卡巴斯基网络安全解决方案 — 协作服务器

协作平台的数据保护和控制，包括 SharePoint 服务器集群。

分享文件与信息的平台也为危险的恶意软件和其他 IT 威胁提供了一个理想的快速传播系统。

为营造一个安全且流畅的共享工作环境，卡巴斯基实验室专门开发了一种易于管理，且能够实时防护恶意软件攻击以及防止 SharePoint 或其他协作平台上机密数据泄露的安全解决方案。

- 一流的反恶意软件引擎
- 机密数据“搜索与保护”
- 数据访问控制
- 基于云的实时保护——卡巴斯基网络安全组件
- 文件与内容过滤
- 反钓鱼保护
- 备份与存储
- 集中化的灵活管理
- 直观的管理控制平台

亮点

充分保障您的 SharePoint 平台。

如果您正在使用 Microsoft SharePoint 服务器，您必然了解端点保护解决方案并不适用，因为所有内容都储存在 SQL 数据库中。卡巴斯基网络安全解决方案 – 协作服务器能够为 SharePoint 服务器集群与所有用户提供一流的反恶意软件保护。通过基于云的卡巴斯基安全网络组件提供针对已知和未知威胁的强大防御，同时反网络钓鱼技术可防止基于网络的威胁侵害协作数据。

防止机密数据泄露。

为控制并保护机密数据的传播，首先应对该数据进行鉴别。通过使用预安装或自定义目录和数据分类，卡巴斯基网络安全解决方案 – 协作服务器能够逐字逐词地检查 SharePoint 服务器中每个文档的敏感信息。个人数据与支付数据会受到特别的保护与控制，同时基于结构的搜索会找出敏感文件，例如客户数据库。

实施通讯策略。

内容及过滤功能有助于执行通讯策略和标准，识别并拦截不适当内容，同时防止存储不适当的文件和文件格式。

易于管理。

整个服务器集群的安全性保护可通过直观的单一控制面板实现集中、迅速且明确的管理，无需额外进行培训。

反病毒保护

• **实时扫描**——在文件上传或下载过程中实时扫描。
• **背景扫描**——利用最新的恶意软件签名对存储在服务器中的文件进行定期检查。
• **集成卡巴斯基安全网络组件**——提供基于云的实时保护防御零日威胁。
支持组织的通讯策略
• **文件过滤**——帮助您实施文件存储策略，降低存储设备需求。通过分析真正的文件格式，无论其扩展名是什么，确保用户无法使用违反安全策略的文件类型。
• **维客 / 博客保护**——保护所有 SharePoint 存储库，包括维客和博客。
• **内容过滤**——防止存储包含不适当内容的文件，不论文件为何种类型。根据关键词对每个文件内容进行分析。用户也可为内容过滤创建自己的自定义目录。

防止机密数据泄露

• **扫描文件机密信息**——卡巴斯基网络安全解决方案 – 协作服务器扫描所有从 SharePoint 服务器上下载的文件的机密信息。

该解决方案集成了可识别特定类型数据的模块，并且符合相关法律标准——例如，个人数据（依照 FZ-152《个人数据防护》法规）或 PCI DSS 标准数据《支付卡行业数据安全标准》。

针对内置、定期更新的主题目录，涵盖各种分类，包括“金融”、“行政文件”以及“侮辱和谩骂的语言”等和定制目录内数据进行扫描。

• **结构化的数据搜索**——如发现消息中含有特殊结构的信息，则将其作为潜在机密信息处理，从而确保敏感数据处于控制之中，例如复杂的客户数据库。

灵活管理

• **易于管理**——完整的服务器集群环境可通过单一的控制平台进行集中管理。直观的界面含有所有常用的管理模式。
• **单一控制面板**——布局清晰的控制面板可对当前产品状态、数据库版本和所有受保护服务器的授权许可状态进行实时访问。
• **备份修改文件**——如发生任何事件，可在必要时恢复原文件，修改后文件的详细备份信息可用于调查研究。
• **集成活动目录**——启用活动目录用户的认证。

系统要求

SharePoint 服务器

• Microsoft SharePoint 2010;
• Microsoft SharePoint 2013。

操作系统（用于安装解决方案）

针对 SharePoint Server 2010:
• Windows Server 2008 x64/ 2008 R2 / 2012 R2
针对 SharePoint Server 2013:
• Windows Server R2 x64 SP1 / 2012 x64 / 2012 R2

请访问 kaspersky.com.cn，了解完整系统要求。

如何购买

卡巴斯基网络安全解决方案 – 协作服务器可作为卡巴斯基网络安全解决方案 – 完整版的一部分或者作为可选解决方案单独购买。

请注意！本产品中防机密信息泄露组件单独销售。