文档编号：**NSF-PROD-AURO-V3-WH**

极光远程安全评估系统
产品白皮书

中联绿盟信息技术(北京)有限公司
NSFOCUS INFORMATION TECHNOLOGY CO.,LTD.

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

期望读者

期望了解本产品主要技术特性的用户、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
- **Linux**和**Windows**操作系统
- **Internet** 协议

获得帮助

获取网络安全相关资料，可以访问绿盟科技网站：www.nsfocus.com

获取本产品最新的相关信息可以访问网址：

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

您也可以给我们的技术支持工程师发送电子邮件，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：020-81301251，81301252

传真：020-81301251/52

沈阳分公司

地址：沈阳市和平区文化路 45 号机械大厦 901 室

邮编：110003

电话：024－83891274

传真：024-23998066

成都分公司

地址：成都市顺城大街冠城广场 8 楼 C 座

邮编：610017

电话：028-86528249

传真：028-86528248

1. 漏洞的危害和发展趋势

随着网络技术的成熟和广泛应用，更多的新技术、新应用融入了人们的生活中。技术的飞速发展给人们带来便利的同时，也给人们带来了不安。从互联网的兴起开始至今，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发展。利用漏洞的攻击的目标也开始转向整个互联网，全球每年由此造成的经济损失也是逐年增加。利用漏洞的攻击已经成为危害互联网的主要因素之一。

1.1. 漏洞的危害

美国 FBI/SANS 协会 2005 年第二季度公布的数据显示，第二季度新增的安全漏洞超过了 422 个。这一数字比第一季度增长了 10.8%，比去年同期增长了 20%。进入 SANS 协会漏洞统计榜的漏洞需要影响大规模的用户，同时这些漏洞还必须能够远程被攻击者利用。

美国计算机安全公司 Symantec 在两年一次的报告中指出，2005 年上半年，来自各个方面所公布的计算机软件漏洞多达 1862 个。与 2004 年下半年相比，漏洞数量增长了 31%；比去年同期增长了 46%。漏洞中 97%的被认定影响严重，73%容易被黑客利用。

上面的数据谈到的漏洞的危害如果不够直观的话，现在来看大多数用户都非常熟悉的蠕虫给全球曾经造成的巨大的经济损失。

发生年份	病毒名称	特征	感染计算机台数	损失金额
2004 年	震荡波蠕虫	攻击 Microsoft 操作系统的漏洞(Port 445)	100 多万台	5 亿多美元
2003 年	冲击波蠕虫	攻击 Microsoft 操作系统的漏洞(Port 135)	140 多万台	30 亿多美元
2003 年	速客一号蠕虫	攻击 Microsoft SQL 服务器的漏洞(Port 1434)	100 多万台	约 12 亿美元
2001 年	红色代码蠕虫	通过 Port 80 传播攻击 IIS Server 漏洞，发动 DDoS 攻击，可远程控制中毒计算机	100 多万台	26 亿多美元
2001 年	尼姆达蠕虫	通过电子邮件、资源共享等多种方式来传播	8 百多万台	6 亿美元

上面的数据充分说明了目前安全漏洞的数量呈逐年增加的趋势，并且对用户的危害程度越来越为严重。

1.2. 漏洞的发展趋势

漏洞是指计算机软件（包括 CMOS 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，通常我们所指的漏洞是可远程利用的漏洞，这些漏洞的危害往往都是大规模的，由此造成的经济损失也是巨大的。

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，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。
- 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。下表充分证明了这一点。

蠕虫名称	微软修补程序公布	蠕虫爆发日期	漏洞发布与蠕虫爆发之间的时间
Worm_Sasser 震荡波蠕虫	MS04-011 04/13/2004	05/01/2004	18 天 (历史最短时间)
Worm_Blaster 冲击波蠕虫	MS03-026 07/16/2003	08/11/2003	26 天
Worm_Slammer 速客一号蠕虫	MS02-039 07/24/2002	01/25/2003	185 天
Worm_Nimda 尼姆达蠕虫	MS00-078 10/17/2000	09/18/2001	336 天

- 利用漏洞攻击的手法越来越诡异，漏洞使计算机遭受的恶意攻击次数目前已达到创纪录的水平，尤其是网络蠕虫的攻击。
- 漏洞的发现、利用不仅仅局限于常见操作系统，不断的向新的应用领域扩散。

2. 安全评估产品重要性

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。其实，从技术角度来讲，漏洞的问题已经有了较为成熟的解决方案，安全评估产品就是这样一类能够有效避免由漏洞攻击导致的安全问题。

安全评估产品就是在攻击者利用漏洞之前，对用户网络中资产的漏洞进行自动发现、统计分析并提供相应的修补措施的系统，对利用这些漏洞的攻击起到很好的预防作用，做到“未雨绸缪”。

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、杀毒产品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工具；简单的漏洞扫描工具不能够解决漏洞和资产的关联问题，只能够扫描出存在的漏洞而不能够对其进行合理的管理，不能够做到真正意义上的安全评估。

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，需要一套有效的漏洞评估管理机制并通过一定的安全评估产品辅助才

能有效地对漏洞进行动态地管理。要从根本上解决漏洞之“本”的问题，需要对漏洞进行定期的评估、分析和修补工作，安全评估产品就能很好地完成上述工作。

使用安全评估产品有以下好处：

- 首先，用户能够通过安全评估产品集中找出安全漏洞，并且集中了解漏洞的内容，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，即使发布了很多用户也不能够及时地获得相关信息。
- 其次，用户能够通过安全评估产品降低网络的风险，安全评估产品对检测出来的漏洞都会提供相应的解决方法，进而减少存在的漏洞降低网络风险指数。
- 最后，安全评估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，通过量化的报表来真是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的工作流程。

3. 安全评估产品评价指标

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
- 安全评估的性能，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漏洞管理能力
- 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
- 产品的可扩展性，与其他系统的整合能力

4. 绿盟科技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，针对网络中的资产进行细致深入的漏洞检测、分析，并给用户提供有效的漏洞修补方案，为企业网络安全维护提供了强有力的保障。

极光远程安全评估系统的主要功能如下：

- **国际领先的漏洞评估功能**

极光具备非常优秀的底层扫描引擎，通过使用 **Profile**、智能端口识别、自动模板匹配等技术，在较高的扫描速度下仍能保持极低的误报率。

- **方便的资产管理功能**

极光能够将网络资产和组织结构紧密结合，并提供图形化的资产管理方式。

- **及时、可靠的升级功能**

极光依托绿盟科技权威的中文漏洞知识库，能够检测到 **1500** 多条不同的漏洞。绿盟科技强大的安全基础研究能力能够保障每两周进行定期升级，对严重漏洞两天内即可提供全部更新。

- **集中管理、分布式部署功能**

极光在国内率先提出并实现了分布式扫描系统的技术路线，完全适用于大型/超大型网络的整体网络安全评估。

- **灵活、实用的报表功能**

极光的报表引擎采用模板驱动技术，能够针对不同用户、不同需求灵活定制报表的格式和内容模块。

- **丰富、强大的扩展功能**

扫描结果支持多种视角的 **html** 和 **doc** 格式查看、打印和保存；中间结果支持 **XML** 格式导出，用户可进行二次开发；支持发送 **SNMP Trap** 与网管系统集成，支持与 **ESP** 系统集成；不同规格的极光设备之间可以进行平滑的升级和数据转移。

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。

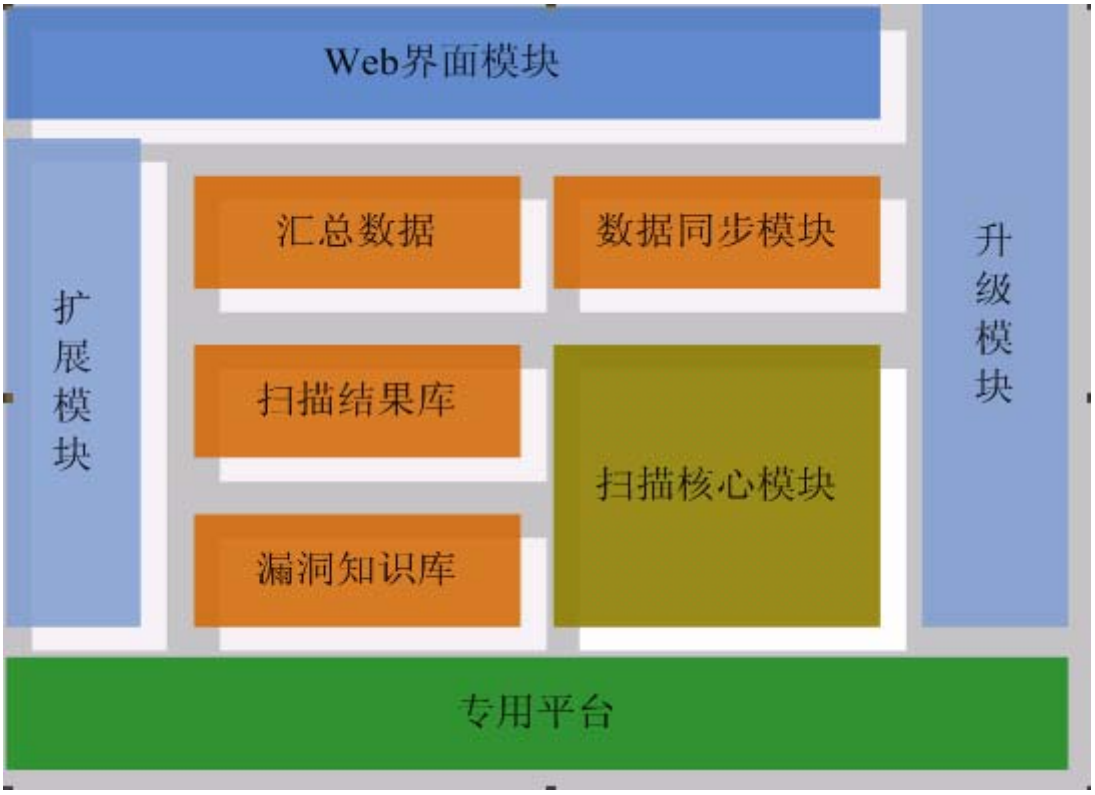

图 1　AURORA 系统整体架构图

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。

- **汇总数据**

汇总数据是综合分析、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，即时找出问题所在，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、hping 命令、nmap 命令、traceroute 命令和 dig 命令这五个常用工具。
8) 系统配置子模块——完成系统自身的维护管理功能。

- **数据同步模块**

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。

- **扩展模块**

扩展模块中主要提供一些与其他网络管理平台、安全管理平台的接口，提高系统与其他系统联动、整合能力。

- **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. 产品特点

4.2.1. 权威、完备的漏洞知识库

绿盟科技安全研究小组 **NSForce** 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 20 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。

经过五年来积累，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，是国内最为权威的中文漏洞知识库之一。极光内置的中文漏洞知识库以绿盟科技中文漏洞知识库为基础，包含的漏洞信息超过 **1500** 条，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。

除此之外，极光的漏洞知识库能够保证每两周进行定期升级，重大漏洞甚至在两天内就能发布更新，使得产品更及时地检测到最新的漏洞。

4.2.2. 高效、智能启发式漏洞识别技术

NSLHP(NSfocus Logical Heuristic Profile)是绿盟智能启发式 **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。**NSLHP** 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。

极光运行在专用安全操作平台上，采用独有的 **NSLHP** 漏洞识别技术，同时辅以自动匹配、端口智能识别、模拟穿透、并发扫描等多种技术，在保证漏洞检测准确性的情况下极大提高了对目标系统的检测速度。除此之外，由 **NSForce** 研究员精心编写的漏洞检测规则插件也很好的保证了检测的准确性。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%**。

4.2.3. 基于资产的可量化安全评估模型

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安全状况。绿盟科技的极光远程安全评估系统将资产、组织结构以及漏洞威胁紧密结合，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，做到真正意义上的安全评估。

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。

4.2.4. 基于用户行为模式的管理架构

通过三年的产品应用和上百个用户的需求和建议调查，极光远程安全评估系统进一步增强了其管理功能。极光在用户界面设计上也充分考虑了用户的使用的行为习惯，并完善了自动运行、维护等功能，使系统可以在无需人工干预的情况下长期使用。

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。

4.2.5. 多维、细粒度的评估分析与统计

极光可以自动生成各种形式的统计报表，包括柱状图、饼图、报表等，以直观、清晰的方式从总体上分析网络上的漏洞分布，为管理人员提供方便。报表可以直接打印，也支持以 **html** 或 **doc** 格式输出下载。

极光检测到的每个漏洞在扫描报告中都有详细的解决方案，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。

极光得到扫描结果后，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。

考虑到在进行大规模网络安全评估或者分布式安全评估时数据汇总统计，极光能够根据用户的需要将扫描结果进行归并分析，方便用户集中管理。

极光的报表从多个视角深刻反映网络的整体安全状况，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。

4.2.6. 高度可扩展性

极光远程安全评估系统对外提供了多种联动接口和二次开发接口。

在扫描结果数据处理过程中能够生成 XML 格式文件，用户能够根据自己的需求提取相应的数据。在扫描任务派发和扫描结果获取方面，极光给授权用户提供了 HTTP 调用的相应接口。在与其他管理平台的整合方面，极光能够通过 SNMP Trap 与常用的网管系统进行无缝结合，能够和多种安全管理平台进行联动。除此之外，不同规格的极光设备之间可以进行平滑的升级和数据转移，并且还能够与绿盟科技的 ESP 系统进行紧密整合。

4.2.7. 灵活的多级分布式部署能力

极光能够支持多级分布式部署和分级授权管理。用户能够对网络中部署的极光远程安全评估系统分等级和角色，低级别的极光将扫描数据同步发送到高级别的扫描器数据库中，这样上层管理人员可以查看下层扫描器的扫描结果，以此监督下层管理员的工作和了解整体安全现状。在分级、分布式部署中不影响各个扫描器的单独使用。分布式部署最大限度地方便了大规模网络和分布式网络的用户进行整体网络的安全评估工作。

4.3. 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：平坦式部署和分布式部署。

4.3.1. 平坦式部署

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平坦式部署方式。平坦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。

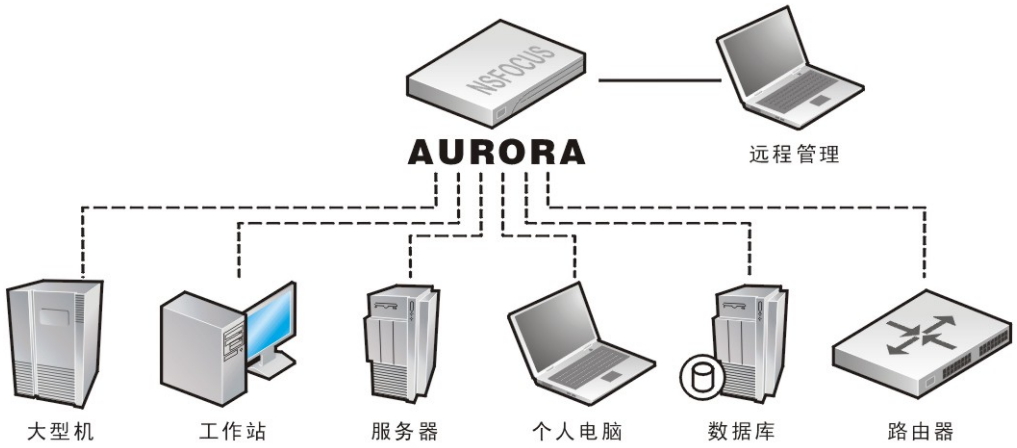

图 2　AURORA 的平坦部署模式结构图

4.3.2. 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。

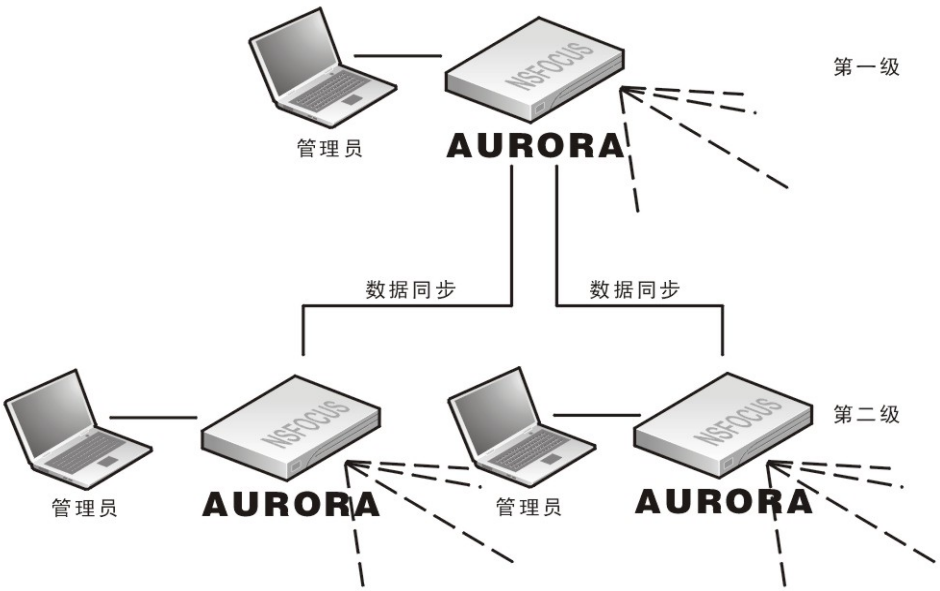

图 3　AURORA 的分布式部署模式结构图

5. 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，才能够有效地杜绝入侵事件的发生。

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基础安全研究小组 **NSForce**，极光远程安全评估系统已经是国际领先的网络安全评估系统之一，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。