

# Content Security Gateway™ Series

*Real-time Gateway Web Security Against Spyware and Viruses*

## 1. Why do I need a Web security or gateway anti-spyware solution?

Malware attack vector is rapidly shifting from email to the Web. The widespread use of the Internet and the increasing number of security vulnerabilities in Web browsers and Web applications have contributed to this shift. While most enterprises have already fortified their networks against email-borne threats, the Web vector is usually left undefended against malware attacks. According to InfoWorld and IDC, the Web is expected to be a growing source for malware attacks over the next decade<sup>1</sup>.

Of today's Web-borne threats, spyware is the most dangerous<sup>2</sup> – because it installs easily and secretly from spyware hosting Web sites and is very hard to detect and remove. Spyware attacks are usually financially motivated – once installed on client computers, they can steal sensitive corporate information (financial data, trade secrets, and account information) and send data back to spyware hosts on the Internet.

The complex nature of malware threats (especially spyware) and the potential damage they can cause to enterprises highlight the need for a Web security solution that can stop them at the gateway – before they enter the network.

## 2. What does Content Security Gateway (CSG) appliance offer?

CSG protects organizations from today's malware threats by preventing spyware and viruses in Web and email traffic from entering the network. Its key features include:

- **Real-time Web Scanning** – CSG's patent-pending stream-based scanning technology enables anti-malware scanning of real-time protocols such as HTTP and HTTPS. Network activities sensitive to latency (for example, Web browsing) are no longer brought to a standstill.
- **Comprehensive Protection** – CSG uses dual scan engines from CP Secure (ICSA Labs-certified for gateway AV detection) and Kaspersky to ensure the most complete and reliable malware coverage. Utilizes both signature-based and heuristic detection to stop known and unknown malware. Signature library includes all known spyware and viruses. Six major network protocols are covered: HTTP, HTTPS, SMTP, POP3, IMAP, and FTP.
- **Automatic Signature Updates** – To ensure up-to-date protection against new malware threats, CP Secure releases updates to malware signatures on an *hourly basis*. Critical new signatures are typically deployed within two hours of a new threat - several hours before they are available from leading antivirus vendors.
- **True Appliance** - Deploys in-line in a matter of minutes, anywhere in the network. Runs automatically and unobtrusively. Simply set and forget.
- **Powerful Management Capabilities** - Secure and intuitive Web-based administration console. Set granular policies and alerts, check summary statistics and graphical reports, drill down to IP address-level data, and integrate log data with standard network management tools.

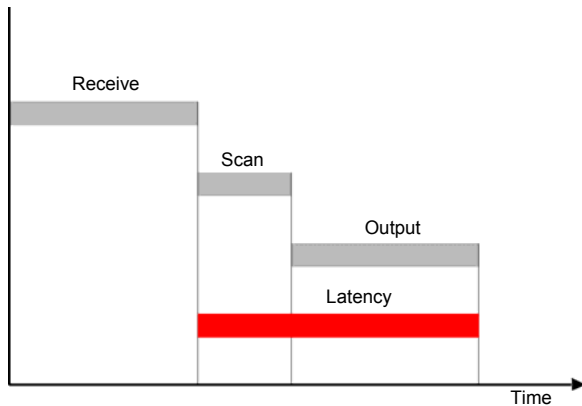
<sup>1</sup> InfoWorld Security Research Report, September 2005; and "Spyware and Other Web-Based Malware: The New Security Threat and Its New Solution", IDC Executive Brief, February 2006.

<sup>2</sup> "[S]pyware has rapidly climbed the priority list of enterprise security threats and now ranks as the second most serious threat facing corporations today." "Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc", IDC, September 2005.

### 3. What is stream-based scanning?

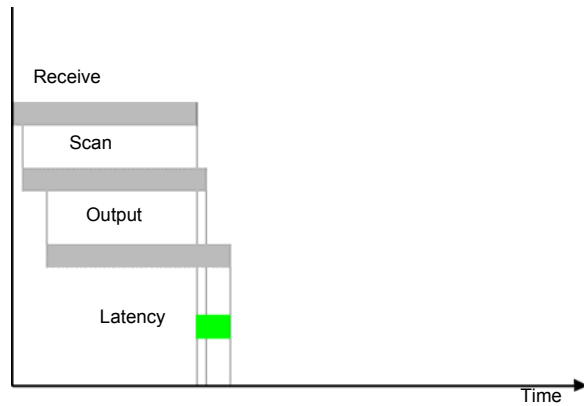
Stream-based scanning is unique, patent-pending technology from CP Secure that enables real-time scanning of Web and email traffic for malware. The anti-malware engine scans streams of Internet traffic, concurrently receiving, scanning, and outputting the traffic, to ensure that network performance is not degraded. The result is that Internet traffic is scanned in real-time, with high throughput, low latency, and a high number of concurrent connections. This is a performance advantage that is easily noticeable to the end-user.

#### Batch-based Scanning



Basic unit scanned: File  
 Processing: Serial  
 Result: Substantial latency, limited throughput, limited scalability

#### Stream-based Scanning



Basic unit scanned: Small, simple internet streams  
 Processing: Parallel  
 Result: Low latency, high throughput, high scalability

Other gateway scanning products use standard batch-based scanning technology, which takes the file as the basic unit for scanning and uses serial processing. Batch-based technology commences scanning only after an entire file is received and starts outputting only after the entire file has been scanned. End-users often experience long delays or sometimes even timeouts while the file is transferred and scanned. When applied to the new malware threats in real-time Web traffic, the traditional scanning approach introduces unacceptable levels of latency that bring enterprise Web activities to a standstill. To defend the real-time Web vector against attack from today's sophisticated malware, high performance anti-malware scanning is no longer optional – it is absolutely required.

CP Secure's stream-based scanning technology takes small, simple internet streams as the basic unit for scanning and uses parallel processing to enable real-time scanning. As the internet stream passes through the gateway, the stream-based architecture concurrently receives, scans, and outputs the data stream, resulting in minimal latency. Because the technology scans small, simple internet streams, it is able to use system resources efficiently, which enables high throughput and a high number of concurrent connections. Stream-based therefore makes real-time scanning feasible by generating high throughput, low latency, and a high number of concurrent connections.

#### 4. Don't other vendors provide real-time, stream-based scanning?

No, they don't. CP Secure invented real-time, stream-based scanning and is the only company that uses this technology in its products. The technology is a major departure from today's standard gateway batch-based scanning, and is therefore in the process of being patented as a major innovation.

Some vendors use phrases such as "stream scanning" or "deep packet inspection" to draw attention to their products. Note that these claimed technologies are neither patented nor patent-pending as major innovations. In competitive customer situations, the performance of their products falls short of the performance achieved by our stream-based scanning technology. Other vendors have used technologies such as Web caching and improved hardware in attempts to overcome the basic performance shortcomings of batch-based scanning, but these have all been incremental changes to the batch-based scanning approach.

#### 5. Whose scan engine do you use?

CSG uses two scan engines – our own scan engine and Kaspersky Lab's – to provide the most comprehensive and reliable protection against known and unknown malware. The CSG's dual scan engine architecture reassures customers that they are stopping the latest-breaking spyware and viruses. CP Secure's proprietary scan engine is one of only nine gateway scan engines certified by ICSA Labs to detect 100% of all currently active viruses and other malware. Kaspersky's scan engine is widely recognized in the industry, and confirmed by extensive third party tests, as having the highest detection rates for known and unknown spyware and viruses. The dual scan engines utilize the most complete signature library available, heuristic scanning, and false alarm detection, ensuring that both known and unknown malware are detected reliably.

CP Secure's and Kaspersky's global malware research organizations complement each other to cover all known malware. The result is that the CSG receives malware pattern updates every hour and new threats are addressed within two hours, by far the most timely malware support of any anti-virus or anti-spyware vendor. And while other security vendors charge for an additional scan engine, the Kaspersky scan engine is included with CSG at no extra charge. You get an extra layer of protection without having to pay extra.

#### 6. How big is your signature library?

The CSG's signature database includes more than 200,000 malware signatures, including over 100,000 spyware signatures. One of the most comprehensive in the security industry, this sizable database enables CSG to detect all known classes and sub-classes of malware. Spyware classes that it covers, for example, include:

- Keyloggers
- Root kits
- Browser hijacks
- Fraudulent dialers
- Trojan horses
- Backdoors
- Hacker tools
- Password tools

- Joke programs
- Adware

## 7. How often is your signature library updated?

CP Secure releases updates to the malware signature library on an *hourly basis* to ensure up-to-date protection against new threats and variants of old threats. You can verify this by checking the system logs.

## 8. Are updates automated?

Yes, CSG automatically downloads and installs any available update that CP Secure may post to its Update Server. CSG can be configured to check the CP Secure Update Server for updates as frequently as *every 15 minutes*.

To ensure fast updates, CSG performs incremental updates of the pattern file. Instead of downloading the entire pattern file every time it updates, CSG only grabs new patterns or signatures that have been added since the last update. This mechanism saves network bandwidth and, more importantly, lets CSG get up-to-date protection in the shortest time possible.

## 9. Is CSG a proxy appliance?

No, CSG is an inline, transparent bridge, which means it does not require network reconfiguration and may be deployed easily in a matter of minutes. This ease of deployment enables customers to simply “drop in” CSG as part of their existing layered defense.

## 10. Is it easy to migrate to CSG?

Migrating from a third-party security appliance is very straightforward. If you are migrating from a network appliance that works in proxy mode, all you need to do is remove the proxy settings in the clients’ browser settings. If your network is using Active Directory, this can be done easily either by using group policy or scripting.

If you are migrating from another appliance that works in transparent bridge mode, just put CSG in its place and you’re all set. Since it works in transparent mode, CSG can be migrated inline without requiring changes to other network configurations such as default gateways.

## 11. What high availability features does CSG provide?

CSG provides four high availability features – RAID, redundant power supply, fail-over, and fail-open – that help guarantee network (and business) continuity and ensure continuous protection against malware.

- RAID – Provides fault tolerance to preserve CSG components and settings in case of a hard disk failure and helps improve access throughput levels.

- Redundant power supply – Provides a backup power unit in case the primary power unit fails.
- Fail-open – Ensures that traffic will continue to pass through the appliance in the event of a hardware failure.
- Fail-over – Multiple CSG appliances can be installed and configured in a failover deployment to ensure uninterrupted scanning of network traffic.

For information on the high availability features available in each CSG model, see the table below.

CSG Model	2500	1500	1000+	300	110
RAID	•				
Redundant Power Supply	•	•			
Fail-open	•	•	•		
Fail-over	•	•	•	•	

## 12. What’s the purpose of the fail-over unit in the price list?

A fail-over unit is a second CSG appliance that you can purchase at a discounted price if you want to add fail-over capability to your CSG deployment. In a fail-over deployment, one CSG acts as the primary appliance (active) and the other as backup (passive). When the primary CSG appliance encounters system or hardware issues, the secondary CSG appliance kicks in and takes over scanning network traffic for malware. Adding fail-over capability to your CSG deployment ensures that the network stays protected in case the primary CSG appliance ceases to function due to system or hardware issues.

## 13. What is the renewal model?

The annual renewal price for CSG is 30% of the product price. CP Secure offers discounts to customers who want to purchase multiple years of support upfront. See the CSG price list for more information.

## 14. What’s your support system like? How do I obtain technical support if I run into a problem?

Responsive, 24/7 technical support is one the key differentiators that put CP Secure ahead of the competition. As a CP Secure customer, you can obtain support in two ways:

- **Live phone support** – Call our technical support hotline anytime and get answers on the spot from our knowledgeable support specialists. No forms to fill out, no automated answering systems, no running around.
- **Virtual onsite support** – A built-in support tunnel via Secure Sockets Layer (SSL) allows CP Secure support specialists to remotely and quickly diagnose and troubleshoot CSG without having to go onsite. You get fast, responsive support for your technical issues without needing to send in the appliance or to call technical support.

## 15. Who is CP Secure?

Founded by gateway anti-virus pioneers, CP Secure is a leading innovator of real-time anti-malware solutions for enterprise-class organizations. The company's CSG anti-malware appliances protect the web and email traffic of some of the most demanding organizations in the world.

CP Secure's malware collection and research is global, its response times are consistently faster than the leading antivirus vendors', its malware signature library includes all known viruses and spyware, and the company is one of only nine vendors to pass the ICSA Labs gateway antivirus detection test and receive certification for detecting all currently active viruses/malware. CP Secure possesses deep network security expertise, as its founders pioneered gateway antivirus technologies and products at Trend Micro™, the market-leader in gateway antivirus.

## 16. I'd like to test drive CSG. Can I get an evaluation unit?

Yes, CP Secure offers a *free* 30-day, no-risk evaluation of CSG. You get:

- Technical support (both telephone and virtual)
- Malware signature updates
- Product documentation set

To request for an evaluation unit, please contact your security or networking solution provider or visit the CP Secure Web site at [www.cpsecure.com](http://www.cpsecure.com), and then click the **Request a Free Evaluation Unit** link. Alternatively, copy and paste the following link into your Web browser – <http://www.cpsecure.com/forms/products/unitrequest/evaluationunitrequest.php>

Fill out the request form, and then click **Send**. A CP Secure representative will contact you shortly.

## 17. Where can I find more information about CSG and CP Secure?

To learn more about CP Secure, CSG, and our other solutions, visit our Web site at [www.cpsecure.com](http://www.cpsecure.com). Here are some of the more popular destinations on our Web site:

- Document center – Download product documentation (installation, deployment, administrator's guides), data sheets, white papers, corporate profile, etc. by visiting <http://www.cpsecure.com/resources/resources.php>
- Product portfolio – For an overview of the security solutions that we provide, visit <http://www.cpsecure.com/products/index.html>

- Contact information – Find contact information for the CP Secure office nearest you by visiting <http://www.cpsecure.com/contact/index.html>
- Awards – Read about the industry recognition CP Secure and our products have received by visiting <http://www.cpsecure.com/company/awards.html>
- Customer testimonials and case studies – Read about what our customers say about CP Secure and our products by visiting <http://www.cpsecure.com/customers/testimonials.html>

#### ABOUT CP SECURE

Founded by gateway anti-virus pioneers, CP Secure, Inc. is a leading innovator of real-time anti-malware solutions for enterprise-class organizations. The company's Content Security Gateway appliances are powered by patent-pending stream-based scanning technology to protect some of the world's most demanding organizations against spyware, viruses, and other malware. CP Secure operates globally, in North America, Europe, and Asia, and may be found on the web at [www.cpsecure.com](http://www.cpsecure.com).

##### GLOBAL HEADQUARTERS

20065 Stevens Creek Blvd., Building C  
Cupertino, CA 95014  
USA

Tel: +1 888.722.6847  
+1 408.873.7778  
Fax: +1 408.873.7779

##### EUROPE

Bendenweg 101  
53121 Bonn  
Germany

Tel: +49 228.85427.0  
Fax: +49 228.85427.29

##### ASIA

4F-1, No. 432, Keelung Road, Section 1  
Taipei 110  
Taiwan, ROC

Tel: +886 2.2723.0936  
Fax: +886 2.2723.1791

Copyright © 2006 CP Secure, Inc. All rights reserved. All product information is subject to change without prior notice. CP Secure, the CP Secure logo, Content Security Gateway, and WormSecure are trademarks of CP Secure, Inc. All other brand, product, service, and company names are registered trademarks, trademarks, or service marks of their respective holders and are acknowledged.  
CPS-FAQ-CSG-061026