



关键信息保护基本指南



Websense

ThreatSeeker Network

Websense ThreatSeeker Network™是 Websense Web、数据和邮件安全解决方案的技术基础，通过实时的信誉分析、扩展的行为分析以及真正的数据识别，从而提供了关键信息保护

(Essential Information Protection) 的智能基础。这种内容智能对于所有 Websense 安全解决方案都极为重要，为客户提供了全面、最新的不必要内容和恶意威胁防护。

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10亿份内容：

- 应用大范围的专利系列数据识别工具和内容分类工具，包括二元分析、启发式、图像分析、词汇分析、统计分析、信誉度、自然语言处理和数据指纹。
- 每天分析超过1亿个Web站点
- 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

高回报+高风险是在Web 2.0世界开展业务的现状

朝九晚五的工作方式已然成为了过去；现在只要有机会，业务可随时随地全天候展开。

要想进行竞争，企业所需的不仅仅是即时互联网连接，同时还需要确保作为企业生命力的关键信息即便横跨各种通信信道仍有受到保护。

不论何时何地只要需要即可使用互联网来获取并交流信息是企业对员工的期望。而如何让员工在不损及企业安全、违背可接受使用策略（AUP）以及危及敏感数据的前提下充分利用互联网巨大能量则是企业所面临的问题。

这个问题给IT机构造成了很大负担。他们必须找到不但能够最小化数据泄露并防止不适当和恶意内容访问，而且还不会损及互联网允许的协作性、公开性和连接性的解决方案；他们必须创建并执行可在保护关键信息的同时简单透明地支持、保护和增强生产力的策略。

根本性问题在于：**各机构如何能保持安全和高效，同时还能发挥出互联网的所有潜力。**

为什么目前安全产品不能解决这一问题

如防病毒、防火墙、入侵防御系统等传统安全产品并不能满足这种需要。这些解决方案一般是基于“好”或“坏”的二元判定方式来进行信息拦截，并不能动态管理不断变化的内容及上下文。由于Web 2.0世界中内容和风险像每家机构一样都是动态且独立的，因此这种二元方式在Web 2.0世界里并不起作用。

即便是最精密的传统安全防护套件也不能有效管理这些动态环境和企业特定环境中数据的通信和交流。

Websense解决方案应能够知道哪些人、哪些信息、以哪种方式和到哪里

Websense® 关键信息保护通过有效管理企业关键信息中“**哪些人、哪些信息、以哪种方式、到哪里**”等内容，从而提供了集成式威胁防护和强有力的基于策略的企业敏感数据控制。

由于业务的开展有赖于Web，因此各企业如不能了解下列内容，那么在Web 2.0世界里他们可能就不再具有可靠的效率、竞争力和安全性：

- **哪些人**拥有信息资产和互联网访问权
- **哪些信息**是关键信息
- 信息能以**哪种方式**进行交流
- 允许用户和数据安全发送到**哪里**

单点安全解决方案只可以有效管理上述的其中两个方面—**哪些信息**和**到哪里**，而唯有Websense可了解并管理到所有上述四个方面。



唯有Websense集成了功能强大的Web安全、数据安全和邮件安全解决方案，可保护关键信息并增强生产力，同时还可放心地允许Web 2.0资源的使用。

Websense解决方案通过共同协作，可提供对下列内容的完整可视性和控制能力：

- **哪些人**有得到授权，可访问Web站点、信息及应用程序
- **哪些信息**是敏感信息，必须加以保护
- 信息能够**以哪种方式**进行交流
- 信息能够被**发送到哪里**

IT机构现在能够尽情享受Web 2.0。员工能够随时随地上网保证了工作效率，从而不仅帮助企业实现了互联网连接的所有潜力，同时还将由于人为错误和恶意攻击所导致的数据泄漏风险降至最低。

Websense Web 安全解决方案

Websense Web 安全解决方案通过帮助管理互联网资源的使用来增强员工生产力并拦截各种基于Web的威胁，从而在保护关键数据和生产力的同时还可帮助IT机构尽情享受各种新的Web技术。

Websense Web 安全解决方案包括：

- **Websense Web 安全网关 (WSG)：**有效安全防护Web流量，同时还可支持具有恶意软件和威胁实时分析与即时分类功能的最新基于Web的工具和应用程序
- **Websense Web 安全：**完整的Web过滤、Web信誉以及前瞻性已知和新兴威胁防护
- **Websense Web 过滤：**业界使用最广泛的Web过滤解决方案，拥有无以伦比的准确性、灵活性和企业可扩展性
- **Websense Express：**易于管理且高度有效的Web过滤工具，适用于中小企业
- **Websense Hosted Web Security：**互联网级Web托管式安全防护—无需任何前置式部署

您正面临的五大威胁

据IDC报告指出，因疏忽导致的数据泄露已被列入企业网络安全最大威胁名单，同时恶意代码、垃圾邮件、来自员工或商业合作伙伴的数据窃取以及黑客行为均榜上有名。

当今的安全威胁普遍存在两种特征：针对企业的敏感数据，使用互联网作为攻击媒介。纳入电子邮件、Web和应用程序的跨渠道威胁融合与动态互联网的结合使得有限的单点解决方案不能实时地对威胁作出准确检测和响应。



企业联系方式:

北京总部
地址: 北京市海淀区大钟寺东路9号京仪科技大厦B座三层
Tel: 010-58844000
Fax: 010-58844032
www.websense.com.cn

上海办事处
地址: 上海市黄浦区延安路550号海洋大厦2308室
Tel: 021-63225616
Fax: 021-63609015
www.websense.com.cn

广州办事处
地址: 广州市环市东路368号广州花园酒店花园大厦1038室
Tel: 020-83876956
Fax: 020-83876823
www.websense.com.cn

Websense 数据安全解决方案

Websense 数据安全解决方案可发现整个企业网络的关键信息, 监控这类信息的使用并防止这类信息的泄露。

- **Websense Data Security Suite:** 遍及静态数据、动态数据、使用中数据的全面安全防护, 可改善业务流程并有效管理风险和法规遵从。

Websense Data Security Suite包括:

- **Websense Data Discover (数据发现):** 识别网络和个别端点上静态数据、风险数据
- **Websense Data Monitor (数据监控):** 通过目的地上下文, 横跨所有业务渠道地识别动态数据
- **Websense Data Protect (数据保护):** 防止内外部数据泄漏
- **Websense Data Endpoint (数据端点):** 防止端点数据泄漏, 不论用户是否在线

Websense 邮件安全解决方案

Websense 邮件安全解决方案拦截垃圾邮件、病毒和出站数据泄漏, 帮助各企业执行企业管治策略并保障宝贵的IT资源。

Websense 邮件安全解决方案包括:

- **Websense RiskFilter:** 全面的邮件安全防护, 可管理进出的电子邮件威胁
- **Websense Hosted Email Security:** 互联网级托管式消息安全防护, 无需任何前置式部署

客户还可以选择通过结合使用托管式和前置式解决方案实现分层式保护的混搭解决方案。

尽情享用Websense

拥有15年的互联网经验, 没有哪家公司能像Websense那样了解Web及其风险性, Websense Web、数据和邮件安全产品通过共同协作, 为客户提供了一款以数据为中心的安全解决方案, 使得企业能够在保护好其最关键数据资产的同时放心地利用互联网和Web 2.0的所有优势。

Websense拥有前所未有的对Web 2.0世界内外部信息活动的可视性。作为整合Web、数据和邮件安全领域的领导者, Websense为世界范围5万多家机构和4200多万人员提供了关键信息保护。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。

欲了解有关关键信息保护和Websense解决方案整体线路的更多信息, 请访问 www.websense.com.cn。