UNIS X1000-12T12F-G2漏洞扫描系统

产品概述

紫光漏洞扫描系统涵盖了资产管理、风险管理、系统扫描、web 扫描、数据库扫描、基线配置核查、口令猜解、移动应用扫描、镜像漏洞扫描、报表管理、辅助工具、日志管理、系统管理等模块，能够全面、精准地检测信息系统中存在的各种脆弱性问题，包括各种安全漏洞、安全配置问题、不合规行为等，在信息系统受到危害之前为管理员提供专业、有效的漏洞分析和修补建议。并结合可信的漏洞管理流程对漏洞进行预警、扫描、修复、审计，防患于未然。

产品适用于政府、公安、教育、电力、医疗、金融、运营商等多个行业，帮助用户解决目前所面临的各类常见的安全风险，同时满足如等级保护、行业规范等政策法规的安全建设要求。

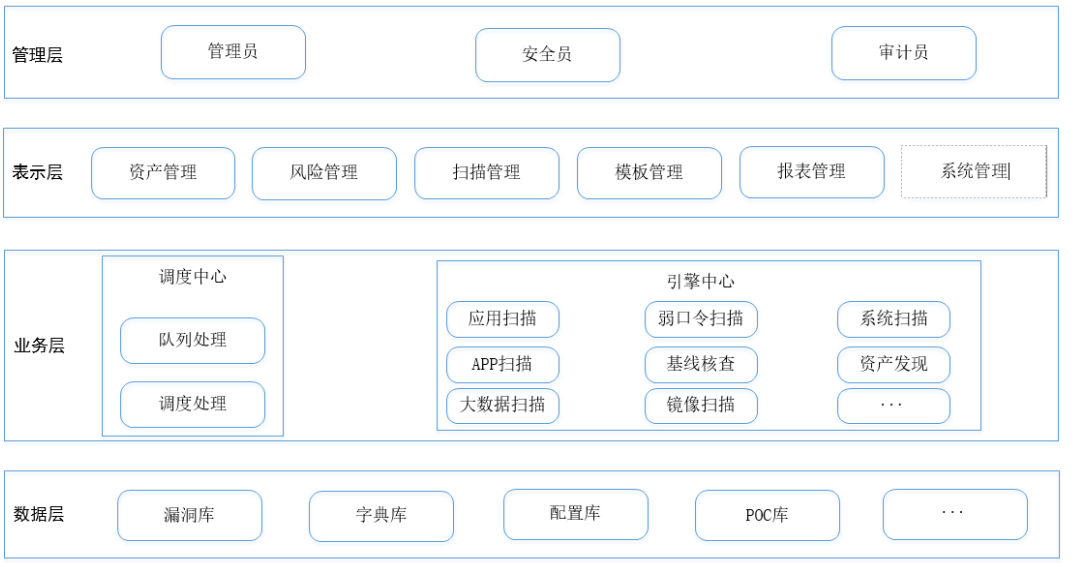
UNIS X1000-12T12F-G2

产品特点

◆ 多合一扫描能力

产品能够全方位检测 IT 系统存在的脆弱性，从系统扫描、应用扫描、数据库扫描、基线核查、口令猜解、移动扫描和镜像扫描等几大类发现信息系统、网站页面、数据库安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，检查不合规的设备配置，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行自我修补。

产品架构



◆ 丰富的扫描对象

支持网络环境中几乎全部类型主机的漏洞扫描和脆弱性检测。

- 操作系统：Windows 系列：NT、2000、XP、2003、Win7、Win10、win11、2008、2012、2016 等。Linux 系列：Amazon Linux、CentOS、Debian、Fedora、Red Hat、SuSE、Ubuntu 等。Unix 系列：AIX、FreeBSD、HP—UX、Solaris、Mac OS X 等。国产操作系统（深度、银河麒麟、中标麒麟、凝思、欧拉、红旗等）等；
- 数据库：Mysql、Oracle、PostgreSQL、DB2、Informix、SQLServer、SYBASE、InterSystems Cache、Clickhouse、Mariadb、神通、达梦、人大金仓等；
- 虚拟化平台：Kvm、VMware、VCenter、OpenStack、Eucalyptus、Vmware EXSi、Citrix XenServer、Microsoft Hyper-V 等；
- 网络安全设备：Cisco、华为、锐捷、H3C、天融信、深信服、绿盟、启明、等主流厂商网络设备；
- 大数据组件：Ambari、Cassandra、Elasticsearch、Flume、Hadoop、Hbase、Hive、 Impala、Kafka、Mongodb、Oozie、Redis、Spark、Storm、Splunk、Yarn、Zookeeper 等
- 应用软件：Microsoft Internet Explorer、Office、RealPlayer、Outlook、Adobe Flash 等；
- 工控设备：S7、Proconos、PCWorx、Omron、Modbus、MMS、MelSecq、IEC104、Fox、ENIP、dnp3、Crimson、MelSecq、Bacnet、Profibus、PROFINE 等；
- 网络安全设备：Cisco、华为、锐捷、H3C、天融信、深信服、绿盟、山石、普联、迈普、中兴、力腾、上元、网神、启明、中科网威、风云、网御星云等；

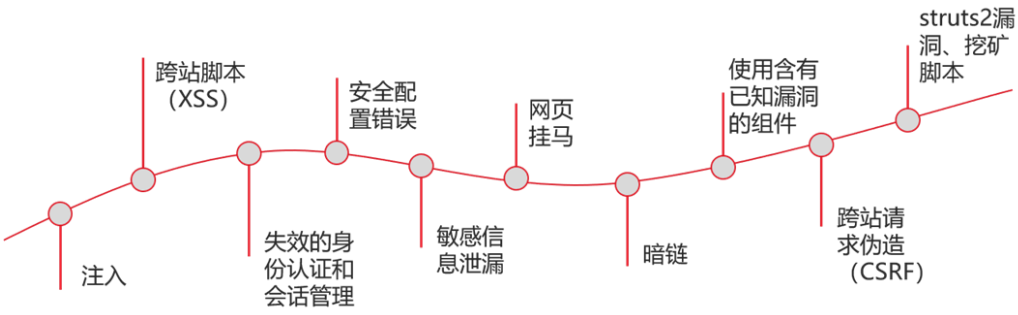
- 物联网：海康、大华、安迅士、三星、索尼、华为、同为、天地伟业、宇视、晶睿、惠普等。

◆ 全面的扫描能力

- 漏洞库涵盖丰富的安全漏洞库，兼容国内及国际标准；
- IPv4/IPv6 双栈协议地址管理；
- 系统登录扫描，应用被动扫描（Cookie 录制，会话录制、代理、Kafka 消费、Agent 采集、全流量镜像）；
- 数据授权扫描；
- 原理扫描，自定义 POC 扫描。

◆ 基于强大爬虫的 web 扫描能力

支持提供 OWASP 定义的 TOP 10 Web 威胁 SQL 注入漏洞、命令注入漏洞、CRLF 注入漏洞、LDAP 注入漏洞、XSS 跨站脚本漏洞、路径遍历漏洞、信息泄漏漏洞、URL 跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞、安全配置错误等漏洞风险等漏洞扫描服务。通过基于爬虫的网站漏洞扫描技术，能够有效识别 Web2.0 以及 Flash，保障 Web 漏洞扫描的全面性。



◆ 国内外数据库厂商漏洞兼容

系统漏洞知识库涵盖各种主流的数据库厂商，涵盖各种常见的漏洞类型。

◆ 便捷的漏洞验证工具集

误报是一种常见的现象，提供一键式漏洞验证工具集，包含 SQL 注入漏洞验证、浏览器漏洞验证及通用漏洞验证。运维人员可以直接在系统界面中选择相应的协议并填充测试字段对目标进行漏洞验证。针对系统已发现的漏洞还可以实现一键填充式自动验证功能，降低人工操作难度的同时保障漏洞扫描结果的准确性。

浏览器验证

一键跳转至漏洞链接所在页面，查看页面情况

SQL注入验证

一键传参、自定义注入点参数

通用验证

一键传参　　自定义请求数据

响应返回头　　返回数据

产品规格

功能	特性及描述
网络协议	支持IPv4 支持IPv6
任务管理	多方式任务录入：手动输入、资产导入、批量导入 支持定时执行、立即执行、周期执行 支持执行优先级别设置 支持新增系统扫描、Web扫描、数据库扫描、弱口令扫描、基线配置扫描任务 支持查看任务趋势，包括存活主机变化趋势、漏洞变化趋势、不同等级漏洞变化趋势等 支持根据扫描结果重新定义漏洞级别，支持接受漏洞风险 任务支持扫描参数模版配置，支持选择端口模板和自定义端口列表，支持漏洞模板过滤 支持扫描完成后自动生成报表、发送扫描结果到邮箱、发送扫描结果到FTP等设置 支持显示每条漏洞结果的漏洞状态，支持人工修改漏洞状态 支持任务概况显示，包括任务总数、正在扫描任务、等待扫描任务、已经完成任务、下发失败任务
资产发现	支持全网资产主动探测，识别协议、智能识别端口对应的服务以及软件版本、配置扫描模式、是否扫描工控协议等，支持一键添加到资产 支持子域名解析 端口探测支持TCP SYN、TCP ConnectTCP ACK、TCP Null、TCP Xmas、TCP Window、TCP Fin等方式 支持仅存活主机探测和端口服务版本深度探测
系统扫描	系统漏洞库数大于300000条，所有漏洞支持通过多种维度对漏洞进行检索，包括：CVE、BUGTRAQ ID、CNCVE、CNVD 、CNNVD、MS ID 编号、危险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息 系统支持支持多种端口探测方式，如TCP ACK、TCP SYN、TCP Connect、TCP Null、TCP Xmas、TCP Window、TCP Fin等 支持设置主机存活探测方式，如ARP、ICMP PING、TCP PING、UDP PING、TCP-SYN PING、

功能	特性及描述
	TCP-ACK　PING等 支持SSH、SMB、TELNET、POP、POP3、IMAP、FTP、RSH、REXEC、WSUS协议的登陆扫描 系统内置40种以上的系统漏洞扫描模板，如针对Windows操作系统、数据库、云平台（虚拟化）、工控系统、物联网、大数据组件、DNS、网络设备、弱密码等，同时允许用户自定义扫描模板 漏洞结果应展示CVSS向量，细化漏洞被利用的维度 系统应支持相同任务的多次扫描结果对比分析，支持不同任务的扫描结果对比
Web扫描	系统应用漏洞知识库数大于10000条 支持任务参数配置,包括HTTP设置、登陆扫描、爬虫配置、扫描配置、代理设置、扫描结果等 支持被动扫描，如代理、Kafka、Agent、流量镜像 支持网站可用性、DNS解析、网页变更、关键字和暗链挂马监控 支持对主流Web漏洞的识别与扫描，包括：SQL注入漏洞、命令注入漏洞、CRLF注入漏洞、LDAP注入漏洞、XSS跨站脚本漏洞、路径遍历漏洞、信息泄漏漏洞、URL跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞等 支持自定义POC，便于用户自行编写符合其需求的POC代码 支持漏洞验证功能，在扫描结束后，能够对结果中的重要漏洞进行现场验证，展示漏洞利用过程和风险 支持扫描结果可展示原始数据包和测试数据包，且包含完整的请求包和响应包 支持POC验证结果高亮显示利用成功的内容 支持Javascript解析引擎的支持，能从Javascript代码中分析出url；支持JavaScript执行高交互爬虫；支持从flash分析url 支持登录预录制功能，能够根据用户操作，录制并指定Web扫描url，使产品能够扫描和分析一些常规页面爬取程序检测不到的url 支持导入证书，做双向认证扫描 支持反连平台，用于辅助发现无回显命令执行漏洞，可在页面配置反连平台 支持自定义爬虫模拟提交时的表单填充内容 支持获取站点信息，包括IP 地址、操作系统、网站标题、网站防护信息、服务器架构、脚本语言等信息 可展示外部域名（关联网址）列表和证书信息
数据库扫描	数据库漏洞知识库数大于4000条，所有漏洞支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVEID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息 支持关系型数据库包括：Mysql、Oracle、PostgreSQL、DB2、Informix、SQLServer、SYBASE、InterSystems Cache、Clickhouse、Mariadb等 支持nosql数据库包括：Redis、Mongodb、Memcache、Cassandra、CouchDB、ElasticSearch等 支持国产数据库包括：华为GaussDB、达梦、人大金仓、南大通用、神通大型、星瑞格等 支持数据库登录扫描，至少应包括数据库账号，密码，SYSDBA、SYSOPER、NORMAL认证，SID、数据库名称、实例名称及实例号等登录选项的设置
弱口令扫描	支持常见服务如SMB、Telnet、SSH、IMAP、SNMP、FTP、POP3、SCP、SMTP、WinRm、RDP、REXEC、RLOGIN、RTSP、VNC等弱口令扫描 支持常见数据库如ClickHouse 、Dameng(达梦):、DB2、ElasticSearch、HighGo(翰高)、kingbase(金仓)、MongoDB、MSSQL、MySQL、Oracle、PostgreSQL、Redis、STDB(神通)、Sybase、UXDB(优炫)等弱口令扫描 支持常见中间件如ActiveMQ Console、JBoss、Tomcat、WebLogic等弱口令扫描 支持视频监控设备如大华、海康、华为、联想、Onvif、SIP等弱口令扫描 支持HTTP如HTTP Basic、Grafana、phpMyAdmin、HTTP Form等弱口令扫描

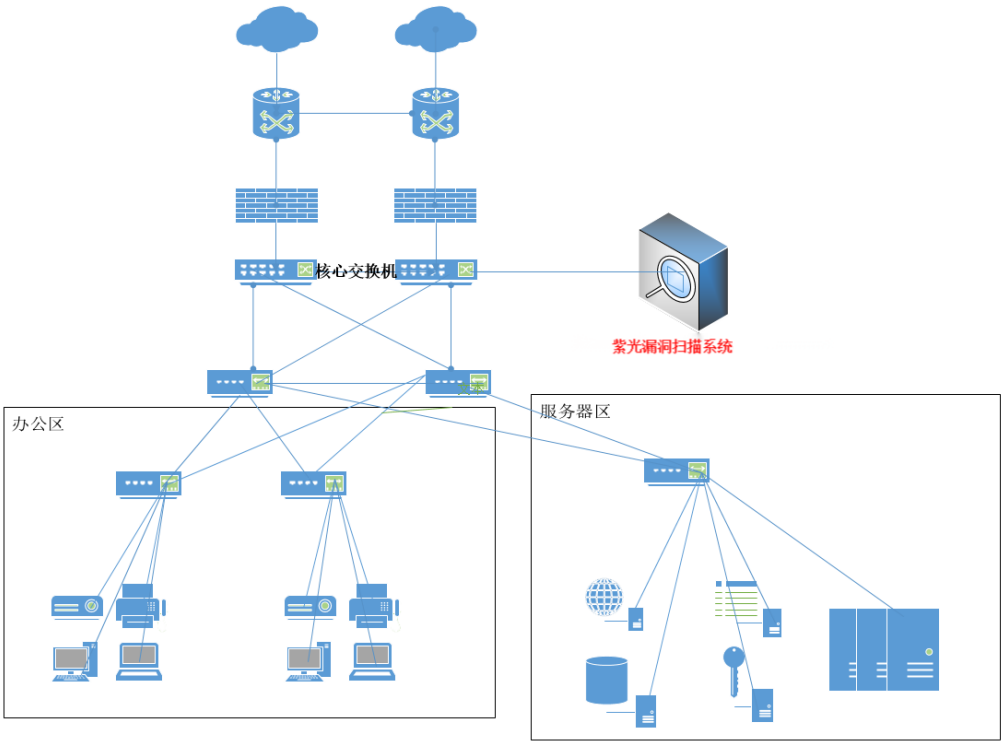
功能	特性及描述
	支持离线Hash爆破如Linux、Mysql(SHA1)、Mysql(SHA256)、MD5、SHA1、SHA256、SHA512等Hash文件进行猜解
基线配置扫描	支持对常见网络设备、安全设备、操作系统、数据库、应用服务器等的配置核查 支持的操作系统包括Windows、Linux（Ubuntu、Centos、Debian、Fedora、Redhat、OpenSuse、Suse等）、Unix（Solaris、FreeBSD、Aix（IBM）、HP—UX等）、国产操作系统（深度、银河麒麟、中标麒麟、凝思、欧拉、红旗等）等 支持的大数据组件包括mpp、Redis、Cassandra、Elasticsearch、Hbase、Hdfs、Hive、Impala、Flume、Kafka、Flink、Oozie、Spark、Splunk、Storm、Yarn&MR、ZooKeeper、Ambari等 支持的虚拟化平台包括vmware esxi、vsphere、vcenter、xenserver、xenapp、kvm、nova、keystone、openstack-keystone、cinder、glance、neutron等、 支持的安全设备包括华为、华三、网神、网御星云、启明、深信服、天融信，绿盟、Cisco、Neiscreen、Junipersrx、Checkpoint、中科网威、上元信安等 支持的网络设备包括Cisco、华三、Juniper、华为，力腾、迈普、锐捷、中兴等 支持的中间件包括Ngnix、Resin、Tomcat、Tongweb、Domino、IIS、JBoss、Weblogic、WebSphere、WebSphere、Bind等 支持在线检查、离线检查和跳转采集三种检查方式 支持通过TELNET、SSH、SMB、RDP、协议进行安全配置核查
移动扫描	支持Android、IOS移动应用静态扫描：支持获取APP相关信息：包括应用名称、版本信息、文件大小、文件md5、第三方sdk数量等 支持检测应用中存在的证书信息、权限信息、敏感函数、数据存储与隐私、网络通信、应用行为、代码质量、第三方组件等安全风险 支持检测结果评分，检测结果汇总统计
镜像扫描	支持对Docker镜像进行漏洞扫描，包括主流的操作系统、应用服务等 支持直接输入镜像标签扫描；支持dockerhub私有仓库扫描 支持输入harbor仓库凭证自动拉取镜像列表并扫描 支持获取镜像中包列表，包括包名、版本、license信息 支持获取镜像漏洞列表，包括漏洞名称、CVE、等级、描述、建议等。支持显示漏洞所在的包名、版本，以及修复漏洞的包版本
报表管理	支持报表形式对扫描结果进行分析，可以预定义、自定义和多角度多层次的分析扫描结果，结果报告的导出等。提供完善的漏洞名称、漏洞编号、漏洞描述、漏洞位置、危险等级、漏洞修复建议、修复建议等 支持提供有关漏洞的国际权威机构记录（包括CVE编号支持），以及与厂商补丁相关的链接 支持输出的报表格式包括：HTML、DOC、PDF、XLSX、XML等，支持对报表进行加密导出 支持报表批量下载 支持报告预览、报告生成（显示生成进度）、下载、删除等 报表生成时支持选择指定资产和资产过滤 支持自定义报表页眉页脚内容 任务报表支持自定义安全结论，并添加到报表中 报表内容支持展示任务参数信息，支持显示产品信息，包括产品名称、系统版本、产品型号、软件序列号
系统管理	支持提供标准、开放的接口，可与其它安全产品进行联动 支持设置预警邮件服务器，包括126、163、qq、139等邮箱，可以将漏洞扫描结果通过邮件发送给安全管理员 支持通过扫描黑名单或白名单的方式自定义用户可扫描IP范围，支持限制每个用户扫描的IP个数 支持与AD域、Radius或其他遵循LDAP协议的第三方认证系统的集成

功能	特性及描述
	支持用户连续登录失败支持设置锁定方式，支持锁定账户和锁定IP两种方式 支持对用户的有效期进行详细设置 支持通过接口获取API KEY 支持对资产及扫描任务结果进行备份恢复 支持与AD域、Radius或其他遵循LDAP协议的第三方认证系统的集成 支持通过扫描黑名单或白名单的方式自定义用户可扫描IP范围，支持限制每个用户扫描的IP个数 支持配置网卡、SSH服务、时间同步、重启、关机等，可以查看引擎版本、漏洞版本、策略版本等信息 支持向下级引擎下达扫描任务，接收下级引擎上传的扫描结果，进行统一分析 可以通过网络或者本地数据包，对漏洞库、软件进行在线升级、本地升级、定时升级，同时具备升级安全措施 支持自定义升级服务器地址，支持设置代理升级 支持编码解码（BASE64、URL、HEX等），哈希散列（MD5、SHA1、SHA224、SHA256、SHA384、SHA512等），加密解密（RC4、AES等），子网掩码计算等辅助功能 提供诊断工具，包括Ping、Telnet、Http、Dig、Nslookup、Traceroute等

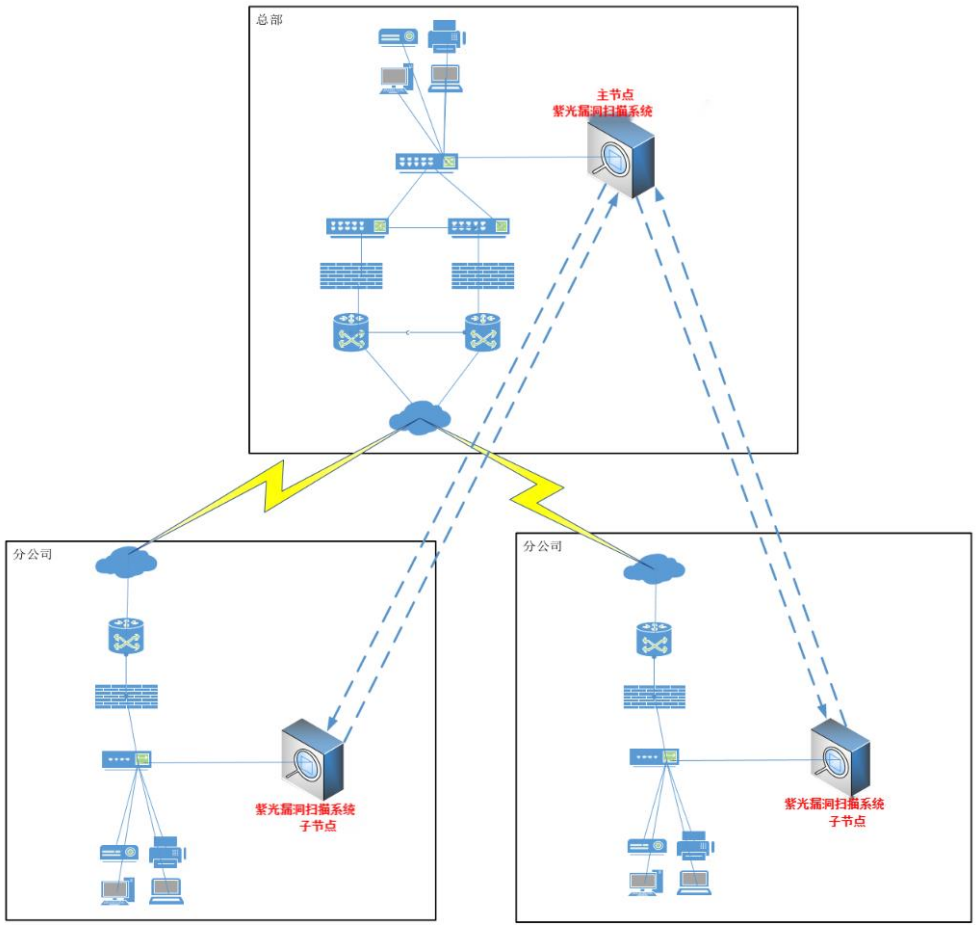
组网应用

系统一般旁路部署在运维管理区，与扫描对象保持 IP 可达，通过配置扫描任务定期地对网络中多个不同网段的主机、数据库、WEB 应用等进行全面、深入的检测，同时生成相应的漏洞解决方案，用户根据这些解决方案来对目标系统和应用做相应的加固和防护，及时降低网络安全风险。

- 单机部署：适用于网络较为集中、独立使用、中小型规模的网络环境，与被检测环境通信可达即可，部署方便“无损”部署，不影响客户网络和业务。



- 分布式部署：适用于层级网络结构，由总部集中进行管理、检查，网络规模较大的网络环境，统一下发、数据汇总、集中管理、统一评估，满足大型或超大型网络环境部署需求。



选配信息

◆ 硬件主机选购一览表

主机	描述	备注
UNIS X1000-12T12F-G2	UNIS X1000-12T12F-G2漏洞扫描系统设备-(12GE,12SFP,2Slots)	必配

◆ 特征库升级授权函选购一览表

特征库升级授权函	描述	备注
UNIS LIS-VS-Upgrade-01-G	UNIS X1000-12T12F-G2-LIS-VS-UPGRADE-01-G-漏洞库升级功能授权-1年	选配
UNIS LIS-VS-Upgrade-02-G	UNIS X1000-12T12F-G2-LIS-VS-UPGRADE-01-G-漏洞库升级功能授权-2年	选配
UNIS LIS-VS-Upgrade-03-G	UNIS X1000-12T12F-G2-LIS-VS-UPGRADE-01-G-漏洞库升级功能授权-3年	选配

◆ 可扫描 IP/域名数量授权函选购一览表

IP/域名数量授权函	描述	备注
UNIS LIS-VS-IP-01-G	UNIS X1000-12T12F-G2-LIS-VS-IP-01-G-系列扫描 128 个 IP 地址授权函	选配
UNIS LIS-VS-IP-02-G	UNIS X1000-12T12F-G2-LIS-VS-IP-02-G-系列扫描 256 个 IP 地址授权函	选配
UNIS LIS-VS-IP-03-G	UNIS X1000-12T12F-G2-LIS-VS-IP-03-G-系列扫描 512 个 IP 地址授权函	选配
UNIS LIS-VS-IP-04-G	UNIS X1000-12T12F-G2-LIS-VS-IP-04-G-系列扫描 1024 个 IP 地址授权函	选配
UNIS LIS-VS-IP-05-G	UNIS X1000-12T12F-G2-LIS-VS-IP-05-G-系列扫描无限个 IP 地址授权函	选配

◆ 接口卡选购一览表

接口卡模块	描述	备注
UNIS Sec-Card-4SFP+	UNIS Sec-Card-4SFP+-4端口万兆SFP Plus接口模块	选配

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