QDocument SE

设计说明书 V1.0

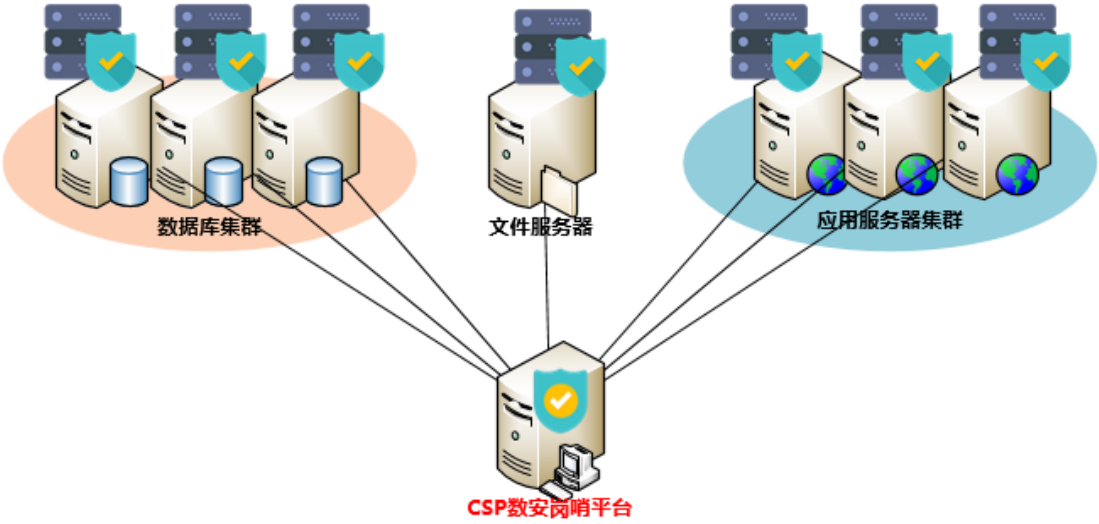
目录

一、概述

针对当前互联网时代各类诸如钓鱼攻击、勒索攻击、内部恶意人员攻击等愈演愈烈，而传统的网络安全方法和方案疲于应付恶报频传的情况，为了长期稳定、可信可靠地服务于客户，避免客户数据被窃取、泄露、破坏、和/或劫持，需要在稳定透明地支持服务器正常运转的条件下，对服务器数据进行全面彻底的保护和监控。

二、产品简介

QDocument 服务器版本 Server Edition （SE）是服务器数据安全领域最具技术创新和安全可靠的软件产品。该软件可以对数据加密保护，根据决定进程行为模式的要素（简称进程基因）决定进程是否有权访问被保护数据，实时监控服务器的被授权进程，并提供详细的访问报告，拒绝所有未获授权的进程，即时有效的保护服务器数据，防止数据泄漏，阻止已知或未知的攻击，如网络钓鱼、勒索软件等。



- 支持主流 Windows Server、CentOS等操作系统以及麒麟等国产操作系统；
- 支持主流的数据库系统；
- 支持主流的大数据系统；
- 支持保护除可执行程序外的任意类型的数据文件；
- 支持对文件、目录进行灵活保护操作；
- 支持两个工作状态：系统配置状态和保护工作进行状态；
- 支持即时退出系统配置状态而进入到保护工作进行状态；
- 在保护工作进行状态下，禁止任何人对系统配置进行修改；
- 支持根据需求，获得授权审批后，由保护工作进行状态切换到系统配置状态；
- 在系统配置状态下，根据需求调整可执行程序对被保护数据文件的访问权限（拒绝访问、授权访问）；
- 未授权的可执行程序在任何情况下都不能读写被保护的数据文件；
- 支持禁止操作系统用户及系统管理员使用未授权程序对被保护数据文件进行复制、移动、删除、或修改；
- 支持对被保护数据的所有访问操作进行监察和记录；
- 支持合法授权可执行程序产生的新数据也被自动保护起来；
- 支持配置中央岗哨平台，用于监控所有被保护服务器的数据保护的访问情况（数据访问授权、拒绝访问、保护、停止保护等），并且对被保护服务器的数据保护策略做中心配置；
- 支持通过中央岗哨平台对被保护服务器进行数据保护信息的收集、审核及日常管

理；

- 支持被保护文件在非易失存储器中以保护格式存储，从而自动实现静态数据保护；
- 支持自动地安全地在多个设备间共享被保护的数据，即可以简单地在多个设备上访问被保护的数据，从而使得服务系统的升级或维护不受数据保护的限制；
- 支持多级数据安全管理流程：将环境系统管理员、服务系统管理员、信息安全管理员的职责进行清晰划分，环境系统管理员负责服务运行环境系统的软硬件维护，信息安全管理员为所用信息安全负责。在本 QDocument SE 中，只有服务系统管理员在信息安全管理员的授权下才能取得被保护数据的访问权限和方法；

三、QDocument SE 专有技术

3.1、软件设计原则

（1）先进性

服务器数据保护的方案要立足于当今世界最先进的数据保护技术，根据进程基因决定进程的数据访问权限，为服务器数据提供防护各类已知或未知的外来恶意软件（如来自钓鱼攻击或勒索攻击的恶意软件）或内部恶意人员对数据的窃取、泄露、破坏、或劫持的可靠可信的解决方案。

（2）透明性

服务器数据保护的方案必须保证在对现行数据库服务器的正常运行逻辑和功能不带来任何干扰或修改的情况下提供对数据的保护。

（3）低资源消耗性

服务器数据保护的方案对被保护的数据库服务器的资源要求必须有严格的控制，例如对数据库吞吐量的影响必须低于5%。

（4）安全性

作为一个安全防护产品，这里的服务器数据保护的方法方案必须具有防卸载、

防关闭等自身保护功能；同时，服务器数据保护的方案必须包含安全有效的自身管理配置系统。由此，在自身保护功能和安全的自身管理配置功能的基础上，结合先进的数据保护技术，提供一个完备的服务器数据保护产品。

（5）可靠性

产品和技术方案在设计和实现的全过程中应有具体的措施来充分保证软件产品本身的可靠性，同时需要提供完整的可靠性测试报告。

3.2、QDocument SE 专有技术功能

3.2.1、QDocument SE 对静态数据保护

静态数据保护指对非易失性存储介质中的静态数据的保护，例如将数据转换为系统独特的不可破解的存储格式，它是任何数据保护系统的首要环节，将保证在非易失性存储介质由于种种可能而脱离数据保护系统控制后，其所存储的数据内容仍然安全而不会被窃取或泄露。由于服务器数据的高度敏感性和私密性，它对静态数据保护的需求非常关键。

3.2.1.1、静态存储格式转换

为防止因非易失性存储介质被盗窃或控制带来的数据泄露，QDocument SE 对被保护数据在非易失性存储介质上以非明文格式存储，而是作系统特有的加密格式转换。在没有相应保护系统软件合作的情况下，攻击者即使取得非易失性存储介质上的数据也无法知晓该数据的真实内容，即具有不可破解性。

QDocument SE 数据存储格式加密转换算法选用公开且标准化的算法。

3.2.1.2、来自信息缺失的数据的不可破解性

QDocument SE 转换结果具有来自信息缺失的不可破解性，即：

- 每次加密转换使用一个和被转换内容无关的一段独立信息（即密钥）；
- 该密钥信息不以任何形式被保存在非易失性存储介质中；

- 对于不同的数据文件，所使用的独立信息（密钥）不同；
- 对以上使用的独立信息（密钥），有安全且方便的自动管理系统；

3.2.2、QDocument SE 对外来恶意软件攻击的防护

由于目前网络安全技术的局限性，来自钓鱼攻击或勒索攻击的各种已知或未知的恶意软件，总是可能侵入到服务器系统中。QDocument SE 需要在假设外来恶意软件侵入到服务器系统内并且系统对恶意软件的性质种类等信息毫无了解的情况下，能保护数据不被恶意软件窃取、破坏、劫持及勒索。

3.2.2.1、功能描述

1. QDocument SE 在外来恶意软件侵入到服务器系统内时，保护关键数据不被恶意软件泄露、破坏或劫持；
2. QDocument SE 在服务器系统对侵入的恶意软件的性质种类等信息毫无了解的情况下，保护关键数据不被恶意软件泄露、破坏或劫持。
3. QDocument SE，在无法预知外来恶意软件的性质、种类、攻击方式、攻击时间的情况下，可阻止外来恶意软件对被保护的服务器数据的访问。具体地讲；QDocument SE 具有以下访问控制：

- 为所有被保护数据目标加注保护标识；
- 获取合法进程基因（即决定进程行为模式的要素，如二进制代码、运行参数、环境变量等）作为该进程的认证信息，建立合法进程名单；
- 对于任何一次数据访问操作提供如下访问控制：检查访问数据目标是否具有保护标识；如果该数据目标具有保护标识，检查访问进程的认证信息；
  - 当数据目标具有保护标识且访问进程的认证信息与合法进程名单中的一项匹配且时，授权该进程访问该数据目标的内容；
  - 当数据目标具有保护标识且访问进程的认证信息不与合法进程名单中任一项匹配时，拒绝该进程对该数据目标的访问；
- 当数据目标不具有保护标识时，跳过数据保护系统控制。

4. 对于被授权的访问进程，在其访问关键的数据库数据时在数据库查询层级上进一步作数据访问行为检测、分析和甄别，以防止恶意软件利用被授权的合法进程来攻击关键的数据库数据。

3.2.2.2、对钓鱼攻击的防护

QDocument SE 弥补了传统对钓鱼攻击防护方法的不足，在假设各类防火墙系统，防病毒软件或沙盒保护均失败的情况下，防止关键的数据库数据被钓鱼攻击侵害，即：

- 在操作系统的文件系统层进行保护，作严格的访问控制，只允许已知的被合法授权的进程从文件系统层访问数据库文件。如：

  a. 只允许 oracle.exe 访问 Oracle 数据文件。

  b. 只允许 sqlservr.exe 访问 MSSQL 数据文件。

  由此保护关键数据在钓鱼攻击发生时不会被泄露或损坏。

3.2.2.3、对勒索攻击的防护

QDocument SE 只允许已知的被合法授权的进程从文件系统层访问数据库文件，可以防护任何勒索软件，比如：

- 没有被任何防恶意软件系统记录上黑名单的勒索软件；
- 只进行简单的文件读写操作的勒索软件；
- 只加密关键的 Oracle 数据库数据文件和 MSSQL 数据库数据文件的勒索软件。

勒索软件可以是一个新编写的勒索软件模拟程序，该程序由于是新编写的，不会出现在任何黑名单中，同时该程序只进行最简单的文件读写操作，从而在行为分析层面具有很高的隐蔽性，这也是上述诸如Zemana Anti-malware 等防勒索软件在这个模拟程序攻击下失败的原因。

3.2.3、QDocument SE 对内部恶意攻击的防护

3.2.3.1、概述

对内部恶意攻击的防护困难通常在于无法甄别恶意人员，因此基于角色的访问控制无法做到有效的针对内部恶意攻击的防护。而 QDocument SE 的访问控制是基于进程的，可以有效的阻止内部恶意攻击。

3.2.3.2、功能描述

1. 对所有内部人员，无论是否是系统管理员，都只能通过 QDocument SE 中由其访问控制策略确定的授权进程才能访问被保护的数据。
2. QDocument SE 系统是被加密保护的，SE 的系统管理员和服务器的计算机系统管理员职责分开，只有 SE 的管理员在一定的安全操作流程下才可以修改其访问控制策略。
3. 安装中央岗哨平台后，中央岗哨平台的管理员对被保护服务器上的 QDocument SE 也有配置权限，但中央岗哨平台的管理员和计算机系统管理员的职责也是分离的，保证即便是拥有系统管理权限的恶意人员也无法窃取被保护数据。
4. 所有被保护数据的访问历史都被记录保存。

3.2.3.3、QDocument SE 的安全操作流程

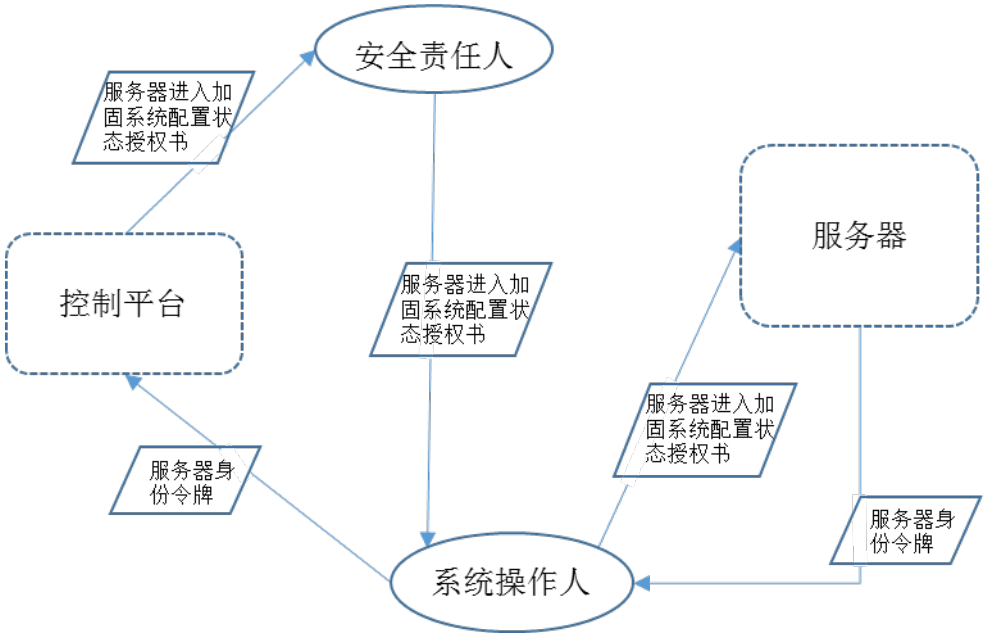
基于防护内部恶意攻击的需求，QDocument SE 定义两个系统状态：

- 保护工作进行状态；
- 系统配置状态；

同时定义并且实现一个严格进入到系统配置状态的流程，例如以下流程：

- 系统操作人员获取一个服务器硬件相关的服务器身份令牌；

- 系统操作人员将服务器身份令牌发给控制平台，以申请进入加固系统的系统配置状态；
- 控制平台将为该服务器产生一个一次性的服务器进入加固系统配置状态的授权书并发给相应的安全责任人；



- 安全责任人在确信安全的情况下将授权书发给系统操作人；
- 系统操作人员使用授权书进入加固系统配置状态。

3.2.4、QDocument SE 对业务系统服务的透明性

3.2.4.1、概述

QDocument SE 的透明性指当前业务系统服务的功能和性能都不能受到相应的保护系统的影响。

3.2.4.2、功能描述

(1) 系统服务的功能在数据被保护后不受到影响，这主要体现在数据被保护后，系统服务无需做任何修改即可正常重启并运行；

(2) 系统服务的性能在数据被保护后不能有显著的恶化，一个量化指标是，数据库服务的吞吐量改变不超过 5%。

3.2.4.3、数据保护流程

对于一个系统服务，譬如说 Oracle/MSSQL/MySQL，一个标准的保护流程是：

- 停止数据服务；
- 保护相应的数据；
- 设置相应的进程访问权限；
- 重启数据服务；

3.2.5、访问控制策略的配置方法的安全性

QDocument SE 配置访问控制策略的方法是安全的：

- 定义了一套清晰的用于访问控制策略的配置方法的流程；
- 明确访问控制策略的配置方法的操作权限；
- SE 所有配置文件是被加密保护的；
- 保证外来恶意软件不能修改本服务器 QDocument SE 的策略配置；
- 保证内部人员只有在严格遵循预定的流程时，才能重新配置或修改本服务器。

为保证访问控制策略的配置方法的安全性，QDocument SE 的访问控制策略的配置方法的流程需要定义两个系统状态，一个是保护工作进行状态，一个是系统配置状态。同时需要实现一系列的对系统配置状态的严格限制和保护。

3.2.5.1、系统配置状态的时效保护

- QDocument SE 的系统配置状态设置了一个严格的时效保护机制。即设置一个在系统配置状态的最大允许时间段，无论在任何情况，一旦超时立即自动从系统配置状态退出，返回到保护工作进行状态。
- QDocument SE 实现一个不依赖于计算机系统时钟的独立计时器，以确保时效保护的安全性，例如攻击者不能通过修改系统时钟而使时效保护失效。

3.2.5.2、系统配置状态的即时退出

QDocument SE 提供一个从系统配置状态即时退出的方法。在进入到系统配置状态后而达到最大允许时段之前，系统操作人员可以随时使用该方法从系统配置状态即时退出。

3.2.5.3、系统配置状态的入口控制

QDocument SE 对系统配置状态的入口作基于多因素认证的严密控制，即：

- 每台服务器需要使用一个与该服务器紧密关联的信息，作为一个必要条件用于产生一个仅用于该服务器的进入到系统配置状态的授权书。该信息需要由系统操作人员从该服务器获取并发送到一个中心平台。同时，该信息必须由在该服务器上的SE 以随机方式产生并予以保存，从而保证该服务器数据的安全性。
- 进入到系统配置状态的授权书应该是由 QDocument SE 操作人员根据需要提出申请，由一个中心平台产生。
- 每个授权书只对一台特定的服务器有效。
- 每个授权书是一次性有效。
- 授权书的分发应该由一个指定的安全责任人监管，即中心平台将新生成的授权书以及相关信息，如申请人、目标服务器等发送给安全责任人，由安全责任人决定是否发送给 QDocument SE 的操作人员。

3.2.6、访问控制策略的配置方法的易用性

QDocument SE 的用于访问控制策略的配置方法具有易用性。即用于访问控制策略的配置流程必须清晰简洁，易于操作实行。

3.2.6.1、集成多个服务器的入口控制

访问控制策略的配置方法的易用性要求实现集成多个服务器的系统配置状态的

入口控制：

- 支持系统操作人员一次性提交多个申请；支持中心平台产生一个集成的授权书；
- 支持各服务器的 QDocument SE 自动从该集成的授权书中识别是否有适用于本服务器的授权书；
- 支持各服务器的 QDocument SE 自动检查该集成的授权书的有效性；
- 支持各服务器的 QDocument SE 在授权书有效时进入到系统配置状态。

3.2.6.2、基于自动进程检测的配置选项设置

访问控制策略的配置方法的易用性是指有自动的进程检测，即QDocument SE 可以自动检测到所有对目标数据提交访问申请的进程的信息，即：

- QDocument SE 可以自动检测所有相关程序的全路径；
- QDocument SE 可以自动检测所有相关进程产生时的输入参数、环境变量等决定其行为模式的要素；
- QDocument SE 可以自动检测到访问申请种类，如读/写真实文件内容，或读写保护格式的文件内容；
- QDocument SE 可以自动检测到当前的授权结果，如被授权读/写真实文件内容，被授权读/写保护格式的文件内容，或被禁止访问；
- QDocument SE 可以自动应该将上述信息汇总显示给系统操作人员，作为配置操作的选项，从而方便系统操作人员为相应的被保护数据作出访问授权配置或修改旧的访问授权权限。

3.2.6.3、灵活的数据匹配选择

访问控制策略的配置方法的易用性要求灵活多样的数据选择匹配方法，例如系统操作人员可以通过指定一个目录路径来选择数据，还可以进一步给定一个路径匹配字符串作为过滤器，方便选择一个或多个满足一定条件的数据文件，即：

- 支持以指定目录的方式选择保护关键数据；
- 支持给定文件路径匹配字符串的方式选择保护关键数据；
- 支持将指定目录和路径匹配结合的方式选择保护关键数据；

3.2.7、关键数据访问的监察

QDocument SE 对关键数据的访问情况作出完整的记录，并且将这些记录进行集中保存管理，以便于统一查证和审计。

3.2.7.1、完整的访问信息记录

QDocument SE 对关键数据的访问情况作出完整的记录，监控记录包括：

- 访问发生的地方，如一个在本地网络中唯一的系统名称或目标系统的 Ip 地址；
- 访问源，即是什么进程进行数据访问；
- 访问目标，即是什么数据目标被访问；
- 访问方式，读/写真实数据内容、读/写保护格式的数据等；
- 访问结果，即是否被授权通过；
- 访问时间。

3.2.7.2、标准的信息记录格式

QDocument SE 使用标准的信息记录格式，如 Windows 的日志信息格式、Json格式等。具体信息可以分类成：错误类，警告类，信息类等。

3.2.7.3、集中的信息平台和信息收集

QDocument SE 建立了一个共同的中心信息平台，将每一个服务器上的关键数据的访问情况记录传输到该中心信息平台上。

3.2.8、QDocument SE 自身的运行情况和工作状态监察

QDocument SE 对自身的运行情况和工作状态作出完整的记录，并且将这些记录进行集中保存管理，以便于统一查证和审计从而保证整体系统的安全性。

QDocument SE 对自身的运行情况和工作状态作出记录，以便于管理并确保整体系统的安全，即：

- 监控记录包括本 QDocument SE 的运行情况：

■记录各个 QDocument SE 的安装过程中的每个流程的执行时间和执行结果，如系统的安装、激活等；

■记录各个 QDocument SE 中进行合法进程授权的命令的内容，执行时间，执行结果；

■记录各个 QDocument SE 中进行初期数据保护格式转换操作的命令的内容，执行时间，执行结果；

■记录各个 QDocument SE 的其他运行情况，如各类系统错误等；

- 监控记录包括本 QDocument SE 的运行状态：

■记录各个 QDocument SE 进入和退出系统配置状态的时间；

■收集记录各个 QDocument SE 的各组件的心跳信息（即一个具有稳定周期的，表示相应组件工作正常的信号）；

■记录各个 QDocument SE 的工作证书信息。

3.2.9、中心信息平台信息审计及处理

QDocument SE 对所有的关于数据访问的监察信息和关于QDocument SE 自身的监察信息进行统一集中的信息审计和处理，即：

- 实现集中的设备管理功能；
- 实现集中的信息记录管理功能；

- 实现集中的告警管理功能；
- 实现集中的进行系统功能管理的功能。

3.2.9.1、设备管理

中心信息平台实现集中的设备管理功能（这里的设备指装有QDocument SE 的服务器），提供对设备的增加，删除，监控、审查等操作。

- 中心信息平台为新接入 QDocument SE 的设备生成其设备基本信息；设备基本信息应包括：设备 IP、设备名称、设备所属部门、设备用途描述等。
- 中心信息平台对设备添加要进行唯一性校验，避免重复添加设备。
- 中心信息平台为每个设备总结生成其安全加固系统的配置表，如被安全保护的文件、对文件的授权进程等。
- 中心信息平台对每个设备进行原始记录分析，对异常操作的设备发出告警通知。

■监测各个设备上加固系统的数据访问情况，如果发现异常立即作出预警；

■监测各个设备上加固系统的各个工作组件的心跳信息，如果发现异常立即作出预警；

■监测各个设备上加固系统的工作证书的时效；

- 中心信息平台自动生成各个设备的 QDocument SE 的运行状态报告。

3.2.9.2、信息记录管理

(1) 信息记录存储

中心信息平台为所有的信息记录提供安全可靠的存储和备份功能，并保证记录存储时间不低于 12 个月。

(2) 信息记录查看

中心信息平台提供对记录内容的精确查询、检索功能，即：

- 中心信息平台支持对记录进行条件查询，如单项查询条件或组合查询条件；
- 中心信息平台提供一些查询条件建议，如建议采用“起止时间+设备 IP”组合方

式开展查询；

- 中心信息平台提供手动和自动两种记录处理方式。手动处理后的记录直接转存至备份数据库中，不再参与结果分析和告警；对于一周以上未处理的非告警信息自动转存至备份数据表中，不再参结果分析和告警。
- 对记录的查看：

  ■支持以设备为维度进行查看；

  ■支持以时间为维度进行查看；

  ■支持以事件级别为维度进行查看；

  ■支持综合维度进行查看；

  ■支持以列表、图标方式进行查看。

(3) 信息记录分析

中心信息平台按照设备、时间、事件类型、事件等级等维度对所有收集的信息进行聚合、汇总，统计各设备一定时间段内的正常信息、警告信息、错误信息等，对级别较高的事件需向相关负责人发送不同形式的告警通知，即：

- 支持多种聚合规则，对检测的事件记录按照时间、设备、级别进行聚合；
- 对严重级别的事件特别是错误操作记录提供告警，并对已处理的告警记录进行标记；
- 避免重复发送警告；
- 支持对同类记录进行分类汇总，以列表，图表的方式进行展示；
- 支持记录分析每 5 分钟自动更新一次；
- 支持记录分析结果以 EXECL 等格式导出。

3.2.9.3、告警管理

中心信息平台支持通过对记录的分析，按照错误状态和事件等级，设置不同的告警方式进行告警。中心信息平台对各设备的信息进行管理，对设备的运行状态、事件级别进行统计分析，对设备运行异常、数据异常操作等情况及时发送告警通知，即：

- 支持设备自身运行状态异常告警。采用轮询访问设备的方式查看设备状态是否正

常，并及时更新设备的状态，建议每次轮询时间为 5 分钟；

- 支持被保护数据的异常操作告警。被保护的数据由于授权进程的不正当访问或由于非授权进程的访问尝试所产生的异常进行告警；
- 支持分级告警功能，并实现用户的可配置；
- 支持屏幕告警、邮件告警、短信告警等多种告警方式。根据事件级别及用户自己的告警配置，对所要进行告警通知自动选择屏幕告警、邮件告警、短信告警等方式进行通知。

3.2.9.4、系统功能管理

(1) 权限管理

中心信息平台实现对系统管理人员、系统使用人员进行权限分配和身份认证，不同身份和权限的用户只能使用所分配的平台功能，未经授权的用户不得使用平台功能。

中心信息平台依据最小授权原则为各账号授予各自承担任务所需的权限，严格限制各账号的权限。

中心信息平台支持各账号角色权限的变更及重新分配，支持权限分配的灵活性。

(2) 人员管理

中心信息平台对使用系统的人员进行创建、授权、修改及删除等管理。人员信息至少包括：用户名称、登陆账号、联系方式、邮箱地址等，系统产生的邮件、短信告警会和用户信息关联。

(3) 操作记录管理

中心信息平台保存系统使用人员登录和操作的记录，记录包括：登录/操作账号、时间、登录用户 IP 及操作内容等。平台提供对操作记录按日期、操作主机 IP 地址信息等进行检索。

3.2.10、支持操作系统和服务器种类

(1) 概述

QDocument SE 支持主流 Windows 服务器操作系统，同时也支持主流的数据库和大数据服务系统。

(2) 功能描述

具体地讲，QDocument SE 支持主流的 Windows 服务器操作系统，如:

(1) Windows 2008R2

(2) Windows 2012

(3) Windows 2012R2

(4) Windows 2016

QDocument SE支持主流的Linux服务器操作系统，如：

(5) Red hat/CentOS 6

(6) Red hat/CentOS 7

(7) 麒麟x86操作系统

(8) 麒麟ARM操作系统

QDocument SE 支持主流的数据库服务系统，如：

(1) Oracle

(2) MSSQL

(3) MySQL

(4) PostgresSQL

QDocument SE 支持主流的大数据平台，如：Hadoop。