卡巴斯基系统管理平台

通过集中化的 IT 管理工具增强安全性，同时降低复杂性。

流行应用程序中的无补丁漏洞是企业所面临的最大 IT 安全威胁之一。IT 技术的日益复杂更加剧了这一风险——如果管理员无法洞察企业网络系统中的资产，又谈何确保其安全?

通过必要的安全配置和管理任务，例如集中化和自动化的漏洞评估、补丁和更新发布、库存管理和应用程序发布等，IT 管理员不仅可节省时间，还能轻松实现最佳的安全性。

卡巴斯基系统管理平台有助于最大限度降低 IT 安全风险与复杂性，通过单一界面即可为管理者提供针对多个设备、应用程序和用户的完整实时的控制和管理。

- 漏洞评估和补丁管理
- 软、硬件库存
- 远程软件安装和故障排除，包括远程办公室覆盖
- 操作系统部署
- 安全信息与事件管理集成
- 基于角色的访问控制
- 集中管理

加强安全性

通过及时的补丁自动修补和更新，提升 IT 安全，减轻日常工作负担。自动发现漏洞，并进行优先处理，能够提高效率，减轻资源负担。独立测试 表明，卡巴斯基实验室能够在最短的时间内提供最全面的补丁自动修补和更新覆盖。

拥有完全可见的控制能力

通过单一控制台呈现完整的网络情况，管理员即可清晰了解所有应用程序和设备（包括客户设备）。如此一来便可集中控制用户和设备对公司数据和软件应用程序的访问，确保符合 IT 策略。

集中管理

卡巴斯基系统管理平台是卡巴斯基网络安全管理中心的一个管理组件。其通过中心控制台对各项功能进行评估和管理，并使用一致且直观的界面与指令实现日常 IT 工作的自动化。

1 卡巴斯实验室参与了由 AV-TEST GmBH 进行的补丁管理解决方案测试。（2013 年 7 月）

亮点

漏洞评估和补丁管理

软件自动扫描有助于快速实现漏洞检测、优先处理和修复。可在最短时间 内自动提供微软及非微软软件的补丁和更新，令管理员获知补丁安装状态。即使计算机关闭，也可利用网络唤醒功能将非关键修复推迟至几小时后。多点传送可将本地补丁和更新分发至远程办公室，降低宽带要求。

软、硬件库存

包括可移动设备在内的软、硬件自动发现、库存、通知和追踪功能使管理员详细了解公司网络中所有设备和资产。可监测外来设备，并提供互联网访问。授权许可控制则有助于了解节点数量和到期日。

灵活的操作系统和应用程序配置

从中央位置轻松创建、存储、复制和部署系统镜像。确保将无问题的系统交付给用户，保证最优安全设置，包括通过网络唤醒功能实现下班后部署。这种工具不仅实现了灵活性，还支持统一的可扩展固件接口。

软件分发

从单个控制台进行远程部署 / 更新。经卡巴斯基安全网络去人的百余种流行应用程序可自动完成安装和更新。完全支持远程故障排除，通过用户授权许可和对话记录 / 审查提升安全性，并且利用组播技术将本地软件分发至至远程办公室，以节省流量。

安全信息与事件的管理集成

直接报告并将事件转移至主要的安全信息与事件管理系统——IBM® QRadar® 和惠普 ArcSight。收集并分析日志及其他与安全相关的数据，将管理员的工作量和所使用的工具数量降至最低，同时简化企业级报告。

基于角色的访问控制

区分复杂网络中的管理角色和职责。根据角色和权限定制控制台视图。

集中管理

作为一个综合的管理控制台，卡巴斯基网络安全管理中心可通过单一界面管理公司网络中所有台式机、移动及虚拟终端系统的安全。

如何购买

作为卡巴斯基网络安全管理中心的一部分，卡巴斯基系统管理平台通过该中心进行管理，其适用于以下产品：

- **卡巴斯基网络安全解决方案 – 高级版**
- **卡巴斯基网络安全解决方案 – 完整版**

卡巴斯基系统管理平台可作为可选解决方案单独购买。请咨询您的本地经销商，了解更多详情。

2 卡巴斯实验室参与了由 AV-TEST GmBH 进行的补丁管理解决方案测试。（2013 年 7 月）

卡巴斯基系统管理平台 /0.3 版本 /2015 年 1 月 / 全球