华汇数据安全云桌面系统及其应用

技术白皮书

二〇一六年八月七日

目录

一、 背景

信息安全是信息化发展的保证基础，但是目前的信息安全保障能力与信息化快速发展水平并不相称。尽管多年来信息安全技术不断进步，信息安全产品不断涌现，但是用户面临的重要数据安全保护问题却依然没有得到根本解决。企业重要信息的泄露和失窃不仅会给用户带来巨大经济损失，而且还可能导致企业在品牌和声誉等其它运营层面的巨大风险。

企业数据安全问题的深层原因主要是：1）传统的信息安全技术和产品在理论基础层面还缺乏足够支持；2）传统的信息安全保护结构有较大的局限性，不能保证安全管理措施的有效落实。

对重要业务数据进行保护，信息安全纵深防御是基础。信息安全纵深防御思想是指信息安全不能只通过某一个环节或某一类产品就可以保证。在技术层面，信息安全纵深防御就是要从系统的计算环境、网络传输、系统边界和安全管理等多个层次部署多样性的安全保护措施和机制，这样即使攻击者成功地破坏了系统中的某个安全保护机制，其它的安全保护措施和机制还能够提供必要的补充保护作用，从而把系统风险程度控制到最低。比如我们在常见的信息安全方案中会看到在系统边界部署边界防火墙，以防止外部对计算环境的非法访问；在传输网络中采用 VPN 措施，以对数据通信进行加密保护，并对通信对方进行身份认证；在计算环境中的服务器和用户终端（如 PC 和移动终端）安装数据加密存储系统，以防范信息失泄密事件的发生。

传统的信息安全方案虽然符合信息安全纵深防御思想，但是其实际安全保护效果往往不尽人意。这是因为：首先，在传统的应用安全结构中，系统最大的风险来源是用户终端，这些终端除了要参与应用的处理，还可能在本地长期或临时性地保存应用数据；另外，用户也可以通过终端设备把应用系统中的数据拷贝出来，也可以把外部的数据拷贝到应用系统中，因此严格地讲，应用系统的边界不仅仅在我们常见的防火墙所处的那些位置，这些用户终端也都构成了应用系统的边界。由于用户终端数量大、分布广，而一般单位的信息化部门编制都很少，要对这些终端实施安全管控的难度非常大，实际上，传统信息安全方案在终端安全上投入了很多，比如杀毒软件、终端安全管理、文件加密，甚至对操作系统进行安全增强，但是由于各种原因，安全效果始终难尽人意，终端安全问题依然严峻。其次，除了安全管理制度之外，传统的信息安全方案很少能从技术层面对内部人员的操作行为进行管控，而管理制度往往很难落地或有效执行，这样实际上内部人员在系统内部可以说是“为所欲为”，

没人管的住了；内部人员的违规操作不仅是数据窃密和泄密行为的直接源头，也是病毒和木马在系统中感染和传播的重要原因。其三，传统信息安全方案对数据的保护粒度比较粗，一般只能对一个较大的数据和文件范围，或一批数据和文件，定义一个安全规则进行保护，用户要么对定义范围内的所有数据和文件都有同样的访问权限，要么都没有，而不能定义用户对单个文件和数据有什么样的访问权限，比如传统的网络防火墙；在这种粗粒度的安全规则控制下，一旦授权用户可以访问某个文件，他有可能借助于这个授权去访问那些他本不该访问的文件和数据，即违规访问或越权访问。

此外，传统的信息安全方案对基于非信息化手段的数据泄密和窃密行径缺乏有效的应对措施，比如有些环境下，通过对用户终端显示器中所显示的敏感信息进行非法录拍就可以窃取敏感数据，而目前方案缺乏对这类行为的有效追踪和威慑机制，也就难以阻止这类安全事件的发生，这也在很大程度上影响了人们对信息安全保护能力的信心。

二、 层次化数据保护方法

既然传统信息安全方案存在那么多的局限性，那么很自然地我们就应该首先要解决这些问题。通过改变系统安全结构，而不是简单的安全功能叠加，可能是目前我们能够采取的比较好的解决方案，其思想核心就是从系统安全结构上使用户终端不再成为系统的风险来源，并在此基础上，解决用户行为规范、多层次的数据访问控制以及用户行为追踪等问题。

层次化数据保护方法的具体内容就是：首先，通过调整系统安全结构，将应用终端集中到统一的平台上，使用户终端不再成为应用系统的一部分，也就是让它们不再是系统的风险点，从而减小应用系统中的数据安全风险范围；第二步就是从技术层面对用户操作进行管控，阻止内部人员的违规操作行为，保证系统运行环境的安全；第三步就是在系统内部多个层次部署细粒度数据访问控制机制，防范内部人员的非法访问和越权访问，保护数据安全；最后，建立快速和有效的安全事件追踪机制，对违规和非法行为进行威慑和吓阻，防患于未然。

层次化数据保护方法并不是要从信息安全防御体系方面提出一种全新的理念，它只是对纵深防御思想的一种创新性实现。显然，采用层次化数据保护方法能够克服传统信息安全方案的主要问题，它从根本上解决了用户终端的安全管控难题，不仅使应用系统的安全结构大为简化，安全保护效果得到有效提升，而且还使系统的管理和运维工作变得更为简便。

层次化数据保护方法在目前的技术条件下是可行的。图 1 就是一种基于虚拟桌面技术和密码技术来实现用户系统的层次化数据保护方法示意：

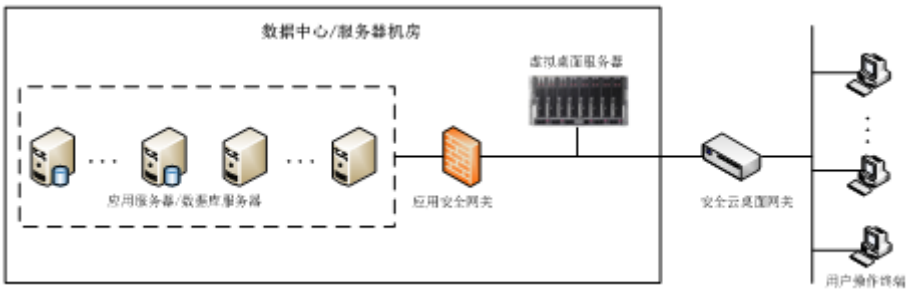

图 1 基于虚拟桌面技术实现的层次化数据保护方法

基于虚拟桌面技术和密码技术层次化实现的数据保护方法实现方案有四个主要内容：

1. 建立集中化的应用终端平台，减少数据安全风险范围

图 1 方案通过虚拟桌面技术将用户系统的客户端功能集中到虚拟桌面服务器中，即所有应用客户端软件都安装在虚拟桌面中；用户操作终端不再安装客户端软件，它们只是作为应用客户端（虚拟桌面）的键盘鼠标和显示器，显然，在实现集中应用终端平台机制后，用户系统的就由应用客户端、应用服务器和数据服务器组成，用户操作终端不再属于用户系统的一部分，因此它们也就不再是系统的风险点了。在集中应用终端平台中，管理人员可以通过母本镜像克隆机制大幅减少应用客户端（虚拟桌面）的管理运维工作量。在实际系统中，运维人员为工作性质相同或相近的应用终端建立一个统一的母本（或者系统模板），所有的应用客户端都自动保持与母本相同的状态；这样，日常对应用客户端的运维工作（比如软件安装、补丁升级等）就只需要针对每类应用客户端所对应的母本进行维护；母本更新后，相关的应用客户端就自动获得与母本一致的更新；对母本的维护过程就如同对单台 PC 的维护过程一样，因此系统运维工作量最大的应用客户端运维部分就变得十分简单快捷，管理的效率和可靠性相应得到大幅提高，管理成本也随之大幅降低。

2. 建立多层次的数据保护机制，确保数据安全保护能力

图 1 方案中有三个重要的数据保护层次，第一个要对数据进行保护的层次是用户系统的边界，采用集中化的应用终端平台后，用户系统的边界主要位于虚拟桌面系统与用户操作终端之间，系统在这个边界位置部署华汇数据安全云桌面网关，实现以下安全功能：对用户身份进行认证、对用户的资源访问进行管理、对用户在用户系统内部和外部之间的数据复制行

为进行控制以及安全审计等。通过华汇数据安全云桌面网关在用户系统边界对数据进行保护，可以保证非法用户“进不来”、窃取的数据“拿不走”。第二个数据保护层次是应用服务边界，应用服务边界位于应用服务程序内部或者应用服务器和应用终端之间，系统在这个边界部署细粒度的访问控制，以防范内部人员的违规访问和越权访问。所谓细粒度访问控制是能够根据用户身份及其所要访问的具体数据（如数据库记录、字段等）来控制用户对数据的访问，细粒度访问控制能够对数据进行精准保护，用户不能超出授权访问数据，即“看不到”被保护的数据。一般来说，如果在软件设计和开发过程中没有考虑安全需求的话，那么在应用服务程序内部实现数据安全访问控制并不现实，因为它需要修改相关的应用程序；此时，图 1 中的应用安全网关就是一个可选方案。应用安全网关对用户访问应用服务器和数据库服务器的网络流量进行监控和解析，获取用户身份及其要访问数据的相关信息，并根据这些信息对用户的数据访问行为进行控制。第三个数据保护层次在图 1 中并未明确标识，这个层次位于数据存储所在的位置，系统应该在该层次采取加密存储方式保护数据，使非法用户“看不懂”被保护的数据。

3. 建立用户行为规范体系，从源头杜绝数据安全威胁

与外部攻击相比，内部人员的安全威胁更加难以防范和控制，后果可能也更为严重。图 1 方案在虚拟桌面系统中部署基于密码技术的白名单安全机制，对操作人员在用户系统内的操作行为进行规范，任何没有经过明确批准的可执行程序不能被用户调用执行，这种白名单行为规范机制既可以有效阻止内部人员的非法操作，又可以有效防范各种已知和未知的病毒木马在用户系统中的传播和感染。白名单安全机制还应该部署在应用服务器和数据库服务器中，以保证系统的整体运行安全。图 2 中显示了白名单安全机制的一个实际应用效果，由于用户试图运行的程序（Webdown.exe）不在白名单中，因此系统提示拒绝执行。

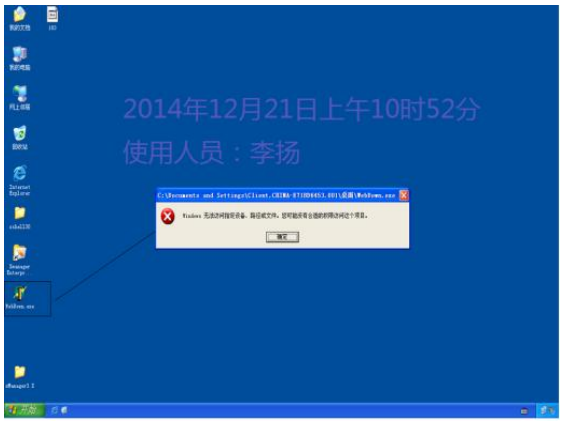

图 2 白名单安全机制效果示意

4. 建立用户行为可视化追踪机制，对违规和非法行为进行威慑

如果对内部人员的行为缺少追踪机制，那么他们违规操作的动机就会更加强烈。图 1 方案中，除了在系统各个层面对用户行为进行审计之外，系统还能够根据用户身份信息、操作时间以及其它相关环境状态，对用户的操作过程进行标记，比如从图 2 中虚拟桌面屏幕背景中的水印信息“2014 年 12 月 21 日上午 10 时 52 分，使用人员：李扬”中，可以看出当时是用户“李扬”在使用该虚拟桌面。如果用户对屏幕进行非法照相或录像，那么这些水印标记就会作为事件追踪的依据，使非法行为“跑不掉”、“赖不掉”。

可以看出，基于安全虚拟化技术的层次化数据保护方法不仅能够从根本上保证用户重要业务数据的安全，而且还具有安全结构简单、安全设备数量少的特点。层次化数据保护方法对既有应用系统的改动要求少，对系统的性能影响小；不仅如此，层次化数据保护方法还可以极大地降低安全管理的难度，减少系统运维的复杂度和工作量，提高系统的安全管理效率。

三、 华汇数据安全云桌面系统

华汇数据安全云桌面系统完全支持图 1 应用系统安全解决方案。华汇数据安全云桌面系统由以下部分组成：

1） 虚拟桌面管理系统。对虚拟桌面服务器、存储服务器、华汇数据安全云桌面网关、用户、安全监控和安全策略等进行集中管理；虚拟桌面管理系统还负责对虚拟桌面的建立、删除、复制、升级进行集中的管理，极大地减少运维人员的工作量，保证系统安全管理效率；

2） 基于“白名单”安全机制的虚拟桌面安全套件。该安全套件可以有效方法各种已知或未知的恶意代码、阻止用户任何不符合操作规程的应用访问行为、防范敏感数据未经允许的泄漏、对用户在虚拟桌面中的操作行为实现可视化审计和追踪；

3） 华汇数据安全云桌面网关。虚拟桌面网关将用户虚拟桌面系统与用户操作终端在网络层面实现隔离，阻断用户操作终端这边的不安全因素，比如病毒木马 DDoS 等攻击，给虚拟桌面系统的传染和破坏；华汇数据安全云桌面网关还强制对用户身份和接入的用户操作终端等设备进行认证，保证未经允许的人和设备“进不来”；在认证成功后，华汇数据安全云桌面网关建立从用户操作终端到虚拟桌面系统的动态连接，用户退出虚拟桌面系统后，该网关自动拆除相关连接，防止用户继续

使用旧连接私自连接虚拟桌面；华汇数据安全云桌面网关还支持从用户操作终端到该网关之间的安全加密通信；

4） 应用安全网关。应用安全网关可以保证不同部门或不同岗位的人员，在访问应用系统时，只能看到自己权限范围内的文件和应用等；系统也可以根据时间对用户访问进行控制，从最大程度保证敏感信息文件的安全保密。

华汇数据安全云桌面系统完全兼容用户已有应用系统，用户操作方式与传统没有区别，用户只需要通过应用系统外部的用户操作终端登录“虚拟桌面管理系统”，如图 所示：

图 4 用户登录

用户登录后从其可用桌面中通过双击图标方式选择并进入其当前虚拟工作桌面，如图所示：

图 5 用户桌面选择

用户进入虚拟工作桌面后，所有应用操作流程与以往方式或习惯没有任何区别，如图 ：

图 6 用户进入虚拟工作桌面

华汇数据安全云桌面系统在不需要安装防病毒软件的情况下，对各种已知和未知的恶意代码进行有效防范，并自动禁止其它任何未经允许的程序在系统中运行，减少黑客攻击机会，如图 所示：

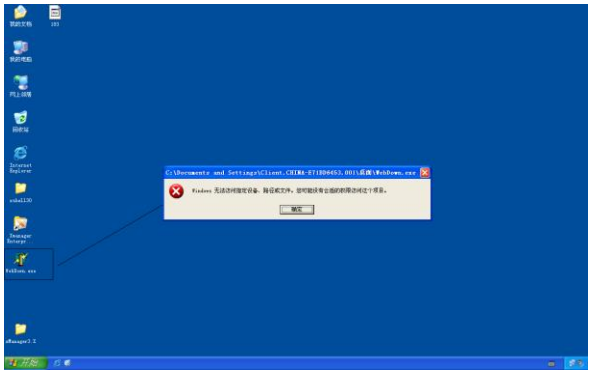

图 7 可执行程序保护机制（白名单）

华汇数据安全云桌面系统可以对用户在应用系统与外部环境之间的数据交换进行安全控制。基于用户身份，对其在虚拟桌面和操作终端之间的数据和文件复制行为进行控制，比如某些岗位只能从操作终端向内部的虚拟桌面中复制数据和文件进行工作，或者只被允许看内部系统当中的文档等数据。基于虚拟桌面系统的安全防护功能，无需再花费精力对用户操作终端进行网络或 USB 等端口的控制和管理，就可以有效保证核心系统敏感数据不被非法复制或外泄。通过终端无痕化管理，当用户退出虚拟桌面后，系统自动将虚拟桌面进行安全清理，保证不保留前一用户的任何使用痕迹，包括各种临时数据等。用户操作终端本地不临时或永久保存业务相关数据，防止敏感信息被非法复制、盗取或失窃。

华汇数据安全云桌面系统支持两种类型的虚拟桌面：普通桌面和 VIP 桌面。普通桌面是指能被多个用户共享的虚拟桌面，系统在每次用户使用完毕退出这些桌面之后，都会采用“无痕终端”安全技术，将虚拟桌面恢复到一个原始的“干净”状态，即当前用户退出后，

这些虚拟桌面不会遗留任何关于该用户的使用信息或其它个人信息；VIP 桌面是指分配给特定用户的专用虚拟桌面，对于这类虚拟桌面，系统也会在预定时间之后，对系统进行重新启动，防止软件老化带来的系统性能下降问题。

对每个用户，系统还可以根据其工作性质和业务需要，配置多个不同的虚拟桌面（应用终端），用户登录之后只需简单的点击对应桌面图标就可以选择当前工作桌面。多桌面支持不仅可以实现不同应用之间的安全隔离，而且可以有效减少实际系统的物理 PC 终端数量。

图 8 多虚拟桌面（应用终端）支持能力

用户从应用系统内部的虚拟桌面（应用终端）访问应用/数据库服务器时，可以通过部署在应用/数据库服务器前面的应用安全网关对用户身份进行认证、对其访问的应用对象和访问方式进行安全控制、对其操作行为进行安全审计，保证应用流程和业务数据的安全。

华汇数据安全云桌面系统对对所有的用户管理操作、虚拟桌面使用情况等状态或行为进行全面审计。如图 9 所示：

图 9 系统的审计功能

四、 应用方向

华汇数据安全云桌面系统作为一种基础设施和通用安全平台，它可以应用在多个方面，比如办公和生产信息系统的安全内控、系统运维服务的过程控制和事件追踪、计算机教室建设和改造等领域。

(一) 安全内控

在办公和生产信息系统中，基于华汇数据安全云桌面系统，层次化数据保护方案可以满足以下安全内控要求：

1、 通过白名单机制规范内部人员的行为，保证办公和生产系统的运行安全和运行效率，防止计算机病毒和木马的破坏；
2、 通过安全虚拟化技术实现对终端设备的集中安全管控，避免了传统终端安全管理中的“数量多”、“分布散”、“管理难”等问题，并极大地降低了终端管理的难度和工作量；
3、 通过基于华汇数据安全云桌面系统的层次化数据保护机制，防止内部人员非法和越权访问，在满足其办公和生产操作要求的基础上，保证业务敏感数据的安全；
4、 对内部操作行为实现全面审计，并通过自动屏幕水印机制提高违法操作的可视化追踪能力；
5、 采用加密传输技术保证通信安全，支持远程和移动办公安全。

(二) 移动业务安全

支持基于互联网的移动业务是很多用户应用业务的发展方向。由于移动业务是使用移动终端设备通过互联网连接并访问用户系统的，因此要保证从移动设备到用户系统之间的通信安全。一个成熟并且可行的方法是在移动终端到用户系统之间实现加密数据传输，比如采用 SSL VPN 方法。

一种实现方式是对移动终端和华汇数据安全云桌面网关之间的数据通信进行加密，如图 3 所示：

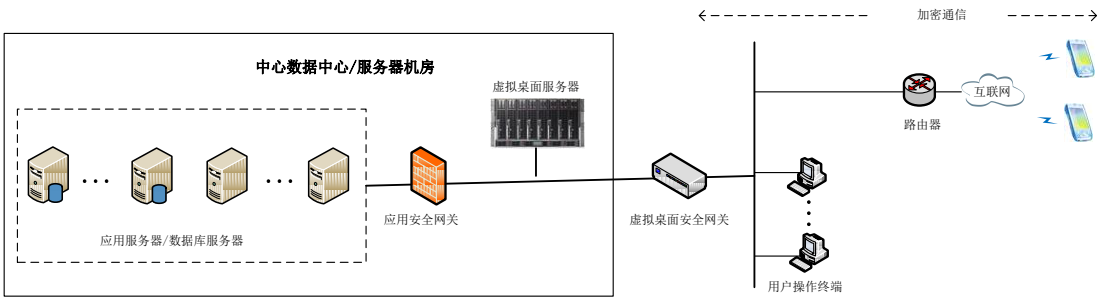

图 3 华汇数据安全云桌面网关加密通信模式

图 3 方案还可以支持所有用户操作终端与虚拟桌面系统之间的安全加密通信。

华汇数据安全云桌面网关还支持对移动终端设备和用户身份进行认证，只有得到批准的用户通过指定的移动设备才可以连接并访问虚拟桌面系统。

图 3 方案还保证了用户移动设备上不会保存任何业务相关的数据，进一步提高数据安全保护能力。

(三)系统运维服务安全保证

在系统运维服务安全保证中，将华汇数据安全云桌面系统与视频检索机制结合，可以对运维过程进行实时监控，帮助管理人员对运维操作进行分析和责任认定。

1、 通过华汇数据安全云桌面网关的网络隔离和准入控制能力，对远程运维人员和设备进行认证，防止未经允许的人和设备连接到运维桌面；
2、 通过白名单机制保证运维环境安全可信，帮助管理人员对运维工具进行规范和控制；
3、 通过基于华汇数据安全云桌面系统的层次化数据保护机制，保护系统内部敏感数据被非法访问和窃取；
4、 基于华汇数据安全云桌面系统实现对运维过程的实时在线监控，保证运维过程安全；
5、 对运维过程进行全过程录屏审计，并基于安全事件对视频记录进行快速定位和检索，帮助管理人员实现快速责任认定；

上述功能不仅可以应用于运维服务安全保证，还适用于所有基于第三方的服务，比如安全风险评估等。

(四) 计算机教室建设和改造

针对传统计算机教室建设和运行过程中存在的局限性，采用华汇数据安全云桌面系统可以极大的降低和保护学校在信息化建设和运行方面的综合投入，提高计算机教室的利用率，减轻机房老师的工作负担。

1、 基于云计算和虚拟化技术，保证计算机教学方式和教学内容的先进性，真正落实“人人皆学、处处能学、时时可学”的要求；
2、 性能体验良好的设备利旧方案 经过华汇公司定制化方式利旧后的 PC 采用机顶盒方式工作，完全免维护，并且从加电开机到登录桌面只要 40 秒左右；
3、 无毒化实训环境保证 通过华汇安全云桌面网关阻断病毒木马对虚拟桌面系统的感染破坏，通过基于密码技术的白名单机制阻止病毒木马在虚拟桌面系统中被激活；
4、 可视化学生实训过程跟踪 老师可以随时对学生操作过程进行监控，并且对其进行录屏；
5、 全生命周期型学生实训档案管理 系统为每个学生建立实训档案，并在整个学生在校学习期间完整保存；学生登录实训系统后，该档案存储系统自动挂载到学生当前实训桌面中。
6、 轻量型系统日常运维管理要求 没有病毒木马、学生操作终端免维护、实训环境免维护、课程选择学生自主操作，老师可能只需要对课件进行维护管理

五、 结论

华汇数据安全云桌面系统将虚拟化技术作为信息安全的一种支撑技术，可以简化用户应用系统的安全结构、显著提高系统的安全性、保护企业重要数据安全，同时它还可以减少信息安全机制在应用系统运行性能、可靠性和易用性方面的影响，降低应用系统在安全维护方面的成本。

华汇数据安全云桌面系统可以用来满足多种业务应用在安全保障方面的需求。比如单位的安全内控、第三方运维服务的安全保障以及学校计算机教室的建设和改造方面，安全虚拟化技术不仅作为用户信息系统基础设施的一部分，而且还将系统的安全保障机制与系统基础设施实现有机的融合，降低系统的安全保障和管理难度，减少单位的信息化建设和运行成本。