NSFOCUS

极光远程安全评估系统

产品白皮书

■ 版本	Ver1.0	■ 密级	公开
■ 发布	解决方案中心	■ 日期	2006-5-26

绿盟科技
NSFOCUS

■ 适用性声明

版权声明

商标信息

绿盟科技、NSFOCUS、极光、AURORA 等是中联绿盟信息技术（北京）有限公司的商标。

第三方信息

Microsoft、**Windows** 是美国 **Microsoft Corporation** 的在美国和其它国家注册的商标。

目录（Contents）

前言.....5
文档范围.....5
期望读者.....5
获得帮助.....5
一 漏洞的危害和发展趋势.....7
1.1 漏洞的危害.....7
1.2 漏洞的发展趋势.....8
二 漏洞管理的必要性与重要性.....10
三 漏洞管理产品评价指标.....12
四 极光远程安全评估系统.....13
4.1 产品体系结构.....13
4.2 产品功能.....15
4.2.1 资产管理.....15
4.2.2 漏洞分析.....16
4.2.3 漏洞修复.....16
4.2.4 漏洞审计.....16
4.3 产品特点.....16
4.3.1 开放漏洞管理流程 Open VM.....16
4.3.2 权威、完备的漏洞知识库.....17

4.3.3 高效、智能的漏洞识别技术 17
4.3.4 全面、实用的应用安全分析 17
4.3.5 量化的基于资产的风险评估 18
4.3.6 多维、细粒度的统计分析 18
4.3.7 基于用户行为模式的管理架构 19
4.4 典型应用方式 19
4.4.1 独立式部署 19
4.4.2 分布式部署 20
五 结论 21

前言

文档范围

本文将列出极光远程安全评估系统（以下简称极光或 AURORA）的基本信息，详细介绍极光的安装方法。

期望读者

期望了解本产品主要技术特性和使用方法的用户、系统管理员、网络管理员等。本文假设您对下面的知识有一定的了解：

- 系统管理
- Unix 和 Windows 操作系统
- TCP/IP 协议簇
- 网络安全
- 漏洞扫描

获得帮助

获取网络安全相关资料可以访问绿盟科技网站：http://www.nsfocus.com

获取本产品相关最新信息可以访问网址：

http://www.nsfocus.com/homepage/products/rsas.htm

您也可以给我们的技术支持人员发送电子邮件，Email 地址是：

product@nsfocus.com

获取更详尽的绿盟科技网络安全专业服务信息、商务信息，您可通过如下方式和我们联系：

北京总部

地址：北京市海淀区北洼路 4 号益泰大厦 3 层

邮编：100089

电话：010-68438880

传真：010-68437328

Email：webadmin@nsfocus.com

上海分公司

地址：上海市南京西路 758 号博爱大厦 9 楼 A 座

邮编：200041

电话：021-62179591/92

传真：021-62176862

广州分公司

地址：广州市人民中路 555 号美国银行中心 1702

邮编：510180

电话：020-81301251/52

传真：020-81301251/52

沈阳分公司

地址：沈阳市沈河区北站路 55 号财富大厦 C 座 2-16-1

邮编：110013

电话：024-22511115/3115

传真：024-22511115/3115

成都分公司

地址：成都市青龙街 51 号倍特康派大厦 15 楼 2 座

邮编：610031

电话：028-86632080/48

传真：028-86632080/48

一 漏洞的危害和发展趋势

从互联网兴起至今，利用漏洞攻击的网络安全事件不断，并且呈日趋严重的态势。每年全球因漏洞导致的经济损失巨大并且在逐年增加，漏洞已经成为危害互联网的罪魁祸首之一，也成了万众瞩目的焦点。人们也在一次次的蠕虫爆发之后在不断地寻求着漏洞的解决之道，不断尝试将由漏洞带来的风险降到最低，虽然也取得了一定成效，但是利用漏洞的攻击也在逐渐表现为多种不同的危害形式并且出现了新的攻击趋势。

1.1 漏洞的危害

漏洞是指计算机软件（包括硬件固化指令、操作系统、应用程序等）自身的固有缺陷或因使用不当造成的配置缺陷，这些缺陷可能被黑客利用对计算机系统进行入侵或攻击。漏洞分为本地漏洞和远程漏洞，通常意义上我们所指的漏洞是可被攻击者远程利用的漏洞，这些漏洞的危害往往都是大范围的，由此造成的经济损失也是巨大的，尤其是近两年来针对 Web 应用安全漏洞的攻击也在逐渐成为主流的攻击方式。

2000 年到 2004 年间，利用漏洞攻击的对象主要是针对网络设备、操作系统和数据库的攻击，其中让人感受最深的就是利用漏洞的网络蠕虫事件。下面是我们都非常熟悉的蠕虫给全球曾经造成的经济损失的统计表格。

发生年份	蠕虫名称	感染计算机台数	损失金额
2004 年	震荡波蠕虫	100 多万台	5 亿多美元
2003 年	冲击波蠕虫	140 多万台	30 亿多美元
2003 年	速客一号蠕虫	100 多万台	约 12 亿美元
2001 年	红色代码蠕虫	100 多万台	26 亿多美元
2001 年	尼姆达蠕虫	8 百多万台	6 亿美元

2005－2006 年间，主要是针对 Web 应用安全漏洞和客户端程序的的攻击。来自 google、Yahoo、Microsoft 以及 eBay 等著名互联网公司或者提供 Web 服务的软件公司都出现了不同程度的漏洞且都被攻击者成功的加以利用。

- 2005 年 10 月，Gmail 在进行帐号验证以及会话管理的过程中出现一个致命的漏洞，这一漏洞导致攻击者可以无须获得他人帐号而进入其邮箱查看其电子邮件；
- 2006 年 2 月，微软公司的 Hotmail 邮件服务被曝存在一个中风险级别的允许进行跨站脚本攻击的漏洞；同期，eBay 也出现类似漏洞；
- 2006 年 4 月，Yahoo 公司邮件服务中出现一个可以被利用进行钓鱼攻击的漏洞；同期微软 MSN Space 以及 Myspace 均出现可以被利用在站点中增加并执行恶意脚本的漏洞。

从上可以看出，安全漏洞的危害范围在逐渐扩大，由系统层扩展到应用层，由服务器端扩展到客户端，由少数操作系统到绝大多数操作系统；由此造成的经济损失也越来越大，尤其是用户不易察觉的隐性攻击造成的损失是无法衡量的。

1.2 漏洞的发展趋势

随着技术的不断进步，漏洞的发现、利用技术也发展到一个较高水平，从总体上来看，漏洞的发展趋势主要表现为以下几个方面：

- 漏洞的发现技术更加自动化和智能化，漏洞发现技术的革新导致了发现的漏洞的数量剧增，下面是国际组织 CERT/CC 的从 1995 年到 2006 年的漏洞统计数据。

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2006

Year	2000	2001	2002	2003	2004	2005	Q1,2006
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	1,597

Total vulnerabilities reported (1995-Q1,2006):**24,313**

- 国际上出现大量的专业漏洞研究组织，漏洞的出现到漏洞被利用的时间在不断的缩短，同时 0-day 攻击的数量在逐渐增加。
- 利用漏洞攻击的重心由服务器端向客户端过渡，由系统层和网络层逐渐向应用层扩展；Web 应用安全漏洞造成危害日益凸显。
- 利用漏洞的蠕虫逐渐减少，利用漏洞攻击的手法越来越诡异，越来越隐蔽。
- 漏洞的发现、利用不仅仅局限于常见的网络设备、操作系统，不断的向新的应用领域扩散。

二 漏洞管理的必要性与重要性

漏洞的危害越来越严重，发展的趋势的形式也是日益严峻。归根结底，就是系统漏洞的存在并被攻击者恶意利用。软件由于在设计初期考虑不周导致的漏洞造成的问题仍然没有得到很好的解决，人们依然用着“亡羊补牢”的方法来度过每一次攻击，利用漏洞的攻击成为人们心中永远的痛。

统计表明其中 19.4%来自于利用管理配置错误，而利用已知的一个系统漏洞入侵成功的占到了 15.3%。事实证明，绝大多数的网络攻击事件都是利用厂商已经公布的、用户未及时修补的漏洞。已经公布的漏洞未得到及时的修补和用户的安全意识有很大的关系，一个漏洞从厂商公布到漏洞被大规模利用之间的时间虽然在逐渐的缩短，但是最短的也有 18 天之久，18 天对于一些安全意识高的用户来说修补一个安全漏洞应该没有任何问题。还有，很多用户对传统安全产品的局限性认识不够深入，认为购买了防火墙、入侵检测、杀毒和扫描器等产品就高枕无忧了，这些产品能够解决所有的安全问题。其实不然，防火墙作为访问控制类设备，这类被动防护设备在蠕虫爆发或者漏洞被利用的时候束手无策，甚至在蠕虫爆发的时候不堪重负不能工作；入侵检测系统作为旁路监测设备，虽然对蠕虫和漏洞被利用能够起到一定的监测作用，但是还是不能有效地对利用漏洞的攻击进行防护；杀毒产品对于利用漏洞的攻击也是“事后诸葛”，只有在造成损失之后才能成为一个有效的辅助工具；漏洞扫描不能够解决资产和风险的关联问题，只能够在漏洞生命周期的某个阶段扫描出存在的漏洞而没有从漏洞生命周期整

个过程从根本上解决问题，只能是治标不治本，因此漏洞扫描在实际的使用过程中收到的实际效果有限，尤其是在大规模网络中使用过程中收效甚微。

到目前为止大多数的用户的安全意识也提高了，但是“冲击波”蠕虫和“震荡波”蠕虫的爆发还造成如此之大的损失，这说明了仅仅提高用户的安全意识是完全不够的，需要一套有效的管理机制并通过一定安全技术手段辅助自动完成整个过程，才能有效地对漏洞进行动态地管理。

目前，从技术和管理两个角度来看，漏洞问题已经有了较为成熟的解决方案，漏洞管理就是这样一套能够有效避免由漏洞攻击导致的安全问题的解决方案，它从漏洞的整个生命周期着手，在周期的不同阶段采取不同的措施，是一个循环、周期执行的工作流程。一个相对完整的漏洞管理过程包含以下步骤：

1. 对用户网络中资产进行自动发现并按照资产重要性进行分类；
2. 自动周期对网络资产的漏洞进行评估并将结果自动发送和保存；
3. 采用业界权威的分析模型对漏洞评估的结果进行定性和定量的风险分析并根据资产重要性给出可操作性强的漏洞修复方案；
4. 根据漏洞修复方案对网络资产的存在的漏洞进行合理的修复或者调整网络的整体安全策略进行规避；
5. 对修复完毕的漏洞进行的修复确认；
6. 定期重复上述步骤 1-5。

漏洞能够管理对利用已知安全漏洞的攻击起到很好的预防作用，做到真正的“未雨绸缪”。使用漏洞管理产品有以下好处：

- 漏洞管理产品从漏洞生命周期出发，提供一套有效的漏洞管理工作流程，实现了由漏洞扫描到漏洞管理的转变，实现了“治标”到“治本”的飞跃。
- 通过漏洞管理产品集中、及时找出漏洞并详细了解漏洞相关信息，不需要用户每天去去关注不同厂商的漏洞公告，因为各个厂商的漏洞公告不会定期发布，即使发布了漏洞公告绝大多数用户也不能够及时地获得相关信息。
- 通过漏洞管理产品将网络资产按照重要性进行分类，自动周期升级并对网络资产进行评估，最后自动将风险评估结果自动发送给相关责任人，大大降低人工维护成本。
- 漏洞管理产品根据评估结果定性、定量分析网络资产风险，反映用户网络安全问题，并把问题的重要性和优先级进行分类，方便用户有效地落实漏洞修补和风险规避 的工作流程，并为补丁管理产品提供相应的接口。
- 漏洞管理产品能够提供完整的漏洞管理机制，方便管理者跟踪、记录和验证评估的成效。

三 漏洞管理产品评价指标

用户在购买一款安全评估产品时应该考虑以下一些因素：

- 厂商是否具备漏洞跟踪和漏洞前瞻性研究能力，漏洞知识库的完备性、权威性和更新及时性；
- 产品提供漏洞管理工作流程支持功能和接口；产品的扩展性
- 漏洞评估的性能，主要是检测的速度和检测的准确性；
- 产品是否具备资产管理和风险定性、定量分析能力；
- 产品是否针对复杂大型网络的分布式部署和集中管理能力；
- 产品的报告内容、形式是否灵活，报告是否具备多角度统计分析的能力。

四 极光远程安全评估系统

基于多年的安全服务实践经验，同时结合用户对安全评估产品的实际应用需求，绿盟科技自主研发了极光（AURORA）远程安全评估系统，它采用高效、智能的漏洞识别技术，第一时间主动对网络中的资产进行细致深入的漏洞检测、分析，并给用户提供专业、有效的漏洞防护建议，让攻击者无机可乘，是您身边专业的“漏洞管理专家”。

- 依托专业的 NSFOCUS 安全小组，综合运用 NSIP 等多种领先技术，自动、高效、及时准确地发现网络资产存在的安全漏洞；
- 对发现的网络资产的安全漏洞进行详细分析并采用权威的风险评估模型将风险量化，给出专业的解决方案；
- 提供 Open VM（开放漏洞管理）工作流程平台，将先进的漏洞管理理念贯穿整个产品实现过程中。

4.1 产品体系结构

极光使用的是基于 Web 的管理方式，用户使用浏览器通过 SSL 加密通道和系统 Web 界面模块进行交互，方便用户管理。极光系统采用模块化设计，内部整体工作架构如图 1 所示。

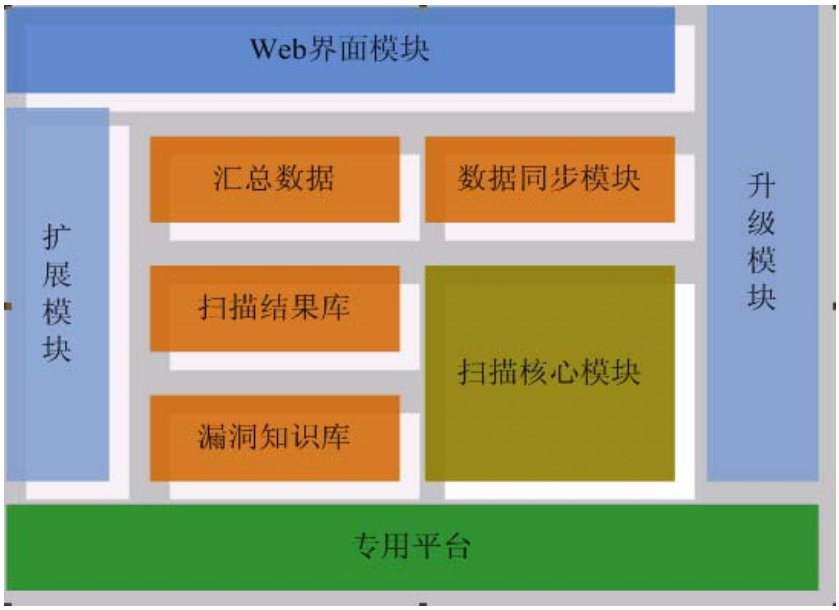

图 1　AURORA 系统整体架构图

◆　专用平台

专用平台是经过优化的专用安全系统平台，具有很高的安全性和稳定性。

◆　扫描核心模块

扫描核心模块是系统最重要的模块之一，它负责完成目标的探测评估工作，包括判定主机存活状态、操作系统识别、规则解析匹配等。

◆　漏洞知识库

漏洞知识库包含漏洞相关信息，是系统运行的基础，扫描调度模块和 Web 管理模块都依赖它进行工作。

◆　扫描结果库

扫描结果库包含了扫描任务的结果信息，是扫描结果报告生成的基础，也是查询和分析结果的数据来源。

◆　数据分析模块

数据分析模块是综合分析、趋势分析和报表合并的统计信息的数据来源，是任务合并、分布式数据汇总之后的结果。

◆　Web 界面模块

Web 界面模块负责和用户进行交互，配合用户的请求完成管理工作。Web 管理模块包含多个子模块共同完成用户的请求，其主要子模块有：

1)　任务管理子模块——完成用户评估任务的管理工作。

2)　报表子模块——读取扫描结果库，并根据漏洞描述信息和解决方案生成扫描报表。

3) 任务报表辅助管理子模块——完成评估任务需要扫描的具体漏洞模板的添加、具体漏洞的选取、模板修改和删除；评估任务使用策略参数的管理；口令字典管理；报表输出模板管理。

4) 地址本管理子模块——地址本作为系统和网络真实状况之间的纽带，方便进行资产的管理，并可在绿盟科技的各产品之间导入/导出。

5) 用户和权限系统子模块——系统支持多用户管理，不同用户可具备不同的权限，可以对相应的系统资源进行管理操作。

6) 系统日志和审计策略子模块——所有用户的每个登录、操作及异常情况都会被系统自动记录到日志中，方便管理员查看，及时找出问题所在，并可自行设置哪类操作进行审计。

7) 常用工具子模块——集成了 ping 命令、traceroute 命令两个常用工具。

8) 系统配置子模块——完成系统自身的维护管理功能。

◆ 分布式模块

极光支持分布式部署功能需要专门的数据同步模块来支撑。数据同步模块完成扫描结果数据后，向上级 AURORA 系统的数据上传，在数据上传中使用 SSL 加密传输通道，保证了数据的保密性。汇总的数据可以进行集中统一的分析。

◆ 漏洞管理模块

漏洞管理模块主要实现了 Open VM 漏洞管理工作流程支持，提供与其他安全产品、网络管理平台和安全管理平台的接口。

◆ 系统升级模块

极光有网络自动升级和用户手动升级的策略，系统的各个模块都可以通过升级模块进行升级。

4.2 产品功能

4.2.1 资产管理

极光的资产管理功能在产品中是通过“地址簿”来实现的，用户可以手动输入资产属性，并且按照资产重要性权值进行资产重要性分类；同时资产输入也可以通过任务管理中的地址导入功能加入。资产管理和用户组织结构或者网络拓扑结构紧密结合，对大规模网络用户，网络资产繁多，IP 地址记忆非常繁琐，用户通过规范的命名方式来统一对网络资产的管理。资产管理的使用，方便用户掌握风险分布情况、定位风险和高效实施风险降低或规避措施。

4.2.2 漏洞分析

极光采用业界权威的风险评估模型，从资产、漏洞和威胁三个维度对资产风险进行评估。极光通过在线报表和离线报表将风险分析结果展示给用户，从多个视角对风险进行深入的分析，权威的评估模型加上评估结果定量和定性分析，让您真正了解业务系统中存在的风险。

4.2.3 漏洞修复

极光在产品设计初期就考虑到漏洞修复问题，在产品实现中提供了多种二次开发接口供漏洞修复产品或补丁管理产品使用，方便用户及时集中对资产漏洞进行修复。

4.2.4 漏洞审计

用户在实际的漏洞修复的过程中往往很难确认自己的漏洞是否真正修复，即使安装了评估结果中厂商补丁也很难确认补丁程序是否真正安装成功。针对这种情况，极光提供了漏洞审计功能，能够通过发送监督邮件的方式来督促相应的资产管理员对漏洞进行修复，同时启动自动的定时任务对漏洞进行审计，提高了管理人员手工验证漏洞是否修复的效率。

4.3 产品特点

4.3.1 开放漏洞管理流程 Open VM

绿盟科技基于最新的“漏洞管理”工作流程，把漏洞管理的循环过程划分为漏洞预警、资产管理、漏洞分析、漏洞修复、漏洞审计五个阶段，在国内首创了 Open VM 工作流程平台。基于这个开放平台，极光将漏洞管理理念贯穿于整个产品实现过程，实现了 Open VM 的部分过程；同时，极光产品通过多种二次开发接口与其他安全产品协作来完全实现 Open VM 的整个工作流程。

4.3.2 权威、完备的漏洞知识库

绿盟科技 NSFOCUS 安全小组的安全研究能力在国内首屈一指，在国际上也有相当的影响力。在这个部门中，有多位专职的研究员进行漏洞跟踪和漏洞前瞻性研究，到目前为止已经独立发现了 30 多个关于常见操作系统、数据库和网络设备的漏洞，并且为国际上的知名网络安全厂商提供相关漏洞的规则支持。NSFOCUS 小组负责极光的漏洞知识库和检测规则的维护，除定期的每两周的升级外，重大漏洞。

依靠专业的 NSFOCUS 安全小组多年的研究，绿盟科技中文漏洞知识库已经有 7000 多条安全漏洞信息，该库中的每条漏洞都有详尽的描述和修补建议，其完备性和权威性在国内厂商内首屈一指。绿盟科技中文漏洞知识库是国际上最大的中文漏洞知识库。极光产品的漏洞信息（1700 多条）精选于该漏洞知识库，涵盖了常见操作系统、数据库、网络设备和应用程序的绝大多数可以远程利用的漏洞，已获得国际权威的 CVE 兼容性认证。

4.3.3 高效、智能的漏洞识别技术

NSIP(NSfocus Intelligent Profile)是绿盟科技智能 Profile 漏洞识别技术的简称，该技术在国内甚至在国际上都是非常领先的漏洞识别技术，它在提高极光的评估速度和准确率方面都起到了很大的促进作用。NSIP 漏洞识别技术就是采用多种技术通过不同途径收集目标系统的多种信息，这些信息就是目标系统的 Profile，在进行漏洞评估过程中，Profile 不断地对中间的结果数据进行调整，保障了最后评估结果的准确性。

极光产品具备业界强劲的底层扫描引擎——NSSE（NSFOCUS Scanning Engine）。通过 NSIP 技术、开放端口服务的智能识别、检测规则依赖关系的自动扫描等技术的运用，再加上由 NSFOCUS 安全小组研究员精心编写的准确的漏洞检测规则，极光在检测速度和检测准确性之间找到了最佳的平衡点。极光加载全部检测规则，对同样的目标系统进行检测时，扫描速度为常见同类产品 3－5 倍，同时仍能保证误报率低于 5%。

4.3.4 全面、实用的应用安全分析

考虑到目前 Web 应用安全漏洞所带来的巨大危害，极光推出了 Web 应用安全漏洞检测，通过对被检测站点进行深度内容分析，找出可被浏览的 ASP、JSP、

PHP、CGI 等页面，同时可以分析被检测站点页面源代码，以检测网站是否存在 SQL 注入或输入验证信息泄露等漏洞。

极光还在漏洞检测中提供了专用的 CGI 漏洞检测插件规则类别和专用的 SQL 注入检测插件，用来发现一些特定、常见的站点隐藏的页面并发现一些文件路径信息泄露的安全隐患，并能深入的分析一些 CGI 的漏洞问题。

4.3.5 量化的基于资产的风险评估

单纯的漏洞扫描产品因没有与资产关联，只能扫描出漏洞并不能反映客户环境中资产的真实的风险状况。绿盟科技的极光远程安全评估系统将资产、漏洞和威胁紧密结合，提供了图形化的资产管理方式，并通过可量化的模型呈现，帮助用户对网络中存在的风险有一个整体、直观的认识，做到真正意义上的风险量化。

在每次安全评估之前，用户需要根据自己的业务系统确定需要进行评估的资产，并且划分资产的重要性。极光根据用户的资产及其重要性会自动在其内部对目标评估系统建立基于时间和基于风险等多种安全评估模型。在对目标完成评估之后，模型输出的结果数据不但有定性的趋势分析，而且有定量的风险分析，用户能够清楚地看到单个资产、整个网络的资产存在的风险，还能够看到网络中漏洞的分布情况、风险级别排名较高的资产、不同操作系统和不同应用漏洞分布等详细统计信息，用户能够很直观地了解自己网络安全状况。

4.3.6 多维、细粒度的统计分析

极光产品不仅提供了常见的离线报表，还提供了强大的在线报表系统。同时，极光为您提供了一个实用的报表过滤器，它能够帮助客户更好地获得有效信息，生成基于不同角色、不同内容和不同格式的报表。极光不仅站在管理员的角度分析结果，也站在公司决策层和网络部门管理人员的角度考虑报告的生成。

极光从宏观和微观两个角度对风险进行了透彻地分析。从宏观角度，极光从多个视角深刻反映网络的整体安全状况，对漏洞分布、危害、漏洞 TOP10、主机信息等多视角信息进行了细粒度的统计分析，并通过柱状图、饼图等形式，直观、清晰的从总体上反映了网络资产的漏洞分布情况；从微观角度，极光对检测到的每个漏洞都提供了详细的解决方案，使得管理员可以快速准确地解决各种安全问题，同时支持用户自己输入关键字进行相关信息的检索，以便用户能够具体了解某台主机或者某个漏洞的详细信息。

极光从多个视角深刻反映网络的整体安全状况，还提供趋势分析功能，不仅对当前的漏洞分布、危害等进行了统计分析，还为未来的网络安全建设提供了强有力的决策支持。

4.3.7 基于用户行为模式的管理架构

作为用户体验性很强的产品，极光始终秉承“以人为本”的理念，在产品设计过程充分考虑了实际用户需求和使用习惯，从用户角度完善了很多管理功能。这些不仅体现在安装和实施的方便程度上，更重要是在于对自动运维的支持。

极光采用 B/S 管理架构，能够以 SSL 加密通讯方式通过浏览器来远程进行管理。极光的专用硬件能够长期稳定地运行，很好地保证了任务的其周期性自动处理，其中能够自动处理的任务包括：评估任务下发、扫描结果自动分析、处理和发送、系统检测插件的自动升级等。同时，极光支持多用户管理模式，能够对用户的权限做出严格的限制，并且提供了登陆、操作和异常等日志审计功能，方便用户对系统的审计和管理。

4.4 典型应用方式

目前用户的网络环境常见的网络拓扑结构有：总线拓扑、星形拓扑、树形拓扑和混合型拓扑。针对上述用户常见的网络拓扑，极光远程安全评估系统为用户“量身定做”了两种部署方式：独立式部署和分布式部署。

4.4.1 独立式部署

中小型企业、电子商务、电子政务、教育行业和独立的 IDC 等用户，由于其数据相对集中，并且网络拓扑结构相对较为简单，大多数采用总线拓扑或者星形拓扑，对于这些用户建议使用独立式部署方式。独立式部署就是在网络中只部署一台极光设备。在共享式工作模式下，只要将极光接入网络并进行正确的配置即可正常使用，其工作范围通常包含客户公司的整个网络地址。用户可以从任意地址登录极光系统并下达扫描任务，扫描的地址必须在产品和分配给此用户的授权地址范围内。

图 2 就是极光的平坦部署模式。从图中可以看出，无论在公司何处接入极光设备，公司网络都能正常工作，完成对网络的安全评估。

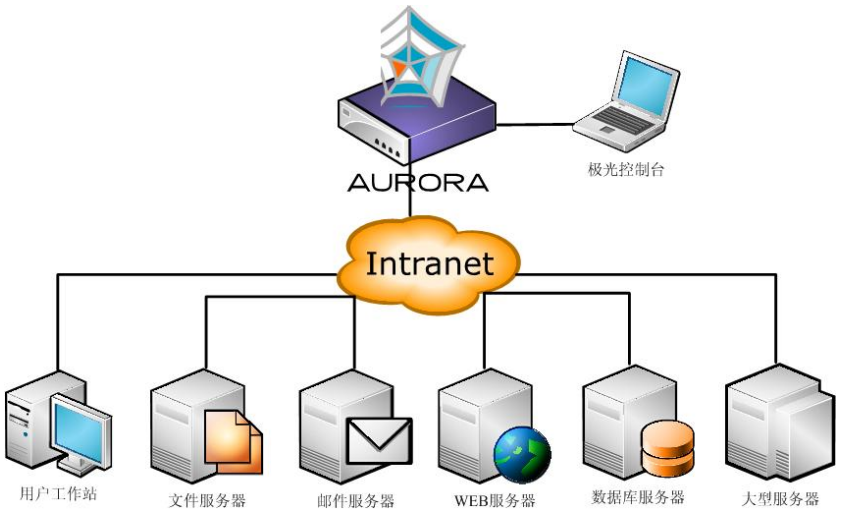

图 2　AURORA 独立式部署结构图

4.4.2 分布式部署

对于电信运营商、金融行业、证券行业、政府行业、军工行业、电力行业和一些规模较大传统企业，由于其组织结构复杂、分布点多、数据相对分散等原因，采用的网络拓扑结果大多为树形拓扑或者混合型拓扑。对于一些大规模和分布式网络用户建议使用分布式部署方式。在大型网络中多台极光系统共同工作时，极光的分布部署支持能力可以使得各系统间的数据能共享并汇总，方便用户对分布式网络进行集中管理。极光支持用户进行两级和两级以上的分布式、分层部署。使用两级分布式部署结构拓扑如图 3 所示。

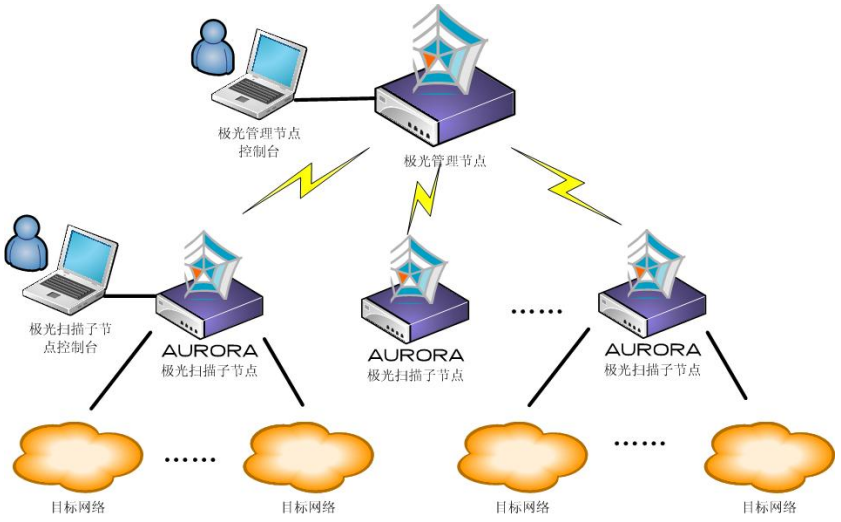

图 2　AURORA 分布式部署结构图

五 结论

每年都有数以千计的网络安全漏洞被发现和公布，再加上攻击者手段的不断变化，用户的网络安全状况也在随着被公布安全漏洞的增加在日益严峻。因此，安全评估对于绝大多数用户都是不容忽视的，用户必须比攻击者更早掌握自己网络安全漏洞并且做好适当的修补，才能够有效地预防入侵事件的发生。

事实证明，99%的攻击事件都是利用未修补的漏洞。许多已经部署防火墙、入侵检测系统和防病毒软件的企业仍然饱受漏洞入侵之苦，其中有更多受到蠕虫及其变种的破坏，造成巨大的经济损失。归根结底，其原因是用户缺乏一套完整的安全评估机制，未能落实定期评估与漏洞修补工作，忽视了漏洞的管理，最终是漏洞成为攻击者攻击的有效途径，甚至成为蠕虫攻击的目标。

依托国内最权威中文漏洞知识库和已在国际上享有盛名的 NSFOCUS 安全小组，极光远程安全评估系统已经是国际领先的漏洞管理产品之一，能够定期和持续地给用户提供可靠的安全评估服务，并且提供完整的漏洞管理机制，能够有效地降低用户网络风险，更大的限度地保证用户网络安全性和稳定性。