

数据丢失防护解决方案

数据安全的集中式管理

数据泄露对组织会构成严重影响，黑客造成的数据丢失或内部员工意外泄露的重要信息可能导致公司声誉受损、卷入数据泄露诉讼，甚至会出现业务流失。

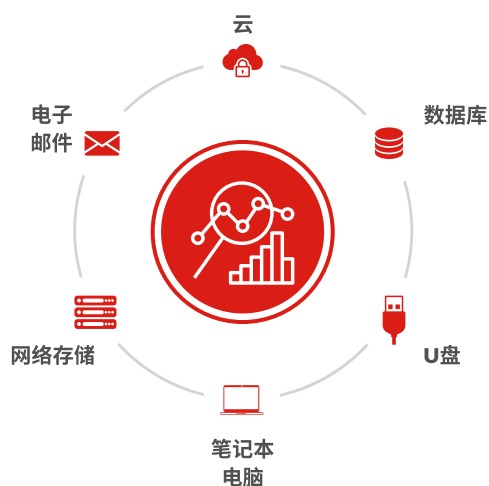
此外，合规性是全球企业需要完成的另一项重要课题，企业应该如何根据其每个员工的重要性和特性，来识别、跟踪和保护从数十个应用程序到数千个端点的所有机密数据？

借助HGC环电数据丢失防护解决方案，企业能够利用易于管理的设置来遵循公司政策，同时通过集中式管理跨员工和设备的数据进出，轻松符合全球合规性要求。

您的获益

- ✓ 获取员工、数据媒体、数据位置、传输方式和与员工个人访问级别相关联的操作之间数据可见性的鸟瞰图
- ✓ 帮助企业根据国际或国内要求履行合规性法规的大量策略模板
- ✓ 通过集中式管理应用程序进行轻松设置和数据控制
- ✓ 显示对组织风险状况的分析和微调安全策略建议的全面执行报告

在员工工作和数据所在的任何位置实现可见性和可控性



- 在任何位置发现数据
- 通过集成对数据进行分类（例如 Microsoft Azure 信息保护、Bolder James、Titus）
- 利用指纹识别等高级检测和取证
- 从可用于合规性和关键知识产权保护的策略模板中快速构建

- ✓ 高级检测
- ✓ 深入取证

- ✓ 发现与分类
- ✓ 以人为本的分析

- ✓ SaaS应用程序保护



利用强大的数据保护功能管理您的合规性风险

客户用例和方案：区域性银行

业务挑战：

- 如何防止敏感数据遭到故意或意外泄露，同时满足相关网络安全法规要求和合规性。
- 如何解决缺乏关于数据所在位置以及如何使用的信息问题。

解决方案：

根据独特的客户需求以多种方法建立全面的数据保护态势：

- 网络通道保护
- 电子邮件通道保护
- 端点通道保护

优势：

- 银行对 PCI（支付卡行业数据安全标准）和 PII（个人身份信息）相关数据保持强有力的控制。
- 从单一管理平台控制所有策略管理。
- 敏感数据在端点上分布情况的完全可见性。
- 识别和分类高风险用户的全面报告。



北京 010-85150531

上海 021-5237 6770

香港 852-2128 5484

广州 020-85561598

深圳 0755-861 53153



www.hgc-intl.com



ibmarketing@hgc-intl.com