
A background image showing a laptop on a desk with a speedometer overlay, suggesting speed and performance.

# Trend Micro Web Gateway Security

Web Security 

 Faster Protection,  
Greater Flexibility,  
Lower Total Cost

*Solution Overview | September 2009*

## I. THE NEED FOR FASTER PROTECTION

As the web becomes more important to modern business, it also becomes more dangerous. A new malware threat is created every two seconds, and cybercriminals are better organized to deliver increasing numbers of sophisticated web-borne threats. URL filtering alone at the Internet gateway is insufficient to protect organizations from threats such as masked URL redirects, multi-stage downloaders, domain hopping communications, obfuscated JavaScript, portable executables, and other sophisticated malware. While implementing acceptable use policies is still important, stale content categories fail to provide timely protection against these fast-moving threats—particularly when the majority of today’s malware hosts are legitimate websites that have been compromised.

## II. INTRODUCING TREND MICRO WEB GATEWAY SECURITY

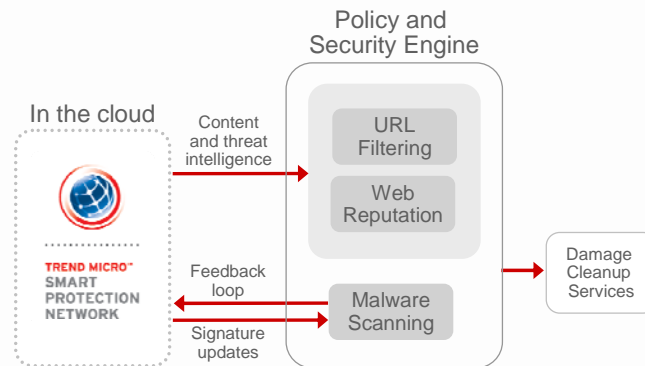
Trend Micro™ Web Gateway Security delivers the multi-layer security and real-time visibility you need to safely manage today’s rich and dynamic Internet content. By combining InterScan Web Security Virtual Appliance and new Advanced Reporting and Management, Trend Micro consolidates the best security elements into a single web gateway security solution with cost-effective deployment options that easily fit into your network infrastructure. For the first time, one solution gives you complete security for the key Internet protocols HTTP, HTTPS, and FTP. And a single console provides the control and visibility necessary to help ensure that your users are protected and can browse content without the risk of infection—even when the material may not be safe.

## III. THE BEST SECURITY TECHNOLOGIES TO ADDRESS TODAY’S CRITICAL WEB THREATS

Unlike most IT security vendors, Trend Micro develops and owns the best security technologies to address today’s critical web threats, both at the exposure layer and infection layer. This gives our experts the ability to develop innovative new security solutions, including the integration of URL filtering, web reputation, malicious content filtering, and other technologies within a common framework. Using this approach allows administrators to create comprehensive policies, dynamic dashboards, and performance reports, dramatically improving your organization’s security posture, and reducing the costs and challenges of managing different point solutions separately. If you currently use only URL filtering to defend your web gateway, now is the time to consider adding zero-hour threat protection tools, including web reputation and malware scanning features, to block known threats that may emerge on new sites or to scrub the content of viruses and spyware before they hit your users’ browsers.



# TREND MICRO WEB GATEWAY SECURITY



*InterScan Web Security Virtual Appliance consolidates multiple layers of security*

Trend Micro helps you move beyond traditional URL filtering and the weaknesses that come with a static local URL category database, giving you the advantage of real-time threat intelligence from the Trend Micro™ Smart Protection Network. A highly correlated source of email, web, and file reputation services and URL categories, the Smart Protection Network is a cloud-based system that is constantly updated by Trend Micro's discovery services and customers. With extensive input, including feedback from Trend Micro's broad-reaching customer base, the Smart Protection Network delivers greater visibility and accuracy across the spectrum of Internet threats. Moving this information into the cloud eliminates the chore of maintaining and updating local databases, helping ensure that every URL request is checked against the most current category and reputation information. By filtering non-business or known malicious content before it gets to the gateway, our system inspects content one last time before your users access it, optimizing the resources deployed in your network.

Malware content filtering continues to be a must-have security requirement for web gateway security solutions. As information passes through the gateway, scanning for viruses and spyware helps ensure that both inbound and outbound content is scrubbed of known bad elements. Instead of just deleting infected files, a complete content filtering engine can clean files and pass them to users. The combination of centralized scanning at the gateway and simplified pattern/signature file updates into a single point dramatically accelerates the delivery of this layer of protection. This approach reduces the window of endpoint exposure, optimizes resource utilization, and helps ensure that only clean content crosses the network.

*Cascadia Labs independent testing shows that Trend Micro's blocking effectiveness against security threats was at least 23% more effective than the leading competitors, and 30% more effective than Websense.<sup>1</sup>*

It takes just minutes to apply a comprehensive web security policy, following these five easy steps:

1. Define URL filtering policies by applying rules to users/groups/IPs against over 80 pre-defined or custom URL categories, including time and disposition criteria
2. Select a desired risk profile or security threshold for Web Reputation services
3. Define malware scanning and file criteria for HTTP, HTTPS, and FTP traffic, along with script security criteria for technologies such as Java
4. Define additional application policies, such as rules for key Instant Messaging protocols
5. Define reporting and dashboard elements for monitoring Internet activity, such as most active users by hits or bandwidth, most popular URLs or categories, most blocked URLs, or riskiest URLs by viruses detected

Once the monitoring process starts, administrators can constantly refine policies to respond to changing business requirements and meet corporate and regulatory compliance standards.

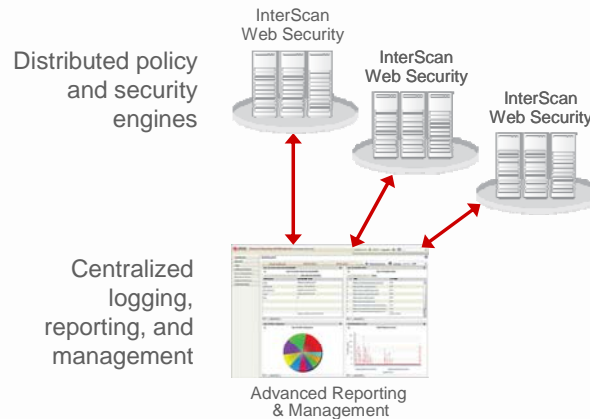
## IV. REAL-TIME VISIBILITY

Having the flexibility to manage the web content that is entering your organization is one requirement, but the Trend Micro Web Gateway Security solution also allows you to understand what is actually happening on your network from a global perspective, in real time. With performance reporting, dynamic dashboards, and real-time activity monitors, Trend Micro Web Gateway Security provides unprecedented visibility into those difficult questions—who, what, when, how, and where? Trend Micro's Web Gateway Security solution is flexible in design and offers actionable information so administrators have the capability to open specific views into live events, conduct forensic analysis against real-time information, and execute corrective actions to reduce or eliminate risky Internet activity immediately. The advanced reporting features support drag-and-drop configurations, selectable charting resources, and configurable timelines to optimize information displays.

As part of web gateway security, Trend Micro's InterScan Web Security servers deliver real-time statistics to Advanced Reporting and Management. With this tool, organizations can centralize their reporting and management and retain the ability to deploy the web gateway across their networks. This approach removes the reporting burden from each web gateway security engine, giving systems greater flexibility to meet the needs of distributed organizations, as well as more capacity to improve server scanning performance.



# TREND MICRO WEB GATEWAY SECURITY



*Centralized logging, reporting, and policy management across a distributed gateway environment*

## V. LOWER TOTAL COSTS

Trend Micro lowers the total cost of securing your web gateway, and has a direct impact on factors such as minimizing productivity loss, simplifying IT management, reducing endpoint cleanup, and alleviating the need for additional server procurement and licensing. Trend Micro's adoption of the software virtual appliance form factor—which provides appliance-like deployments on standard hardware platforms and virtualization frameworks such as VMware—also leads to savings on hard costs. By supporting both software appliance and virtual appliance options, Trend Micro Web Gateway Security allows IT departments to take advantage of the latest high-performance, multi-core processors and virtualized environments without paying for proprietary hardware appliances, excess capacity, or additional licensing fees for operating systems.

Trend Micro software virtual appliances include a hardened and tuned OS that supports the security application. To provide the highest level of expertise and commitment, we also complete additional certifications:

- VMware Ready validation to help ensure that the InterScan Web Security Virtual Appliance and Advanced Reporting and Management are fully tested and supported in a VMware environment
- Certified by Trend Micro assurance program to verify that your Trend Micro security applications are fully compatible with independent hardware vendors' servers

*Osterman Research shows Software Appliance deployments are 47% less expensive than a traditional hardware appliance model.<sup>2</sup> Virtual Appliance deployments and virtualization can reduce management costs by more than 40%.<sup>3</sup>*



## VI. CONCLUSION

As you continue to integrate the Internet into your business processes—and as malware becomes more and more web-based—security has become the top priority for defending the web gateway. Relying on URL-filtering products alone leaves you exposed to today's sophisticated web threats, but deploying more point solutions increases complexity and cost, diminishing system performance. By consolidating web security technologies and leveraging in-the-cloud security services from the Smart Protection Network, Trend Micro Web Gateway Security offers better protection that is faster, smarter, and more comprehensive. The solution's new advanced reporting capabilities give organizations the resources to understand the interaction between users and the Internet in real time.

The bottom line: IT security professionals and business leaders require an innovative security solution that incorporates the latest technologies targeted at addressing new and existing threats in a cost-effective manner—and that's exactly what Trend Micro delivers.

For more information on InterScan Web Security Virtual Appliance, visit

<http://us.trendmicro.com/us/products/enterprise/interscan-web-security-virtual-appliance/index.html>

For more information on Advanced Reporting and Management, visit

<http://us.trendmicro.com/us/products/enterprise/advanced-reporting-management/>

For information on the Trend Micro Smart Protection Network, visit

<http://us.trendmicro.com/us/trendwatch/core-technologies/smart-protection-network/>

Or please call or visit us at:

[www.trendmicro.com/go/enterprise](http://www.trendmicro.com/go/enterprise)

+1-877-21-TREND

<sup>1</sup> Cascadia Labs Comparative Report: *Cascadia Labs URL Filtering and Web Security*, Summer 2009

<sup>2</sup> Osterman Research White Paper: *Why You Should Consider Deploying Software Appliances*, December, 2008

<sup>3</sup> Osterman Research White Paper: *Why You Need to Consider Virtualization*, September, 2008

© 2009 by Trend Micro, Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, InterScan and Private Post are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. (SB01\_IWSVA-ARM\_090814US)

