Feature (Filtering)	Benefit
Dynamic Content Analysis™	Screens the content, context and construction of web pages in detail, accurately detecting and blocking all objectionable, inappropriate, hidden or malicious content (including anonymous proxies).
SSL (secure) proxy blocking	Blocks HTTPS proxies, UltraSurf and VTunnel, whilst allowing legitimate HTTPS traffic.
Customizable URL Blocklists	Current and categorized URL blocklists (updated daily with the latest content from the IWF database) control access to a pre-defined list of undesirable websites. Blocklists can be customized and include a reverse-lookup option to block users attempting to access sites using IP addresses instead of domain names.
Whitelist mode	Users can only access a customized list of 'allowed' sites
Temporary 'Banner User' list	Ban selected users until a selected date or time.
MIME, File extension, download size, advert, cookie & PICS blocking	Filtering policies can be set to detect PICS codes, file types, download sizes, adverts and cookies; and block such content as required. PICS codes indicate the nature and severity of the website content and MIME type checking helps to stop the downloading of viruses and other malicious code from websites, as well as music and other copyright material.
Policy based controls	Different filtering policies can be set for different groups of users, in accordance with organization policy or the AUP. Policies are created from sets of customizable filter objects.
Time and room based controls	Filtering can be set at different levels for different times of the day (enables filtering to be relaxed outside of core hours) and for different rooms or deparments, defined by IP or computer names
Logging, Filtering and Censoring of Instant Messenger applications	Control and monitor the use of Instant Messaging applications such as MSN, Yahoo, AOL and ICQ. IM file transfers and attachments can be logged or blocked and selected words or phrases can be censored and set to trigger alerts.
Deep URL searching	Selectively block the results of a Google image search if the images found are from a domain that is configured to be blocked.
Force SafeSearch	Enforce safe search usage on popular search engines
Temporary bypass controls	Flexible and user-friendly filtering is provided with options to bypass the filter on a temporary basis for individual users.
Configurable 'Site Blocked' page	Allows administrators to customize the 'site blocked' page to include a logo, message text, a reason for blocking and bypass controls (un-block buttons) alongside the IP address and name of the user.
'Softblock' option	Instead of automatically blocking inappropriate content, users are issued warning messages about content and given options to either continue or cancel.
Stealth mode	Web pages are filtered and logged as normal, but are not actually blocked, allowing administrators to monitor if people are visiting 'bad' sites and downloading dangerous files without affecting the user in any way. This feature is particularly useful when testing a new installation as it allows the filtering rules to be fine-tuned before 'going live'.
Flexible request and content modification	Modify web page requests and content 'on the fly' to enable neutralization of malicious JavaScript.
Anti-Virus Scanning	Automatically scan web content for viruses, using either built-in ClamAV scanning, or offload to an external server via the ICAP protocol.
Web proxy Cache	Reduce bandwidth utilization by storing and retrieving frequently accessed web pages from local disk storage.
Default 'safe' configuration	Guardian can be installed with a default 'safe' configuration which filters out a standard range of illegal and objectionable content that most organizations would want to block. Note: Guardian's default 'safe' configuration matches the requirements of CIPA and BECTA filtering tests.

Feature (Authentication)	Benefit
Integrates with User Authentication systems including, AD, Novell etc	Control access based on authenticated identity as opposed to assumed identity derived from a computer's IP address.
Multiple filter groups	Different filter policies can be allocated to different groups of users. Particular users can also be configured to not be subject to any filtering at all.
Transparent proxy mode	System administration is simplified with support for NTLM authentication in transparent proxy mode; which avoids the need to configure proxy settings for each user computer.
Password-protected authentication	The use of NTLM with password verification provides seamless single sign-on without the need for users to log into Guardian or enter their ID/password again.
Ident integration	Ident (Windows User Identification) can be enforced so that any user that has not been identified from Ident information (ie their PC is not running an Ident client) will be not be allowed to browse the web.

Feature (Reporting)	Benefit
Built-in report templates	Users can create, customize and save their own report templates and utilize an extensive range of standard reports, including 'most visited domains', bandwidth utilization by user and the worst offending users (in terms of requesting pages that were blocked by Guardian). Report options include URL-specific reports (e.g. YouTube top viewed videos) and IM reporting (time spent messaging and chat friends per user).
Drill down to a single user or IP	Reports include the user name and IP address of the user PC so AUP violators can be quickly identified. A drill-down facility allows data to be explored to a greater depth - e.g., from a list of blocked sites that users have attempted to access, drill-down to find out which users have been trying to access any particular site. It is possible to view the entire browsing history of a single user.
Automated reports	User-specific reports can be automatically time-scheduled to run on a daily or weekly basis. Reports can also be automatically saved or distributed to recipient lists via email.
AJAX real-time logs & traffic graphs	View web activity instantaneously, with the option to filter by user name, IP address or web site.
Export into PDF, HTML, Excel, Crystal Reports®	Reports can be produced in a range of formats for ease of viewing (with pie charts/graphs) and to aid integration with existing systems.
Reports via domains or categories	Report on top domains, categories, page visits and offenders based on user, group and/or IP address
Group/aggregate reports	Automatic data aggregation from multiple remote systems provides district wide reporting.
Incident Alerts	Alert messages can be sent by both email and SMS text message to cell (mobile) phones for issues requiring immediate attention.

Feature (Operation)	Benefit
Non-English ASCII character support	Allows non-English characters (i.e. those with accents etc) to be entered.
Rate limiter and QoS by URL	The speed or rate at which the proxy server can download information from the Internet can be limited. Bandwidth use can also be limited for specific URLs (e.g. YouTube)
Support for browser autoconfiguration files	Provides WPAD (Windows Proxy Auto-Detection) and PAC file support, for automatic configuration of proxy settings in client browsers.
Hardware healthcare alerts	Notifications about system resource issues (eg low disk space, high memory use, high CPU loads, UPS failures) and network intrusions or violations.
VMWare support	Full VMWare compatibility (including network drivers) so multiple instances of Guardian can be installed on 'virtual machines'
Hardware and Software RAID	RAID1 mirrored support for SCSI, SAS, SATA or IDE disks.