

websense[®]
ESSENTIAL INFORMATION PROTECTION™



安全无边界 防护无止境

Websense TRITON™ 解决方案帮助企业实现现代安全保护

Web 2.0 工作平台： 新的机遇，新的风险

Web技术应用的兴起正在重塑现代企业。诸如 SalesForce.com 和 Workday 等功能强大且基于云平台的业务工具提供了创建、共享和管理信息的新方法。Google Docs 和 Zoho 等 Web 2.0 应用程序已经改变了企业的桌面系统，同时博客、维基和社交型网络站点提供了革命性的协同运作功能。

这些创新使新的无国界企业与以往相比更加快速灵活，同时反应速度更为敏捷。然而，它们仍然会面临新的安全风险。

构建于动态 Web 2.0 内容（包括当今大多数顶级在线目的地）之上的站点特别容易受到侵略性强且移动迅速的安全威胁。与 LinkedIn 和 Facebook 等社交型网络站点合作的销售人员可能会遇到基于脚本的攻击，这类攻击的目的就是传播恶意软件。网络诈骗者针对可执行代码利用复杂的“鱼叉式网络钓鱼”技术实施诈骗攻击。员工可能会看到不正确的内容或发布机密的业务数据，从而造成严重的责任和管制风险。

传统的安全解决方案无法处理这些威胁。当 Web 和电子邮件攻击同时出现时，就很容易避开单独的防恶意软件工具。基于 URL 过滤和信誉的工具可以捕捉到传统形式的安全威胁，但在识别与动态在线内容相关的威胁或针对合法 Web 2.0 站点的攻击方面速度较慢且不够灵敏。所有以点为基础的安全解决方案都会留下攻击者能够找到并进行攻击的漏洞。

企业必须同时考虑到与传统点式安全解决方案相关的成本。重复的产品、多个供应商以及多余的管理和报告系统都会在降低投资回报率的同时增加拥有成本。应对不断变化和快速发展的安全威胁需要投入额外的资金以用于软件、硬件和基础设施，所有这些都会增加成本和复杂性。由此得来的杂乱安全解决方案不但没有显著改善企业的总体安全，反而添加了额外的管理和集成困难。

一个完整统一的集成安全解决方案是可供摆脱此窘境的唯一解决方法。此解决方案将使用新的通信和协作工具来解决 Web 和电子邮件安全威胁，降低由于外部攻击和内部泄露而丢失宝贵业务数据的风险。同时，它还将消除部署、管理和维护多种传统安全产品的复杂程度。

综上所述，这款统一内容安全解决方案将以较低的总拥有成本 (TCO) 提供针对现代威胁的更好保护。它能够在不必牺牲安全性的前提下实现创新。



TRITON™

提供现代安全

通过 Websense TruContent™ 智能 - 首个也是唯一一个统一内容可视性并在数据进出组织时分析到数据级别的系统。组织能够阻止动态入站 Internet 威胁，控制未经授权的内容，确保生产效率，并有效防止在关键信息交换（包括 Web 和电子邮件）通道上发生出站数据丢失。

降低安全成本

通过提供业内首个用于网络内容安全技术、安全即服务 (SaaS) 以及 Websense TruHybrid™ 部署功能的统一入站和出站管理、报告和部署模式达到降低安全成本的目的。这样组织就可以在降低管理不同系统和部署方法的复杂性、开销和成本的同时，增加覆盖范围和部署的灵活性。



TRITON 能够以最低的总拥有成本提供针对现代威胁的最佳保护。

解决方案： 统一内容安全

业内首个统一内容安全解决方案

Websense® TRITON™ 是业内首个且唯一的统一内容安全解决方案，以最低的总拥有成本提供对入站威胁和出站风险的最佳现代安全防护。即便企业没有基础架构，且用户、资料及应用程序皆移至网络，Websense 仍然可以确保现代企业的安全。

借助 Websense TRITON，组织可以：

获得最佳的现代的安全

- 可帮助充分利用 Facebook、LinkedIn、Twitter 等新型通信、协作和社交网络工具及其他基于云平台的服务所带来的便利，能够消除来自恶意软件的威胁、抵挡各种能够避开防病毒软件的新型 Web 攻击、过滤掉不正确的内容或避免机密数据丢失和泄漏。
- 确保能够安全使用安全即服务 (SaaS) 和在线应用程序，而不会失去数据可视性和对信息的控制能力。
- 防范各种利用电子邮件和 Web 来危害用户、感染系统或盗取信息的混合式攻击。

实现最低的总拥有成本

- 将 Web、电子邮件、应用程序控制和数据泄漏防护的管理整合到一个统一的控制台以确保整个组织的安全。
- 合并安全应用程序的基础设施，并使用安全即服务 (SaaS) 来降低成本和复杂性，同时扩展覆盖范围和可视性。
- 通过一个管理和报告控制台对移动员工、分布式站点和中心站点实现持久控制。

Websense TRITON 是业界首个唯一能够提供真正统一内容安全的解决方案，旨在降低部署和管理的成本，同时提供业内领先的安全保护。该 Websense 解决方案包括统一策略管理，可用于 Web 安全、电子邮件安全和数据泄漏防护基于云平台的边界(on-premise)部署。其混合式部署架构可覆盖全球企业，将企业总部的高性能应用程序与分支机构和远程办公室的安全即服务 (SaaS) 结合起来。

Websense TRITON 提供多种独特功能:

快速灵活、混合部署的架构使企业能够像保护公司总部一样高效地保护远程办公室和移动员工。通过混合式部署：

- 安全管理员可使用一个单独的统一的界面来设置策略。
- 网络管理员可部署具备成本效益的、基于云平台的网络基础设施。
- IT 主管能够以较低的总拥有成本管理风险并实现更高的安全覆盖范围。

完全可扩展的嵌入式数据泄漏防护解决方案，将企业级出站内容检查与业内领先的入站 Web 及电子邮件安全解决方案结合起来。此方法与完整的数据泄漏防护工具相结合可提供细致深入的内容控制功能，并能集成到单一或已整合的 Web、电子邮件解决方案中。通过嵌入式数据丢失防护：

- 安全管理员可执行单独的统一内容安全架构。
- 网络管理员可避免耗费大量资金升级基础设施的必要。
- IT 主管可省去因多供应商和解决方案引发的成本和复杂性。

统一的策略管理和报告，与多供应商点式解决方案相比，可提供更高级的控制和灵活性。单独的管理界面可控制整个公司的 **Web**、电子邮件和数据安全策略，同时高级、可完全自定义的报告工具使组织对其安全操作具有可视性。通过统一策略管理和报告：

- 网络管理员能够查看公司的基础设施使用情况。
- 安全管理员可提高策略定义和管理流程的效率。
- IT 主管可获得实时工具来监控关键安全指标、确定趋势、以及强行定制合规方向。

TRITON 架构： 快速灵活，功能强大

TRITON 将业内领先的 Web、电子邮件和数据泄漏防护 (DLP) 安全技术合并为一个统一的内容安全解决方案，将集成的架构与异常强大的功能与灵活性结合到一起。随之得到的 Websense 技术组合将提供一系列独特且强大的连锁安全功能。

统一内容分析

Websense TRITON 高级分类引擎 (ACE) 为 TRITON 解决方案提供实时威胁分析基础设施。ACE 由 Websense ThreatSeeker® Network 支持，结合了包括 URL 过滤、防病毒、信誉服务、数据指纹识别等在内的多种分析方法，可对传入和传出的内容进行动态分类。

ACE 通过执行多点分析来评估用户、Web 站点、脚本及可执行代码的意图，而不是依赖旧版文件和受数据库驱动的检测方法。例如，如果一家银行站点以一种类似基于脚本的攻击方式植入 Javascript，ACE 将立即识别出此潜在的恶意活动并进行阻止。



“Websense 当前具备的所有功能和以套件为方向的产品战略使其成为内容安全套件市场的领头羊。”

来源于独立报告：

“The Forrester Wave™: 内容安全套件, Q2 2009”,

Forrester Research, Inc.,
2009 年 4 月



Websense TruHybrid 部署

ThreatSeeker Network 是一个全球网络，通过使用高级实时信誉分析和行为分析技术来分析潜在的安全威胁。它会将最新发现的安全威胁反馈给 ACE，后者是 Websense Web、电子邮件和 DLP 解决方案的一部分。

通过部署统一内容分析模型，无论何处出现攻击，Websense 都能对这些混合式新兴威胁施行实时保护。客户不必耗费大量资金和精力部署点式安全解决方案，且能够获得增强型管制功能，同时享用基于 Web 的全新通信和协作技术所具备的功能。

统一平台

现代企业网络技术设施的覆盖范围远远超过某个单一位置；它必须涵盖分部办公室和移动员工。Websense 凭借集成了基于云平台 and 边界解决方案(on-premise)交付平台的混合式解决方案来应对此挑战。公司可根据需要，自由选择单一的平台，或混合使用这两种平台。在此过程中，此统一平台使管理员能够降低复杂性，充分利用现有基础设施，并省去管理开销 — 所有这一切都可以在降低总拥有成本 (TCO) 的情况下实现。

Websense V-Series™ 应用程序 - 简单可扩展，功能强大

V-Series 应用程序融合了独特的灵活性、性能和简易性。它能够帮助 Websense 客户显著减少部署时间并降低运营成本，同时还能进行高度扩展，甚至连最大的企业环境也能支持。V-Series 应用程序可与 Websense 安全即服务 (SaaS) 平台无缝集成，为客户提供部署和管理内容安全解决方案的另一选择。

安全即服务 - 快速，简单，高效

Websense SaaS 提供部署 Websense 产品的快捷途径。SaaS 将所有安全检查、实施和管理流程从客户位置转移到“云平台”中的 10 处全球可用数据中心。客户不仅可摆脱部署和升级边界解决方案(on-premise)硬件的负担，还能获得该业内领先的内容安全解决方案的所有好处。



安全启用企业

如今，有越来越多的公司希望借助动态 Web 2.0 技术赢得一定的竞争地位，它们的安全解决方案也必须迎接新的挑战。而提供业内首个且唯一的统一内容安全解决方案的 Websense 就能满足这一要求。

在 Websense 的帮助下，组织可构建出一个完善的安全基础设施，提供针对 Web、电子邮件和数据安全威胁的全面保护。组织可以将面临安全风险的可能性降至最低、最大化生产效率并不断创新 - 所有这些都可以在无需其他成本、复杂性和管理开销的情况下实现。通过统一内容安全解决方案，企业可以跨越创新障碍，同时开发关键的新技术。

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

统一解决方案

TRITON 将 Websense Web、电子邮件和数据防护技术的管理和报告功能整合为一个单独界面，提供更为强大的可视性、控制和管理功能。通过 Websense TRITON 控制台，用户可以从一个基于 Web 的集中式管理程序设置策略、管理事件、运行报告和执行管理任务。

Web 安全

Websense Web Security Gateway 检查入站和出站内容，保护企业不受到动态 Web 恶意软件的危害，避免重要数据丢失，并提高员工生产效率。TruHybrid™ 部署支持边界解决方案(on-premise)和 安全既服务 (SaaS)，同时可通过单独的策略和报告基础设施管理整个环境。与其他方法不同，Websense 客户可自由选择适合于他们独特运行要求的部署选项，而无需被迫管理多个系统或处理多个供应商。

Websense Web Security Gateway 可部署为预置软件、Websense V-Series 应用程序、SaaS 或进行混合式部署。

电子邮件安全

借助 Websense 电子邮件安全解决方案，客户能够利用值得信赖的 Essential Information Protection™ 实施关键业务安全，并开发整合式安全战略。

Websense Email Security 可用于防范 Web 和电子邮件集中威胁，这些威胁包括避免数据丢失和违反法规。Websense Email Security 独树一帜，融合了 Websense ThreatSeeker Network 的智能，提供电子邮件合规性与安全。

Websense Email Security 可部署为边界解决方案(on-premise)软件、基于云平台和安全即服务 (SaaS) 的平台或作为混合式部署选项。

Websense 数据泄漏防护

Websense 提供业内领先的数据泄漏防护技术，旨在识别、监控和保护关键数据。利用 Websense Web 安全和数据泄漏防护 (DLP) 技术提供的统一内容分析功能，Websense DLP 解决方案能够准确防止数据丢失，确保业务流程安全，并管理合规性和风险。

Websense 利用模块化方法抵挡数据泄漏的威胁。其解决方案提供无与伦比的可见性，能够查看发送敏感数据的人员；所发送数据的类型；以及此数据的发送目的地。与其他竞争解决方案相比，Websense 数据泄漏防护解决方案可赋予组织以较低的成本及复杂性解决 DLP 问题的能力。

Websense 是首个且唯一提供完整内容安全平台的公司，该平台将所有这些元素集中到一个完全集成的解决方案中。与依赖冗繁的多供应商管理工具相比，统一解决方案可确保策略定义和实施的一致性，允许管理员设想满足组织特定需求的安全行为，减少复杂性和管理开销且明显节省成本。

查看 Websense 所有产品的相关评论或观看 在线演示，请访问 www.websense.com/evaluations.