佰倬数安服务器版

（QDocSE v2.0.0）

简介

佰倬信息科技有限责任公司

2021 年 11 月

1 QDocSE v2.0.0介绍

QDocSE v2.0.0 版 代表了较早期版本在设计方面的重大进步。 这也代表了对它进行了重大的提高与改进。 因此，以下提供了更多详细信息，以帮助您了解 **QDocSE** 系统不同部分发生的变化。

我们将几个不同的 **QDocSE** 安全功能称为 守卫。 所有 守卫 都与 **QDocSE** 安全模块（Security Module (SM)）通信。 每个守卫 的简短描述如下。 这些守卫共同来保护静态数据、使用中的数据，限制程序对数据的访问、并验证程序和共享库、保护运行的程序免受修改和数据提取等提供全面的安全保护。

安全的最后一个防线是 **QDocSE** 的自我保护。 这是一组功能，因此获得管理权限的入侵者无法关闭、摧毁和或重新配置 **QDocSE**。 这些功能的副作用是它将安全性扩展到操作系统的其他部分，从而在整个操作系统范围内进行了安全性增强。

数据守卫(DG)

此 守卫 的主要目的是控制对保存在文件中的受保护数据的访问。 它与 安全守卫 SecurityGuard (SG) 和 QDocSE Security Module (SM) 结合使用。 在受保护文件列表被添加到配置文件中之后，根据对这些静态数据的保护配置在对这些文件进行加密的同时大大提高了安全性。

被保护的数据文件只能被授权的程序访问。 授权程序由 安全守卫 SecurityGuard (SG)处理（有关详细信息，请参见下一节）。 数据守卫 Data Guard(DG) 检查正常的文件访问权限，同时咨询 安全模块 Security Module (SM) 并询问 安全守卫 SecurityGuard (SG) 访问数据的程序是否经过验证。 如果所有检查都成功通过，则允许访问。 这种控制程序意味着勒索软件不能对数据文件进行双重加密，也不能泄露数据。 这种严格的访问控制串起了静态数据和使用中的数据的保护。

使用 **QDocSE** 加密文件意味着增强了对静态数据保护。 如果有人真的移除了磁盘，那么他们将无法访问明文数据。 只有经过授权和验证的程序才允许解密访问。 同时授权程序不需要关于被加密文件的任何额外知识，因此您不需要修改您的程序。

加密和解密由 数据守卫 Data Guard(DG) 处理。 每个客户都有一个唯一的密码学主密钥。 这允许企业或组织内部在运行 **QDocSE** 的不同计算机之间轻松共享文件。 因此即使在其他企业或组织安装了 **QDocSE**，但由于使用不同的主密钥因此也无法访问别家的这些被加密的文件。 “一文一密”作为增强手段，每个加密文件都有一个唯一的且独立的密钥，这样如果有人有计算能力来破解一个文件的密钥，由于密钥之间的互信息为“零”，因此其他文件仍然受到保护而不用担心被解密。

数据守卫 Data Guard(DG) 作为我们的文件系统 **DGFS** 的一部分。这意味着对文件访问的无缝、实时控制。 没有时间间隔或机会窗口。

数据守卫 Data Guard(DG) 提供的访问控制可防止典型的勒索软件攻击，因为黑客的加密工具无法访问这些文件。 同样，意图破坏或更改这些文件中数据的恶意软件也会被阻止。

安全守卫 (SG)

一旦启用 了 **QDocSE**，此 守卫负责检查程序及其共享的、可加载的库。 当配置生效后添加到授权程序列表的每个程序都有一个为其创建的签名。 并且该程序使用的每个共享库，以及这些共享库使用的共享库，都会创建一个签名。 这将创建一个综合目录，安全守卫 SecurityGuard (SG) 稍后将使用该目录来验证正在运行的程序。

有许多安全产品可以在定期扫描中计算磁盘上的程序签名。 但这为被劫持/利用的程序的留下了许多机会窗口 - 受到侧加载的影响。 安全守卫 SecurityGuard (SG) 是作为文件系统 SGFS 的一部分，它可以实时、无缝地监控磁盘上的程序和库。安全守卫 SecurityGuard (SG) 将立即知道磁盘上何时发生更改。 与 安全守卫 SecurityGuard (SG) 相关的命令甚至将“监视器”作为其名称的一部分。

安全守卫 SecurityGuard (SG) 通过在加载到内存中运行时确认程序和库的签名来提高安全性。 这样黑客就没有了机会窗口。 加载程序和共享库后，运行程序的安全性将进程守卫 ProcessGuard (PG) 提供（下一节将详细介绍）。

安全守卫 SecurityGuard (SG) 向 安全模块 Security Module (SM) 和 数据守卫 Data Guard(DG) 报告每个程序的有效性，以便访问受保护文件的权限仅授予经过授权、经过验证的程序。 安全守卫 SecurityGuard (SG) 以故障安全方式运行。 例如，如果入侵者替换了您的授权程序之一，则 安全守卫 SecurityGuard (SG) 会立即将该程序标记为无效。 即使在重新启动后，安全守卫 SecurityGuard (SG) 也知道该程序无效。 并且不允许无效程序访问受保护的数据文件。

目前 安全守卫 SecurityGuard (SG) 不会阻止管理员更改程序和共享库的文件。 如果发生此类更改（无论是谁做的），程序将被标记为无效，并且将拒绝访问受保护的数据。

管理员有正当理由更新程序。 要使这些更新或更改被识别为有效，需要 **QDocSE** 接受更改。 要接受更改，需要 **QDocSE** 处于提权模式，然后重新计算授权程序和共享库的签名。 有关签名重新验证的更多详细信息，请参阅命令 verify_monitored 和 monitor_update。

进程守卫 (PG)

该守卫负责保护正在运行的程序，以便无法提取或更改敏感数据，防止进行代码注入。无论哪个用户试图访问正在运行的程序都会阻止。只有授权访问受保护数据文件的程序才受进程守卫 ProcessGuard (PG) 保护。

例如 gdb 等保护程序尝试修改运行 **QDocSE** 授权程序时将不起作用。诸如 ps 之类的程序将继续工作，但有关运行授权程序的可用信息将非常有限。

进程守卫 ProcessGuard (PG)会询问 安全模块 Security Module (SM) 以了解哪些程序得到授权。然后，对每个授权进程的内存、可执行代码、堆栈、文件句柄等的访问仅限于进程本身，任何其他进程都将被拒绝访问。这有时会对未经授权的程序产生副作用，因为它们无法随意读取其他进程的内存，但安全是首要任务。

自我保护

以前入侵者专注于绕过、欺骗或躲藏安全程序的检测。然后入侵者意识到，如果他们有管理权限，他们可以关闭安全程序。即使外部监控通过在出现问题时提供的告警来保护这些安全程序，也存在时间延迟。另外，收到告警的管理员可能正忙于做其他事情，或者管理员可能正在家里睡觉。更糟糕的是，入侵者可能也破坏了外部监控工具！

正如《用户指南》前面提到的，我们的理念是，入侵者入侵了您的系统时，而不是他们试图入侵时。假设入侵者将被限制在一个没有特权的账户上是一厢情愿的想法。

因此，拥有 **QDocSE** 的每台主机都必须能够完全独立地保护您的数据。当然每个主机可以都有外部监控，但安全性需要全面和深入，这意味着每个安装有 QdocSE 的主机都需要防止入侵者禁用、欺骗或重新配置 **QDocSE** 本身的能力。

QDocSE 有多种自我保护技术，包括使用守卫。当 **QDocSE** 处于降权模式时，自我保护完全处于激活状态。处于降权模式意味着不能更改任何配置，不能被去挂载、不加载或禁用活动安全模块，也不能修改计算机系统其他关键部件。

安全不是静态设计，**QDocSE** 的自我保护也受此条件的影响。因此，当 **QDocSE** 新的更新可用时，您必须尽快安装它。

保护操作系统的关键部件

在不同的操作系统上，入侵者发现了绕开安全的新方法。虽然入侵者可能有直接攻击和/或禁用某些安全程序的方法，但有时攻击操作系统更容易、更快——为什么在不必要的情况下还要做更多的工作？

例如，一些攻击 Linux®系统的勒索软件团伙会修改 GRUB 文件并重新启动系统。添加的修改包括但不限于在引导过程中加密数据。这对勒索团伙来说是有效的，因为系统的所有资源都可用于其恶意的目的，没有安全程序处于活动状态，也没有人可以登录来停止此过程。**QDocSE** 保护 GRUB 文件（和其他系统文件）不被更改，甚至不被读取，除非在引导期间。这样一来，勒索团伙就不能通过 GRUB 文件更改来勒索您的操作系统——重新启动只不过是使用原始未修改的 GRUB（和其他）文件重新启动。

我们也为其他一些系统文件提供同样的保护。佰倬在未来的版本中将在这方面有更多的增强功能。

非法程序和 SO 文件

如上所述，在安全守卫 SecurityGuard (SG) 一节中，在加载程序时验证程序和共享对象（SOs）的签名。如果程序和/或一个或多个 SO 签名无效，则该程序被标记为无效–该程序仍将运行，但被拒绝访问所有受保护的数据文件。

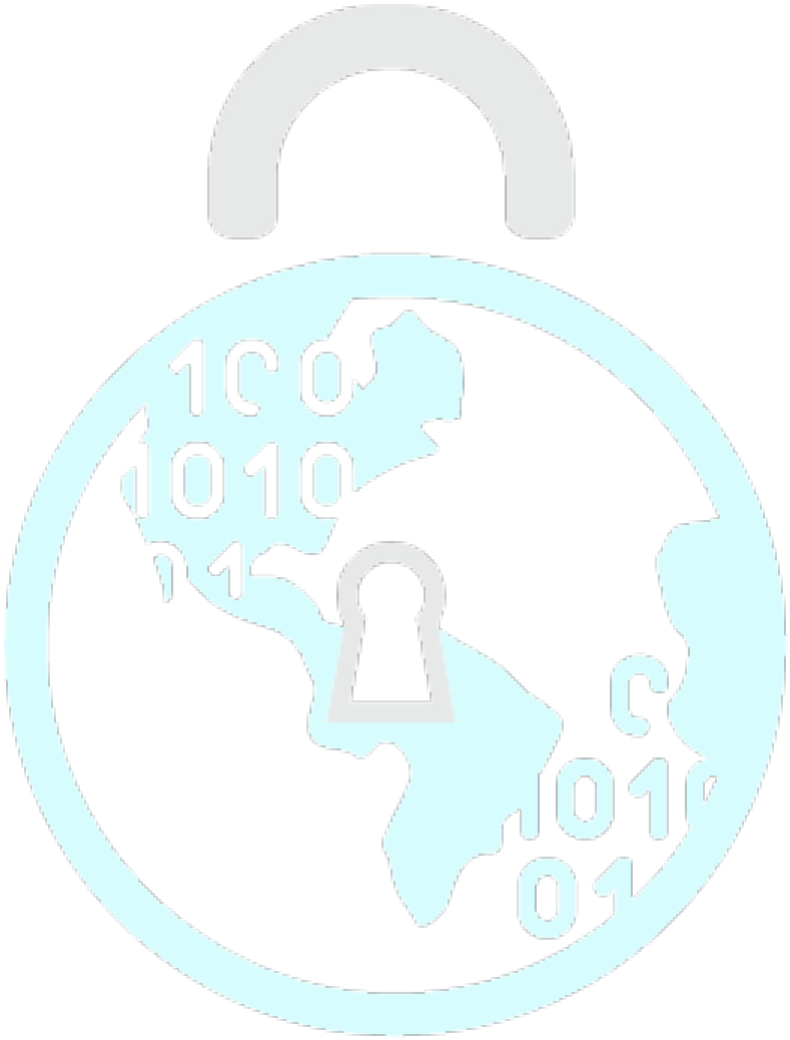
您可以使用 QDocSEConsole 实用程序的 view 和 verify_monitored 的命令进行查看。您可以使用 view 命令检查该程序是否在允许访问受保护数据文件的程序列表中。您可以使用 verify_monitored 命令显示哪些程序和/或 SOs 已更改签名。

如果程序不在授权列表中，则需要将 **QDocSE** 置于提权模式，以便使用 adjust 命令添加程序。

如果程序和/或一个或多个 SOs 的签名已更改，则可能存在安全问题。某些操作更改了程序或文件，从而产生了新的和不同的签名。安全守卫 SecurityGuard (SG) 不会对其进行验证。您需要开始调查，以确定更改是否合法和安全，或者更改是否意外且可能是恶意的。

如果确定更改有效且安全，则需要更新 **QDocSE** 认为有效的签名。别着急！如果您不想被欺骗或愚弄，进行双重检查确认和多次检查确认。

如果更改是意外的，则您的系统可能已被破坏。**QDocSE** 提供了自我保护的安全功能，这使得挖矿程序和 C&C 程序等恶意软件更难隐藏和更改系统。**QDocSE** 的设计和实现旨在继续保护您的数据，即使恶意软件入侵者已进入您的系统，但您仍然需要采取行动！关于您应该采取的操作的完整描述超出了本用户指南的范围。



2 联系我们

佰倬信息科技有限责任公司

地址：江苏省无锡市国金中心59楼（钟书路99号）

客服热线

客服：0510-85762088

传真：0510-85762588

技术支持

support@bicdroid.com

0510-85761176

销售与合作

business@bicdroid.com

0510-85767576