



“百大网站中90%的网站被归类为社交或搜索网站，其中超过47%的网站支持客户生成的内容。”

WebSense安全实验室，2009年

WebSense®

Web 安全网关解决方案

动态交互的Web 2.0技术让Web俨然变成了一个核心的业务应用平台。传统的客户关系和支付应用程序均可通过Web互动交付，而类似社交网络这样的应用程序更是被用于企业的日常招聘、销售线索生成等商务流程中。但与此同时，Web 2.0的动态性和允许用户自己生成内容的特性也为使用者带来了新的风险，传统的安全技术如反病毒、URL过滤等受到了巨大冲击，失去了本应有的效力。而且这些技术对于被粘贴到Web 2.0网站的敏感出站数据也缺乏控制能力。

市场领先的WebSense® Web安全网关 (WSG) 解决方案可以最低的总体拥有成本 (TCO) 提供了对现代Web 2.0威胁的最佳防护。它们是唯一可提供企业级数据泄露防护及为云与边界解决方案的混合部署提供统一管理的解决方案。Web安全网关解决方案让企业能够充分利用Web 2.0的能量，同时又不必担心Web恶意软件、不当内容或敏感信息泄露等问题。

工作原理

Web安全网关解决方案会检查所有经过企业边界的进站和出站内容，以保护企业远离动态Web恶意软件，防止敏感数据出站泄漏，并增强员工的生产效率。WebSense TruHybrid™部署同时支持边界解决方案设备及服务即安全(SaaS)平台，通过统一的策略和报告基础设施来管理整个组织环境。与其它方案不同，WebSense客户可以灵活地选择最合乎其运营需求的平台或平台组合，同时还不会产生管理多个系统的费用问题。

WebSense Web安全网关解决方案提供了：

- 出站数据泄漏防护和合规性控制 – 内置式企业级数据泄漏防护，实施必要控制，让出站流量能够顺利到达如Web邮件、社交网络等目的地，同时遵从必要的合规性规范，控制敏感数据的泄漏。
- 恶意软件防护 – WebSense TRITON™高级分类引擎(ACE)可防范传统文件型攻击，还能防范绕过传统反病毒解决方案的动态脚本攻击。
- Web 2.0员工生产效率 – TRITON高级分类引擎可以删除传统URL过滤解决方案无法准确分类的来自复杂、动态、有密码保护的Web 2.0网站的不当内容。
- 最低的总体拥有成本(TCO) – WebSense TRITON控制台和TruHybrid部署减少了整个企业必须支持的设备、管理系统和供应商数量。
- 一致的企业范围安全覆盖 – TruHybrid部署统一了对边界解决方案和SaaS的策略。不论用户是在不同工作地点间移动还是在家办公，均可一致执行这项独特的策略。

“百大网站中90%的网站被归类为社交或搜索网站，其中超过47%的网站支持客户生成的内容”

WebSense 安全实验室，2009年

高级分类引擎

WebSense Web安全网关解决方案包含有最精确的*双向安全分析引擎——WebSense TRITON高级分类引擎(ACE)，它集入站分析与深层的出站数据泄漏防护功能于一身。ACE将这两种传统安全功能与反病毒、URL过滤、信誉服务和指纹识别等最先进内容分类技术完美结合，能够精确分类入站和出站风险。拥有WebSense ThreatSeeker® Network的支持，这款高级分类引擎凭借实时安全扫描、实时内容分类和企业级数据泄漏防护，可在任何内容经过网关时对其进行分析。

实时安全扫描

动态脚本攻击主导着Web威胁前景，单凭反病毒技术并不能跟上它的发展步伐。WebSense专有的实时安全扫描分析技术无需参考之前已知的攻击数据库即可实时识别恶意内容，从而可解决这类“零日”威胁。

实时内容分类

使用最为普遍的网站中，有许多都是传统URL过滤技术无法精确分类的网站。例如：一个Google或Facebook页面可能是包含有多种类型的内容元素——这就使得我们无法将它归类任一种类型中。最终，许多组织被迫不是无差别地拦截有价值资源，就是忽略可接受使用策略，允许所有的动态Web 2.0目的地访问。

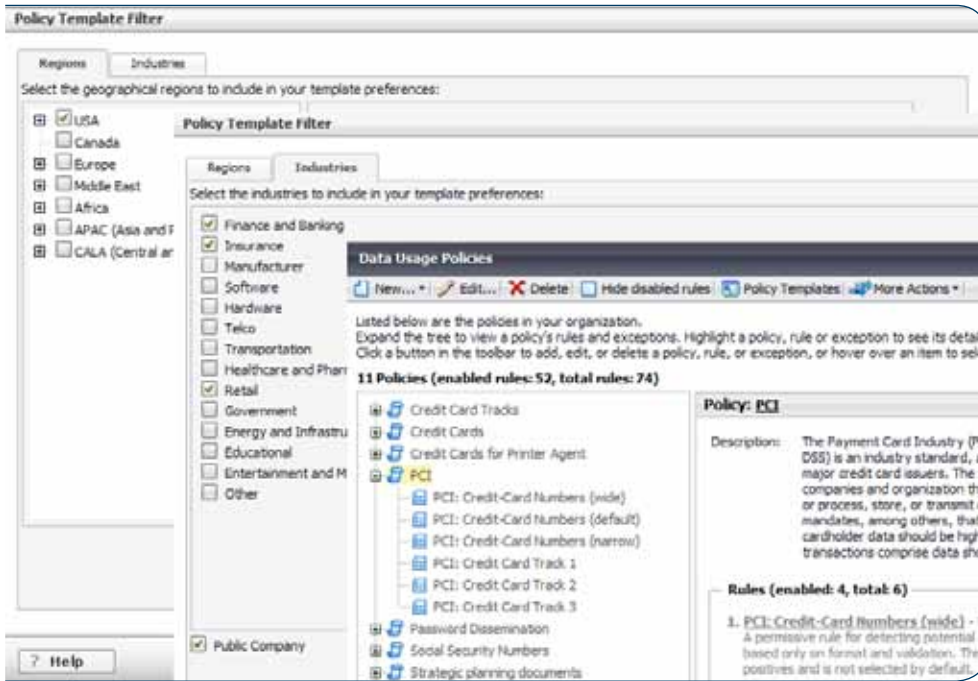
Web安全网关解决方案提供了实时内容分类，通过实时分类每张网页内所包含的内容元素，将可接受使用策略精确地扩展到动态Web 2.0网站上。如网页有个别内容元素违反了策略，那么这些元素将会被从页中剔除而只允许其中合规信息通过。这项独特功能在保持生产效率和可接受使用策略遵从的同时实现了对Web 2.0业务目的地的广泛访问。

企业级数据泄漏防护

内置式企业级数据泄露防护(DLP)实施了必要的控制，让以电子邮件、社交网络等为目的地出站业务通讯能够顺利到达，并同时遵从必要的合规性规范，控制敏感数据的泄漏。与DLP功能仅局限于关键词检查或需要复杂第三方集成的其它方案不同，WebSense Web安全网关解决方案提供了市场领先WebSense DLP解决方案,可提供面向http、https和FTP网络流量的所有功能，同时还包括了800多个创新性策略、针对深层内容检查的指纹识别以及全面合规性报告。

Web DLP与Web安全网关解决方案的集成去去除了在每个办公地点部署专门的第三方DLP硬件的需求，显著降低了TCO。对于有数据泄露防护长期计划的组织，Web DLP还提供了稳定的投资保护，只是需要简单的软件升级，即可将控制范围扩展到Web以外，包含进其它流量类型（电子邮件、IM、P2P）、端点和静态数据（如：数据库、文件共享、Exchange、Share Point）。这也使得从Web DLP到其它渠道的范围扩展并不需要进行架构重建，现有策略和基础设施投资依然能够保留下来。

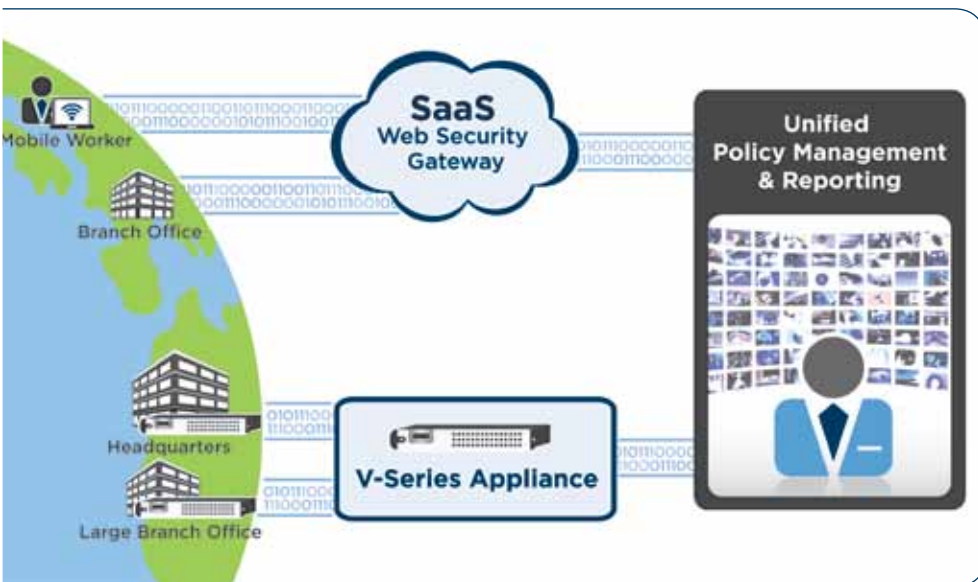
* <http://www.websense.com/content/tolly-report-reg.aspx>



简单的DLP策略向r可r助管理r快速定r可r足r域和行r特定法r要求的最佳r策略。

TruHybrid部署

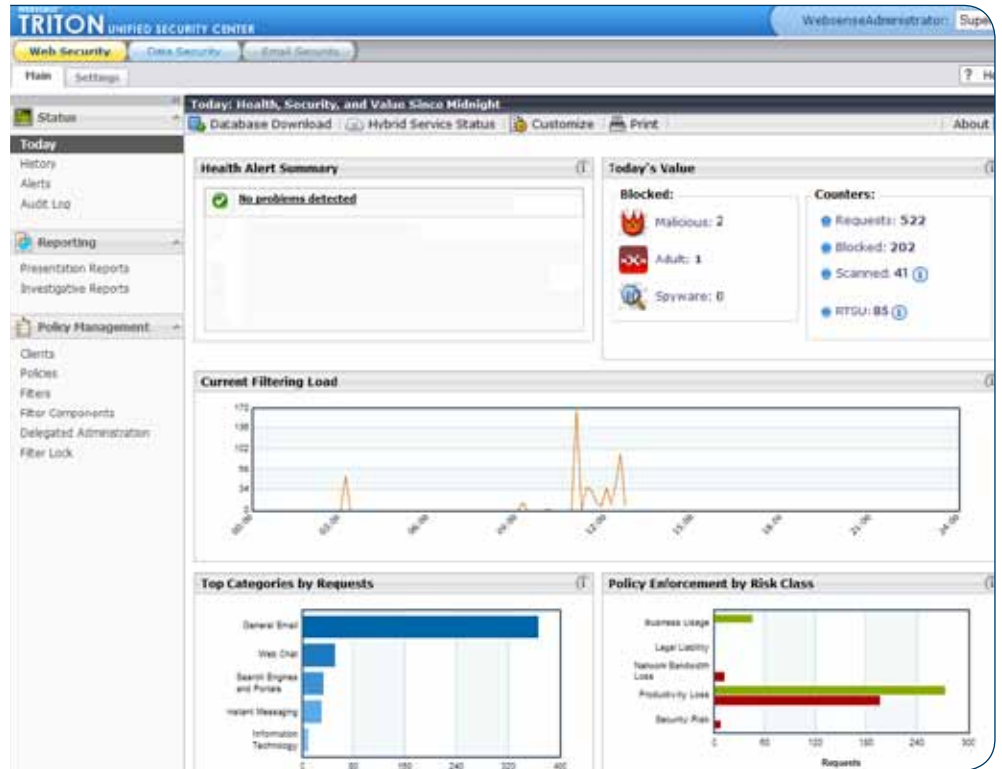
TruHybrid部署让企业可以灵活地选择将边界解决方案和SaaS部署平台混合，同时使用一个独一无二的统一管理系统来管理整个环境。您可利用SaaS平台将安全防护范围扩展到分支机构或移动用户，同时还可将高性能设备部署在企业大型分支机构或数据中心。不论您选择与SaaS组合或边界设备，您只需在一个地点设定策略便可适用于整个企业。这种统一方案不仅消减了边界解决方案/SaaS部署组合的管理成本，而且还确保了对所有环境的一致安全覆盖。



TruHybrid部署统一了边界解决方案/SaaS部署组合的管理。

“多达57%的恶意Web攻击都包含有数据窃取代码。”

WebSense 安全实验室，2009年



TRITON控制台的交互式控制面板可在出现威胁和策略违规行为出现的第一时间做出反应。

SSL可视性和控制

SSL流量使用率的提高给传统的URL过滤器造成了许多盲点，打开了威胁和数据泄露的后门。Web安全网关解决方案提供了对SSL流量的可视性和控制，允许组织对所有Web通讯设定策略。

高级应用程序控制

如IM、P2P等网络应用程序的增长给黑客提供了一种阻断商业活动及窃取机密数据的手段。Web安全网关解决方案提供了对超过125种网络协议、数千种应用程序的控制能力，可缓解安全风险，防止未经授权应用程序造成的数据泄漏。策略动作可从简单的应用拦截扩展到高细粒度的带宽控制。

统一的内容安全管理和报告功能

Web安全网关解决方案还有个重要功能，且这个功能只通过WebSense提供——就是TRITON控制台。它将所有的WebSense Web、数据和电子邮件安全解决方案的管理整合到一个单一的基于Web的界面中。直观的控制面板包括了超过55种内置报表和广泛定制功能，可帮助说明用户行为、促进故障排除、进一步降低风险。该解决方案提供了大量易于使用的功能，包括广泛的挖掘功能、策略向导、配置模板、调度子系统和自动内容更新，与其它类似解决方案相比，其管理工作和成本有了大幅降低。由于内容安全防护范围随时可能扩展Web安全以外，因此TRITON控制台的统一管理功能将可轻松扩展包括进对电子邮件和全面DLP的集中化管理。

Features	Benefits
TruHybrid部署	通过统一管理边界解决方案和SaaS部署，降低总体拥有成本 (TCO)并确保整个企业策略的一致性。
企业级数据泄漏防护	防止出站数据泄露并实施必要的合规性控制。通过避免复杂的DLP部署，降低TCO。
实时内容分类	通过实时Web内容过滤，确保动态、密码保护、混合内容Web属性的安全使用。
实时安全扫描	通过实时识别动态、脚本和未知威胁，保护组织免遭Web恶意软件。
TRITON控制台	通过统一管理Web、数据和电子邮件安全解决方案，降低TCO和供应商管理成本。
整合式反病毒	结合使用第三方和先进Websense Web反病毒技术，防范文件型的病毒攻击。
带有先进信誉分析功能的Web过滤	应用基线可接受使用策略并拦截已知恶意站点。多点信誉分析包括：属性类型、词汇信誉、Web 2.0贴、URL类型、最近邻、搜索信誉、历史、年限和地理位置。
ThreatSeeker Network实时更新	每五分钟更新一次，降低暴露于新兴威胁的风险性。
SSL可视性	以全面SSL代理和整合式证书管理，实现对加密Web流量的检测
应用控制	通过管理网络协议和应用程序的使用，最小化风险、提高生产效率并降低带宽成本。
企业级Web代理/缓存	通过优化流量，提高性能并降低带宽成本。支持透明式和显式代理配置。
灵活的用户认证	以经由活动目录 (AD)、LDAP、RADIUS、Novell、NTLM v2的灵活认证，应用用户和基于组的策略。
高可用性和负载平衡	利用WCCP或外部负载平衡器，实现系统冗余和大型企业可扩展性。

Websense在Gartner最新的《Web安全网关魔力象限》将定位为领导者象限。

Gartner公司
 “Web安全网关魔力象限”* (Peter Firstbrook , Lawrence Orans)
 2010年1月8日

公司联系方式：

北京：
tel +8610-58844000
fax +8610- 82139022

上海：
tel +8621-63609085
fax +8621-63609015

广州：
tel +8620-83876956
fax +8620-83876823

www.websense.com.cn
chinasales@websense.com

部署平台可用性

边界解决方案 (On-premise) 部署可通过Websense V系列硬件™设备或作为通用服务器上运行的软件进行实施。SaaS部署由Websense托管型Web安全网关解决方案提供支持。

- V系列硬件设备 - V系列硬件设备为边界解决方案部署提供了企业级性能、可靠性和简单部署。经过财富100强企业环境的验证，V系列硬件设备不仅集成了组件层冗余功能，同时还支持一系列企业部署功能，包括负载平衡和高可用性。V系列硬件设备还被设计为支持未来的Websense解决方案，完全无需升级硬件 — 延长了这一平台的寿命并为其提供了增值。
- 托管式Web安全网关 - Websense托管式Web安全网关 (Hosted Web Security Gateway) 解决方案将安全检查流程转移到了位于“云端 (in the cloud) ”的十大全球可用的冗余数据中心。这种SaaS交付模式不仅加快了部署速度，而且通过去除了企业须在每个办公地点边界部署硬件支持这一需求，还显著降低了运营成本。Websense数据中心经ISO 27001认证完全符合严格的安全和可用性标准，对于单个的组织来说要在边界，特别是远程机构达成这些标准代价不小。Websense托管式Web安全网关作为独特的SaaS-only解决方案部署时还可提供更多可选的SaaS电子邮件安全集成优势。



Websense V10000™设备

Websense Web安全网关解决方案选项

Websense Web Security Gateway Anywhere — 适用于需要TruHybrid边界解决方案*/ SaaS管理、企业级Web数据泄漏防护或Websense远程过滤客户端的部署

Websense Web Security Gateway — 适用于边界解决方案*部署

Websense Hosted Web Security Gateway — 适用于SaaS部署。

软件部署的最低服务器需求：

操作系统

Red Hat Linux v4,
update 5*或Windows Server 2003/ Server
2008+
CPU : 2 x双核2.8GHz处理器
内存
4GB RAM

硬盘驱动

2个物理磁盘：
* 100GB的OS、应用程序和临时数据空间，100GB的缓存空间*
* 100GB (推荐RAID 1)*
网络接口
2 x 10/100/1000以太网接口

* 边界解决方案部署可通过Websense V系列硬件设备或作为通用服务器上运行的软件进行实施。

*魔力象限 (Magic Quadrant) 用图形来呈现某一特定时期内的市场状况，描述了Gartner依据自身制定的标准对该市场内的厂商行为进行的分析。Gartner并不对在魔力象限中描述的任何厂商、产品或服务出具官方认可，也不建议技术用户只选择那些位于“领导者”象限里的厂商。魔力象限仅作为一种研究工具，并不意味着行动的具体指导。Gartner对于该项研究不承担任何明示或暗示的担保，包括适销性或适用于某一特定用途的任何担保。

查看在线产品演示或Websense Web安全方案免费评估，请访问
www.websense.com/evaluations.