

DATALOCKER

SAFECONSOLE集中管理

DataLocker的平台是管理数十万设备和终端的强大方式。

它使您可以随时随地轻松配置、保护、管理和审核加密的USB驱动器、USB端口和加密的虚拟驱动器。可在本地和云(SaaS)中部署，SafeConsole还具有可选的高级支持，以及包括单点登录等在内的企业功能。



增强便携式USB驱动器和
工作站USB端口的安全性



减少部署和管理安全USB
驱动器的时间



利用先进的审计和报告工
具，简化安全USB闪存盘的
跟踪和合规性



使用简单易用的设备和动
态安全姿势，使您的工作
人员保持高效工作

在云 (SAAS) 或本地部署*

SAFECONSOLE[®] DEVICE CONTROL

远程调配、配置、管理和审核您的加密USB驱动器，您还可以解锁DataLocker驱动器的强大安全功能。



SAFECONSOLE[®] ANTI-MALWARE

板载Trellix[®]防病毒软件始终处于开启状态，可扫描安全USB驱动器上的文件、删除或隔离恶意软件威胁，并将信息报告给SafeConsole。



Trellix[™]



SAFECONSOLE[®] SAFECRYPT

在加密的虚拟驱动器中存储和保护本地或云数据。



SAFECONSOLE[®] PORTBLOCKER

确保您的员工只使用经批准的USB设备，以防止恶意软件入侵或意外文件丢失。

*使用Windows安装程序，它可以从裸机，虚拟映像或任何云，包括私有云工作。



	BASIC	PROFESSIONAL	ENTERPRISE
密码策略配置和远程重置	√	√	√
自动盘点所有用户和设备的目录	√	√	√
设备操作和文件移动的审计跟踪	√	√	√
托管独立登录(K350和DL4FE)	√	√	√
远程引爆和出厂重置	√	√	√
审计模式(限制访问和禁用编辑)	√	√	√
远程将设备重新分配给新用户	√	√	√
写保护和文件限制	√	√	√
地理围栏(基于主机IP)	√	√	√
在Windows或Mac上管理	√	√	√
本地部署或云部署选项	√	√	√
板载设备Trellix®反恶意软件**	√	√	√
自动删除或移除设备上的恶意软件	√	√	√
实时报告受感染的文件和设备	√	√	√
确保只使用经批准的USB设备	√	√	√
在硬件层完全锁定USB端口	√	√	√
临时USB设备访问	√	√	√
报告未经批准的设备尝试	√	√	√
集中管理的SafeCrypt虚拟加密驱动器	√	√	√
锁定的驱动器与操作系统分离	√	√	√
ZoneBuilder: 安全自动登录和设备限制	√	√	√
高级和优先级支持 (最长2小时响应时间)	×	√	√
使用RMA进行高级硬件更换	×	√	√
REST API 访问	×	×	√
管理员单点登录 (SSO, SAML v2)	×	×	√
SIEM外部记录	×	×	√
安全的Active Directory用户同步 (LDAPs) (仅限本地服务器)	×	×	√
自定义地理服务器位置(合规性)	×	×	√



Ready to Get Started?

简单，智能远程USB设备和端口安全

从任何地方提供、保护、管理和审计加密的USB驱动器、USB端口和虚拟文件夹。

SafeConsole优势

- 增强便携式USB驱动器和工作站USB端口的安全性。
- 减少部署和管理安全USB驱动器的时间。
- 通过在虚拟驱动器中加密工作站数据来保密数据。
- 通过易于使用的设备和动态安全姿势，保持员工高效工作。

**需额外购买

