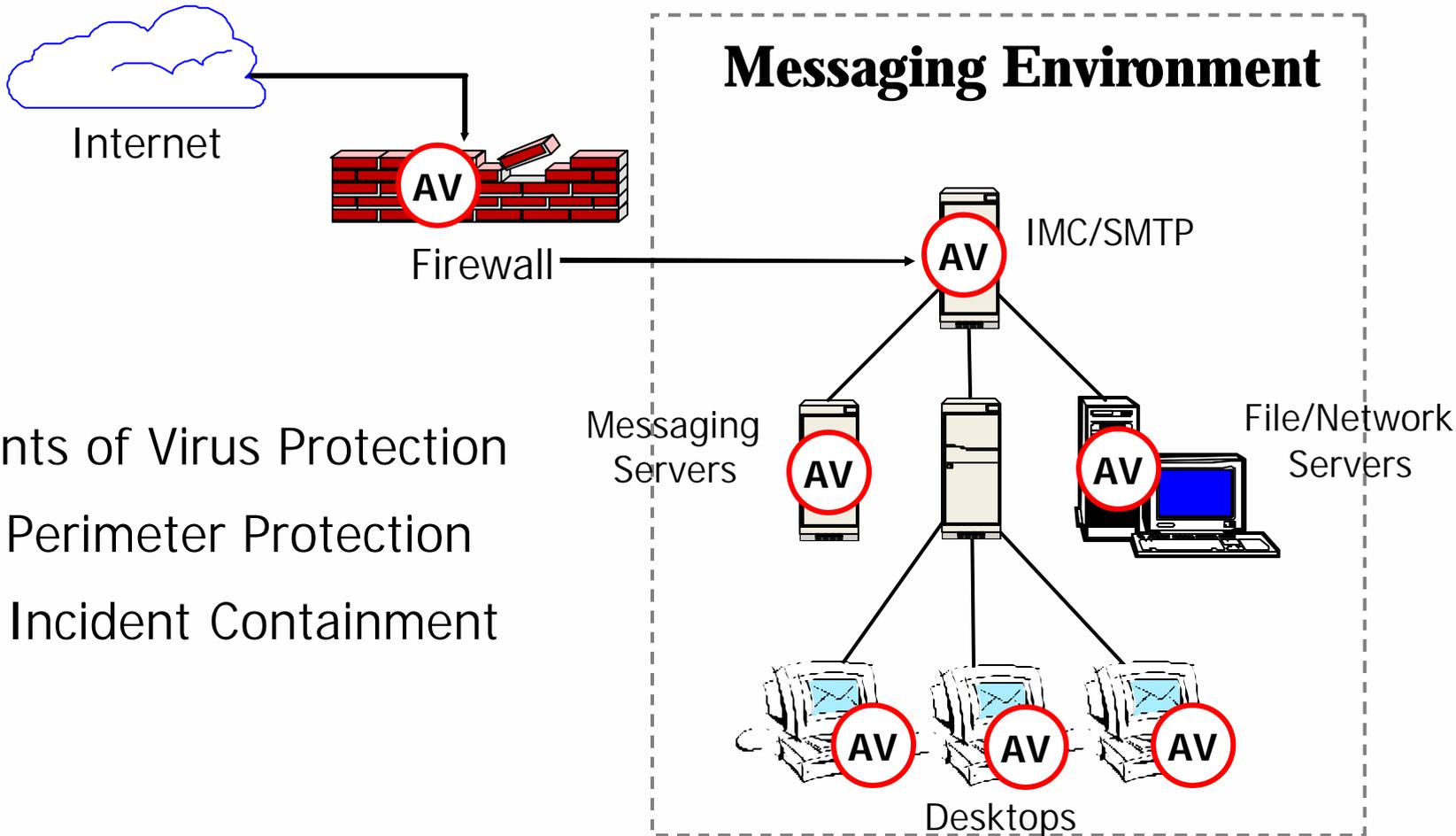
Antivirus Strategy



Points of Virus Protection

- Perimeter Protection
- Incident Containment

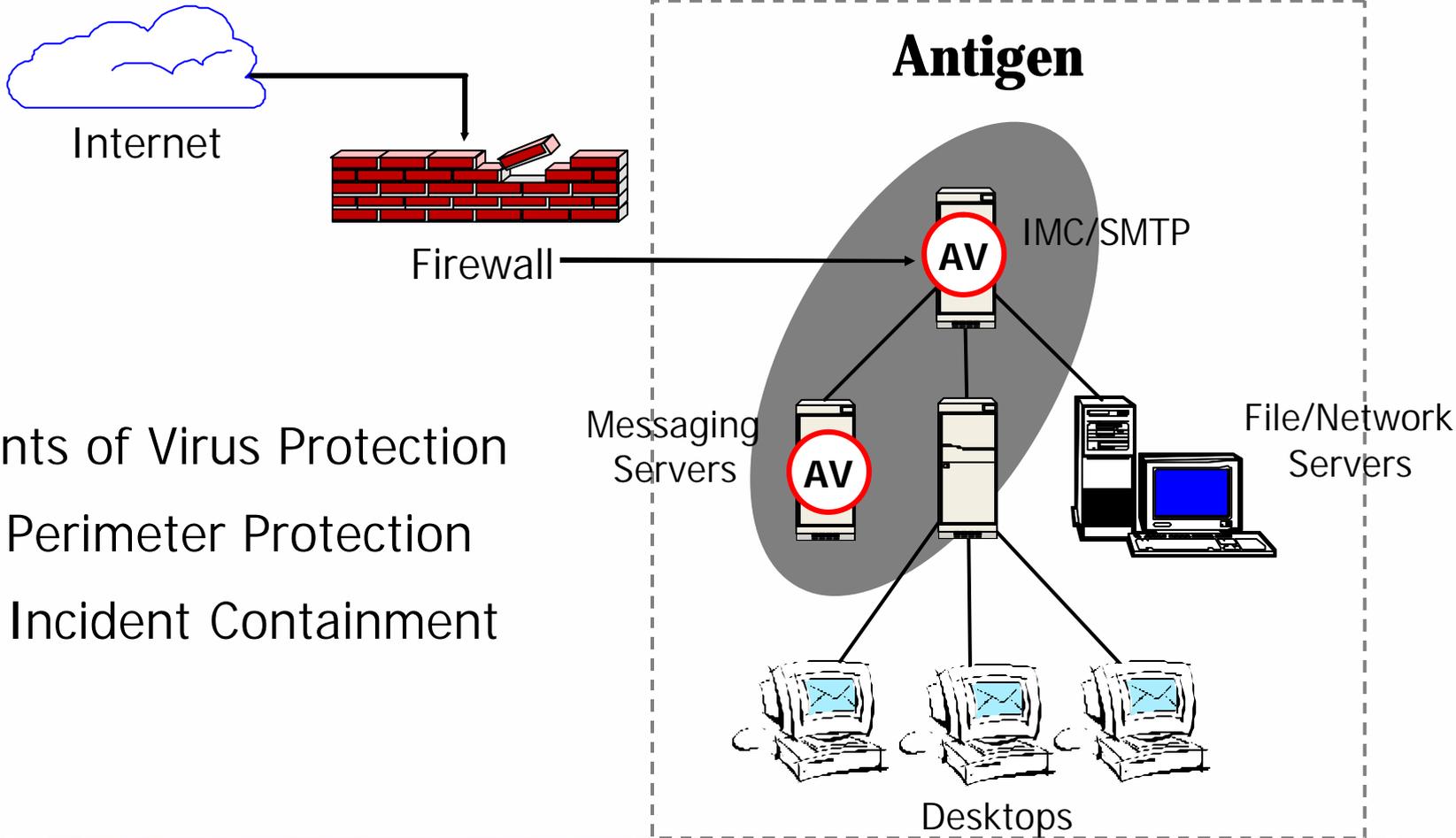
Antivirus Strategy



Points of Virus Protection

- Perimeter Protection
- Incident Containment

Antivirus Strategy



Points of Virus Protection

- Perimeter Protection
- Incident Containment

Sybari
EVER-VIGILANT PROTECTION

Antigen

HIGH-PERFORMANCE
GROUPWARE SECURITY

Antigen 6.5
Features and Benefits

Antigen 6.5 for Exchange



- Antigen has been designed and architected to provide 100% reliability and top performance.



Please visit us at www.sybari.com

Subari

Antigen 6.5 for Exchange

- Design and architecture provides leading Sybari's ESE interface for Exchange 5.5, migration and mixed environments
- Dual-mode design provides both VSAPI 2.0 compliance and ESE support options in Exchange 2000

Antigen 6.5 for Exchange

- Web Store & IMC Protection
- Multiple Scan Engine Management
- Worm Purge
- Selectable Modes – ESE & VSAPI
- Content Filtering
- Enterprise Deployment

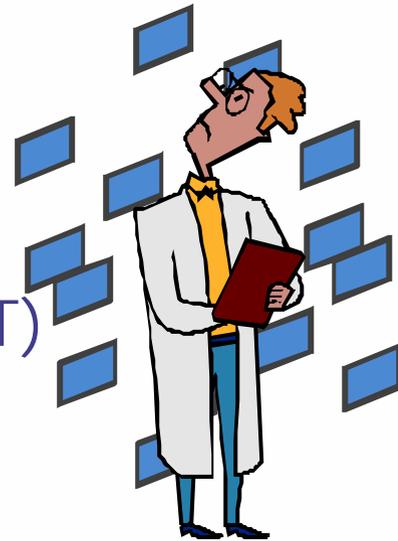
Web Store & IMC Protection

- Real-time and manual store protection
 - ESE (Extensible Storage Engine)
 - VSAPI 2.0 option
- IMC protection (Exchange 5.5)
 - Real-time protection of Inbound and Outbound queues of the Exchange Internet Mail Connector
- SMTP protection (Exchange 2000)
 - Uses Transport Event Sinks on Win2000 SMTP stack
- MTA protection (Exchange 2000)
 - For X.400, cc:mail, Notes, MSmail, etc.

Multiple Scan Engine Management

Antigen OEMs and integrates:

1. Norman Data Defense
2. Sophos Antivirus
3. CA eTrust Solutions (Innoculate+VET)
4. NAI (McAfee) VirusScan
5. Kaspersky Labs AVP



Best of Breed solution designed for 100% Detection Rate



100% Rate of Detection

Subari

Multiple Scan Engine Management

- “Multiple scanning” of attachments per Antigen job
- Intelligent scanning and engine use adjustments
- Performance Tuning and Bias Settings allow the administrator to set appropriate for their environment
- Crash protection – if one engine fails, the others continue to provide protection
- Ability to vary settings per job and storage group
- Continue email and scanning during engine updates

Supports current corporate strategy away from “suites” to point products with different scan engines

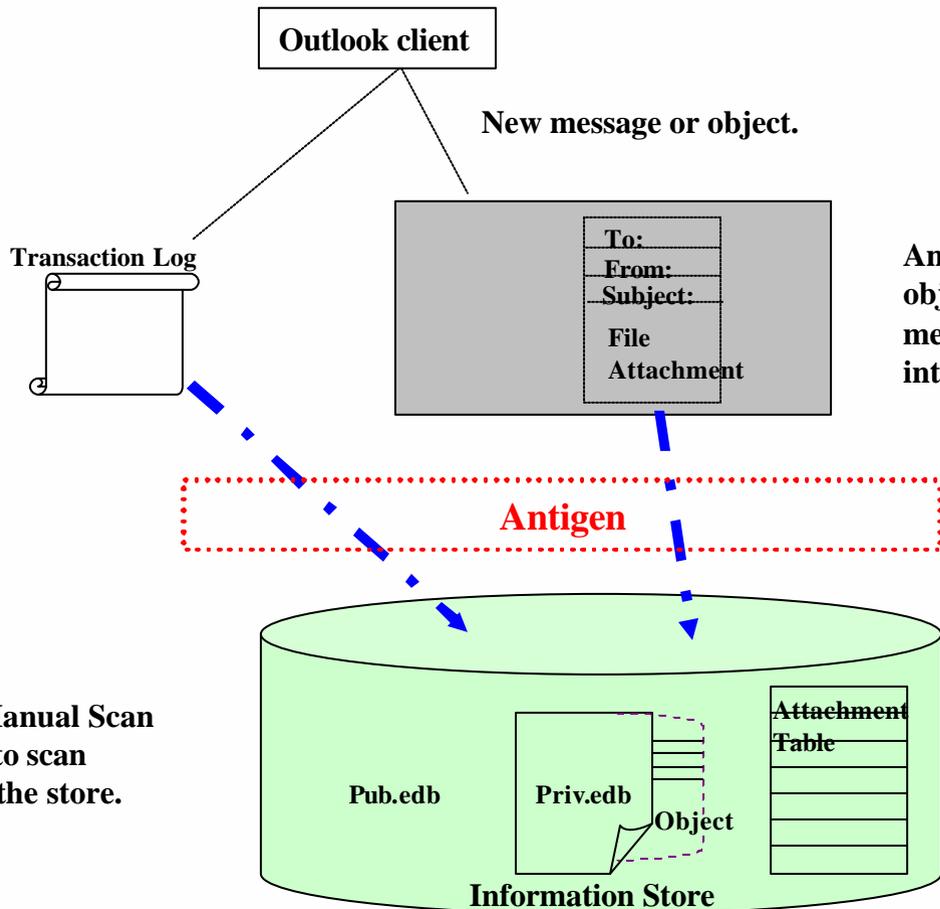
Worm Purge

- Purge all inbound email messages with identified worm viruses at the IMC/SMTP
- Purge outbound email messages at the IS
- Sybari Worm List and updates
- Custom List available
- File Filter Purge option

Antigen ESE Store Protection

- Scan the “writes” into Exchange Information Store
- In-Memory Scanning
 - File Attachments
 - Multi-level .ZIP files
- Single instance message scanning
- All Exchange objects with attachments are scanned when created or modified.
- Private and Public Stores protected with the same approach.
- Both Manual and Real-time scanning

Antigen ESE Interaction



Antigen scans against the object here in Exchange memory before it is written into the store..

(ESE API) Antigen Real time Scan monitors the ESE "write" and "modify" calls on the object "commit" from either memory or Transaction log.

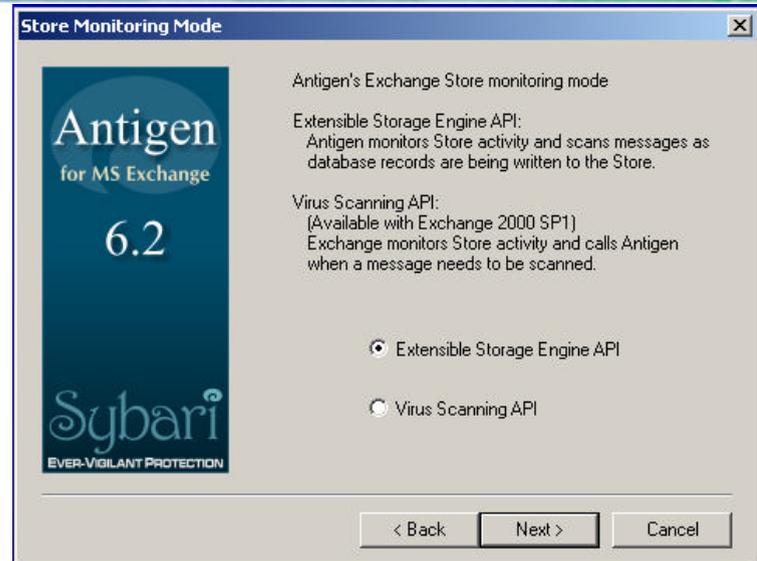
Antigen Manual Scan Uses ESE to scan objects in the store.

VSAPI 2.0

- Microsoft released in July 2001 for Exchange 2000
- Overcomes MAPI and AV API 1.0 limitations
- Sender/Recipient info now available
- Enables scanning of attachments in Web Store (inc. stm or streaming file)
- Enables message body scanning
- Enables “on-access” scanning to allow messages to be stored quickly

Selectable Modes – VSAPI 2.0 and ESE

Installation option



Antutil utility



```
D:\Program Files\Sybari Software\Antigen for Exchange>antutil /mode ese
```

```
-----  
Antigen Admin Utility - v6.20.0834  
1998-2001 - Sybari Software, Inc.
```

```
Successfully switched from USAPI2 mode to classic Antigen shim mode.
```

Install in either mode and switch at any time! 

Selectable Modes – VSAPI 2.0 and ESE

- Admins benefit from no single point of failure
- Key Differences:
 - Scanning location and when messages are scanned
 - Client access and performance
 - Worm Purge
 - Manual and Quick Scans vs. Background scans
 - Manual Scan provides selection of mailboxes, separate scan engine configuration and file filters

Content Filtering

- Antigen File Filtering
- Subject Line Filtering
- Sender/Domain Filtering

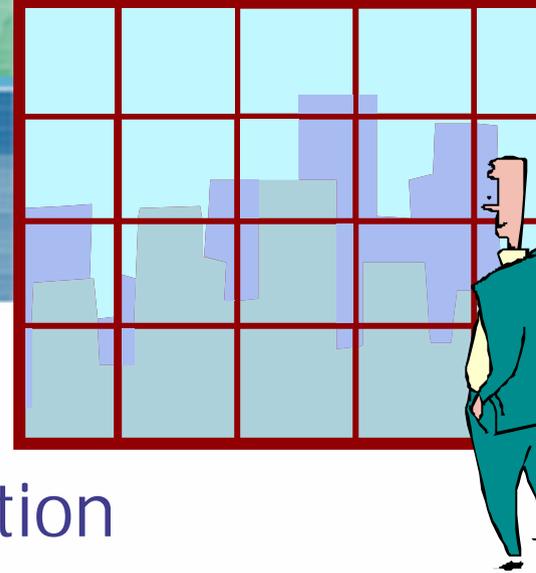


Content Filtering

- Delete and/or Quarantine attachments based on name match, wild card, file type or file extension
- Deleted files can be replaced with a customizable text file or the entire message can be purged
- Ideal for new virus outbreaks before signature files are ready
- Subject line filtering ideal for Virus Hoaxes and email policy management
- Sender/Domain filtering delivers anti-spam and email policy management
- Quarantined documents can be virus scanned and delivered to intended recipient(s) at a later date

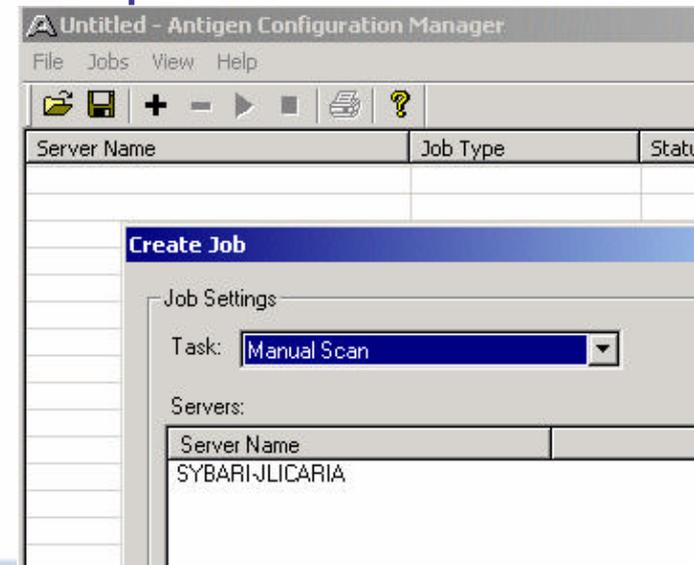
Enterprise Management

- Antigen Central Manager (ACM)
- Remote Installation and Administration
- Automatic Virus Signature Updates
- Virus Incident Reporting
 - Full Event Notification
 - Sender, Receiver(s), Admin List and Others receive customized message(s)
 - Logging to screen, file and NT Event Log
 - Performance Monitor Statistics



Antigen Central Manager

- Central management console
- Update scan engines from central location
- Retrieve log files
- Retrieve virus engine version and update info
- Centrally initiate manual scans
- Install and Uninstall Antigen
- Deploy templates
 - New file filter settings
 - New Configurations



Summary - Benefits

- **A Single** antivirus and security solution for Exchange 2000 and Exchange 5.5 – no service pack restrictions
- **Multiple Scan Engine** support for reliable and comprehensive virus detection
- **Worm Purge** eliminates messages generated due to worm viruses
- **Content Filtering** provides proactive virus protection and policy enablement

Summary - Benefits

- **Real-time** protection of multiple Storage Groups and their databases and full protection of the Exchange 2000 **Web Storage** System
- **Manual scan** protection - scheduled or on demand
- **IMC and SMTP** message protection using Exchange 2000 server transport events
- **Dual-mode support** for VS API 2.0 and ESE technologies

Summary - Benefits

- **Antigen Central Manager (ACM)** for Central Console Management of Enterprise Servers
- **Reliably** scans 100% of messages in Real-time
- **In-memory scanning** results in minimal performance impact
- **MTA Scan Job** provides x.400 scanning
- **Cluster** and Data Center support

Besuchen Sie uns auf der Orbit

Sybari lädt Sie gerne vom 24. bis 27. September auf die
Orbit 2002 nach Basel ein. Sie finden uns am **Stand C22,**
Halle 1.1

Wir hoffen, Sie dort willkommen heißen zu dürfen.

Sybari
EVER-VIGILANT PROTECTION

Antigen

HIGH-PERFORMANCE
GROUPWARE SECURITY

For more info, please see www.sybari.com

Thank You

