华为UMA运维审计产品规格对比表

	华为UMA	江南科友HAC	思福迪LOGBASE	齐智科技SHTERM
市场份额/地位		华南占有率较高，全国推广	运维审计产品属于非主推产品，华东有一定占有率	全国市场占有率较高，主要竞争对手
竞争力的体现		江南科友凭借之前的密码机，在金融行业有一定的客户优势	运维审计系统属于新推产品，市场切入较晚。	具备较完善的技术水平，对用户的使用体验较好
战略控制点		以金融行业为主，对其他行业进行覆盖	非核心产品	只有一款产品，对各个行业进行覆盖
市场战略		对没有把握的项目打低价		基本不打低价
部署模式	旁路部署，逻辑串联，支持双机热备，配置和审计日志，实时同步，支持集群部署/分级部署	旁路部署，逻辑串联，支持双机热备，只能实现配置日志同步，支持集群部署	旁路部署，逻辑串联，支持双机热备，只能实现配置日志同步，不支持集群部署	旁路部署，逻辑串联，支持双机热备，只能实现配置日志同步，日志定时同步，支持集群部署
系统安全性	采用精简系统，开放端口数量10，IP自动禁止功能，账号登陆错误自动锁定	采用精简系统，开放端口数量19，无IP自动禁止功能，账号登陆错误自动锁定	无IP自动禁止功能，账号登陆错误自动锁定	采用精简系统，开放端口数量2，无IP自动禁止功能，账号登陆错误自动锁定
角色管理	系统除了预设的角色外，角色权限可自定义配置，实现菜单级别授权，可根据用户需求增加新的用户角色	只能选择预设的角色	只能选择预设的角色	只能选择预设的角色
授权管理	授权可以从设备、设备组和用户、用户组、进行“一对一”，“一对多”，“多对多”进行灵活授权。以树状结构进行方便授权	只能以设备组，用户组的模式进行批量授权，缺乏灵活性	只能以设备组，用户组的模式进行批量授权，缺乏灵活性	只能以设备组，用户组的模式进行批量授权，缺乏灵活性
认证模式	系统提供身份认证，自然人（员工帐户）登录系统时支持静态口令、双因素认证、AD域和PKI证书认证，并能够支持多种认证混合使用，用户可以通过多种认证方式进行登录	系统提供身份认证，自然人（员工帐户）登录系统时支持静态口令、双因素认证、AD域和PKI证书认证，但是无法支持多种认证混合使用	系统提供身份认证，自然人（员工帐户）登录系统时支持静态口令、双因素认证、AD域和PKI证书认证，但是无法支持多种认证混合使用	系统提供身份认证，自然人（员工帐户）登录系统时支持静态口令、双因素认证、AD域和PKI证书认证，但是无法支持多种认证混合使用
应用发布	通过window服务器实现应用发布功能模块，支持微软RemoteAPP功能，实现应用无缝应用发布，用户调用应用发布时，体验和本机调用程序一致，带给用户极大的感官和操作提升。	通过window服务器实现应用发布功能模块，实现的是桌面发布，而不能仅对应用进行发布，无法支持Remoteapp功能	通过window服务器实现应用发布功能模块，无法支持Remoteapp功能	通过window服务器实现应用发布功能模块，无法支持Remoteapp功能
协议密码代填	全面支持字符类：SSH、Telnet；图形类：RDP、VNC、X11；文件传输类：FTP、SFTP	只能支持字符类：SSH、Telnet；图形类：RDP；文件传输类：FTP、SFTP	只能支持字符类：SSH、Telnet；图形类：RDP；文件传输类：FTP、SFTP	只能支持字符类：SSH、Telnet；图形类：RDP；文件传输类：FTP
应用中心密码代填	能够实现应用中心支持客户端的账号密码代填功能，此功能业内领先	完全不支持	完全不支持	支持oracle、sqlserver部分客户端的代填
运维模式（页面调用）	支持B/S页面运维，无需安装特定运维程序（JAVA APPLET），通过页面调用本地客户端程序进行运维	页面安装特定运维程序（JAVA APPLET）实现	可通过配置实现调用本地客户端实现	页面安装特定运维程序（JAVA APPLET）实现
运维模式（客户端连接）	支持C/S客户端直接运维，可直接使用运维客户端（secureCRT、PUTTY、MSTSC）直接访问UMA地址进行登录和资产选择从而进行运维操作。	只能支持字符类（secureCRT、PUTTY等）	全面支持	只能支持字符类（secureCRT、PUTTY等），且必须指定终端模式为XTERM
审计能力（字符）	除了常规的命令和录像， 支持分析功能，能够将输入命令和输出结果的智能分离，可以做到从任意命令点开始回放	无分析功能	无分析功能	支持
审计能力（文件传输）	系统可以对传输文件进行备份，提供文件审查依据	无法支持	无法支持	无法支持
审计能力（图形）	支持RDP控制台操作模式，RDP标题栏识别功能：能够对用户打开工具和目录以及IE地址栏等信息进行提取和捕获，并支持定位录像回放	都不支持	无法支持RDP标题栏识别功能	支持
审计能力（数据库运维）	系统能准确解析数据库访问过程，记录SQL语句。并将SQL语句同录像会话关联记录。	不支持	不支持	支持
服务器改密	系统能够对被管理设备定期自动修改账户口令，实现无需在服务器安装引擎，支持linux、unix、windows服务器	不支持	不支持	支持，但是windows必须开启telnet或ssh

华为UMA运维审计产品规格对比表-齐智

对比项		测试内容	华为	齐智	目的
数据库审计	管理方便性	统一运维安全平台是否可以代填各种数据库维护工具（PISQL/TOAD/SQLPLUS/OEMC）的登录账号和密码	支持	奇智不支持代填	通过代填方式可以最大限度的保护系统安全，对于那些临时访问的客户，只给其操作权限，无须告诉数据库登录密码
	管理的精细性	是否可以在统一运维安全平台中针对同一台目标数据库的账号和服务进行授权	支持	奇智不支持	针对同一台Oracle服务器的各个数据库服务、不同账号是否可以授权管理，而不是只能针对某台Oracle服务器
	数据库数据的防泄露	是否可以授权运维人员具备保存、复制权限的控制	支持	奇智无法控制剪贴板复制粘贴功能	实现敏感数据安全保护，防止复制、另存、截屏等方式的信息泄露
	数据库支持全面性	是否支持oracle、sybase、DB2、SQLserver、informix、mysql主流数据库的各类数据库客户端单点登录和SQL语句提取。	支持	奇智只支持一部分	数据库运维审计全面覆盖，保障用户运维审计无缺失，漏洞
用户特有客户端应用发布	特有客户端应用发布	支持发布Radmin、PCAnywhere、AS400、DameWare、CiscoASDM、RealVNC4	支持	奇智只支持一小部分	完整支持用户环境各类特定应用，通过应用发布平台集中管理和审计，保障用户运维审计无死角
	特有客户端单点登录	支持Radmin、PCAnywhere、AS400、DameWare、CiscoASDM、RealVNC4的账号密码代填，实现单点登录	支持	奇智完全不支持	通过代填方式可以最大限度的保护系统安全，对于那些临时访问的客户，只给其操作权限，无须告诉数据库登录密码。
图形操作审计（RDP、VNC、X11）	RDP客户端多版本支持	测试RDP客户端支持各种版本MSTSC，包括RDP6.0，WINDOWS XP SP3，WINDOWS VISTA SP1，WIN7访问目标资产	支持	奇智无法支持MSTSC直接连接远程桌面，必须使用特定客户端	很多客户希望沿用原有的RDP访问方式，不改变用户习惯，便于统一运维安全平台的推广
	是否可以全屏访问	是否可以实现真正意义上的全屏操作（完全满屏），包括各种电脑终端（宽屏笔记本）	支持	奇智只提供几种分辨率选择，对全屏支持不完善，且经常需要拖动IE控制条以查看全部屏幕	如果不能够全屏操作，用户需要拉动滚动条来调整，操作体验很难受
	拷贝粘贴	是否支持各版本RDP客户端双向拷贝/粘贴功能，测试剪贴板通道支持情况	支持	奇智无法对剪贴板的负责粘贴功能进行打开/关闭控制	尽可能保留RDP客户端通道各个有价值功能，并对其进行控制，避免信息泄露
	功能键支持	是否支持WINDOWS系统功能键，如ctrl+alt+end WIN+L等	支持	奇智对windows功能键无法支持严重影响运维人员的操作习惯，降低运维效率	功能键大大方便了用户的操作效率，对功能键的完整支持是尊重用户习惯，适应运维发展的体现
	分辨率和屏幕大小设置	是否支持通过RDP客户端里面的选项设置目标资产服务器的登录屏幕大小和分辨率	支持	奇智只支持特定分辨率，且全屏化有缺陷	严重影响用户使用体验
	X11单点登录	测试是否支持X11单点登陆，用户不需要二次输入密码	支持	奇智不支持X11单点登录，单点登录体系崩坏	通过代填方式可以最大限度的保护系统安全，对于那些临时访问的客户，只给其操作权限，无须告诉操作系统登录密码
	VNC单点登陆授权	是否支持对VNC服务器的单点登录管理，用户不需要二次输入密码	支持	奇智不支持VNC单点登录	通过代填方式可以最大限度的保护系统安全，对于那些临时访问的客户，只给其操作权限，无须告诉操作系统登录密码
	VNC高版本功能支持	VNC高版本功能完整支持，如采用windows系统认证，加密传输，文件传输等，支持最新VNC版本，无需对VNC服务器进行改造	支持	奇智不支持VNC高版本功能	完整支持VNC各版本所有功能，保留用户原有运维习惯
字符操作审计（SSH、Telnet）	终端工具支持	是否可以通过PuTTY，SecureCRT，XTERM等终端工具进行运维操作	支持	□支持 □不支持	既支持WEB方式访问统一运维安全平台，也支持客户端方式，满足不同客户的需要，保持原有操
	终端属性要求	支持任何TELNET、SSH终端属性，命令捕获效果与终端属性无关，典型终端属性包括VT100，VT102，VT220，LINUX，ANSI，XTERM等,支持在上述终端属性下,命令识别和记录功能以及回放功	支持	奇智必须指定终端属性为XTERM，否则命令识别和命令控制功能失效	对各种字符终端的各种属性均支持，不改变用户习惯，便于统一运维安全平台的推广
	B/S字符模式下分辨率和字符编码	支持分辨率任意调整大小，和灵活调整字符编码适应不同目标服务器编码设定。	支持	奇智B/S模式下提供特定分辨率，且不同终端适应性不好，影响操作，字符编码无法灵活调整，出现乱码情况高。	运维产品必须完整支持客户端属性，灵活配置调整，满足各类用户需要。
	客户端窗口任意调整大小	是否支持客户端应用窗口任意调整大小，测试在任意调节客户端窗口大小情况下，操作、审计与命令控制是否正常	支持	□支持 □不支持	若不能任意调整客户端窗口大小，将极大不方便用户的操作使用。
SFTP/FTP	FTP/SFTP实时监控，切断和录像回放	是否支持FTP/SFTP的完整操作，包括实时监控、切断、录像回放、命令分析。	支持	奇智只支持命令，查看文件的上传下载，其他功能无	文件传输的涉及到敏感信息，需要提供强大的审计功能支持，加强审计力度
	FTP/SFTP 文件传输备份	是否支持FTP/SFTP上传文件备份	支持	奇智无该功能，应对用户上传恶意脚本执行无能为力	可以将用户上传文件进行备份，防止用户上传恶意脚本进行执行，从而逃脱审计系统的审计。
HTTP/HTTPS操作	HTTP/HTTPS账号密码代填	是否可以支持HTTP/HTTPS账号密码代填	支持	奇智无该功能	完整支持系统所有应用单点登录，无缺失，保障第三方运维人员的运维安全。
虚拟应用共享	细粒度应用共享	支持细粒度应用共享，做到细粒度发布目标服务器上的单个应用，精细化授权控制，实现用户应用程序精细授权，避免用户直接登录服务器桌面。	支持	奇智无该功能	细粒度应用共享提供了进一步的图形授权，提高了图形运维的安全性
	前置机发布	支持客户环境现有终端服务器自动成为“前置机”，发布、利用和共享现有终端服务器上安装的任何应用程序；	支持	奇智无该功能	前置机发布功能提供了高扩展性，方便整合
	无限云扩展	支持无限应用共享扩展，充分发挥用户服务器闲置服务器计算能力，解决前置机计算能力限制、应用共享冲突问题、集中应用共享维护问题等；	支持	奇智无该功能	无限云扩展提供了前置机集群发布的能力，大大解决前置机计算能力限制、应用共享冲突问题、集中应用共享维护问题等
扩展能力	会同功能	支持会同功能，核心设备登录需要第三方人员再次临时授权，做到二次授权，保障目标服务器的高安全性，支持RADIUS认证结合。	支持	奇智无该功能	会同功能提供了二次授权功能，符合金融等重视安全企业的运维理念，和现有用户环境完整结合，大大简化了运维流程的复杂度
	标准SYSLOG日志输出	系统可输出标准SYSLOG日志。日志包含字符，图形，图形应用的登录情况，以及系统命令告警等，方便和第三方系统整合	支持	奇智有syslog，但不完整	
	系统自身支持集群、负载均衡	支持集群，负载均衡部署，提供高扩展性	支持	奇智无该类部署模式	方便进行部署扩展

华为UMA运维审计产品规格对比表-思福迪

功能点	华为UMA	思福迪	说明
C/S、B/S双运维接入方式支持	对所有支持的协议、应用，均支持C/S和B/S两种方式的运维操作。C/S方式支持现有运维客户端软件，无需安装独立软件工具。	所有协议只支持B/S运维方式。并且需要在管理界面中指定运维工具的绝对路径，否则无法调用。是前置机的概念。	B/S是指通过web页面进行运维操作。 C/S是指直接使用运维客户端软件直接进行运维操作，无需web登录。 在受限环境，例如无法随意安装软件情况，B/S方式可能会失效，造成完全无法运维。 运维操作完全基于Web，造成运维操作体验不友好。且IE浏览器的不稳定会造成运维操作过程的中断，严重影响运维操作的安全性一致性。
运维操作现有客户端的支持	完全支持现有运维操作客户端软件。字符类如：putty、SecureCRT。 图形类支持各版本“远程桌面连接客户端”。 支持各类字符终端属性，支持远程桌面连接完整功能。	对客户端工具的属性是无法满足。	客户端的完整支持影响用户的使用体验，每个用户都有可能有偏好的运维工具，不能强制用户使用某一特定客户端。 字符终端属性支持不完整，有可能导致用户规避审计。 远程桌面连接功能支持不完整，导致用户使用体验下降，操作复杂化。
字符类终端审计，命令识别	在各类系统环境下，准确识别用户命令。用户无法通过修改系统配置参数等方法规避审计与命令识别。	在典型系统环境下可正确识别命令。修改相关系统配置参数后，命令无法识别，只能识别为命令返回数据流。由此造成：1、无法进行命令检索；2、命令控制策略完全失效。	具体测试方法为：修改系统命令提示符，使命令提示符为空或与测试命令相同。某些审计产品的命令识别依赖于命令提示符，造成上述方法绕过审计。
字符类终端审计，命令控制策略	UMA命令控制策略基于UMA特有的底层精确命令识别功能，在任何情况下都能有效控制授权用户的操作行为，防止越权操作。	有命令控制策略。 由于命令识别能被绕过，造成命令控制策略可能完全失效。	没有严格的命令控制功能，就无法对高危命令进行有效控制。
图形类终端传输控制	支持图形终端和图形应用的文件传输控制功能：剪切板、粘贴复制、磁盘映射。	无此功能	如果不能有效控制图形传输，那不仅会造成审计纰漏；而且会造成用户本地无法与服务端进行文件传输，从而影响使用。
SFTP/FTP传输审计	支出SFTP/FTP的文件传输控制，可以完整记录原始的传输文件、文件大小、上传动作、下载动作、用户名等信息。并且可将传输文件下载下来查看其内容。	可以审计，但是无法审计原始的文件内容。	对服务器进行传输文件，关系到服务器的安全：上传升级包、补丁、脚本等；下载数据库文件、服务器的机密文件等。
字符类终端审计，命令分析	具备字符审计命令分析功能，每个命令结果可展开、收起，可从任一命令处开始播放。	无命令分析功能	命令分析功能方便用户快速定位命令操作及其操作结果，节约审计时间，提高审计效率。
图形类终端接入，单点登录	完备支持各类图形类终端接入的单点登录，包括RDP，VNC，X11。	X11不支持单点登录	单点登录功能统一用户账号管理，简化了用户操作过程。
应用类终端审计，单点登录	能够支持各类应用系统的单点登录，包括各种数据库管理开发工具；基于Web的管理工具；Radmin、PcAnywhere等第三方图形管理工具；及其他自定义应用。	不支持单点登录 用户手动进行基本配置，手动输入账号密码进行登录。	应用类的单点登录相比字符或图形的更加复杂，没种应用的登录都不相同，还包括一些配置工作。UMA系统不但能代填账号密码，还能自动配置相关服务器信息，真正做到单点登录。如Oracle服务器，需配置TNS文件。
数据库运维审计，SQL语句分析	使用数据库管理开发工具进行数据库运维操作时，能够准确记录实际提交到服务器的SQL语句，包括GUI操作、后台自动操作产生的SQL语句。 SQL语句支持查询检索，并与审计录像关联。	无法记录SQL语句	数据库管理操作，实际产生作用的是最后提交到服务器的SQL语句。很多数据库管理工具都提供GUI界面，数据库操作无需输入完整命令，进行鼠标操作即可。若无法准确提取实际提交的SQL语句，则仅凭审计录像很难定位用户的操作及其产生的后果。

华为UMA运维审计产品规格对比表-江南科友

功能点	华为UMA	江南科友	说明
当配置为外部认证模式时，双认证方式支持	当外部认证失败时，能够再进行本地认证。	只能进行外部认证，无法自动转为本地认证。	当认证服务器出现故障时，若无法自动转为本地认证，则整个服务变为不可用
C/S、B/S双运维接入方式支持	对所有支持的协议、应用，均支持C/S和B/S两种方式的运维操作。C/S方式支持现有运维客户端软件，无需安装独立软件工具。	仅telnet ssh协议支持C/S方式，其他所有协议只支持B/S运维方式。需安装基于Web的运维工具软件。	B/S是指通过web页面进行运维操作。 C/S是指直接使用运维客户端软件直接进行运维操作，无需web登录。 在受限环境，例如无法随意安装软件情况，B/S方式可能会失效，造成完全无法运维。 运维操作完全基于Web，造成运维操作体验不友好。且IE浏览器的不稳定会造成运维操作过程的中断，严重影响运维操作的安全性一致性。
运维操作现有客户端的支持	完全支持现有运维操作客户端软件。字符类如：putty、SecureCRT。 图形类支持各版本“远程桌面连接客户端”。 支持各类字符终端属性，支持远程桌面连接完整功能。	字符支持putty 图形使用自开发WebRDP控件	客户端的完整支持影响用户的使用体验，每个用户都有可能有偏好的运维工具，不能强制用户使用某一特定客户端。 字符终端属性支持不完整，有可能导致用户规避审计。 远程桌面连接功能支持不完整，导致用户使用体验下降，操作复杂化。
字符类终端审计，命令识别	在各类系统环境下，准确识别用户命令。用户无法通过修改系统配置参数等方法规避审计与命令识别。	在典型系统环境下可正确识别命令。修改相关系统配置参数后，命令无法识别，只能识别为命令返回数据流。由此造成：1、无法进行命令检索；2、命令控制策略完全失效。	具体测试方法为：修改系统命令提示符，使命令提示符为空或与测试命令相同。某些审计产品的命令识别依赖于命令提示符，造成上述方法绕过审计。
字符类终端审计，命令控制策略	PLD命令控制策略基于PLD特有的底层精确命令识别功能，在任何情况下都能有效控制授权用户的操作行为，防止越权操作。	有命令控制策略。 由于命令识别能被绕过，造成命令控制策略可能完全失效。	
字符类终端审计，命令分析	具备字符审计命令分析功能，每个命令结果可展开、收起，可从任一命令处开始播放。	无命令分析功能	命令分析功能方便用户快速定位命令操作及其操作结果，节约审计时间，提高审计效率。
图形类终端接入，单点登录	完备支持各类图形类终端接入的单点登录，包括RDP，VNC，X11。	X11不支持单点登录	单点登录功能统一用户账号管理，简化了用户操作过程。
应用类终端审计，单点登录	能够支持各类应用的单点登录，包括各种数据库管理开发工具；基于Web的管理工具；Radmin、PcAnywhere等第三方图形管理工具；及其他自定义应用。	不支持单点登录 用户手动进行基本配置，手动输入账号密码进行登录。	应用类的单点登录相比字符或图形的更加复杂，没种应用的登录都不相同，还包括一些配置工作。PLD系统不但能代填账号密码，还能自动配置相关服务器信息，真正做到单点登录。如Oracle服务器，需配置TNS文件。
数据库运维审计，SQL语句分析	使用数据库管理开发工具进行数据库运维操作时，能够准确记录实际提交到服务器的SQL语句，包括GUI操作、后台自动操作产生的SQL语句。 SQL语句支持查询检索，并与审计录像关联。	无法记录SQL语句	数据库管理操作，实际产生作用的是最后提交到服务器的SQL语句。很多数据库管理工具都提供GUI界面，数据库操作无需输入完整命令，进行鼠标操作即可。若无法准确提取实际提交的SQL语句，则仅凭审计录像很难定位用户的操作及其产生的后果。
字符类终端审计	没有该问题	字符审计数据大于一定量（10M左右）就会导致该会话的字符命令完全无法打开，只能进行录像回放，无法快速定位指令操作。	直接导致字符审计无效
	可以通过命令控制功能对字符操作下的数据库操作命令进行控制，如阻止对某个表的操作。	无该功能	对字符命令的SQL语句命令控制能够有效保证数据库操作的安全
	江南科友支持C/S字符运维，但是在细节上不够重视，如不提供目标设备IP动态匹配功能，当运维设备较多时，难以快速找到希望运维的目标设备。	C/S字符运维支持，但是没有IP动态匹配功能，当运维设备较多时，难以快速找到希望运维的目标设备。	提供目标IP动态匹配功能，能够快速定位到要访问的目标设备

华为UMA运维审计产品规格对比表-国迈

对比项		测试内容	华为	国迈	说明
数据库运维操作审计	管理方便性	统一运维安全平台是否可以代填各种数据库维护工具（PISQL/TOAD/SQLPLUS/OEMC）的登录账号和密码	支持	国迈不支持代填	通过代填方式可以最大限度的保护系统安全，对于那些临时访问的客户，只给其操作权限，无须告诉数据库登录密码
	管理的精细性	是否可以在统一运维安全平台中针对同一台目标数据库的账号和服务进行授权	支持	国迈不支持	针对同一台Oracle服务器的各个数据库服务、不同账号是否可以授权管理，而不是只能针对某台Oracle服务器
	数据库数据的防泄露	是否可以授权运维人员具备保存、复制权限的控制	支持	国迈无法控制剪贴板复制粘贴功能	实现敏感数据安全保护，防止复制、另存、截屏等方式的信息泄露
	数据库支持全面性	是否支持oracle、sybase、DB2、SQLserver、informix、mysql主流数据库的各类数据库客户端单点登录和SQL语句提取。	支持	国迈只支持一部分	数据库运维审计全面覆盖，保障用户运维审计无缺失，漏洞
用户特有客户端应用发布	特有客户端应用发布	支持发布Radmin、PCAnywhere、AS400、DameWare、CiscoASDM、RealVNC4	支持	国迈只支持一小部分	完整支持用户环境各类特定应用，通过应用发布平台集中管理和审计，保障用户运维审计无死角
	特有客户端单点登录	支持Radmin、PCAnywhere、AS400、DameWare、CiscoASDM、RealVNC4的账号密码代填，实现单点登录	支持	国迈完全不支持	通过代填方式可以最大限度的保护系统安全，对于那些临时访问的客户，只给其操作权限，无须告诉数据库登录密码
图形操作审计（RDP、VNC、X11）	RDP客户端多版本支持	测试RDP客户端支持各种版本MSTSC，包括RDP6.0，WINDOWS XP SP3，WINDOWS VISTA SP1，WIN7访问目标资产	支持	国迈无法支持MSTSC直接连接远程桌面，必须使用特定客户端	很多客户希望沿用原有的RDP访问方式，不改变用户习惯，便于统一运维安全平台的推广
	是否可以全屏访问	是否可以实现真正意义上的全屏操作（完全满屏），包括各种电脑终端（宽屏笔记本）	支持	国迈只提供几种分辨率选择，对全屏支持不完善，且经常需要拖动IE控制条以查看全部屏幕	如果不能够全屏操作，用户需要拉动滚动条来调整，操作体验很难受
	拷贝粘贴	是否支持各版本RDP客户端双向拷贝/粘贴功能，测试剪贴板通道支持情况	支持	国迈无法对剪贴板的负责粘贴功能进行打开/关闭控制	尽可能保留RDP客户端通道各个有价值功能，并对其进行控制，避免信息泄露
	Console控制台模式支持	是否支持RDP的console/admin控制台模式	支持	国迈不支持	该功能在特定的场景下具备不可替代的作用，必须予以支持
	分辨率和屏幕大小设置	是否支持通过RDP客户端里面的选项设置目标资产服务器的登录屏幕大小和分辨率	支持	国迈只支持特定分辨率，且全屏化有缺陷	严重影响用户使用体验
	X11单点登录	测试是否支持X11单点登陆，用户不需要二次输入密码	支持	国迈不支持X11单点登录，单点登录体系崩坏	通过代填方式可以最大限度的保护系统安全，对于那些临时访问的客户，只给其操作权限，无须告诉操作系统登录密码
	VNC单点登陆授权	是否支持对VNC服务器的单点登录管理，用户不需要二次输入密码	支持	国迈不支持VNC单点登录	通过代填方式可以最大限度的保护系统安全，对于那些临时访问的客户，只给其操作权限，无须告诉操作系统登录密码
	VNC高版本功能支持	VNC高版本功能完整支持，如采用windows系统认证，加密传输，文件传输等，支持最新VNC版本，无需对VNC服务器进行改造	支持	国迈不支持VNC高版本功能	完整支持VNC各版本所有功能，保留用户原有运维习惯
字符操作审计（SSH、Telnet）	终端工具支持	是否可以通过PuTTY，SecureCRT，XTERM等终端工具进行运维操作	支持	国迈不支持	既支持WEB方式访问统一运维安全平台，也支持客户端方式，满足不同客户的需要，保
	终端属性要求	支持任何TELNET、SSH终端属性，命令捕获效果与终端属性无关，典型终端属性包括VT100，VT102，VT220，LINUX，ANSI，XTERM等,支持在上述终端属性下,命令识别和记录功能以及回放功能正常	支持	国迈必须指定终端属性为XTERM，否则命令识别和命令控制功能失效	对各种字符终端的各种属性均支持，不改变用户习惯，便于统一运维安全平台的推广
	B/S字符模式下分辨率和字符编码	支持分辨率任意调整大小，和灵活调整字符编码适应不同目标服务器编码设定。	支持	国迈B/S模式下提供特定分辨率，且不同终端适应性不好，影响操作，字符编码无法灵活调整，出现乱码情况高。	运维产品必须完整支持客户端属性，灵活配置调整，满足各类用户需要。
	客户端窗口任意调整大小	是否支持客户端应用窗口任意调整大小，测试在任意调节客户端窗口大小情况下，操作、审计与命令控制是否正常	支持		若不能任意调整客户端窗口大小，将极大不方便用户的操作使用。
SFTP/FTP	FTP/SFTP实时监控，切断和录像回放	是否支持FTP/SFTP的完整操作，包括实时监控、切断、录像回放、命令分析。	支持	国迈只支持命令，查看文件的上传下载，其他功能无	文件传输的涉及到敏感信息，需要提供强大的审计功能支持，加强审计力度
	FTP/SFTP	是否支持FTP/SFTP上传文件备份	支持	国迈无该功能，应对用户上传恶意脚本执行无能为力	可以将用户上传文件进行备份，防止用户上传恶意脚本进行执行，从而逃脱审计系统的审计。
	文件传输备份		支持		
HTTP/HTTPS操作	HTTP/HTTPS账号密码代填	是否可以支持HTTP/HTTPS账号密码代填	支持	国迈无该功能	完整支持系统所有应用单点登录，无缺失，保障第三方运维人员的运维安全。
虚拟应用扩展	前置机发布	支持客户环境现有终端服务器自动成为“前置机”，发布、利用和共享现有终端服务器上安装的任何应用程序；	支持	国迈无该功能	前置机发布功能提供了高扩展性，方便整合
服务器集体改密	改密功能	支持对目标资产linux/Unix/网络设备、windows服务器进行密码自动修改	支持	国迈无此功能	自动改密大大降低了管理员的工作量，做到密码统一管理
扩展能力	会同功能	支持会同功能，核心设备登录需要第三方人员再次临时授权，做到二次授权，保障目标服务器的高安全性，支持RADIUS认证结合。	支持	国迈无该功能	会同功能提供了二次授权功能，符合金融等重视安全企业的运维理念，和现有用户环境完整结合，大大简化了运维流程的复杂度
			支持		
	标准SYSLOG日志输出	系统可输出标准SYSLOG日志。日志包含字符，图形，图形应用的登录情况，以及系统命令告警等，方便和第三方系统整合	支持	国迈有syslog，但不完整	
	系统自身支持集群、负载均衡	支持集群，负载均衡部署，提供高扩展性	支持	国迈无该类部署模式	方便进行部署扩展

华为UMA运维审计产品规格对比表-启明网域星云

	技术指标	华为UMA	网御星云
1	资质要求		产品需具备中华人民共和国国家版权局核发的《计算机软件著作权登记证书》
			需具备国家保密局涉密信息系统安全保密测评中心核发的《涉密信息系统产品检测证书》
			需具备公安部监制的《计算机信息系统安全专用产品销售许可证》
			产品具有中国信息安全认证中心颁发的强制认证证书；
2	专用硬件	采用华为专用应用服务器	需采用专用工业用计算机硬件设计
3	端口数量	需提供至少4个10/100/1000网口	需提供至少4个10/100/1000网口
4	并发会话	≥1000个	≥1500个
5	审计操作延迟	<100毫秒	<100毫秒
6	最大功耗	<300W	<300W
7	支持审计协议	▲图形会话操作：Windows RDP、VNC、X-Window ▲字符会话操作：Telnet、SSH ▲文件传输：FTP、SFTP、SCP ▲WEB操作方式：HTTP、HTTPS	终端命令操作：Telnet、SSH、Rlogin
		系统支持微软远程桌面客户端各版本以及各版本RDP通道功能，包括但不限于RDP磁盘镜像、剪贴板、串行口。支持RDP控制台操作模式。支持图形会话下的文件传输控制，如可控制剪贴板复制粘贴，磁盘映射，以及对智能卡的支持	Windows图形操作：RDP多版本
		系统支持Unix/linux下X-windows、Xmanger以及VNC的图形会话监控和审计	Unix/linux图形操作：X-windows、Xmanger等
		系统支持监控通过ftp/sftp协议进行的文件传输过程，并可实现实时监控及切断传输功能。并且支持对传输文件进行备份。	文件传输操作：FTP、SFTP、SCP等
		WEB监控审计支持HTTP/HTTPS应用。并且支持数字KVM平台运维审计及密码代填。	浏览器操作：http、https等
8	支持设备类型	支持各类目前所有的操作系统版本，包含主流的windows、AIX、HP-UNIX、Solaris、AS400、linux等各版本操作系统	服务器系统：windows、AIX、HP-UNIX、Solaris、AS400、linux等各版本操作系统
		支持各类目前所有的终端设备类型，包含主流的VT100、VT102、VT220、ANSI、XTERM、windows CE等。	终端设备：VT100、VT102、VT220、ANSI、XTERM、windows CE等。
		支持主流的网络设备，包含：华为全系列设备、cisco全系列设备、H3C设备、各类网络防火墙	网络设备：华为全系列设备、cisco全系列设备、H3C设备、各类网络防火墙
9	用户管理	支持管理员创建用户、用户自注册，实现系统用户与自然人间一一对应。 支持用户在所有权限的资源上建立账号，及配置扩展属性。 按照SOX方案要求定义用户密码强度，自动更新账号密码，可通过邮件方式通知用户修改后的密码。 对于用户有效期、密码有效期、密码修改有限制	具有创建、修改、删除、查找、冻结、恢复用户账号等基本功能，通过记录手段保留账号创建、分配、变更删除整个过程的信息
			具有临时帐户功能，支持一般用户功能，而且可以定期定时回收
			支持从堡垒主机统一管理资源帐号，包括新建，修改，同步等
10	角色管理	具有创建、修改、删除、查找、冻结、恢复用户角色等基本功能，支持一个用户拥有多个角色，可根据需要（登录系统、数据库的不同，使用系统用户的不同等）划分多个角色。	具有创建、修改、删除、查找、冻结、恢复用户角色等基本功能，支持一个用户拥有多个角色，可根据需要（登录系统、数据库的不同，使用系统用户的不同等）划分多个角色。
11	流程与工单		堡垒主机添加被管资源、增加主帐号授权时，需提供相应流程与工单支持以针对增加资源和权限进行审计
12	从帐号管理		需支持双人共管、共管、接管等不同类型的从帐号管理机制
13	登录控制	支持Solaris,IBM AIX,HP-Unix, UNIXWARE, SCO Unix,DEC,Linux 系列主机Telnet/SSH接入并提供单点登录功能。支持B/S结构、C/S结构应用系统单点登录功能并提供用户自服务功能	支持单点登录，即一次登录可访问多个系统、数据库，可与指纹识别、CA、LDAP等系统集成，提供临时CA解决方案

14			可实现基于用户、目标设备、系统账号、时间设定比较详细的访问控制列表，可以对用户访问权限进行查看、变更、删除等操作。
15	数据库运维审计	系统支持oracle、sybase、DB2、informix、mssql、SQL Server主流数据库；	支持oracle、sybase、DB2、informix、mssql、mysql等主流数据库；
			按照客户需要，可以添加不同的数据库客户端程序（可根据具体情况协商），
16	密码托管	支持各种操作系统Windows系列、linux系列、Unix系列、AIX等；	支持各种操作系统Windows系列、linux系列、Unix系列、AIX等；
		支持各种网络设备、防火墙设备；	支持各种网络设备、防火墙设备；
		支持单台设备、操作系统单个密码自动修改；	支持单台设备、操作系统单个密码自动修改；
		支持部分设备、操作系统部分密码自动修改；	支持部分设备、操作系统部分密码自动修改；
		支持不同级别的密码负复杂程度修改策略；	支持不同级别的密码负复杂程度修改策略；
		密码修改策略灵活可配置	密码修改策略灵活可配置
17	实时监控当前操作	可实时监控用户当前在进行的操作	可实时监控用户当前在进行的操作
		能够对操作进行拒绝、禁止的控制	能够对操作进行拒绝、禁止的控制
		支持黑名单（不许执行）和白名单（只允许执行）	支持黑名单（不许执行）和白名单（只允许执行）
		支持对关键操作进行多种警告方式	支持对关键操作进行多种警告方式
18	操作控制	完整、清晰记录用户所有操作内容，包括鼠标点击和键盘输入等图形操作；	完整、清晰记录用户所有操作内容，包括鼠标点击和键盘输入等图形操作；
		完整、清晰、无延迟回放用户操作过程；	完整、清晰、无延迟回放用户操作过程；
19	操作警告	无	支持web界面直接回放；
20	操作回放，搜索定位	支持高/低倍速回放、快进、后退、暂停、进度任意拖放等快速定位功能；	支持高/低倍速回放、快进、后退、暂停、进度任意拖放等快速定位功能；
		支持无延时的拖拉式回放；	支持无延时的拖拉式回放；
		回放时自动过滤静止时间；	回放时自动过滤静止时间；
		回放时可以任意截取当前屏幕，并保存为图片	回放时可以任意截取当前屏幕，并保存为图片
		可以根据操作内容、执行语句对记录内容进行搜索，快速定位	可以根据操作内容、执行语句对记录内容进行搜索，快速定位
	日志记录	支持最低3年的日志存储要求	可以按照需要产生日志文件
21	报表查看	可以根据日期、审计用户、来源IP、目标设备、系统账号、服务类型（终端命令，图形操作）进行统计和查询；	可以根据日期、审计用户、来源IP、目标设备、系统账号、服务类型（终端命令，图形操作）进行统计和查询；
		统计结果显示为登录时间、退出时间、用户账号、用户地址、设备名称、设备地址、系统账号、服务类型、操作结果	统计结果显示为登录时间、退出时间、用户账号、用户地址、设备名称、设备地址、系统账号、服务类型、操作结果
22	会话安全	用户登录运维系统设备的传输过程必须采用SSH、https方式加密；用户通过各种运维客户端如CRT、MSTSC登录远程资源时，采用一次性会话口令登录	用户登录运维系统设备的传输过程必须采用SSH、https方式加密；用户通过各种运维客户端如CRT、MSTSC登录远程资源时，采用一次性会话口令登录，而不是资源从帐号
23	操作系统	提供服务器以及操作系统加固	堡垒主机本身操作系统需保证其安全性
24	部署安全	部署堡垒主机不能给网络带来新的安全隐患，如增加新的开放端口等	部署堡垒主机不能给网络带来新的安全隐患，如增加新的开放端口等
25	集群部署	支持多台服务器分布式部署以及集群部署，采用统一中心策略对各个服务器进行动态运维压力均衡	支持多台堡垒主机分布部署、集群部署，采用同一登录入口登录多台堡垒主机
26	支持双机	支持两台服务器进行双机热备，提供服务器的运行可靠性	支持两台或两台以上堡垒主机互相备份部署，以提高可靠性
27	支持外接存储	服务器配备7块1T SATA盘作为数据盘，磁盘做了RAID冗余，保障了审计数据的安全； 配备2块1T SATA盘作为系统盘，保障UMA系统的冗余。 并提供最大20T的存储扩展	需支持与NAS等外接存储设备相连
28	支持4A项目扩展	堡垒主机需支持已建4A项目结合或将来与扩展的4A项目方案结合	堡垒主机需支持已建4A项目结合或将来与扩展的4A项目方案结合
29	售后服务	提供原厂5年7*24小时用户现场免费硬件保修及免费软件系统升级维护，并提供原厂售后服务承诺函	提供原厂5年7*24小时用户现场免费硬件保修及免费软件系统升级维护，并提供原厂售后服务承诺函

华为UMA运维审计产品规格对比表-Citrix

功能	细节	UMA	Citrix
产品侧重点		UMA侧重于运维操作的统一平台实现和行为的审计记录，关注人机交互的过程记录。实现统一认证，集中授权，集中账号管理，统一审计4A管理。	Citrix 致力于桌面，应用和服务器虚拟化变革，专注于应用和桌面的虚拟化交付。
网络部署		旁路部署，逻辑网关：不受客户网络设备影响；不影响客户的网络架构；不加装任何服务端引擎；不用安装任何客户端软件；不影响业务数据流；支持双热备；支持分级部署，集中管理。	网关部署，在企业应用和用户层之间增加了一层虚拟化层，实现对应用和桌面的虚拟发布。
互补点	总体	UMA和Citrix的侧重点不同，UMA侧重运维操作的4A管控，Citrix侧重虚拟化应用和桌面交付，双方的互补大于竞争。Citrix的虚拟化交付的同时，缺少了对其整个交付过程和交付应用的审计记录功能，缺少人机交互的有效授权（Citrix可以对应用进行授权，却无法对应用的交互对象和其使用账号的授权）以及对服务器账号的集中管理，这些缺失内容都可以通过部署UMA进行完善	
	对象	1、UMA系统建立UNIX类服务器、LINUX类服务器、Windows类服务器、网络\安全等重要设备、数据库运维的统一操作管理平台，统一操作管理入口，并对用户操作管理等网络访问行为进行控制，避免用户直接接触目标服务器重要资源，构建安全规范的服务器操作管理唯一通道。 2、UMA系统建立统一的字符终端操作审计平台、统一的图形终端操作审计平台、统一的文件传输操作审计平台、统一的KVM操作审计平台、统一的WEB操作审计平台、统一的数据库操作审计平台以及统一的企业环境应用操作审计平台。	Citrix XenApp 是一个按需应用程序交付解决方案，可以实现在数据中心中对任何 Windows 应用程序进行虚拟化、集中化和管理，并立即作为服务交付给任何设备上的任何用户。 XenApp 减少了高达 50% 的应用程序管理成本，提高了 IT 交付应用程序给分发的用户时的响应，并改进了应用程序和数据的安全性。
	统一认证	1、在部署UMA系统的同时需要给每一个运维人员建立唯一的自然人账号，配置要管辖的主机资源，建立主机的资源账号，根据业务需要，配置访问控制策略，每个人能以什么身份访问主机，建立自然人与主机账号的对应关系。 2、UMA系统同时提供账号密码集中管理模式和分散管理模式。账号密码集中管理模式集中管理目标设备账号密码，自动实现单点登录；账号密码分散管理模式提供密码手工输入和用户名、密码都手工输入两种形式。 3、UMA系统统一身份管理支持本地认证、RADIUS认证、Windows双域认证和PKI认证。	Citrix可以在部署虚拟化的前提下对桌面虚拟化和应用虚拟化统一账号管理，该认证主要是针对桌面或应用的访问权限，而UMA针对的是远程运维操作的身份认证。
	集中授权	UMA可以对远程运维的权限进行集中授权，可以对资源IP，访问协议，访问账号密码进行3元授权，实现对谁用什么方式采用什么账号登录哪台设备进行集中管控。	Citrix授权针对应用和桌面进行授权，即谁能够访问哪台设备或能够使用什么应用程序。
竞争点	主要竞争点	Citrix XenApp最近应中国市场需求推出了黄金版，该版本推出了安全审计功能，该功能和UMA的审计产生了冲突和竞争，是UMA和Citrix的最大竞争点	
	访问控制	1、UMA系统为运维人员的实名用户建立统一的授权访问控制视图。包括：用户所能访问的主机、数据库、网络设备地址、使用的相应帐户，以及相应的协议及相应策略等信息。 2、UMA系统已经实现用户接入访问控制，可以根据用户发起访问地址、地址段、目标设备、设备账号、访问时间等进行访问控制。在授权的同时，进一步提供访问控制视图。如：某用户非工作时间不能访问某授权主机等。 3、UMA系统提供文件传输授权控制，可以控制FTP、SFTP文件传输；可以控制用户RDP剪贴板拷贝粘贴；可以控制用户RDP磁盘镜像文件传输等。	Citrix XenApp只能对用户到应用工具的调用做到访问控制，即应用工具授权，但是无法对利用该工具连接目标资源的行为进行深入的访问控制。其能做到的文件传输控制只有本地和目标资源的文件复制粘贴等子通道控制
	命令控制	UMA系统可以对任何UNIX类服务器、LINUX类服务器、Windows类服务器、网络\安全等重要设备、数据库等服务器进行命令上的管控：可以通过账号、IP、时间、单个命令、命令集实现允许、警告和拒绝功能。防止不良命令的执行给服务器带来问题，如：关机，脚本命令、下载命令、上传命令等。	无法做到命令级别的控制
	审计记录	1、UMA系统提供统一的监控和回放机制 2、UMA系统实时识别用户操作命令，可根据命令，时间进行回放，节约审计时间。 3、UMA系统提供多因素匹配查找搜索定位会话功能，审计用户可以根据用户名称、账号、IP、时间、操作命令等进行回放。 4、UMA系统提供中止/暂停/强制退出等动作，审计用户实时监控用户操作，当发现违规事件，可随时中止/切断用户操作，防止灾害发生。 5、UMA系统提供审计数据批量导出功能，导出数据可回放，可审计。	审计记录只有录像回放，无法对其行为进行深度解析，无有效的查询和搜索手段，导致审计日志处于不可用状态
	账号管理	UMA可以对目标服务器账号密码进行统一管理，实现对这些应用的单点登录，并能够自动执行改密任务，自动更改服务器密码	无法对账号密码进行有效管控