高级威胁防御设备

产品概述

瞻博网络高级威胁防御设备是一个分布式软件平台，结合了高级威胁检测、综合安全分析和一键式威胁缓解，可保护组织免受网络攻击，并提高安全团队的工作效率。ATP 设备会检测 Web、电子邮件和横向流量中的威胁。此外，它 还可以从安全设备提取日志并应用上下文分析，以整合方式呈现环境中的所有威胁。

产品说明

全球各地的组织每天都面临着安全和生产力方面的挑战。零日恶意软件常常无法被检测到，这是由于传统的安全设备依赖基于签名的检测，发现不了这些恶意软件。这就使得被大量警报所淹没的安全团队更加窘迫，越发难以识别和处理重要事件。

Juniper Networks® 高级威胁防御设备则针对 Web、电子邮件和在网络中活动的横向传播流量，连续地进行多阶段的检测和分析。此设备通过从多个攻击媒介收集信息和使用先进的机器学习和行为分析技术，在 15 秒之内就能识别高级威胁。随后，此设备将这些威胁与网络中其他安全工具收集的数据结合，进行分析，并建立关联，从而创建与受感染主机相关的所有恶意软件事件的合并时间线视图。一旦发现威胁，设备就会将“一键式”策略更新推送到内联工具，以防高级攻击再次发生。

ATP 设备的检测组件可监控网络流量，以识别攻击链过程中的威胁，并检测网络钓鱼、漏洞利用、恶意软件下载、命令和控制通信以及内部威胁。包括静态、负载、机器学习、行为以及恶意软件声誉分析的多阶段威胁分析流程借助瞻博网络的全球安全服务不断适应着持续变化的威胁环境；此服务基于云，提供由安全研究人员、数据科学家和白客组成的团队开发的最新威胁检测和缓解信息。

ATP 设备的威胁分析组件提供了从各种来源（如 Active Directory、端点防病毒、防火墙、安全 Web 网关、入侵检测系统、端点检测和响应工具）收集的、有关身份和威胁活动的整体视图。分析组件查看来自这些来源的数据，识别高级恶意特征，并关联事件，以便全面了解威胁攻击链。安全分析师收到全面的主机和用户时间线，了解主机或用户上发生的事件是如何发展的。该时间线可提高确定事件优先顺序和调查恶意软件事件的 1 层和 2 层安全分析员的工作效率。

ATP 设备可以与其他安全设备集成，以缓解威胁，从而使用户能够使用 REST API 自动隔离 Google 和 Office 365 上的电子邮件。恶意 IP 地址被推送至防火墙设备，以阻止命令和控制服务器和受感染端点之间的通信。与网络接入控制设备集成可隔离受感染的主机。ATP 设备的开放式 API 架构还使得它能与许多第三方安全供应商（如 Cisco、Palo Alto Networks、Fortinet、Bluecoat、Check Point、Carbon Black 和 Bradford 等）集成。

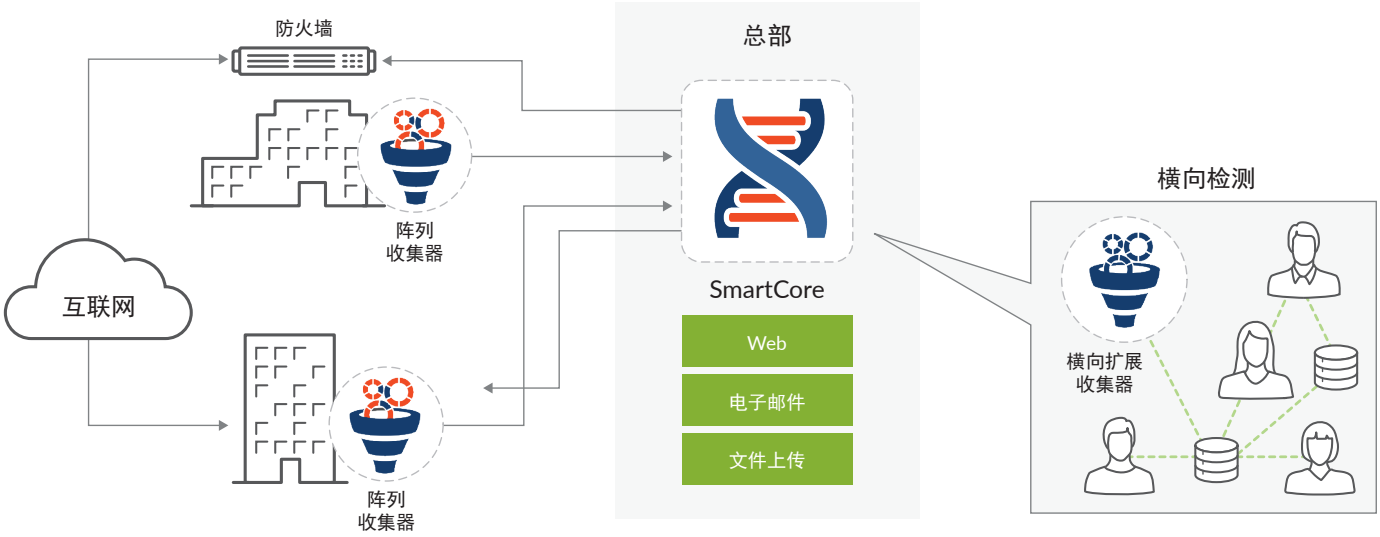

图 1：瞻博网络 ATP 设备架构

架构和关键组件

ATP 设备的架构由部署在网络中关键点（包括远程位置）的收集器构成。这些收集器的行为与传感器相似，它们收集有关 Web、电子邮件和横向流量的信息。跨阵列收集的数据和相关可执行文件将交付至与瞻博网络 SRX 系列服务网关完全集成的 SmartCore 分析引擎。当 SRX 系列防火墙部署为收集器时，解决方案可在内联威胁防御模式下运行。连同来自本机收集器的流量，ATP 设备还会提取其他身份和安全产品（例如 Active Directory、端点防病毒、防火墙、安全 Web 网关、入侵检测系统、端点检测以及响应工具）中的日志。这些日志可直接从第三方设备提取，也可从现有 SIEM/syslog 服务器转发。

有了从各种来源收集的数据后，SmartCore 分析引擎将执行以下多阶段威胁分析流程：

- **静态分析**：连续应用更新后的规则和签名，查找可能已逃避内联设备检测的已知威胁。
- **有效负载分析**：利用智能沙盒阵列，通过触发可能会以 Windows、OSX 或 Android 端点设备为目标的可疑的 Web 和文件内容，更深入地了解恶意软件行为。
- **机器学习与行为分析**：使用正在申请专利的技术来识别最新的威胁行为（例如，随时间变化的多元攻击），快速检测到先前未知的威胁。
- **恶意软件声誉分析**：将分析结果与类似的已知威胁进行比较，以确定新检测到的威胁是现有问题的变体还是全新的威胁。
- **优先级、风险分析、相关性**：根据威胁严重性、网络中的资产目标、端点环境和攻击链上的威胁进展，安排威胁的优先处理顺序。例如，Mac 上的高严重性 Windows 恶意软件的风险分数比受保护服务器上的中等严重性恶意软件要低。来自 ATP 设备和其他安全设备的所有恶意软件事件都将根据端点主机名和时间建立关联，然后在主机时间线上绘制关联图，从而使安全团队能够评估威胁的风险，以及是否需要立即关注。举个例子，已由 ATP 设备检测到但被防病毒解决方案漏过的威胁将获得更高的风险分数。这使安全团队可以及时追溯并评审受感染主机上发生的所有恶意事件。

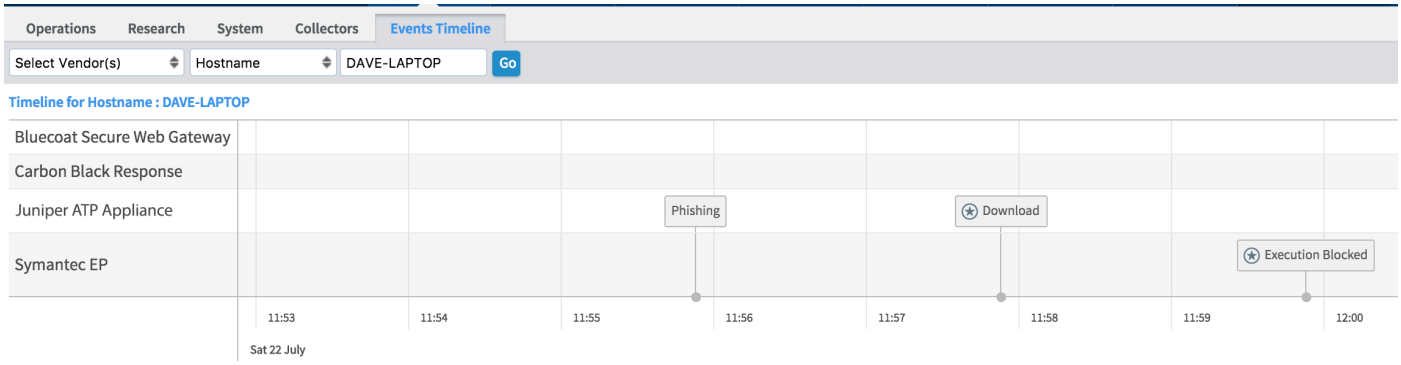

图 2：ATP 设备事件时间表

功能与优势

ATP 设备具备以下功能和优点：

- 跨多个媒介（如 Web、电子邮件和横向扩展）检测流量
- 通过 Web UI 上传可疑文件，以进行处理
- 支持 Windows 7 和 OSX 10.10 操作系统
- 与 SRX300、SRX4000 和 SRX5000 系列以及 SRX550M 和 SRX1500 完全集成；Junos 18.1 是能够集成 SRX 系列产品的最低版本
- 如果在内联模式下与 SRX 系列防火墙结合使用，则可以在内联阻止模式下运行
- 对多种文件类型进行分析，包括可执行文件、DLL、Mach-o、Dmg、PDF、Office、Flash、ISO、ELF、RTF、APK、Silverlight、存档文件和 JAR
- 包括检测技术，例如漏洞检测、有效负载分析、命令和控制 (C&C) 检测、YARA 和 SNORT 规则
- 提供全面、完整记录的 API，允许与第三方安全设备轻松集成
- 与瞻博网络、Palo Alto Networks、Checkpoint、Cisco、Fortinet 和 Bluecoat 解决方案集成，以自动阻止恶意 IP 地址和 URL
- 自动隔离 Office 365 和 Gmail 的电子邮件
- 与 Carbon Black Protect and Response（端点解决方案）集成，以便能够上传在端点上执行的二进制文件
- 能够通过可扩展架构对多个辅助核心进行群集化，从而提高处理能力
- 包括 Manager of Central Managers (MCM) 功能，此功能可在需要多个核心的大型部署中实现集中的单一管理平台管理
- 支持使用 SAML 和 RADIUS 的访问和身份验证
- 将不同攻击链阶段的事件关联，以监控威胁进展和风险
- 实现恶意软件活动可视化并对恶意软件特征进行分组，帮助事件响应团队更好地了解恶意软件行为
- 基于从威胁严重度、威胁进展、资产价值和其他情景数据计算得出的风险程度来划分威胁的优先级
- 提供时间表主机视图，以获取有关主机上发生的恶意软件事件的完整情景

产品选项

ATP 设备有物理和虚拟两种规格。物理设备（1U JATP400 和 2U JATP700）可在一体化模式（SmartCore 和阵列收集器安装在同一物理设备上）或分布式模式（SmartCore 和阵列收集器安装在不同的设备上）中部署。虚拟设备仅可在分布式模式中部署。此外，还支持针对 MacOS 的恶意软件检测。客户将需要提供可作为辅助核心部署的 Mac mini 硬件。MacOS 沙盒映像可在 JATP 软件下载页面上找到。

物理

一体化

产品编号	性能（排除的对象数）[1]	性能
JATP400	最高 25,000 个对象/天	1 Gbps
JATP700	最高 61,000 个对象/天	2.5 Gbps

SmartCore

产品编号	性能（排除的对象数）[1]	日志记录性能
JATP400	最高 50,000 个对象/天	1500 个事件/秒
JATP700	最高 130,000 个对象/天	1500 个事件/秒

[1] 此处的数字基于与真实环境性能近似的流量组合。实际数字可能会因流量组合、重复对象和用户环境特有的其他因素而不同。

收集器

产品编号	性能
JATP400	1.5 Gbps
JATP700	4 Gbps

电子邮件 MTA 接收器

产品编号	每天最大电子邮件数
JATP400	700,000
JATP700	200 万

虚拟

支持的虚拟机管理程序

产品编号	版本
VMware vSphere ESXi	5.5、6.0

虚拟 SmartCore

产品编号	性能（排除的对象数）	虚拟 CPU	虚拟内存	虚拟磁盘
vSC-8	最高 46,000 个对象/天[1]	8	32 GB	1.5 TB
vSC-24	最高 116,000 个对象/天[1]	24	96 GB	1.5 TB

虚拟收集器

产品编号	性能	虚拟 CPU	虚拟内存	虚拟磁盘
FC-v500M	500 Mbps	4	16 GB	512 GB
FC-v1G	1 Gbps	8	32 GB	512 GB
FC-v2.5G	2.5 Gbps	24	64 GB	512 GB

虚拟电子邮件 MTA 接收器

产品编号	每天最大电子邮件数	vCPU 数	虚拟内存
vMTA-M	720,000	8	16 GB
vMTA-L	140 万	16	16 GB
vMTA-XL	240 万	24	32 GB

JATP700

JATP400

JATP700 规格

规格	JATP400	JATP700
重量	30.4 磅（13.79 千克）	42 磅（19 千克）
尺寸（宽 x 高 x 深）	17.2’’ x1.7’’ x25.6’’	17.2 x 3.5 x 24.8 英寸（43.7 x 8.9 x 63 厘米）
外形	1 U（可架装）	2 U（可架装）
AC 电源	500 W 高效（94% 以上）AC-DC 冗余电源； 交流输入：-100-240 V，50-60 Hz，11-4.4 A	920 W 高效（94% 以上）AC-DC 冗余电源； 交流输入：-100-240 V，50-60 Hz，11-4.4 A
直流电源	650 W，高效冗余 DC 到 DC 电源；DC 输入：650 W；-44Vdc 到 -74Vdc，20A	850 W/1010 W 高效冗余 DC 到 DC 电源；DC 输入：850 W；-35Vdc 到 -42Vdc，30-25A
风扇	5 个 40x40x56 mm 13K-11K RPM 风扇	3x8 cm 7 K RPM，4 针 PWM 风扇
工作温度	50° 到 104° F（10° 到 40° C）	50° 到 104° F（10° 到 40° C）
存储温度	-40° 到 158° F（-40° 到 70° C）	-40° 到 158° F（-40° 到 70° C）
相对湿度（运行）	8% 到 90% 非冷凝	8% 到 90% 非冷凝
相对湿度（存储）	5% 到 95% 非冷凝	5% 到 95% 非冷凝
海拔（运行）	最高 6,500 英尺	最高 6,500 英尺
海拔（存储）	最高 35,000 英尺	最高 35,000 英尺
安全认证	CAN/CSA-C22.2 No. 60950-1 信息技术设备安全 EN 60950-1 UL 60950-1（第 2 版） IEC 60950-1：2005/A2:2013	CAN/CSA-C22.2 No. 60950-1 信息技术设备安全 EN 60950-1 UL 60950-1（第 2 版） IEC 60950-1：2005/A2:2013

规格	JATP400	JATP700
排放认证	47CFR 第 15 部分，(FCC) A 类 ICES-003 A 类 EN 55022 A 类 CISPR 22 A 类 EN 55024 CISPR 24 EN 300 386 AS/NZA CISPR22 A 类 CNS13438 A 类 EN 61000-3-3 VCCI A 类 KN22 A 类 EN 61000-3-2 BSMI CNS 13438	47CFR 第 15 部分，(FCC) A 类 ICES-003 A 类 EN 55022 A 类 CISPR 22 A 类 EN 55024 CISPR 24 EN 300 386 AS/NZA CISPR22 A 类 CNS13438 A 类 EN 61000-3-3 VCCI A 类 KN22 A 类 EN 61000-3-2 BSMI CNS 13438
NEBS	无	无
RoHS	是	是
CPU	10 核	2 个 10 核
内存	32GB	128 GB
存储	8TB (4 x 2TB)，RAID 6	8 个 900 GB 2.5” 10K SAS，RAID 6
流量端口	2 个 SFP+ 10GbE，4 个 RJ-45 GbE	2 个 SFP+ 10GbE，4 个 RJ-45 GbE

订购信息

瞻博网络 ATP 设备支持灵活的部署选项。所需的组件取决于部署模式。

- **物理部署**需要物理 JATP 设备和相关软件订阅。
- **虚拟部署**仅需要软件订阅

软件订购许可分为两种功能包，汇总见下表。

功能包	包含的功能
标准 (STD)	北南 Web 流量、自动缓解、分析、电子邮件 (BCC)、手动上传
企业 (ENT)	所有标准功能、横向流量 (SMB)、电子邮件 (MTA)

硬件

产品编号	说明
JATP700-AC-CORE	JATP700 设备，AC 电源，核心软件（已安装）
JATP700-AC-COL	JATP700 设备，AC 电源，收集器软件（已安装）
JATP700-AC-ALL	JATP700 设备，AC 电源，一体式软件（已安装）
JATP700-DC-CORE	JATP700 设备，DC 电源，核心软件（已安装）
JATP700-DC-COL	JATP700 设备，DC 电源，收集器软件（已安装）
JATP700-DC-ALL	JATP700 设备，DC 电源，一体式软件（已安装）
JATP400-AC	JATP400 设备，AC 电源，已安装单个映像（可配置为一体式、核心或收集器）
JATP400-DC	JATP400 设备，DC 电源，已安装单个映像（可配置为一体式、核心或收集器）

软件订购许可

订阅许可证基于吞吐量/带宽。支持的吞吐量级别为 100 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps 和 10 Gbps。

注意：与 SRX 系列防火墙集成需要将 AppSecure 功能安装到 SRX 系列设备上。根据平台型号，可能单独需要一个许可证。

产品编号	说明
JATP-100M-STD-1	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 100 Mbps，1 年期。含支持服务。
JATP-500M-STD-1	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 500 Mbps，1 年期。含支持服务。
JATP-1G-STD-1	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 1 Gbps，1 年期。含支持服务。
JATP-2G-STD-1	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 2 Gbps，1 年期。含支持服务。
JATP-5G-STD-1	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 5 Gbps，1 年期。含支持服务。
JATP-10G-STD-1	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 10 Gbps，1 年期。含支持服务。
JATP-100M-STD-3	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 100 Mbps，3 年期。含支持服务。
JATP-500M-STD-3	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 500 Mbps，3 年期。含支持服务。
JATP-1G-STD-3	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 1 Gbps，3 年期。含支持服务。
JATP-2G-STD-3	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 2 Gbps，3 年期。含支持服务。
JATP-5G-STD-3	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 5 Gbps，3 年期。含支持服务。
JATP-10G-STD-3	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 10 Gbps，3 年期。含支持服务。
JATP-100M-STD-5	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 100 Mbps，5 年期。含支持服务。
JATP-500M-STD-5	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 500 Mbps，5 年期。含支持服务。
JATP-1G-STD-5	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 1 Gbps，5 年期。含支持服务。
JATP-2G-STD-5	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 2 Gbps，5 年期。含支持服务。
JATP-5G-STD-5	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 5 Gbps，5 年期。含支持服务。
JATP-10G-STD-5	高级威胁防御设备（硬件或虚拟）的软件订阅。标准功能包，最高 10 Gbps，5 年期。含支持服务。
JATP-100M-ENT-1	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 100 Mbps，1 年期。含支持服务。

产品编号	说明
JATP-500M-ENT-1	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 500 Mbps，1 年期。含支持服务。
JATP-1G-ENT-1	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 1 Gbps，1 年期。含支持服务。
JATP-2G-ENT-1	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 2 Gbps，1 年期。含支持服务。
JATP-5G-ENT-1	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 5 Gbps，1 年期。含支持服务。
JATP-10G-ENT-1	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 10 Gbps，1 年期。含支持服务。
JATP-100M-ENT-3	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 100 Mbps，3 年期。含支持服务。
JATP-500M-ENT-3	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 500 Mbps，3 年期。含支持服务。
JATP-1G-ENT-3	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 1 Gbps，3 年期。含支持服务。
JATP-2G-ENT-3	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 2 Gbps，3 年期。含支持服务。
JATP-5G-ENT-3	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 5 Gbps，3 年期。含支持服务。
JATP-10G-ENT-3	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 10 Gbps，3 年期。含支持服务。
JATP-100M-ENT-5	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 100 Mbps，5 年期。含支持服务。
JATP-500M-ENT-5	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 500 Mbps，5 年期。含支持服务。
JATP-1G-ENT-5	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 1 Gbps，5 年期。含支持服务。
JATP-2G-ENT-5	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 2 Gbps，5 年期。含支持服务。
JATP-5G-ENT-5	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 5 Gbps，5 年期。含支持服务。
JATP-10G-ENT-5	高级威胁防御设备（硬件或虚拟）的软件订阅。企业功能包，最高 10 Gbps，5 年期。含支持服务。

关于瞻博网络

瞻博网络将简单性融入到了全球互联的产品、解决方案和服务当中。通过工程创新，我们消除了云时代网络的限制和复杂性，可应对我们的客户和合作伙伴日常面临的最苛刻的挑战。在瞻博网络，我们坚信网络是交流改变世界的知识和人类进步的资源。我们致力于设想开创性的方式并以符合业务发展的速度，提供自动化、可扩展且安全的网络。

公司和销售总部

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

电话： 888.JUNIPER (888.586.4737)

或 +1.408.745.2000

www.juniper.net

APAC 和 EMEA 总部

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

电话： +31.0.207.125.700

JUNIPER NETWORKS | 精研至简

了解瞻博网络

获取应用程序。

JUNIPER 1ON1

Available on the App Store

ANDROID APP ON Google Play