IS Decisions 安全软件帮助企业达到支付卡行业数据安全标准

www.isdecisions.com

IS Decisions
Secure & Master your Windows® Infrastructure™

IS Decisions 安全软件帮助企业达到支付卡行业数据安全标准

PCI DSS 标准有什么要求？

简单地说，PCI DSS 要求最高级别的网络安全性。这一标准如今广泛应用于需要存储、管理、传输客户（或持卡人）个人数据的行业和领域。

施行严格的访问监控措施

为了保证关键数据只能被授权者访问，系统和程序需要从以下方面严格限制访问：

- 通过部署访问控制如 RBAC （基于角色的权限控制） 限制对持卡者的数据访问
- 或者只允许工作职责中有此项访问需求的个人进行访问
- 规范访问控制策略，指定享有访问特定数据权限的人员名单
- 拒绝所有未被授权用户对数据的访问

使用 **UserLock**（**保护网络访问**）和 **FileAudit**（**保护文件访问**），你可以立即识别任何不符合访问策略的访问尝试。

UserLock 能对基于 **Windows 的网络**和其中所有数据提供保护，依据**自定义的用户访问策略**通过用户登录限制和监控访问。在一个新颖的界面中，你可以轻松制定访问规则，依靠 UserLock 自动监控用户在何时何地访问了网络里面的资源，访问时长等。

FileAudit 可为 Windows 环境下的所有**文件服务器**提供保护，通过对所有文件和文件夹的访问（或访问尝试）进行监控、归档并发送报告。不时检查和记录关于读、写、删除访问的信息，以及关于文件所有权变更及修改权限的所有信息。IT 人员可以立即发现和跟踪任何不当访问。

为每一个用户提供一个独特的 ID

为每个用户分配一个独特的访问认证可以保证对于关键数据和系统的操作是由授权用户实施且是能被跟踪的。

登录是保护 Windows 网络数据的第一道防线。通过防止并行登录，我们可以确定访问只源自于一个人。防止并行登录，这样在同一时间段也只有一个人能够登录，从而阻止恶意用户盗取有效认证信息冒充用户登录。正因为这样，用户共享密码可能就会对自己的登录造成影响，所以也大大减少了用户随意共享密码的发生。

定期监控和测试网络

对于很多商场、地区办事处、公司总部或者通过远程访问，都要求对持卡人的数据和相关网络资源的访问进行跟踪和监控。而 **UserLock** 和 **FileAudit** 可提供大量的报告，在接受监管审计的时候能够帮助这些单位出示符合相关标准的证据。

通过制定和实施自定义的访问监控策略，你可以**限制和管理用户访问**。UserLock 对所有登录和会话事件持续监控，并实时提供带有详细的、图表化的仪表盘和警告的报告，并可根据会话类型（工作站、终端机、交互式设备、Wi-Fi 或者 VPN）跟踪授权用户，确保网络的安全性和可见性。

基于多种标准自定义的报告保证**审计的安全性和合规性**。通过集中并归档一个或多个 Windows 网络全部的文件访问事件，FileAudit 提供总是可见且可被搜索的审计安全保障。