

UNIS A2000-E60系列 运维审计系统

➤ 产品概述

随着国产 IT 信息化的建设，自主可控的业务应用、网络设施、存储服务、数据库等系统及设备也不断增加，面临因开发、运营、维护等核心工作过程中带来了诸多管理风险，如身份不明、越权访问、违规操作、操作过程不透明、事件不可溯等。

与此同时，安全系统及设备在保护其他信息化对象的情况下，其自身也面临需要实现真正的自主可控，既要符合信息中心的整体国产化建设目标，又要符合法律法规的要求：

- 《国家安全法》第二十五条明确规定“加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控。”
- 《网络安全法》第十六条明确要求“支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务。”
- 《网络产品和服务安全审查办法》（试行）则明确提出是“为提高网络产品和服务安全可控而制定的。”
- 等保 2.0 中从安全技术、安全人员、安全流程、安全运维等维度对“安全管理”提出了明确的要求。

紫光恒越基于多方面的技术积累与多年的数据中心建设经验，并结合各种法律法规的要求，从硬件平台到核心芯片再到操作系统全新设计了安全自主可控的运维管理系统，帮助用户解决国产化数据中心 IT 管理过程中存在的操作风险与管理问题，并更好应对严苛的政策合规要求，日益复杂的运维环境变化，以及不断革新的技术挑战。



UNIS A2000-E60 系列 运维审计系统产品

➤ 产品特点

◆ 国产化的安全产品

- 采用了国产 CPU，让 UNIS 运维安全管理平台的核心器件实现国产化
- 采用了银河麒麟操作系统，让 UNIS 运维安全管理平台的操作系统层面实现安全可靠
- 采用了经国家密码管理局认证的国密标准动态令牌，让 UNIS 运维安全管理平台的身份认证实现安全可靠

◆ 全面的运维兼容性

- 支持通过 IE、Firefox、Chrome、Safari 等浏览器进行系统管理及资产访问，同时不依赖 JRE、Flash 环境
- 操作终端兼容 windows 及 Mac 操作系统，在此基础上，支持统信、中标麒麟、银河麒麟等国产化终端桌面操作系统的运维环境
- 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP；可通过应用发布的方式进行协议扩展，如数据库 Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具
- 支持主流 IT 资产，包括主机、网络设备、安全设备、应用、中间件、数据库等
- 支持通过应用发布进行访问协议扩展，统一纳管 B/S 和 C/S 资产，创新性的支持 Linux 外置应用发布服务器，满足用户信创环境下的场景需求
- 支持基于 HTML 5 的会话访问技术，全面兼容 Windows、Linux、国产麒麟系统、Android、IOS、MacOS 等客户端仅需通过浏览器即可访问 SSH、Telnet、VNC、Xdmcp、Xfwd、RDP、应用发布等协议

◆ 可视化的管理模式

- 支持按不同属性对资产进行多级分类并自动生成动态的树状结构视图，清晰的展示各资产的层级关系
- 借助数据状态标签，自动的统计敏感、异常的用户及资产数据，帮助管理员在海量用户及资产信息应用场景中洞察异常数据
- 通过权限自动化关联分析，直观的展示出用户/资产的权限划分情况，落实权限最小化管理

◆ 细粒度的权限控制

- 系统支持多种认证方式，包括本地静态认证、TOTP 认证、手机 APP 认证，同时可与第三方 AD 域、LDAP、radius 认证系统相结合

- 借助属性建模的方式创建动态的访问控制策略，与动态权限规则相匹配的用户、资产及系统账号会自动赋予相应的访问权限，以此简化权限管理复杂度
- 采用变更单模式实现权限的一键维护，变更单无需审批，但可以自动生成具有时效性的访问权限，使得权限管理变得更加灵活
- 领先的会话复核技术，在传统双人授权的模式上，提供深层次的会话管控手段，复核人可对用户的操作权限进行回收、下放及命令实时批复，进一步提升运维管控能力

◆ 可靠的密码管理

- 支持自动化密码管理功能，实现资产账号定期改密，同时具备密码自动拨测、多人分段保管、改密前后异地备份、改密触发校验等多种改密冗余机制确保密码变更的可靠性
- 提供密码动态管理模式，通过密码工单实现资产系统账号密码的动态申请、下放，工单具有时效性，过期后交由系统自动回收变更密码，降低密码管理风险
- 支持资产密码版本库，可同时记录资产系统账号的历史维护密码，并可根据用户需求进行密码备份及回退

◆ 全面的行为审计

- 完整记录各类运维操作行为，包括图形会话、字符会话、数据库会话及文件传输会话
- 独特的图形审计存储机制，采用协议分析记录、高压缩比、空闲操作审计记录无变化，减少审计日志的大小，提高空间利用率
- 精准的指令识别技术，确保各种非常规操作指令的准确识别，同时支持指令分层展示，敏感操作智能标记及命令分级播放功能

◆ 丰富的检索方式

- 采用三层存储架构，将配置信息、审计数据、审计索引分离存储，有效解决了在大数据应用场景下，数据响应慢的问题
- 基于专业的大数据检索引擎 ES，通过全量、全索引的检索模式，缩短 TB 级审计数据的检索时间，进一步提高审计检索效率
- 具备丰富的、多维度的检索方式，提升问题定位效率，包括会话热点排序、敏感会话统计局、多关键字检索、审计会话合并、图形切片等

◆ 高效的运维管理

- 具备运维账号自动化同步功能，可自动同步 AD/LADP 域认证服务器中账号的变更信息，降低管理复杂度
- 支持会话批量启动及基于网盘的文件批量分发功能，简化运维操作
- 通过脚本一键批量执行帮助管理员提高运维管理效率

◆ 领先的 IPv6 管理能力

- 全面兼容各类 IPv6 环境，满足数据中心的未来发展规划
- 支持基于 IPv6 环境的系统管理、集中认证、权限管控及行为审计，实现 IPv6 资产的全面集中管控
- 借助 IPv4/IPv6 双栈及隧道技术，帮助用户实现数据中心 IPv4 到 IPv6 的迁移过渡

◆ 支持国密改造要求

- 支持对使用国密动态令牌和国密 USBkey 登录的用户进行身份鉴别，保证应用系统用户身份的真实性；
- 支持国密 HTTPS 数据通道加密技术，保证信息系统应用的重要数据在传输过程中的完整性及机密性；
- 支持对资源访问控制信息及日志记录进行签名和验签，保证其数据的完整性和真实性。

◆ 可靠的部署模式

- 采用旁路部署模式，不需要调整用户网络架构，不需要在服务器上安装插件
- 支持双机 HA 热备，实现运维审计系统冗余化部署
- 支持自身多机集群部署，无需第三方负载均衡设备或共享存储，即可满足用户高并发、高可用的应用需求
- 支持多站点部署模式，满足多个数据中心高冗余的应用需求，实现异地灾备运维管理
- 支持总分部署模式，满足总部集中管控、分支分散运维的运维安全管理需求

产品规格

表1-1 UNIS A2000-E60 系列运维审计系统产品规格

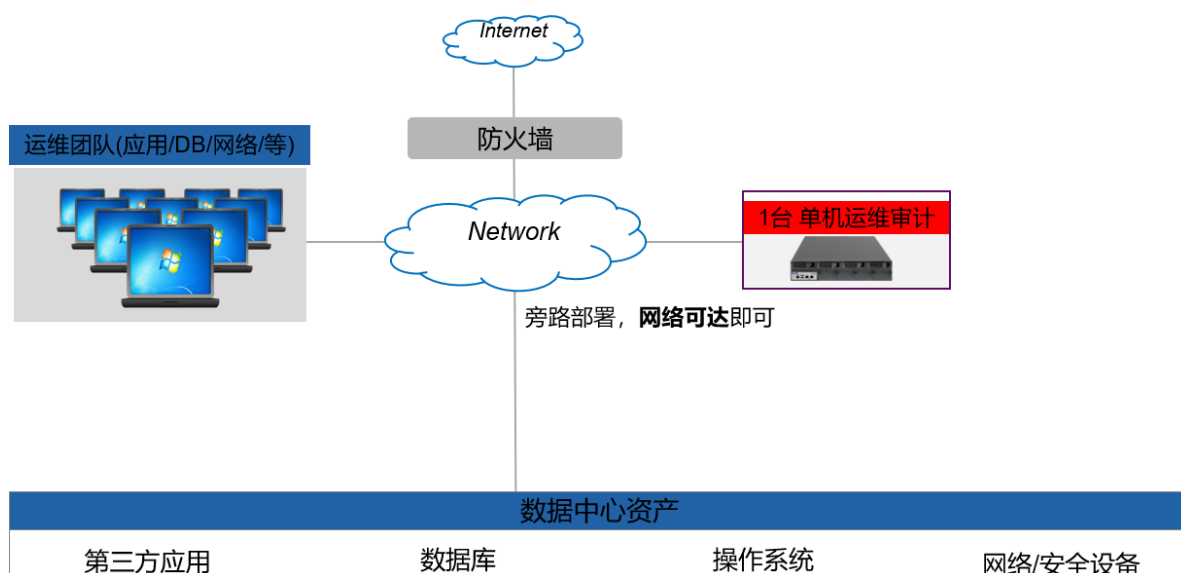
属性	A2000-E60
兼容性	支持IE、Firefox、Chrome、Safari等多种浏览器 支持Windows、Mac及主流国产化操作终端 支持中/英文界面切换 支持基于HTML 5的会话访问技术，全面兼容Windows、Linux、国产麒麟系统、Android、IOS、MacOS等客户端 支持IPv4及IPv6应用环境
部门管理	支持部门分级管理 支持部门分权管理，不同部门管理员仅能管理审计各自部门的用户及资产
用户管理	支持通过内置的用户角色实现系统分权管理 支持自定义用户角色，并可依据角色灵活配置相应系统模块的管理访问权限 支持本地静态密码认证 支持与AD、LDAP、RADIUS、短信平台等第三方认证平台对接 支持动态令牌、国密算法动态令牌、手机令牌、USBKEY等双因素认证 支持用户组管理 支持通过EXCEL表格批量导入、导出用户信息 支持通过LDAP用户批量同步 支持通过WEB页面批量修改用户属性
资产管理	支持主机资产管理，包括Windows、Linux/Unix等 支持大型机资产管理，包括IBM AS 400等 支持网络设备资产管理，包括Cisco、Huawei、Juniper、H3C等 支持管理各种C/S和B/S应用 支持数据库资产管理，包括Oracle、MS SQL Server、MySQL、DB2等 支持中间件资产管理，包括WebLogic等 支持自定义资产类型 支持按资产不同属性对资产进行多级分类，并以树状结构进行图形化展示 支持资产组管理 支持通过EXCEL批量导入、导出资产信息 支持通过WEB页面批量修改、删除资产信息
密码管理	支持资产账号密码托管，实现资产单点登录功能 支持系统账号密码触发式校验功能，对托管的口令进行验证 支持基于资产、系统账号、改密时间等因素创建改密计划 支持自定义密码规则，包括密码策略、是否分段保管、密码备份方式等
权限管理	支持配置基于用户（组）、资产（组）、系统账号、协议的静态访问权限 支持按用户、资产和系统账号属性设定动态访问规则 支持通过变更单导入方式动态管理用户访问权限 支持工单授权审批管理，工单具有时效性，过期后自动回收 支持自定义高危命令列表，并可灵活设置不同命令的响应策略（允许、拒绝、告警、复核等）及优先级

属性	A2000-E60
	支持会话审批模式，审批复核人可实时控制用户的操作权限，包括操作权限的下放、回收等 支持以用户、资产维度统计相应访问权限
资产访问	支持WEB、MSTSC、SSH Client等多种访问方式 支持会话批量启动功能 支持会话共享功能
应用发布	应用发布中心操作系统支持Windows Server2008R2、2012、2016版本，并支持linux应用发布部署 支持通过应用发布方式实现对B/S、C/S运维管理工具统一管理 支持应用发布权限管控，如URL白名单控制 支持多应用发布中心负载均衡模式
审计管理	支持RDP、X11、VNC等图形协议的行为审计 针对图形会话支持键盘、剪切板、窗口标题等事件审计 支持通过图形会话缩略图定位用户操作 支持TELNET、SSH等字符协议的行为审计 针对字符会话支持命令输入、输出分级展示 支持指令级操作回放 支持文件传输审计及附件留痕功能 支持ORACLE、MYSQL、MSSQL等数据库的行为审计，包括图像及SQL语句审计 支持在线会话实时管控 支持多关键字、多条件的审计检索，支持多条审计结果合并查看
脚本任务	支持脚本任务功能，可将用户自定义的脚本文件批量下发至目标资产执行
统计报表	支持统计用户、资产、账号和会话的基本及变更信息 支持以日、周、月、季度、年等周期自动生成相应报表数据
部署管理	支持HA部署管理 支持集群部署管理 支持多站点部署管理 支持总分部署管理

典型组网

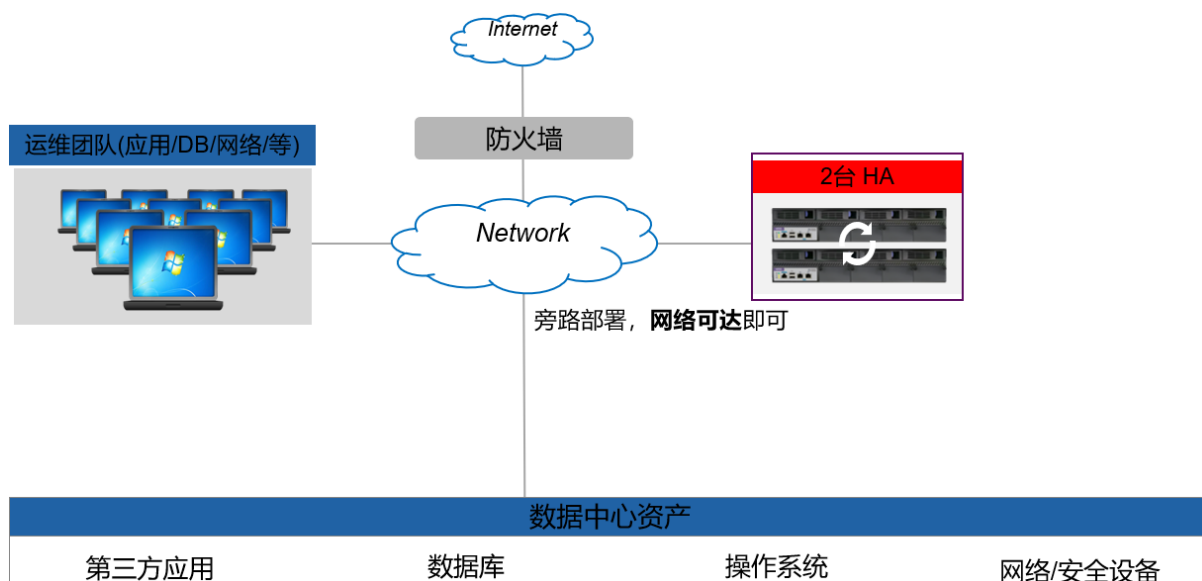
◆ 单机部署

运维审计系统单机采用物理旁路、逻辑串联的部署模式，不需要改变用户网络架构。系统上线后，运维审计系统成为唯一的运维入口，运维人员通过访问运维审计系统，实现对后端托管资源的集中管理。



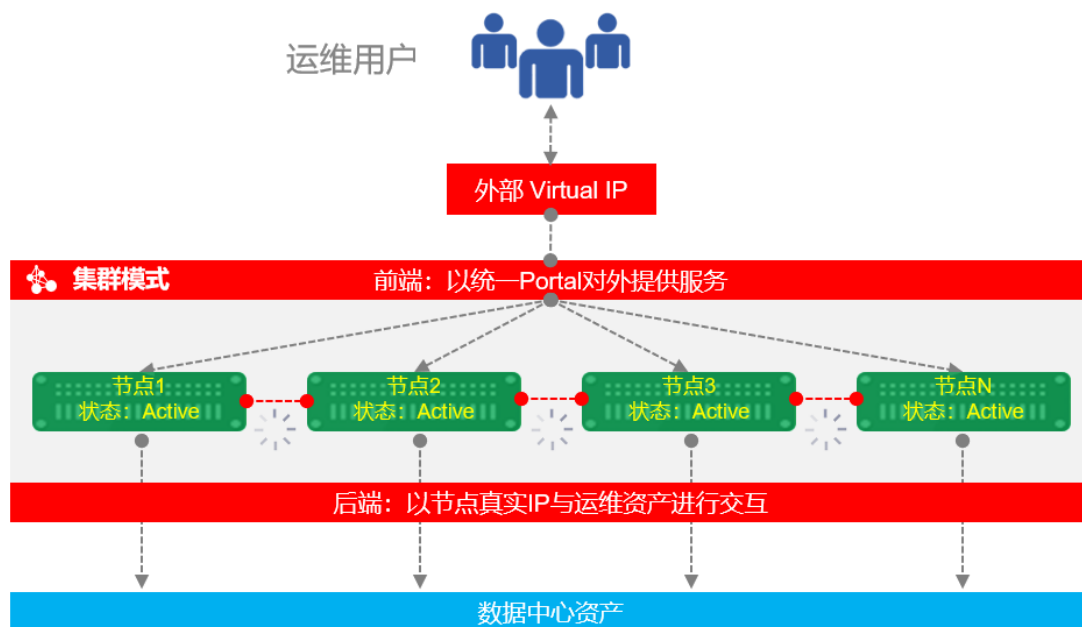
◆ 双机 HA 部署

运维审计系统支持双机 HA（一主一备）部署模式，系统部署后通过 VIP 向用户提供服务，主备设备之间定期自动同步配置数据和审计日志，当主设备异常时，由备设备自动接管相应服务，通过 HA 的部署方式提高系统的高可用性。



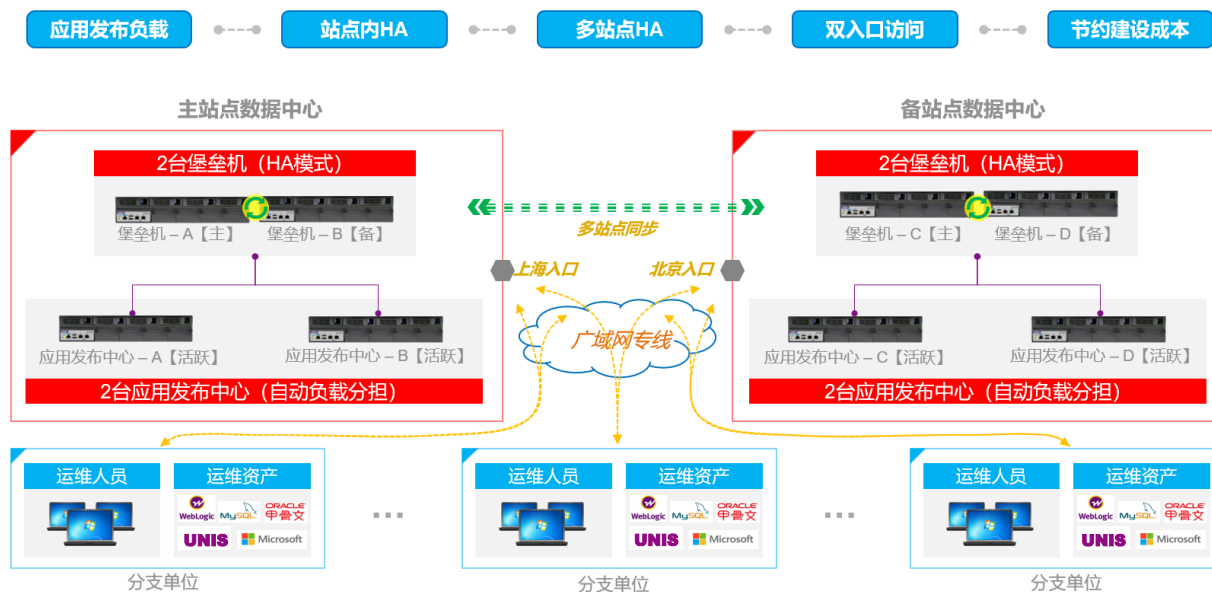
◆ 集群部署

支持三台或以上的运维审计系统组建集群部署模式，通过 VIP 对外提供服务，集群之间定期自动同步配置数据。当集群中任何一台设备出现故障时，由其他节点自动接管服务，以满足高并发、高冗余的应用需求。系统不依赖第三方负载均衡或存储设备及可完成自身集群的搭建。



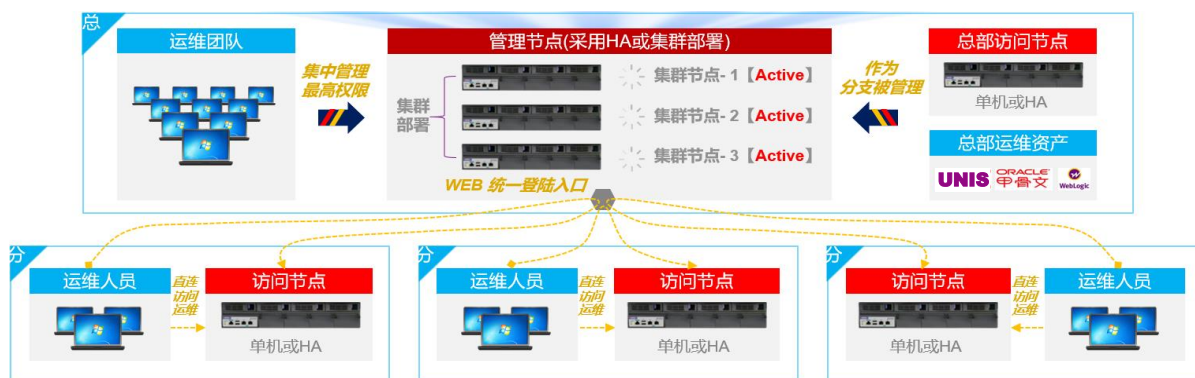
◆ 多站点部署

支持两台或以上的运维审计系统组建多站点部署模式，主站点的配置数据定期自动同步至备站点，当主站点的运维审计出现故障时，可由其他站点的运维审计按顺序自动接管服务，以满足多个数据中心高冗余的应用需求，实现异地运维管理。



◆ 总分部署

支持三台或以上的运维审计系统组建总分部署模式，通过总部的运维审计对外提供统一运维入口。总部运维审计可以部署为 HA 或集群模式，分支运维审计可以为单机或 HA。总部管理节点的配置数据定期自动同步至分支访问节点中。总分部署模式可以实现总部集中管理，分支分散运维的效果。



订购信息

UNIS A2000-E60 系列运维审计系统是紫光恒越技术有限公司自主研发的产品，用户可以根据实际需求按照型号进行选购。

◆ 主机选购一览表

主机	描述	备注
NS-A2000-E60+LIS-Z	UNIS A2000-E60运维审计系统设备	必配

◆ 资产数扩展授权函选购一览表

资产数扩展类型	描述	备注
LIS-A2000-EXT-100-Z	UNIS A2000系列 运维审计设备100资产数量扩容授权函	选配
LIS-A2000-EXT-500-Z	UNIS A2000系列 运维审计设备500资产数量扩容授权函	
LIS-A2000-EXT-UL-Z	UNIS A2000系列 运维审计设备无限资产数量扩容授权函	

◆ 配件选购一览表

配件	描述	备注
NSQM1PCGT4GP4A	4端口千兆以太网电接口+4端口千兆以太网光接口模块	选配
NSQM1PCGT8A	8端口千兆以太网电接口模块	
NSQM1PCGP8A	8端口千兆以太网光接口模块	
NSQM1PCTG4A	4端口万兆以太网光接口模块	
HDD-1T-SATA-6G-LFF-B-Z	UNIS IPC 1T SATA 3.5 寸机械硬盘模块	
HDD-2T-SATA-6G-LFF-B-Z	UNIS IPC 2T SATA 3.5 寸机械硬盘模块	
HDD-4T-SATA-6G-LFF-B-Z	UNIS IPC 4T SATA 3.5 寸机械硬盘模块	
HDD-8T-SATA-6G-LFF-B-Z	UNIS IPC 8T SATA 3.5 寸机械硬盘模块	
应用发布中心RDS授权函	应用发布中心RDS授权函	
双因素认证 动态口令卡	双因素认证 动态口令卡	
双因素认证 国密动态口令卡	双因素认证 国密动态口令卡	
双因素认证USBKey	双因素认证USBKey	

📖 说明：

“必配”表示所描述项目是设备正常运行的最小配置。

“选配”表示所描述项目是用户根据实际使用需要可选择配置。



紫光恒越技术有限公司

北京基地
北京市海淀区中关村东路1号院2号楼402室
邮编: 100084
电话: 010-82054431
传真: 010-82054401

www.unisyue.com

客户服务热线
400-910-9998

Copyright ©2023 紫光恒越技术有限公司 保留一切权利
免责声明: 虽然紫光恒越试图在本资料中提供准确的信息, 但不保证资料的内容不含有技术性误差或印刷性错误, 为此紫光恒越对本资料中的不准确不承担任何责任。
紫光恒越保留在没有通知或提示的情况下对本资料的内容进行修改的权利。