WEB SECURITY

websense®
ESSENTIAL INFORMATION PROTECTION™

Websense
Web安全网关

Websense
Web安全防护

Websense
Web过滤

Websense
Hosted托管式Web安全防护

Websense® Web
安全解决方案

Web 2.0 问题

随着互联网的飞速发展，Web 2.0技术势必将显著改变人们交流和工作的方式。Web 2.0强大的协作属性正逐渐生成一种新的业务执行方式，但同时也引入了前所未有的安全风险。Web 2.0应用程序正快速出现在桌面上，从基于Web的混搭到托管式服务、再到用户产生内容和应用程序。

Web 2.0所普遍存在的动态的用户产生的内容是信誉数据库、URL过滤等老式的安全模式并不能监控到的。这就给IT安全团队带来了冲突性问题 — 如何在挖掘出Web 2.0的大量潜力的同时保持网络、终端用户和敏感数据的安全性。

不断变化的桌面：Web混搭、用户产生的内容、widgets和托管应用程序带来了新的安全问题

尽情享用Web 2.0

随着可能由Web 2.0所形成的新功能进入商业主流，简单的拒绝访问这些技术或拦截这些技术使用已不再是可行性选择。要想充分利用Web 2.0的商机，企业必须明确知道必要的企业信息有得到很好保护。

采用Websense，IT专业人士不仅可提供对最新基于Web的工具和应用程序的访问，同时还可保持企业安全以免遭攻击。拥有Websense Web安全解决方案中所发现的无与伦比的威胁前景知识、实时的动态内容分析以及全面的出入境安全防护，IT专业人士现在可尽情享用Web 2.0。

“WebsenseThreatSeeker Network 是我们在市场上所发现的最好的一套安全分类和检测技术。”

Beth Cannon,
Thomas Weisel Partners
投资银行

“Websense 防止了针对我们网络的攻击，潜在地防止了对保密数据和病人数据的窃取。”

Central Coast
Community Healthcare

可选插件

Websense Web安全产品的功能通过可选插件模块可得到进一步扩展：

- **Websense** 客户端策略管理器（**CPM**）为台式机、笔记本电脑和服务器提供了一款全面的端点安全解决方案，可防范已知和未知的安全威胁。它可防止非授权应用的安装和实施，利用全面的分类应用程序数据库来执行策略。
- **Websense**远程过滤可将**Web**过滤和安全保护范围进一步扩展到远程机构和移动笔记本电脑用户上。即便用户和设备不在网络内使用时它也可提供保护，从而随时随地确保了互联网的安全使用。

直观的安全仪表版可提供有关威胁、用户行为和策略控制的即时反馈.

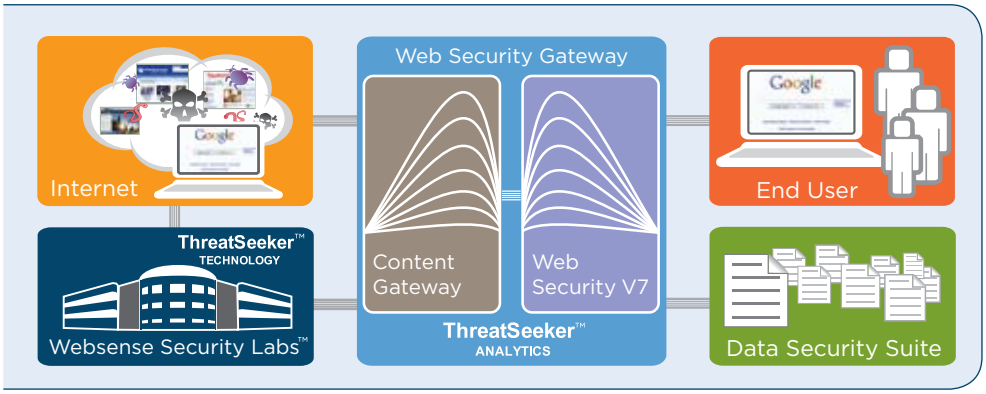
Web安全产品

Websense Web安全网关

Websense Web安全网关可实时分析并保护Web流量安全，实现最新Web 2.0站点和应用的安全使用。Web安全网关可添加前置式基于代理的Web和SSL流量内容分析到健全的Websense Web安全和Websense Web过滤平台中，从而不仅允许对新站点和动态内容进行即时分类，同时还可前瞻性发现安全风险并拦截危险的恶意软件。Websense Web安全网关包括：

- 主动安全模块（ASM）- 在网关处部署最先进ThreatSeeker分析技术以在恶意代码进入网络前就加以检测、拦截并去除。通过采用先进的启发式规则、特征码和行为检测，这些分析技术可与全球ThreatSeeker Network相集成，提供持续更新和微调以检测最新威胁。
- 内容网关模块（CGM）- 提供新内容在线分类以及SSL流量解密和扫描。基于健全的Web代理和缓存平台而创建，内容网关模块可识别代理规避、成人内容、黑客行为和许多其它类型内容，保护用户免遭新的未知Web内容的潜在威胁。

Websense Web安全网关集强大的安全性与无与伦比的易于使用性于一身。直观的管理仪表版可提供有关网络安全、威胁检测、流量负载和用户行为的即时反馈。集成式策略管理、报告与委托管理的结合使用可帮助管理人员节省时间和精力，同时还可降低可能导致安全漏洞的失误。



Websense Web安全防护

Websense Web安全防护(前Websense Web Security Suite™)集业界领先的URL过滤与广泛安全功能于一身。该解决方案包括了Web信誉服务与全面安全类别，如：间谍软件、网络钓鱼、按键记录以及恶意移动代码。Websense Web安全防护由于可在威胁发现的几分钟内即通过ThreatSeeker Network应用最新信息，从而可将威胁爆发机率降至最低。同时，它还提供了对可能是数据泄露和恶意攻击的一个主要来源——即时消息(IM)和IM附件的控制能力。Websense Web安全防护拥有基于Web的GUI和安全仪表版、直观的策略控制、委托管理和灵活的集成报告，极易于管理。

Websense Web安全防护包括了Web Protection Services™（Web保护服务），可持续监视企业的网站、品牌和相关URL的恶意行为以防止其被用于欺诈攻击。

Websense Web过滤器

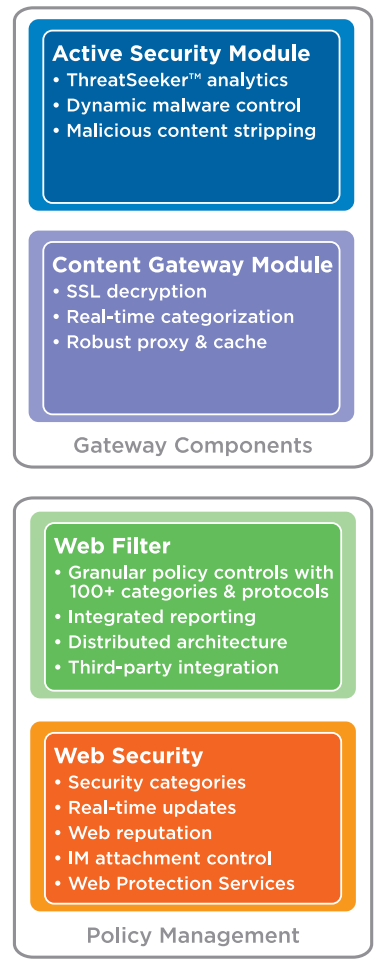
Websense Web 过滤器(前Websense Enterprise®)是全球领先的Web安全解决方案，可改善员工生产力、减少法律责任并优化网络资源的使用。它拥有直观的基于Web的GUI和灵活的集成报告，允许定制策略以满足专门需要并将管理费用降至最低。除了控制网站访问以外，Websense Web过滤器还提供了对100多种网络协议的基于策略的控制，可防止混和式安全威胁和带宽耗尽。该解决方案采用了分布式架构，拥有高度可扩展性，同时还提供了与第三方网络设备的广泛集成。

也可由**Websense**提供

Websense托管式Web安全防护

Websense还为提供了一款适用于拥有诸多远程地点及漫游用户的分布式企业的方案。Websense托管式Web安全防护(前SurfControl® WebDefense®)可前瞻性发现并拦截互联网级威胁、去除对前置式软硬件部署的需求。该托管式服务可跨多个网关、地点和漫游用户站点地集中化Web保护，在威胁到达网络前就去除威胁。Websense数据中心已通过ISO 27001标准认证，其服务得到了业界领先的SLA的支持，可保障正常运行时间和竞争性灾难恢复供应。

Websense解决方案和模块组合灵活



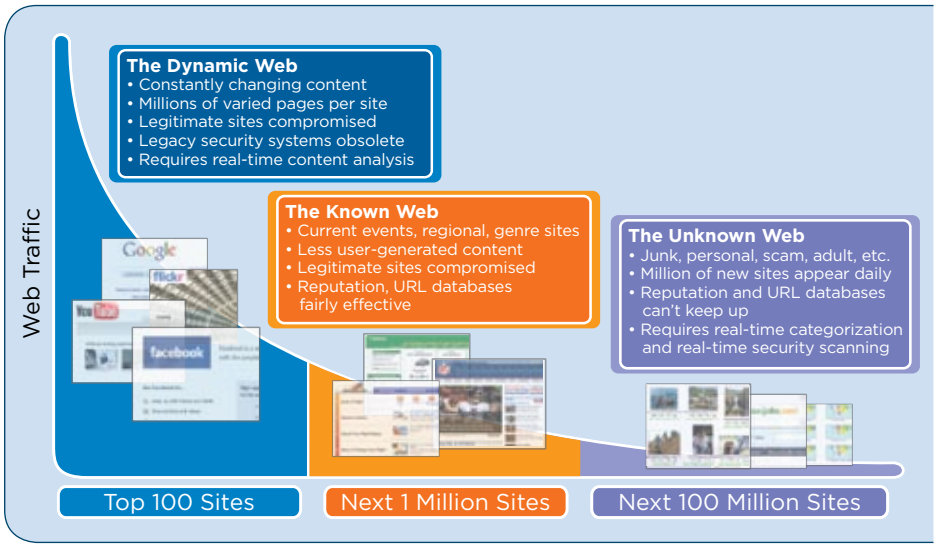
Websense Web Filter
optional

Websense Web Security
optional

Websense Web Security Gateway

Websense 方案

过去，大多数Web内容是静态和可预测的。但今天摆在我们面前的现实情况是：即便是来自所谓“信任”站点的Web内容也会随着终端用户粘贴、编辑或伪造内容而发生经常性不断变化。最受欢迎且流量大的站点往往可最大限度地利用动态Web 2.0内容，同时也最易于受到攻击。事实上，据Websense® 2008年上半年研究发现，前100大站点中有超过60%站点或是有托管恶意内容、或是包含了到非法站点的隐蔽性重定向*。



Web安全前景不断变化：大流量站点包含了最多动态内容，而这些内容可绕过多数老式安全系统。

Websense通过其业界领先的ThreatSeeker Networkand来了解互联网前景内容和前后情况，并将这种智能提供到其所有安全解决方案中。Websense通过在客户网关部署ThreatSeeker在线分析技术，提供了对新威胁和未分类内容的动态、适应性防护，是首家可解决Web 2.0风险的安全供应商。

Websense客户现在不仅能充分享用Web 2.0的能量，同时通过出入境HTTP和SSL加密流量内容检测还可控制住安全风险。实时内容分析通过与强大的防恶意软件、Web信誉和URL过滤保护结合使用，可在其它安全解决方案甚至还不知道有恶意内容存在前就前瞻性将其拦截下来。 该方案不仅可保持网络安全性，同时还可支持最新基于Web的工具、应用程序和法律内容。

* Websense安全实验室威胁报告，2008年7月

Websense ThreatSeeker Network

Websense ThreatSeeker Network适应性安全技术通过采用超过5000万个实时数据采集系统，可持续监控可能导致新兴威胁的互联网内容，包括新内容和动态内容。Websense ThreatSeeker Network可将这种智能提供到其Web安全、消息安全和数据泄露防护解决方案中。这就使得Websense能够以传统安全解决方案和基础电子邮件过滤解决方案所不可能达到的速度来适应不断快速变化的互联网。

ThreatSeeker Network:

- 每小时分析超过4000万个网站
- 每小时为超过200万个域、网络、IP地址和主机分配信誉度
- 每小时对近1000万封电子邮件进行不必要内容和恶意代码扫描
- 每天捕捉超过1000万次不请自来的垃圾邮件、网络钓鱼及攻击活动

系统要求

Web安全网关

Websense内容网关
- RedHat® Enterprise Linux® 4, update 5

Websense Web安全防护
- RedHat® Enterprise Linux® 4, update 5
- Microsoft® Windows Server® 2003 标准版或企业版，包含SP1
- Microsoft Windows® 2000 包含SP3，或更高

Websense内容网关
- RedHat® Enterprise Linux® 4, update 5

Websense安全防护
- RedHat® Enterprise Linux® 4, update 5
- Microsoft® Windows Server® 2003标准版或企业版，包含SP1
- Microsoft Windows® 2000 包含SP3，或更高

Web过滤器
- RedHat® Enterprise Linux® 4, update 5
- Microsoft® Windows Server® 2003标准版或企业版，包含SP1
- Microsoft Windows® 2000包含SP3，或更高

公司联系方式：

Websense, Inc.
San Diego, CA USA
tel +1 800 723 1166
fax +1 858 458 2950
www.websense.com

中国代表处

北京
tel +8610-58844000
fax +8610-65123067

上海
tel +8621-63609086
fax +8621-63609015

广州
tel +8620-83876956
fax +8620-83876823

www.websense.com.cn

所有其它地址
www.websense.com/international

办公地点：

澳大利亚 websense.com.au	以色列 websense.com
中国 websense.com.cn	意大利 websense.it
法国 websense.fr	日本 websense.jp
德国 websense.de	荷兰 websense.com
香港 websense.cn	新加坡 websense.com
印度 websense.com	西班牙 websense.com.es
爱尔兰 websense.co.uk	阿拉伯联合酋长国 websense.com

websense®
ESSENTIAL INFORMATION PROTECTION™

解决方案背后的公司

Websense是整合Web、数据和电子邮件安全领域的领导者，为全球4200多万人们的必要信息提供了保护。Websense软件和托管式安全解决方案可帮助企业拦截恶意代码、防止保密信息泄露并执行互联网使用和安全策略。

拥有15年的互联网经验，没有哪家公司能像Websense那样了解Web。Websense对Web 2.0世界内外部信息活动拥有前所未有的可视性以及下列知识：

- 哪些人有得到授权可访问网站、内容及应用程序
- 哪些数据必须加以保护以免泄露
- 用户可从哪里上网，敏感数据可从哪里发送
- 敏感数据可以哪种方式进行交流，在线资源可通过哪种方式使用

Websense 通过采用ThreatSeeker Network方式为用户提供了无以伦比的保护。ThreatSeeker Network 是Websense Web 、数据和电子邮件安全防护解决方案的技术基础，通过提供实时的信誉分析、扩展的行为分析以及真正的数据识别，所提供智能可作为Essential Information Protection™ （信息保护）的基础。

Websense ThreatSeeker Network通过采用超过5000万个实时数据采集系统，每天可分析10亿条内容、超过1亿个站点，每小时可为超过200万个域、网络、IP地址和主机分配信誉度、对近1000万封电子邮件进行不必要内容和恶意代码扫描。

欲了解有关Essential Information Protection （关键信息保护）、ThreatSeeker Network和Websense解决方案整体线路的更多内容，请访问www.websense.com。采用Websense，您将可尽情享用 Web 2.0。

欲知所有**Websense**产品的免费评估内容或是观看我们的在线演示，请访问 **www.websense.com/evaluations**