



Streaming Malware Defense

High Speed Bridge Based Anti-Virus Gateway

KEY FEATURES:

- Multiple Signatures Scanning
- Bi-Directional Real-Time Scanning
- Ransomware Protection
- Threat Isolation
- Web Threat Reporting
- Ultra-High Performance Design

MAIN BENEFITS:

- Web Threat Protection
- Centralized Management
- Multi-Layered Mobile Security
- Increased Productivity
- Scalability / Reliability
- Forensic Security Awareness

Eliminate Proxy Based Anti-Virus Bottlenecks

ContentKeeper Streaming Malware Defense (CK-SMD) combines the power of BitDefender and Kaspersky's streaming malware intelligence feeds with ContentKeeper's high speed, bridge based scanning and malware defense systems.

Overview

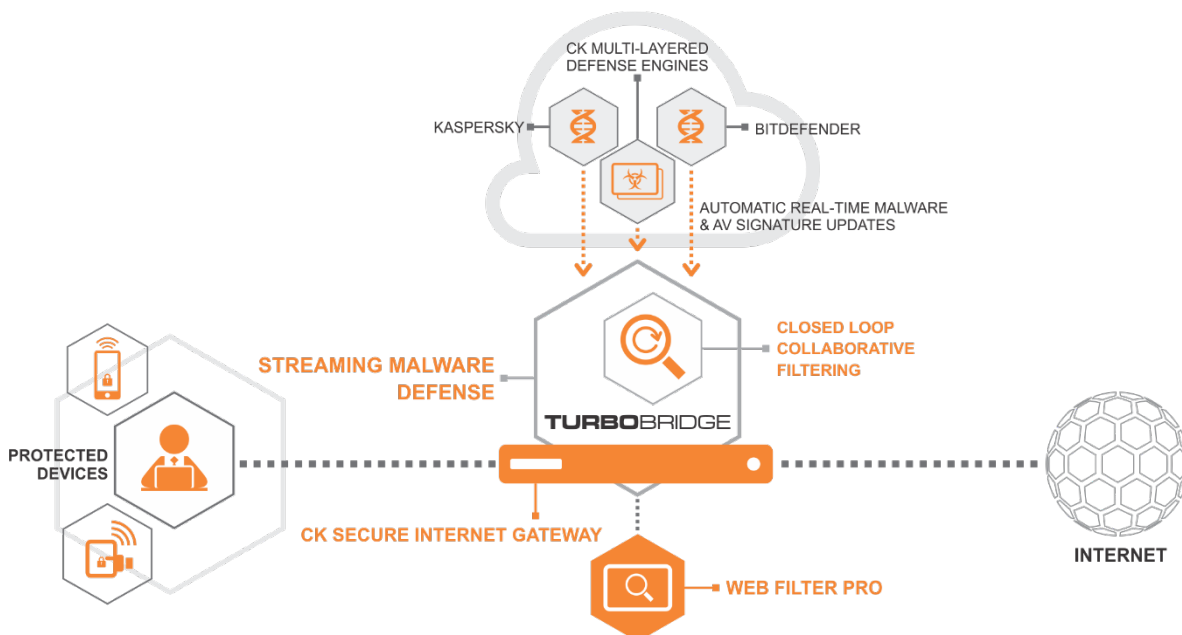
Traditional Anti-Virus gateways are based on slower proxy based technology where the file or object to be scanned must be spooled in RAM or to disk before any scanning can start. These types of systems must wait for the last packet containing the end of file marker to be received before scanning can begin. This causes delays and network bottlenecks as users browse the web, negatively impacting productivity.

Why Use ContentKeeper Streaming Malware Defense?

ContentKeeper Streaming Malware Defense is based on ContentKeeper's high speed TurboBridge technology. It utilizes a different set of signatures strings designed to scan data in motion as it flows through the bridge at near wire speed. This real-time approach eliminates Anti-Virus gateway bottlenecks along with end user delays, allowing for greater user satisfaction and major productivity gains.

Signature strings are automatically updated from Kaspersky and BitDefender in near real-time as part of ContentKeeper's patented Closed Loop Collaborative Filtering™ system. Other threats detected by any of ContentKeeper's other multi-layered defense engines are also retrieved and added to the system.

The Streaming Malware Defense is included with the ContentKeeper Secure Internet Gateway and is an add-on module with ContentKeeper's Web Filter Pro. In addition, it is designed to run alongside ContentKeeper's Malware Defense modules.



ContentKeeper Web Security & Web Filtering for Desktop and Mobile Devices



Web Security

- Multi-layered advanced threat defense
- Predictive Malware Blocking (powered by Cylance)
- Behavioral and sandboxing analysis
- Forensic malware analysis and reporting
- Block zero-day malware & vulnerability exploits
- Streaming Anti-Virus



Mobile Device Identification and Control

- Identify and control individual mobile devices
- Block unknown and/or unwanted devices
- Identify device type, manufacturer, version, browser utilized, operating system and more



Device Agnostic

- BYOD support (no client software required)
- Mobile device web access control & accountability
- Seamless integration with Directory Services for accurate identification and reporting



Comprehensive Centralized Reporting

- Real-time monitoring and historical reporting
- Consistent user reports across devices
- Delegated administration



Granular Application / Social Media Controls

- Policy based access controls
- Application sub-function controls
- Facebook, Twitter, Google, YouTube and more
- Time-of-day and bandwidth quotas



DLP / Document Content Scanning

- Flag confidential files
- Restrict file downloads and uploads
- Manage authorized user access
- Prevent privacy breach



SSL / HTTPS

- High speed HTTPS filtering
- SSL certificate security
- High speed full and/or selective decryption
- Ensure policy compliance
- Close malicious backdoors
- Protect, log and report on SSL web activity at multi-gigabit speeds



Web Filtering

- High performance real-time web content inspection
- Layer 2 Ethernet Bridge
- Closed Loop Collaborative Filtering™ network
- TurboBridge technology supports migration to multi-gigabit filtering

