

The background is a vibrant green with a gradient. On the right side, there are large, overlapping, semi-transparent shapes in various shades of green, including a large circle and several smaller circles and lines. Faint, large, semi-transparent text is visible in the background, including "Web" at the top, "e-mail" in the middle, and "intranet" at the bottom. The main text is centered and reads "MIMEsweeper™" in a bold, white, sans-serif font.

# MIMEsweeper™

policy-based content security



**MIMEsweeper™**  
policy-based content security

# Agenda

---

- Introduction
- What are the Issues
- WEBSweeper Messaging
- How WEBSweeper Adds Value
- WEBSweeper 4.1 Functionality and Benefits
- WEBSweeper Training and Collateral
- WEBSweeper Q&A





**MIMEsweeper™**  
policy-based content security

# The Need for Content Security

- What is Content Security?
  - Content Security allows organizations to analyze, protect and manage the content of e-mail and other communications over the Internet and intranets in accordance with security policies developed to govern the flow of information within, to and from the organization. Content Security thereby helps organizations protect their network and business integrity.
- What is Policy-Based Content Security?
  - Content Security policies establish e-mail and Web usage rules that define what is considered appropriate and inappropriate e-mail and Web content for individual employees, departments or for the organization as a whole; Content Security policies must be established, communicated and enforced.



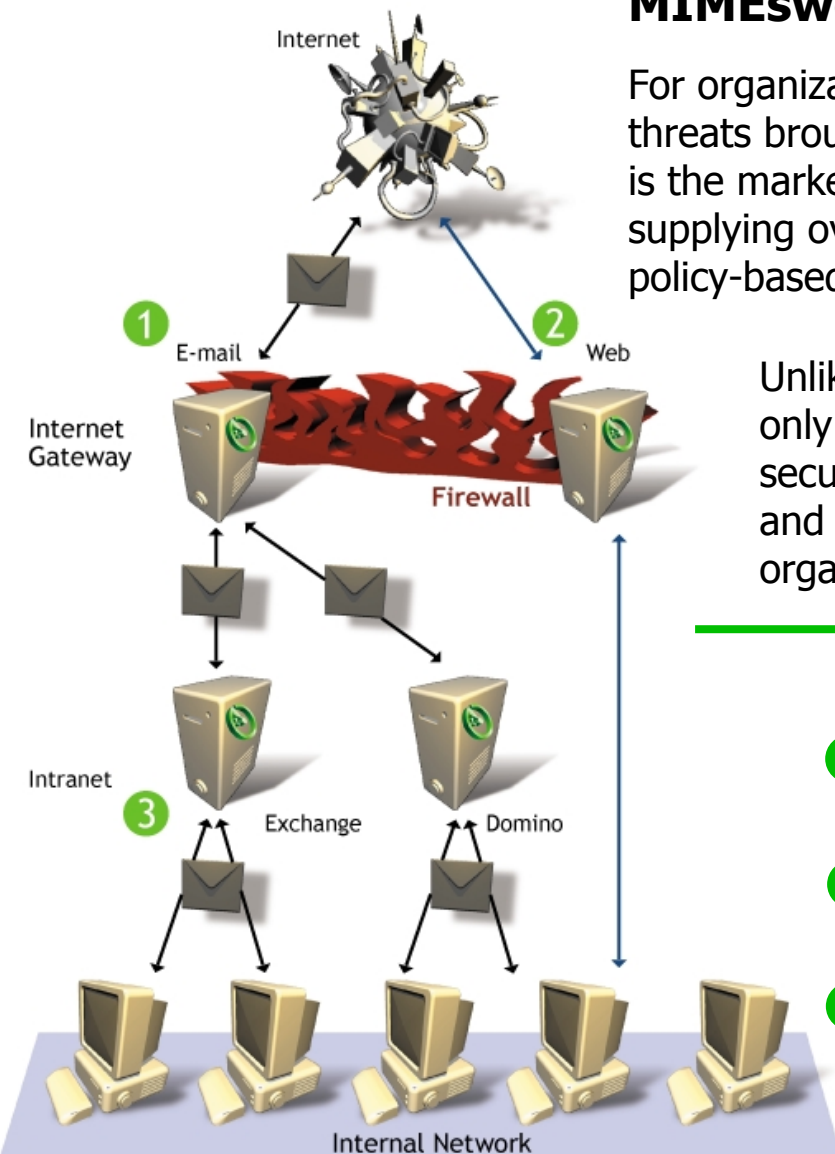
**MIMESweeper™**  
policy-based content security

# The MIMESweeper Family

## MIMESweeper Positioning

For organizations who face both network and business integrity threats brought on by use of both e-mail and the Web, MIMESweeper is the market leading provider of solutions for Content Security, supplying over 10,000 customers and 10 million users worldwide with policy-based Content Security defenses.

Unlike Anti-Virus and URL blocking tools, MIMESweeper is the only Content Security solution enforcing comprehensive security policies on otherwise unsecured internal/external email and Web-based information exchanges within and around your organization.



## How MIMESweeper Provides Total Protection

- 1 Managing Email at the Internet Gateway
  - MAILsweeper for SMTP
- 2 Managing Web Uploads and Downloads
  - **WEBSweeper**
- 3 Manage Internal Email
  - MAILsweeper for Exchange
  - MAILsweeper for Domino



# What are the Issues?

Not protecting against threats contained within Web uploads/downloads, either in Web content or Web-based email, leaves organizations open to the following threats:

- Loss of Confidential Information
  - Theft of data
  - Unintentional or intentional transmission of confidential materials or information outside the organization
- Legal Liability
  - Copyright infringements
  - Damage to reputation
- Employee Productivity
- Network Productivity
  - Degradation or loss of service
  - Data corruption





# Loss of Confidential Information

- Breaches in Confidentiality
  - The Web provides a way around SMTP e-mail security systems, allowing employees to transmit confidential information via online postings or Web-based email accounts (Hotmail, Yahoo! Mail)
- Theft of Data
  - Without the user being aware, downloaded information code can siphon off network data via hidden forms, "mailto" commands and cookies
- From the Press:
  - "A survey of 498 employees working in a variety of organizations revealed that 40% of respondents admitted to receiving confidential information about other companies via the Internet" Network World, 09/10/2001



# Legal Liability

- Legal Liability
  - By downloading copyrighted materials or pirated software, employees can expose the organization to copyright infringement lawsuits.
  - Sexual harassment lawsuits can emerge from the display of inappropriate images
- Damage to reputation
  - Inappropriate link is unintentionally distributed to a broad group
  - Employee lawsuit highlights offensive workplace conduct related to Web use
- From the Press:
  - "Content-filtering companies estimate that 30 to 80 percent of U.S. workers' online time is spent surfing sites not related to business, according to Wright. But limiting a company's legal liability is even more important than limiting surfing not related to work. An employee's browsing of porn sites, for example, could offend a coworker. The cost, in public embarrassment and legal fees, of replacing an offender and fielding harassment suits can be onerous." PC Magazine- 05/10/01



# Network Productivity

- Degradation or Loss of Service
  - Network throughput can be compromised or even suspended entirely as a result of nonwork-related Web surfing, or downloading images, MP3 files, video clips, illegal software, etc.
- Data Corruption
  - Web-borne viruses (like Nimda) can be downloaded in files, spread through contact with infected sites and propagated via Web-based email accounts. In addition, malicious code and executable files can be downloaded, impacting network and business performance
- From the Press:
  - “What's really scary about Nimda is that it uses not one or two, but four different methods to spread--talk about aggressive! Nimda scans the Internet looking for vulnerable IIS servers, which makes it similar to Code Red and Code Blue. It also sends mass e-mail like SirCam and Apost do (in fact, it uses the same attachment, readme.exe, that Apost used). And Nimda looks for open network shares in a way similar to Magistr.B. But what's really menacing is its use of malicious Web-page content. Until now, we've been warned about this kind of malicious code attack, but haven't really seen it used to great advantage.” ZDNet Anchor Desk- 09/19/2001



# Employee Productivity

- Lost Productivity
  - Surfing non-work related sites (sports, finance, pornography, job sites, shopping, banking, etc.)
  - Using Web-based email accounts for personal use
  - Downloading files (MP3s, movie trailers, pornographic images, games, executables)
- From the Press:
  - “Despite the threat of lawsuits, a study from the Society for Human Resource Management found that among companies that monitor employees electrically, less than one-quarter do so to mitigate legal risk. Some 45 percent do it because they suspect employees are slacking” Ziff Davis Smart Business for the New Economy, 09/01/2001



**MIMEsweeper™**  
policy-based content security

# WEBSweeper Messaging

- Protection from Loss of Confidential Information
  - Through enforcement of content security policies, WEBSweeper protects against intentional and unintentional loss of information through monitoring and reporting on inbound and outbound web-based communications.
- Protection from Loss of Productivity
  - Through enforcement of content security policies, WEBSweeper provides protection against lost productivity and network downtime brought on by inappropriate inbound and outbound web-based communications and unproductive Web surfing.
- Protection from Legal Liability
  - Through enforcement of content security policies, WEBSweeper provides protection against the threat of legal liability brought on by inappropriate inbound and outbound web-based communications and Web surfing.

# How WEBSweeper Adds Value to Your Business



**MIMEsweeper™**  
policy-based content security

- Providing your organization with an excellent solution to sell value added services to new customers
  - Security Audits- Help organizations determine where they are vulnerable
  - Policy Consulting- Assist organizations in creating, implementing and managing Web usage and Web email usage policies that protect against threats related to:
    - Loss of confidential information
    - Diminished network productivity
    - Lowered employee productivity
    - Protection from Legal Liability
- Providing your organization with an excellent product to upsell to your existing customer base
- WEBSweeper along with the rest of the MIMEsweeper family provides you with a comprehensive Content Security solution to offer to your customers.





**MIMEsweeper™**  
policy-based content security

# WEBSweeper Functionality

---

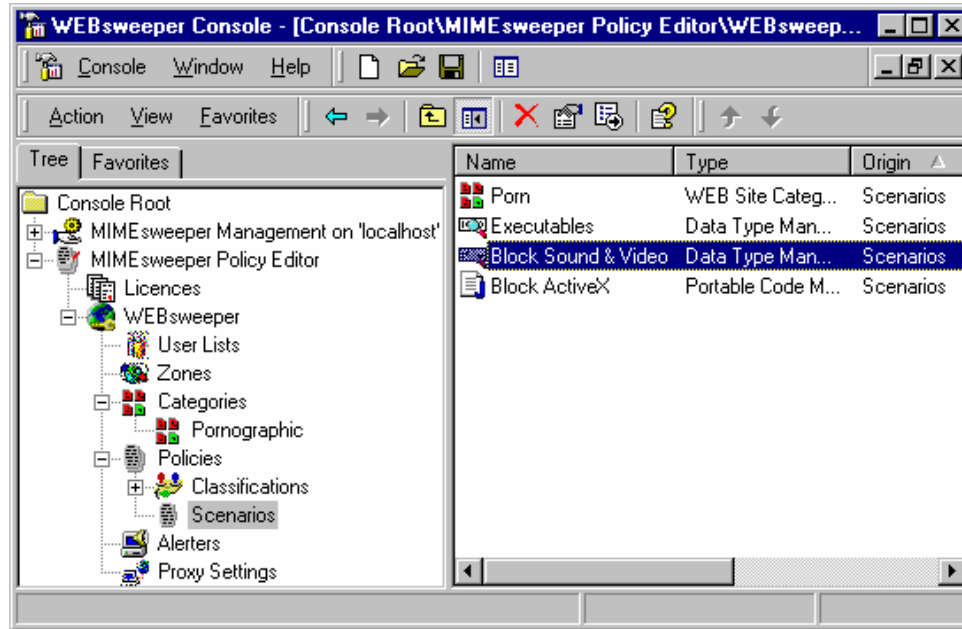
WEBSweeper provides a caching proxy that checks the contents of Web transfers (Web uploads/downloads AND Web-based email- like Hotmail and Yahoo! Mail) based on a company's Web security policies.



# Policy-Based Content Security for the Web



**MIMEsweeper™**  
policy-based content security

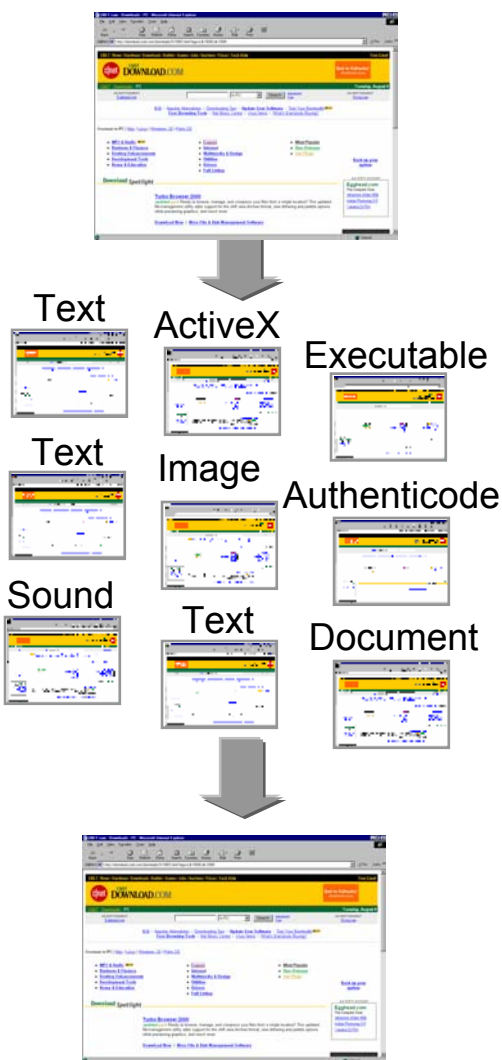


- WEBSweeper gives organizations a way to take control of the flow of Web content into and out of their organization
  - WEBSweeper's Policy Editor allows organizations to define and manage security policies for Web usage
  - Policies can be applied to different groups and users, depending on their roles and responsibilities within the organization

- WEBSweeper allows for time-specific policies, allowing for flexibility when policies are applied to groups and users (e.g. allowing users to browse non-work Web sites during non-work hours or lunch time)
- Policies are arranged in a hierarchical structure, so that employees at lower levels of the organization can inherit the policies specified at higher levels



# How WEBSweeper Works



- Step 1: User initiates a Web transfer
  - WEBSweeper authenticates the user and applies the user's Internet access privileges according to the security policy
  - WEBSweeper integrates with existing LDAP, Windows or text-based user directories
- Step 2: Content Disassembly
  - WEBSweeper breaks the Web transfer down into individual objects
  - WEBSweeper identifies files by its file architecture, not just by file extension
- Step 3: Content Analysis
  - Each object is then scanned according to policy as it applies to the user who is sending or receiving the transmission
- Step 4: Classification
  - WEBSweeper implements the policy by letting the content pass, cleaning and recomposing infected content, or blocking the transmission



# WEBSweeper Content Analysis

- **WEBSweeper Categories:**
  - Administrators can block access to categorized pages or restrict access to certain times of the day
  - A combination of text analysis, PICS rating and URL lists can be used to scan Web content to determine category match
  - New in WEBSweeper 4.1 is the option to subscribe to a separately maintained URL list
- **WEBSweeper Scenarios:**
  - Virus Manager Scenario: Run virus-checking software on downloaded files to detect and possibly clean infected data
  - Data Type Scenario: Block executables, MP3s or other file types
  - Data Type Scenario: Block large downloads, or provide configurable progress status messages during their transfer
  - HTML Manager Scenario: Recognize and remove Internet shortcuts, automatic mailtos, and HTML scripts (JavaScript and VBScript)





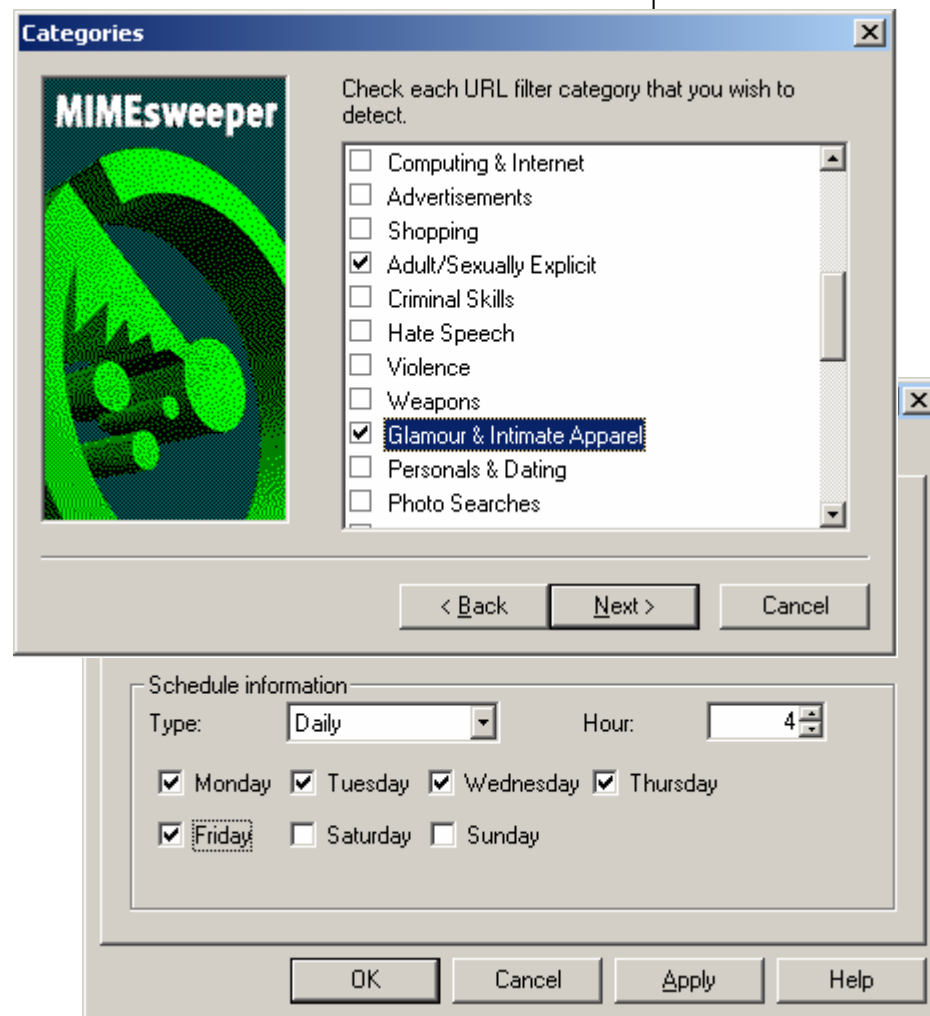
# WEBSweeper Content Analysis

- WEBSweeper Scenarios (continued):
  - Portable Code Manager Scenario: Recognize block and/or remove ActiveX components, Java scripts/VB scripts and Java programs
  - Pattern Matcher Scenario: Identify files types by defined byte sequence
  - File Blocker Scenario: Block files by file name and file extension
  - Authenticode Manager Scenario: Check the authenticity of digitally signed data
  - Cookie Manager Scenario: Recognize and remove Web cookies found in HTTP data and headers
  - Text Analyzer Scenario: Detect text phrases or words in Web transfers



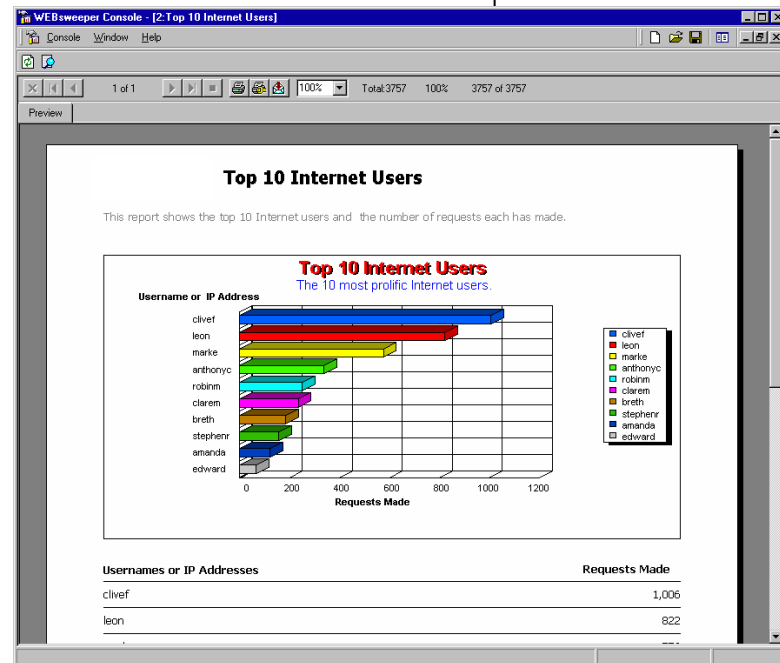
# New in 4.1: URL Filter Category

- 40 clearly defined categories
- References to more than 689 million Web pages
- Approximately 2.4 million domains covered
- International content, 14 languages represented
- Maintained by 40+ professional researchers, automated tools, and relevant customer submissions
- Automatic daily updates to WEBSweeper
- More than 15,000 updates a week
- Constant culling and aging



# Administrative and Reporting Capabilities

- Auditing and Graphical Reporting Capabilities
  - Generate standard or custom built graphical reports based on accumulated WEBSweeper data (such as reports on most intensive system users, sites visited and threats detected)
  - Integrates with SQL server back end
- Intuitive User Interface and MMC Integration
  - WEBSweeper UI plugs right into Microsoft Management Console
- Real-time monitoring
  - Provide up-to-the-minute management statistics, such as recently accessed sites, connected clients etc
- Security Alerts
  - Security events can be configured to trigger administrator alerts via e-mail





# Requirements

- PIII 800 MHz or higher
- At least 512 MB RAM
- 2 GB Hard disk on an NTFS-formatted partition for WEBSweeper
- Operating System (Windows 2000 Support new in 4.1)
  - Windows 2000 Professional Version 5.0 w/ Service Pack 1
  - Windows 2000 Server Version 5.0 w/ Service Pack 1
  - Windows NT Workstation Version 4.0 with Service Pack 5 or 6a
  - Windows NT Server Version 4.0 with Service Pack 5 or 6a
- Microsoft Management Console 1.2\*
- Internet Explorer 5.0 with Service Pack 1\*
- Microsoft Data Access Components\*
- Microsoft Outlook 98
- User's choice of anti-virus tools, DDL recommended for performance
- TCP/IP Networking

\*Included on WEBSweeper product CD



# Performance Summary

- WEBSweeper performance is highly variable and difficult to predict
- Best performance is realized with WEBSweeper on fast dual-processor Windows 2000 machine(s)
- General guidelines are 500-1000 users per WEBSweeper server
  - Based on an estimate of 10% concurrency
  - 50-100 users concurrently uploading/downloading information at exactly the same time