网络安全：如何避免企业内部的恶意操作或操作疏忽带来的安全威胁

www.isdecisions.com

IS Decisions
Secure & Master your Windows® Infrastructure™

网络安全：如何避免企业内部的恶意操作或操作疏忽带来的安全威胁

来自企业内部的安全威胁

Clearswift 一则新的报告指出，在数据安全上，**58%的威胁来自于企业内部**（如现有员工、离职员工、合作伙伴等） 其中部分源于意外的行为操作，部分则是源于恶意。

无论是意外还是恶意，**网络安全**问题给企业带来的损失都是巨大的。一个内部人员的蓄意攻击可能会令企业损失 412000 美元，算下来一年的损失将近 1500 万美元。对于一些大型企业来说，这样的损失甚至超过 10 亿。

无论是处理疏忽的或是恶意的活动，都要涉及到**授权用户**。要避免来自内部人员的威胁，企业要意识到如何更好地管理网络访问，消除现存的**网络安全漏洞**。

在以前，相对高调的外部骇客的破坏行为让我们将注意力转向了他们，而很少去留意公司内部员工和内部程序。现在的情况却是，据最新的 **2013 网络安全调查**显示，三分之二的调查对象都认为企业内部的威胁才是目前网络安全最大的威胁——无论是意外的数据泄露还是恶意操作。

专注于保护用户访问 减少内部威胁

IT 团队应如何避免来自企业内部的恶意操作或操作疏忽带来的安全威胁呢？ 由著名网络安全管理软件供应商 **IS Decisions** 提供的 **UserLock** 从以下方面解决安全漏洞，帮助降低内部威胁，保护 **Windows** 和 **Active Directory** 中的敏感信息。

1. 密码盗取 - 阻止流氓用户无缝使用有效的认证信息

39%的恶意数据破坏是因为疏忽，包括对密码盗取的疏忽。**UserLock** 能够阻止恶意用户无缝使用有效认证。通过限制同一时间只有唯一的合法主人能够登录使得流氓用户无法使用有效密码再登录。通过这种**禁止并行登录**的方式能够有效保护数据访问。

另外，通过从地域位置（如工作站、IP 范围、部门、楼层、建筑物等）限制用户的个人访问，UserLock 能够保证未被授权的访问被阻止，即使认证是正确的。

2. 管理来自共享密码的威胁

尽管公众的密码保护意识不断提高，共享密码仍然是企业中存在的一个问题。上月发生在美国的病人病历安全被破坏的事件，就是合作商里的个人通过使用他人的密码、未经授权就访问了 1800 个病人的病历。

因 **UserLock** 阻止并行登录，用户共享密码给他人的情况大大减少，因为会影响到他们自己的访问。UserLock 为保护密码安全提供了动力，有助于保护企业的关键资产。

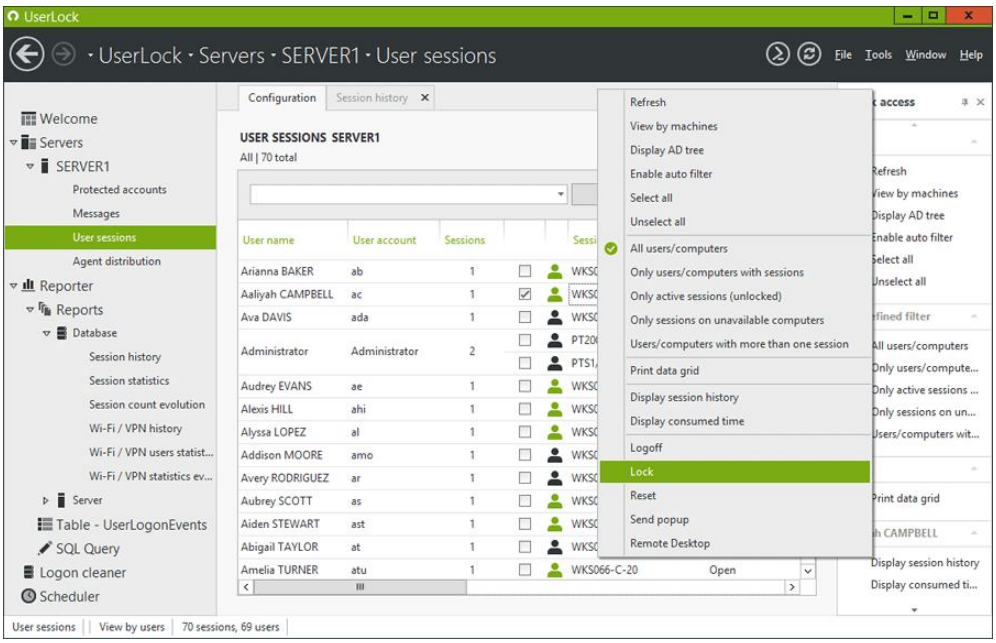
3. 确保对企业关键信息的所有访问都来自于单个用户

特定的事件需要与特定的人联系起来，以便问责。企业需要清楚知道谁正在网络上操作，他们正在做什么。

使用 **UserLock** 的**粒状规则**和策略来保护网络访问，在出现问题问责的时候用户就无从抵赖，UserLock 可自动识别每一个用户的每一项活动。

4. 对可疑或破坏性行为提供及时反馈

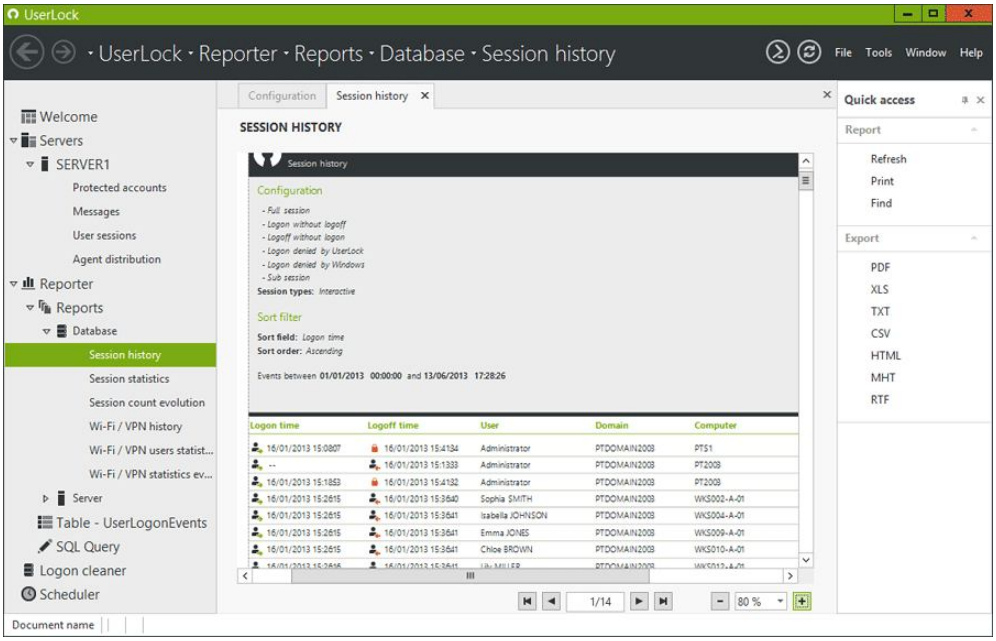
UserLock 赋予 IT 人员监控、记录及自动拦阻所有可疑会话的权利。并且，UserLock 能够积极主动地应对可疑或尝试破坏的用户，减少发生恶意事件的风险。一旦检测到任何可疑访问事件，**UserLock** 可提醒管理员，让 IT 人员在第一时间通过远程锁定、退出或重置适当会话来快速反应。



5. 对于任何 IT 安全漏洞 执行准确的 IT 取证

除了实时会话监控和监测，**UserLock** 在一个 **ODBC 数据库**（Access，SQL Server，Oracle，MySQL …）记录所有会话登录和锁定事件，为 IT 管理员提供问责证据、合法调查和内部趋势分析。

如果发生 IT 安全漏洞，UserLock 可以提供准确、详细的信息，如关于是谁在登录、从哪个系统进入、何时开始、持续多久等问题。



6. 培训员工的数据安全意识

员工需要明白**安全策略**和程序是怎样的，有哪些存在的必要性，以及使用了何种安全措施。掌握详情的员工是**网络安全防卫**的第二道防线。（禁止并行登录是第一道防线）

UserLock 允许企业在用户访问系统前发送一条自定义的提醒消息，提示相关法律和合同性后果，提醒员工不要进行网络犯罪，警惕他们不要有攻击企业网络的企图。