Kingston TECHNOLOGY

与 Matrix42 携手阐释和探索最优端点安全解决方案

MATRIX42

#KingstonIsWithYou

与 Matrix42 携手阐释和探索最优端点安全解决方案

简介

数据保护是当今企业、政府和个人的基本要求。

世界各地的数据泄露、黑客攻击和人为因素不断提醒威胁与风险的存在。数据泄露可能会让组织付出极其巨大的金钱和声誉代价。要满足高级网络安全与端点 DLP（数据丢失防护）策略的要求，都依赖于可靠、高效的存储和内存。

运用加密、快速存储和内存，结合最佳实践、标准和策略，算是迈出一大步。笔记本电脑和 USB 闪存盘丢失，会导致个人和公司容易暴露个人和隐私信息。金士顿提供威胁防护解决方案帮助降低风险，同时补充现有或开发中的安全计划。

与 Matrix42 携手阐释和探索最优端点安全解决方案

目录

这本篇幅短小的电子书将探讨端点解决方案，以及金士顿的加密 USB 闪存盘和定制计划与 Matrix42 EgoSecure Data Protection 软件如何帮助六个不同行业应对挑战，并向这些行业提供与业务需求相符的解决方案。

我们深入研究了这六个行业，并了解它们如何应对各自的端点安全挑战。

目录

第 1 章：行业用例
公共部门

背景：

在公共部门，USB 设备的使用非常普遍。例如，公共秩序办公室必须利用 USB 数据线，将数码相机中的违停和行政违法相关照片复制到当局系统中。警察局接收外部数据存储设备中的调查数据。这类数据需要被重写，未经授权严禁访问。

挑战：

由于 USB 设备需求旺盛，员工会定期申请 USB 闪存盘。出于安全考虑，组织必须禁止使用个人未经授权的数据存储设备。如果员工需要新的 USB 存储设备，组织应通过用户帮助台尽快提供设备，确保员工在工作中不受影响。需要指出的是，使用合适的 USB 设备不会引发安全问题。

解决方案：

通过结合设备控制、数据过滤和加密，有望实现以下情形：

通常会阻止在计算机端点使用未知设备。仅可使用数码相机等数据存储设备的特定功能，例如读取图像文件。写入操作通常会加密，并且只允许在授权的 USB 设备上执行。所有数据访问都记录在案。通过定制序列号和硬件 ID，可以简化授权设备的管理。因此，Matrix42 Service Management 让用户可以在自助门户申请个性化的金士顿科技 USB 闪存盘。经批准后，USB 设备自动获准在 EgoSecure Data Protection 中使用。

> “我们的员工很高兴看到，经过简短的审批流程，就可以轻松、快捷地获取新 USB 设备。对于金士顿科技的定制项目和易于管理的 Matrix42 服务管理和端点安全方案，我们非常满意。”
>
> **公共部门帮助台主管**

第 2 章：行业用例
医疗保健

背景：

外部存储设备仍是与员工和其他机构交换数据的常用工具。

例如，德国的医院必须向癌症登记中心 (Cancer Registry) 提供有关最新癌症病例及其发展过程的信息为了方便起见，医院常常利用移动数据存储设备传输这类数据。

医生们也喜欢在做报告时使用 USB 闪存盘携带研究数据等文档。

挑战：

病人数据非常敏感，决不能落入未经授权的人员之手。因此，需要提升和加强数据保护。如果数据载体丢失，从欧盟一般数据保护条例 (GDPR) 和病人健康角度看，这都将成为一个重大问题。由于这个原因，非常有必要对 USB 数据存储访问进行控制、监控和加密。

解决方案：

EgoSecure Data Protection 在一款解决方案中整合了各种不同的保护举措，例如访问控制、数据审计、过滤和加密。IT 管理员能够决定向哪些员工授予哪些设备的访问权限。利用序列号和硬件 ID 等特性可以实现例外。得益于金士顿科技的定制计划，组织可以定义这些身份标识，因此只需在 EgoSecure Data Protection 管理解决方案中配置一个值，即可确保员工只能使用经公司授权的设备。由于访问经过加密和监控，这可以最大限度减少管理工作量并提高数据安全性（GDPR、CCPA、HIPAA 等）。

> “我们之前已在使用金士顿加密 USB 闪存盘。现在，利用 EgoSecure Data Protection，我们还可以确保按照 EU-GDPR 实现病人数据传输的可追溯性。”
>
> **大学医院首席信息安全官**

第 3 章：行业用例
金融

背景：

银行需要满足各种不同的法规要求。其中一项要求是遵守 PCI-DSS（支付卡行业数据安全标准）。PCI-DSS 要求包括需要进行数据加密、漏洞分析和数据过滤。目标是最大限度减少甚至彻底杜绝威胁和 IT 安全隐患。

挑战：

端点存在许多 IT 安全方面的危险因素。员工必须日复一日地使用来自消费者和企业的支付卡信息，并处理来自金融机构的敏感数据，因此，若保护不当，来自云、电子邮件、USB 设备和网络的数据可能会遭到恶意软件的破坏，或数据意外落入第三方手中。根据 GDPR、PCI-DSS 或萨班斯-奥克斯利法案，这类事件可能对银行造成金融性威胁。此外，网络犯罪分子试图以各种方法影响或操控银行系统，并在这个过程中变得越来越高明。例如，在最近的一起 ATM 相关网络犯罪事件中，犯罪分子切断电源并用可引导 USB 设备启动系统，以窃取现金。

解决方案：

IT 系统必须部署多层保护举措。要实现这一点，可以利用应用程序控制、设备控制、异常检测、UEBA（用户和实体行为分析）、监控和全盘加密以及引导前身份验证。Matrix42 可在一个自动化的完整生态系统中实现多层保护，确保只有允许的应用程序和加密 USB 设备获准使用。此外，还会检测可疑或恶意活动，并自动采取进一步举措。在 USB 闪存盘使用方面，通过结合使用金士顿科技的定制 USB 闪存盘，有助于确保设备轻松包含在白名单中并以可追溯方式加密数据。这样一来，无需额外工作，即可大幅改善合规。

> “利用 EgoSecure Data Protection 和白名单功能，我们只允许金士顿加密 USB 闪存盘获得批准。我们使用个性化的硬件 ID 将金士顿加密 USB 闪存盘加入白名单，并禁用其他设备。这可以大幅减少管理工作量并提高安全性！”
>
> **金融公司 IT 经理**

第 4 章：行业用例
汽车

背景：

在汽车行业，USB 设备广泛应用于各个不同的领域。例如，研究数据存储在外部存储设备中，并在公司内的各个工程师之间交换。为了配置生产机器，文件从 IT 环境传输到操作技术 (OT) 环境。所有此类数据高度敏感，必须防范工业间谍和数据盗窃，否则积累的专门知识可能落入坏人之手。

挑战：

汽车行业需要遵守各种法规要求，例如 ENX TISAX 样机保护、ISO27001 与第三方连接和 GDPR。在 TISAX 中，Control 9.1、9.5 和 10.1 条款要求数据访问必须得到控制、监控、过滤和加密。在汽车公司的各个方面，还应按照 GDPR 和 ISO27001 等其他法规要求执行这些举措。

解决方案：

金士顿科技的加密 USB 闪存盘利用基于硬件的加密技术保护数据。这些设备可以获取个性化的序列号和硬件 ID，并可在 EgoSecure Data Protection 中使用以自动加入特定数据用途的白名单。此外，还可以监控和分析数据移动情况，确定是否存在任何可疑活动。

> “借助 Matrix42 和金士顿科技，我们能够满足 TISAX 要求，例如 Control 9.5（信息和应用程序访问）和 Control 10.1（加密），同时无需大幅改变用户行为。”
>
> **汽车供应商首席技术官**

第 5 章：行业用例
电信

背景：

电信提供商拥有大量关于客户的信息。这类信息高度敏感，特别是考虑到 GDPR。因此，应采取充分举措防范数据丢失和数据盗窃。

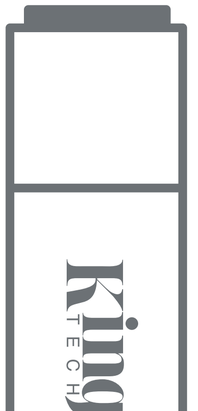
挑战：

电信公司的员工每天都在处理客户数据。多数数据存储在业务应用程序中。不过，客户合同甚至是数据库导出内容也有可能存储在相连的端点和外部设备上。用户常常使用外部设备进行数据交换。因此，检测并纠正或防范不正确的数据存储做法非常重要。

解决方案：

为了简化采购流程，可以通过 EgoSecure Data Protection 中的预定义白名单快捷采购包含个性化产品 ID 的金士顿科技加密 USB 闪存盘，并通过 Matrix42 Service Catalog 进行交付。对于可能包含敏感信息的数据存储和导出，可以利用基于“使用中数据”和“静态数据”扫描的深度内容检测自动识别和修复。还会集中记录数据移动情况。因此，在提出申请并获得批准后，员工可以迅速获得新的数据存储硬件。这可以确保符合 GDPR 法规要求。

> “得益于 Matrix42 的自助服务门户，我们的用户可以申请所需的存储介质。一旦订单获得批准和交付，设备就会获得 EgoSecure 设备控制的批准。Matrix42 与金士顿科技携手提高了我们公司的生产效率和安全性。”
>
> **电信提供商首席技术官**



第 6 章：行业用例
制造业

背景：

数字数据是未来的宝贵资产。制造业的宝贵数据包括生产计划、客户和供应商相关数据，以及公司专门知识。一旦此类数据丢失，不但可能会遭到 GDPR 法规极其严厉的惩罚，还会造成巨大的声誉问题。不幸的是，每天出租车、洗衣店、机场、火车站或公园停车场都有丢失的 USB 设备。

挑战：

存储设备常常包含高度敏感的数据，不幸的是，此类数据常常未经加密。此外，服务技术人员可能使用外部数据载体为生产机器安装更新。这些外部设备有可能会将恶意软件引入网络。

解决方案：

金士顿科技的加密 USB 闪存盘利用基于硬件的加密技术保护数据。这些设备可以获取个性化的序列号和硬件 ID，并可在 EgoSecure Data Protection 中使用以自动加入特定数据用途的白名单。此外，还可以监控和分析数据移动情况，确定是否存在任何可疑活动。

> “加密我们的生产数据对于防范数据盗窃非常重要。这些高度敏感的数据只能通过 EgoSecure Data Protection 的文件过滤存储在经过批准的金士顿加密 USB 闪存盘中。所有其他 USB 设备被禁止存储生产数据，对外部数据存储的写入访问由 EgoSecure 的即时加密和日志记录提供保护。”
>
> **制造业 IT 安全官**

第 7 章：金士顿科技与 Matrix42 解决方案

运用加密、快速存储和内存，结合最佳实践、标准和策略，算是迈出一大步。笔记本电脑和 USB 闪存盘丢失，会导致个人和公司容易暴露个人和隐私信息。金士顿科技提供威胁防护解决方案帮助降低风险，同时补充现有或开发中的安全计划。

金士顿科技加密 USB 闪存盘

金士顿科技提供硬件加密 USB 闪存盘，为组织防火墙之内和之外的移动数据提供数据保护解决方案。这些闪存盘旨在保护需要极高安全性的数据，帮助您满足特定的行业标准、指令和法规要求。它们符合 TAA 标准、通过 FIPS 认证，并提供最高 128GB 的存储容量，非常适合企业用户和政府部门。

安全定制计划

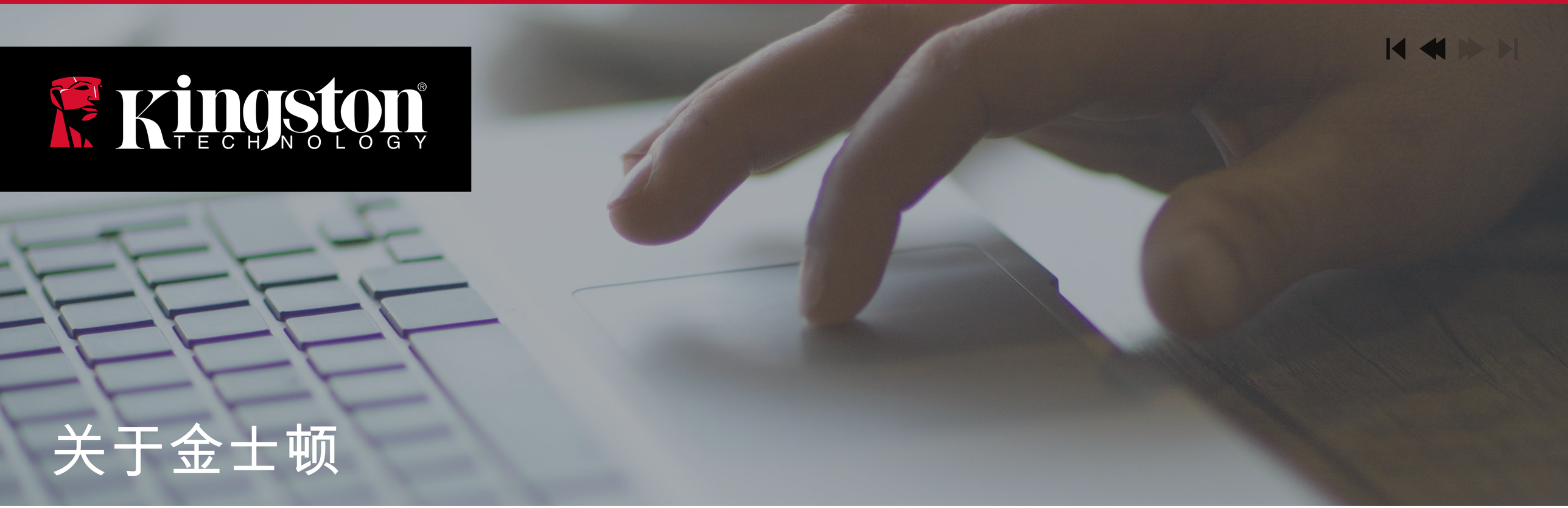
您可以通过多种方式定制金士顿科技的加密 USB 闪存盘，以满足贵公司需求。添加选中的功能，打造独一无二的必备闪存盘。通过您的首选经销商，金士顿科技让您轻松便捷地订购定制的加密 USB 闪存盘。金士顿科技加密 USB 产品线包括 DTVP30、DT4000G2 和 IKD300S 系列。此计划提供客户频繁请求的选项，包括序列号、双密码和定制徽标。此计划支持 50 件起定量和 25 件再订购量，可精确满足组织的需求。

Matrix42 EgoSecure Data Protection

Matrix42 EgoSecure Data Protection 为公司提供 360° 全方位安全管理，为设备、系统和数据提供预防和保护。从预防和检测到出现损害时的应对举措，此解决方案实现整个流程的自动化，不会导致生产效率下降。

总结

数据保护和网络安全可能让人感觉是一项艰巨的责任。数字工作要求出现巨大变化，员工能够自行决定何时、在哪里使用哪些设备进行工作。正确结合使用基于硬件的加密 USB 闪存盘和端点软件管理，有助于组织获得对组织内设备的控制权。从而降低数据泄露风险并支持组织持续的 GDPR 合规策略。



关于金士顿

凭借 30 多年的经验，金士顿科技积累了丰富知识，能够在不影响组织的情况下识别和消除端点安全挑战。

#KingstonIsWithYou