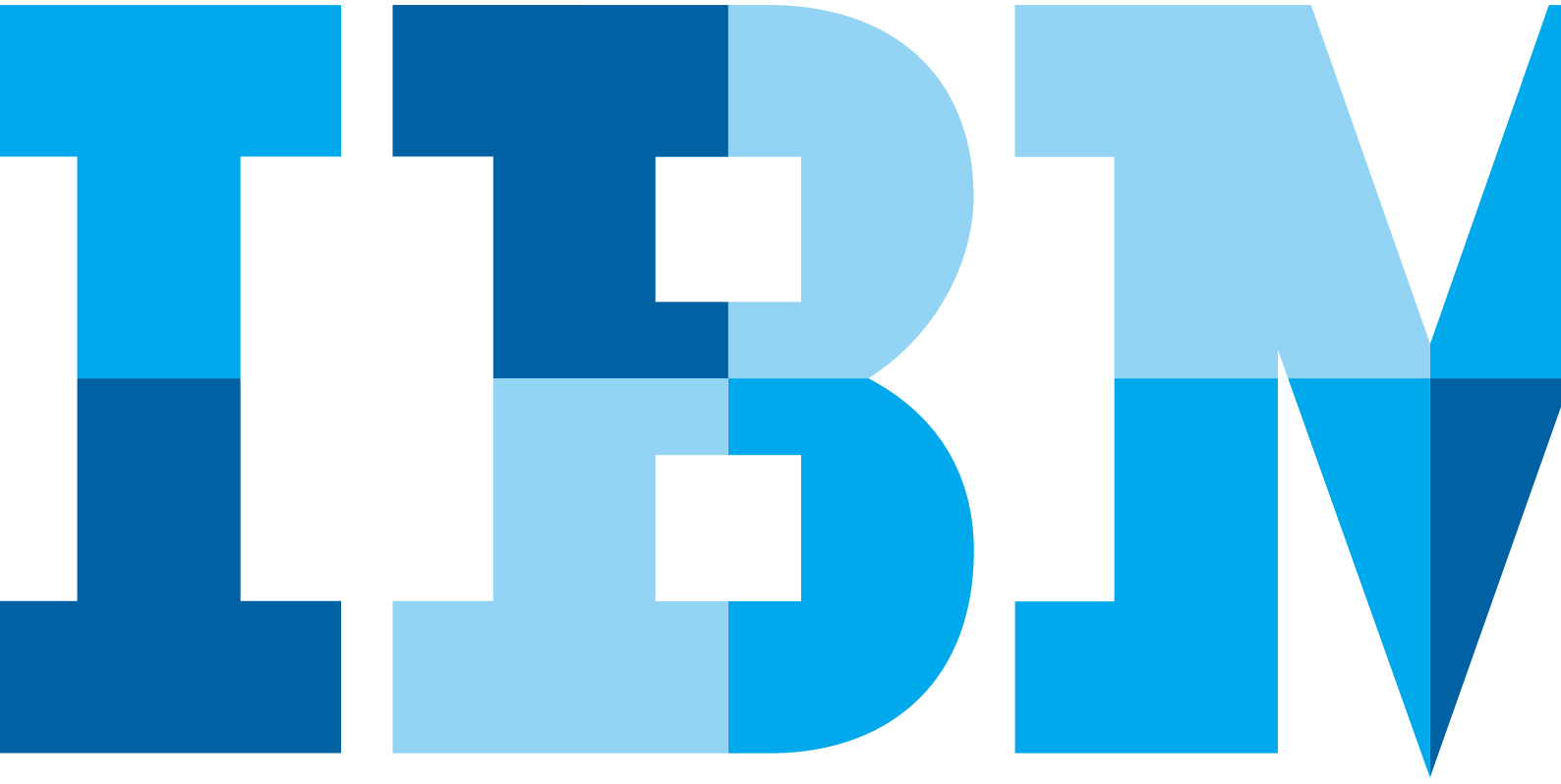
IBM软件

思想领袖白皮书

利用大数据解决方案扩展安全智能

充分利用大数据技术，揭示对现代高级数据威胁的可操作洞察



简介

复杂的网络犯罪和高级持续性威胁正在以惊人的速度出现。在新型攻击技术、更多的资金支持以及易于利用的社交连接的帮助下，攻击者比以往任何时候都更容易获得成功。传统的安全解决方案已无法抵御这些不断升级的威胁。

IBM® Security QRadar® 使用大数据功能来帮助您跟上各种高级威胁的步伐，并在攻击发生前阻止它们。它有助于揭示在大量安全数据中隐藏的各种关系，使用经过验证的分析技术将数十亿个安全事件缩减为一组可管理的高优先级事件。

具有前瞻意识的组织正在探索自定义分析，对各种非结构化数据源(包括电子邮件、社交媒体提要、业务事务和完整的网络数据包有效负荷)使用其他的大数据技术。为了满足此需求，IBM集成了业界领先的安全智能功能与IBM InfoSphere® BigInsights™ 世界级的分析功能，以及相关的大数据软件和服务。这种组合提供了一个全面的解决方案——旨在实时检测威胁并确定其优先级的一个安全智能平台，以及一个成熟的、基于Hadoop的自定义数据挖掘和分析解决方案。

理解并识别各种高级威胁

各种高级威胁已成为IT安全行业中讨论最多的主题之一。今天，有组织的团队通过精心策划的、有耐心的、长期运行的攻击来追逐特定的目标，他们往往采用高度自定义的恶意软件和战术。例如，攻击者可能会渗透进入一个受信任的合作伙伴网络，然后将恶意软件加载到目标网络。恶意软件可能被定制为只感染目标组织，以防被安全提供商识别出来。

攻击者还进行大量鱼叉式钓鱼目标侦察，然后通过社会工程战术攻陷目标帐户。对手通常利用零日漏洞来访问数据、应用程序、系统和端点，并且他们通过多种渠道进行通信，从目标组织中盗取数据。

为了应对这些威胁以及其他复杂的威胁，组织必须采用全新的方法来帮助发现各种异常和微妙的攻击迹象。为此就需要收集和分析来自安全基础架构和其他来源的数据——包括传统的日志和事件数据，以及网络流数据、漏洞和配置信息、身份上下文、威胁智能等。总之，安全已经成为一个大数据问题。

安全智能: 经过验证的大数据安全方法

安全智能是指对用户、应用程序和基础架构所生成的数据进行持续的实时收集、规范化和分析。它集成了在第一代安全信息和事件管理(SIEM)解决方案中通常被隔离的功能，包括日志管理、安全事件关联和网络活动监控。

数据收集和分析不仅支持日志和事件，还支持在单一仓库中记录网络流、用户身份和活动、资产档案和配置、系统和应用程序漏洞，以及外部的威胁智能，这些都已经远远超出了传统的SIEM。如图1所示。

利用IBM Qradar Security Intelligence Platform扩展可见性

IBM QRadar Security Intelligence Platform是一个从头开始设计的大数据平台，可提供下一代SIEM技术的优势。它旨在扩展对网络活动、虚拟活动、用户活动和应用程序活动的可见性，帮助对整个组织中的潜在安全违规提供可操作的洞察。

大型企业使用QRadar解决方案每天在部署中收集和关联数十亿个事件和网络流，这些部署可覆盖多个位置，并将以前孤立的运营小组连接起来。示例包括:

- 某“财富”百强电信运营商每秒收集和监视一百万个事件(每天超过850亿个事件)，在其全球运营中帮助实现安全性与合规性。
- 某全球能源公司每天监控六百万次刷卡事件并关联二十亿个事件，以帮助符合North American Electric Reliability Corporation (NERC)和Payment Card Industry Data Security Standard (PCI DSS)等标准的要求。由QRadar解决方案提供的实时分析每天确定25至50个优先事件——实现了约四千万比一的数据缩减率。

有几个因素让QRadar解决方案成为协助对抗各种高级威胁的一种理想方法:

- **互操作性和可扩展性:** QRadar解决方案支持400多种信息源，并可帮助提供一个统一的架构，以收集、存储、分析和查询与日志、威胁、漏洞以及风险相关的数据。专用数据库有助于提供可扩展性和性能调优，让组织能够搜索数百万个事件并实现亚秒级的响应速度。
- **攻击前和攻击后的洞察:** QRadar解决方案收集有关现有安全漏洞的信息并确定其优先级，从而帮助您防止出现违规现象；它有助于识别在网络中已经发生的可疑行为，帮助检测各种违规问题。
- **异常检测功能:** QRadar解决方案创建一个当前活动的基线，以识别与正常行为的偏差。然后它确定哪些偏差是有意义的，从而帮助检测正在进行的攻击。

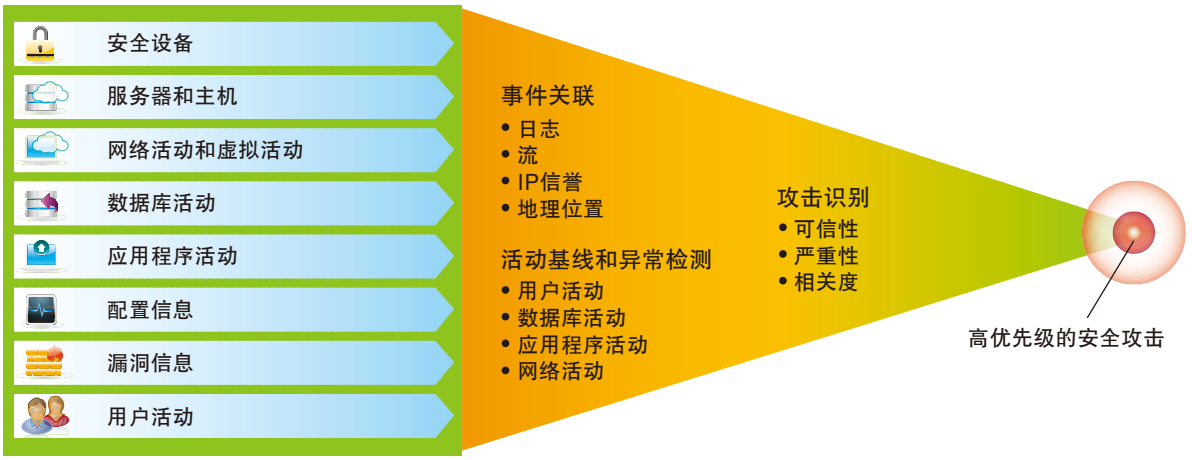


图1. 可扩展的IBM QRadar Security Intelligence Platform可捕获各种来源的数据，并使用现有规则以及客户定义的规则将这些数据缩小为一个可管理的攻击列表。

- **实时关联和分析:** QRadar解决方案实时关联大量的数据集，帮助您更早且更准确地检测各种高级攻击。
- **减少误报:** QRadar解决方案可以帮助您快速检测损害，并将不同寻常但为良性的活动的优先级降低，以缩短分析师调查潜在违规情况所需的时间。
- **取证功能:** QRadar解决方案提供了跨数千个系统和资源的日志数据、网络流量以及其他安全遥测数据的单一控制台视图——可安全和网络工作人员减轻负担，帮助他们迅速评估违规的来源和影响。
- **灵活性:** 有效防御各种高级攻击的办法应该支持IT环境和威胁格局的频繁变化。QRadar解决方案可让您轻松地添加数据源、创建和调优分析、创建新的用户视图和报告，以及扩展和发展整体部署架构。

充分利用并行处理、高速临时查询功能和分析来关联数百万个安全事件，并将其提炼为一组可管理的高优先级攻击，QRadar平台是利用大数据实现IT安全性方面的领袖。

使用更多大数据工具来解决新问题

前瞻性的组织正在转向大数据平台，如基于Hadoop的平台，帮助解决各种高级安全挑战。这些平台提供的分析类型通常使用历史基线、统计和可视化功能来发现过去的欺诈或安全漏洞证据。示例包括:

- 通信服务提供商关联数百万个全球DNS请求、HTTP事务和完整的数据包信息，从而识别与僵尸网络相关的恶意通信。
- 国际金融服务公司通过关联实时活动与历史帐户活动，并使用基线来发现不正常的用户行为、可能性较低的申请途径和可疑交易，从而找到了揭露欺诈的新方法。
- 各种组织使用语言分析和预测分析对电子邮件和社交网络通信进行分析并识别可疑的活动，在事件发生前就采取主动的行动措施。

这些用例中采用的大数据分析必须存储、处理和分析目前的安全解决方案尚未进行分析的结构化、半结构化和非结构化数据，这些数据的种类繁多且数量庞大，如图2所示。

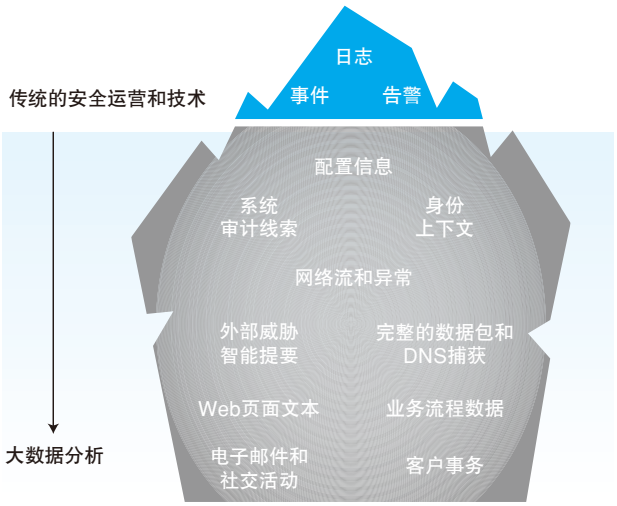


图 2.数据的种类和数量正在推动实现新的大数据用例，帮助企业保持安全性。

利用IBM InfoSphere BigInsights扩展安全智能

IBM将QRadar Security Intelligence Platform的专家安全功能与各种高级分析技术相结合，包括IBM InfoSphere BigInsights，这是一个基于Hadoop的平台，可帮助组织发现隐藏在大量数据中的洞察。QRadar解决方案执行实时的关联和报告，以快速响应威胁和风险，然后将大量的安全信息发送给InfoSphere BigInsights进行更多的分析。

InfoSphere BigInsights可以使用和分析来自非结构化和半结构化来源的海量数据，满足高级安全用例所需的数据种类与数量要求。InfoSphere BigInsights可以帮助您随着时间的推移逐步提高分析的准确度，并将洞察馈送回QRadar，从而提供了一个可实现闭环持续学习的设施。其结果是一个智能的集成解决方案，帮助使用以前无法实现的方式来收集、监测、分析并报告安全和企业数据，如图3所示。

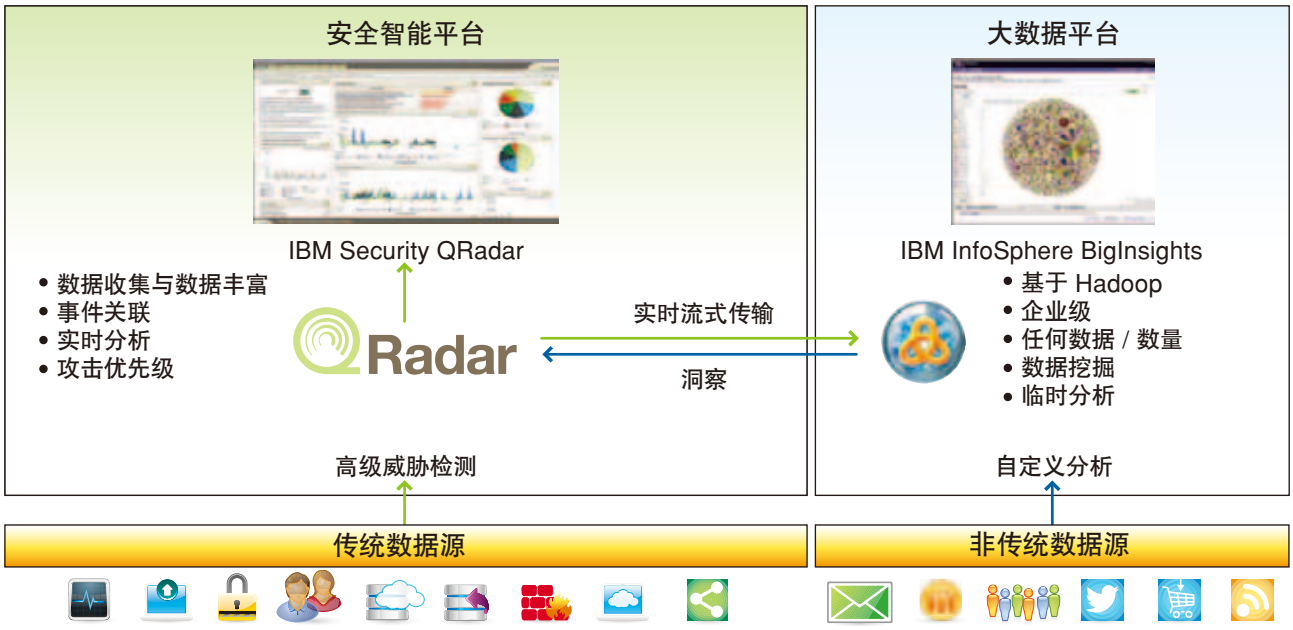


图3. InfoSphere BigInsights采用自适应分析方法，帮助通过大数据功能扩展QRadar Security Intelligence Platform。

InfoSphere BigInsights利用大数据处理特性来补充QRadar解决方案，包括:

- 复杂的文本分析，提供了丰富的提取器库，支持从大量原生文本数据中提取可操作的洞察。
- 机器数据分析加速器，使用分面搜索来摄取、分析和提取各种机器数据，轻松实现导航、发现和可视化。
- 自适应MapReduce，自动适应用户的需求和系统工作负载，帮助提高性能并简化作业的调优，用户无需理解和操作Hadoop中的多个调优按钮即可完成这些任务。
- IBM BigSheets，一个类似于电子表格的工具，让用户无需编写代码就可以探索InfoSphere BigInsights集合并发现新的洞察。

InfoSphere BigInsights包括各种高级分析功能，以及面向安全分析师(非开发人员)的用户界面。该解决方案不要求进行模式定义或数据预处理，并支持在不同的信息类型之间动态添加结构和关联。该平台可在常见的低成本硬件上并行运行，在商用硬件上支持线性的可扩展性。根据用例的要求，可以使用其他IBM大数据技术补充InfoSphere BigInsights。

来自大数据的巨大价值: Internet规模的僵尸网络发现

通过识别被僵尸网络感染的主机并限制它与指挥和控制主机之间的通信，组织可以明显改善其安全状况。

技术挑战

通过请求新的命令并在一段时间内零星地发送信息，僵尸网络可以导致网络内被感染的主机泄漏非常少量的数据。检测此类随机的、不频繁的活动很困难，并且涉及到监视大量带有快速变化的标识符的高速数据，如DNS流量和其他用于指挥和控制的协议流量。

其他IBM大数据技术

- IBM InfoSphere Streams: 并行处理技术，以每天高达数PB的速度对大量运动数据执行复杂的分析，这些数据包括文本、图像、音频、语音、IP语音电话(VoIP)、视频、Web流量和电子邮件内容。该解决方案可用于需要在几毫秒而不是几秒内完成分析且高度自定义的高速用例。
- IBM SPSS® Modeler: 一个数据挖掘工作台，可以帮助数据分析师使用结构化和非结构化数据快速直观地构建预测模型。
- IBM i2® Intelligence Analysis Platform: 一个强大的可视化工具，帮助分析师发现各种趋势，并向企业传播可操作的威胁信息。
- IBM PureData™ System: 一种高性能设备，有助于为分析应用程序简化数据服务并优化性能，能够在几分钟内即可运行非常复杂的算法，而不是几小时。

IBM解决方案

- 使用QRadar解决方案实现网络流量的本机收集，帮助识别僵尸网络，实时检测异常，并根据IBM X-Force® 的全球威胁情报关联恶意活动。
- 使用InfoSphere BigInsights在整个企业中收集几乎所有DNS事务并应用自定义分析，从而帮助识别僵尸网络所用的可疑域名。分析多年的历史数据，帮助检测已被感染的主机和过去的入侵活动。
- 将来自InfoSphere BigInsights的发现(包括需要修复的指挥和控制域以及资产)集成到QRadar，构建实时关联规则，从而帮助发现新的入侵。

来自大数据的巨大价值: 全方位的欺诈检测

组织每年都因欺诈性索赔、帐户盗用和无效的交易造成可观的收入损失。尽管这一问题如此严重，但许多组织都没有意识到自己正在受到他人的欺诈。

技术挑战

欺诈分析涉及到寻找各种异常和行为模式，并建立一个正常活动的配置文件。安全团队和欺诈调查人员需要深入访问这些信息，并且能够解析非结构化文本，以了解客户事务、索赔等行为方面的差异。

IBM解决方案

- 采用QRadar解决方案收集、标准化并丰富应用程序和用户访问日志以及事务数据，实时搜索异常，并将处理后的信息发送到InfoSphere BigInsights。
- 使用InfoSphere BigInsights对事务执行自定义分析，并确定几个月乃至几年的PB级帐户活动，然后将洞察发送回QRadar平台，以便在欺诈行为发生时将它检测出来。
- 将该信息扩展到IBM I2 Intelligence Analysis Platform进行链接分析、可视化和传播，帮助欺诈分析师进行调查并与其他人沟通调查结果。

来自大数据的巨大价值: 全面的内部威胁分析

内部威胁和数据丢失对于所有组织来说都是重大的风险，并且风险性很高，在扩展客户/个人信息存储库时尤其如此。

技术挑战

大多数安全技术只寻找用户或应用程序“正常”活动的特定模式或短期配置文件。为了准确地检测内部威胁，组织可能需要分析数月甚至数年的网络流量、IP地址和URL目的地，以及更广泛的公司间和公司内的通信内容，从而更好地了解人与人之间的联系，以及哪些是有风险的行为。

IBM解决方案

- 使用QRadar解决方案打破数据孤岛，并关联实时系统和用户活动，帮助发现普通用户和特权用户在访问敏感信息时有风险的行为。
- 充分利用InfoSphere BigInsights来改进分析，这对于发现和调查高风险行为很有用，能够找出标志着异常员工活动的模式。
- 与现有的身份和访问管理系统(如IBM Security Privileged Identity Manager)共享调查结果，帮助对可疑的用户采取纠正措施，并控制对敏感信息的共享访问。

结束语

大数据安全分析解决方案必须摄取由企业内多种安全数据源提供的数据，以及来自企业内外的非结构化和半结构化数据。它还必须适应不断变化的威胁环境，提供企业环境的全面视图，并推动实现可操作的智能，从而防止各种已知和未知威胁。

使用IBM Security Intelligence与大数据，安全组织可以更灵活地分析更多的数据，并获得更准确的结果。通过分析整个企业中强化的结构化安全数据以及非结构化数据，IBM解决方案可帮助您找出深深隐藏在组织大量数据中的恶意活动，实现对各种高级威胁和风险的检测。

更多信息

要了解有关IBM大数据安全解决方案的更多信息，请联系IBM销售代表或IBM业务合作伙伴，或者访问：**ibm.com**/security

IBM Corporation Software Group Route 100
Somers, NY 10589

在中国印刷
2013年4月

本文包含截至出版之日的最新信息，IBM可能随时更改这些信息。不是所有产品都可用于IBM运营的每个国家/地区。

本文出现的所有客户例子均为了说明这些客户使用IBM产品的方式，以及他们可能已达到的效果。根据客户配置和条件的不同，实际的环境成本和性能特征也会有所差别。

良好安全实践声明：IT系统安全性涉及通过预防、检测和响应来自企业内外的不当访问，保护系统和信息的安全。不当访问可能导致信息被篡改、销毁或挪用，也可能导致系统被损坏或误用，包括攻击他人。任何IT系统或产品都不应被认为是完全安全的，并且没有任何单一产品或安全措施对于防止不当访问是完全有效的。IBM系统和产品的宗旨是成为一个全面的安全方法的一部分，它一定会涉及额外的运营程序，并可能需要其他系统、产品或服务配合才能获得最好的效果。IBM不保证系统和产品可以避免任何人的恶意或非法行为。

本文档中的信息按 "原样" 提供，不提供任何隐含或明确的担保，包括但不限于适销性、特定用途的适用性，以及有关非侵权性的任何担保或条件。IBM产品的担保依据的是它们所遵循的协议中的条款和条件。Hadoop不是IBM产品。视具体情况，根据随产品提供的Apache条款和条件将Hadoop出售或许可给用户。可用性和针对Hadoop的任何形式的担保、服务和支持都是Apache的直接责任，并且由Apache直接提供给用户。

客户负责确保遵守适用的法律和法规。IBM不提供法律建议，也不表示或保证其服务或产品将确保客户遵守任何法律。

请回收利用

WGW03020-CNZH-01