



# Secure Internet Gateway

Mobile Security, Advanced Malware Protection,  
Web Filtering and Integrated Reporting

## KEY FEATURES:

- Multi-Layered Malware Defense
- Advanced Threat Prevention
- BYOD Management
- SSL Traffic Management
- Web Activity Reporting / Alerting
- Scalability / Reliability

## MAIN BENEFITS:

- Multi-Layered Web Security
- Centralized Management
- Lower TCO
- Policy Compliance
- Reduced Legal Risk
- Forensic Security Awareness

## Multi-Layered Web Security for Today's Organization

ContentKeeper's Secure Internet Gateway provides multi-layered web security for today's distributed, cloud-based organization by combining web filtering, anti-malware and reporting technologies into one cohesive solution. Its dynamic malware analysis and advanced threat prevention technologies protect devices and systems, regardless of location, against web-borne and targeted threats. It seamlessly integrates the following features:

- Mobile device web access control, identification and accountability
- Real-time, high speed SSL inspection, filtering and controls
- Anti-malware predictive file analysis, behavioral analysis and cloud sandboxing
- Granular policy-based domain and social media controls
- Real-time web content classification
- Comprehensive analysis, monitoring and reporting

## Advanced Threat Prevention

ContentKeeper's Secure Internet Gateway is a multi-layered anti-malware and malicious web threat security system. It combines multiple layers of advanced malware identification technologies to provide protection against malware and advanced persistent threats including:

**Streaming Malware Defense** – high performance signature-based anti-virus with fast, real-time packet inspection. SMD identifies known viruses and spyware.

**Predictive Malware Blocking (powered by Cylance)** – uses artificial Intelligence and machine learning to predict, identify and prevent unknown and advanced malware attacks.

**Behavioral Analysis Engine** – isolated virtual browser attack evaluation environment. Automatically tests unknown Web files, intelligently assesses the behavior of JavaScript (including obfuscation) and unpacks PDF files looking for any signs of malicious activity.

**Cloud Sandbox** – a virtualized test computer environment where suspicious samples are executed and analyzed for any signs of malicious behavior. CSB analyses files that pass the previous layers of anti-malware inspection.

## Intelligent SSL Inspection and Controls

ContentKeeper's Secure Internet Gateway helps organizations manage the rapid growth of SSL traffic on their networks. Intelligent management of SSL traffic is essential in ensuring policy compliance and preventing malware attacks. ContentKeeper provides high speed SSL decryption and inspection enabling organizations to protect, filter and control encrypted web traffic without impacting network performance. Selective decryption ensures proper domain management and logging and reporting at multi-gigabit speeds.

# ContentKeeper Secure Internet Gateway

**FREE 30 DAY  
EVALUATION**  
Register at  
ContentKeeper.com

## Web Filtering

ContentKeeper's Secure Internet Gateway helps ensure policy compliance and enable a safe and productive mobile workforce. Organizations can effectively monitor employee Internet use and protect users from inappropriate or harmful content via a comprehensive website category database, dynamic web content classification and granular domain, social media and application controls. Intelligent SSL inspection allows in-depth visibility into secure web traffic for effective policy management and additional malware protection at multi-gigabit speeds.

## Comprehensive Centralized Reporting

ContentKeeper's Secure Internet Gateway provides comprehensive enterprise-class reporting for web traffic, user activity, policy compliance and malware threats. Management friendly real-time dashboards and summary and forensic drilldown reports are provided as well as roles-based reporting access, scheduled report generation and automated email delivery or HTML publishing. Real-time, online threat monitoring and alerts help prevent potential individual or organization-wide threats such as bullying, shootings or other malicious plans.

Key Features	Technical Description	Key Benefits
Web Filtering	High performance real-time web content inspection. Heuristic, dynamic web content classification. Collaborative global feedback network. Custom URL categories.	Prevent exposure of harmful content to workers. Maintain safe working environment. Acceptable Use Policy monitoring & enforcement.
Granular Application / Social Networking Controls	Policy-based access permissions. Application sub-function controls for Google, YouTube, Facebook, Twitter and more.	Control Web 2.0 applications & their specific functions. Safeguard privacy & reduce excessive time-wasting or bandwidth consumption.
Anti-Virus / Malware Protection	Proactive malware prevention. Predictive file analysis. Advanced proactive threat analysis sandbox. Isolated threat identification. Active exploit, script detection. Signature-based anti-virus/spyware detection. Forensic malware reporting.	Robust protection against known & new zero-day threats. Confidence & peace of mind that users can browse the web securely on any device in any location.
Keyword Detection / Search Controls	Define prohibited custom words & phrases for search engines. Detect & block profanity or threatening language in Facebook chat, Twitter comments, blogs. Detect keywords embedded in documents or files.	Block inappropriate web searches. Take action against inappropriate behavior and harassment.
Data Protection / File Controls	Restrict files by type & size. Policy-based blocking and control. ICAP compatible interface for integration with major 3 <sup>rd</sup> party DLP, AV, IPS, Sandboxing and other systems.	Instantly block access to inappropriate downloads. Preserve bandwidth. Help safeguard confidential documents.
Advanced Reporting & Alerts	Web-based multi-tenancy, multi-user enterprise level reporting. Real-time dashboard, summary & drilldown detail reports. Scheduled reporting & automatic email distribution/publishing. Roles-based access permissions for IT staff & departmental managers.	Monitor policy compliance. Gain meaningful insight into user web activity & security events. Enable key personnel to oversee their area of responsibility & empower managers with valuable information to ensure policy compliance & curb inappropriate behavior. Scalable to support large multi-gigabit network sites.
SSL Decryption, Inspection, Controls / Certificate Validation	Full de-coding & filtering of encrypted web traffic. Policy enforcement of SSL credentials. Full and/or selective decryption. Protect, log and report on SSL web activity at multi-gigabit speeds. No client software required.	Full scanning of all web traffic, including HTTPS. Ensures policy compliance. Detection of potentially malicious websites (e.g. Phishing). Control and filter secure web traffic without degrading network performance.
Roles-Based Administration & Reporting	Role-based access permissions. Hierarchical policies across multiple offices or domains. Delegated areas of responsibility, local policy ownership. Full configuration & administration auditing.	Establish high-level & local policy settings. Delegate responsibilities to local IT administrators but maintain oversight & control of large scale environments. Complete flexibility to conform to your IT organizational structure.
Maintenance	Automated updates & upgrades.	Worry-free administration. Save time & energy. Always up-to-date with latest security & web content classifications.
Directory Integration / Username Resolution	Automated synchronization with user authentication directories such as Active Directory, LDAP, Google, Open Directory, SAML, OAUTH. Transparent and end-user client free.	Automatically maintain accurate user identification & policy control. Minimal maintenance & administration.
BYOD / Mobile Device Security	Support for iOS/OS X, Windows, Chrome & Android devices. Laptops, tablets, iPads & Smartphone devices. Seamless device registration, authentication and accountability.	Enable mobility & flexible working environments. Safely & efficiently support large scale rollouts of devices & utilize the latest technology & hardware as it becomes available.
Cloud / Appliance / Virtual Server Deployments	A range of gateway deployment options are available including a cloud or hybrid cloud-based Secure Internet Gateway platform based on your requirements.	Choose your preferred IT deployment architecture to best fit your environment & apply web security to all your users everywhere.
Physical In-Line Layer 2 Ethernet Bridge	All Internet traffic passes through the bridge. Supports migration to multi-gigabit filtering. Full native support for IPv6.	High scalability & availability. Most robust security available today. Future-proof Internet security. Ready for IPv6 & future requirements to scan beyond standard web traffic.



ContentKeeper.com



info@ContentKeeper.com



US: +1 888.808.6848  
Intl: +61 2 6261 4950

Copyright © 2016 ContentKeeper Technologies. All rights reserved. ContentKeeper is protected by U.S. and international copyright and intellectual property laws. ContentKeeper is a registered trademark of ContentKeeper Technologies in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.