NetIQ Sentinel 7

功能强大而又简单的安全管理

简介

各组织正在对他们的 IT 基础设施及其使用方式进行重大改造。这些转变产生了一系列难题和挑战，反过来可能会影响组织对其企业的保护能力。

例如，虚拟化、云计算和移动技术改变了组织开展业务的方式。这些技术使用户以令人兴奋的新方式操作，并实现用户与信息的互动以及用户之间的互动。但是，这些技术也推动了分布式互连企业的发展，信息安全分析人员发现，对于这些企业而言，它们越来越难有效地监控和维护安全性。

为了改善其整体安全状况并作出更明智的决策，组织需要有关安全事件的实时信息和分析。他们需要能够解决管理大量安全数据、处理复杂威胁和实行持续策略控制的复杂性问题。他们需要一个解决方案来帮助他们快速而准确地确定在大量事件数据中，哪些事件构成关键事件和安全异常。

产品概述

NetIQ® Sentinel™ 7 为组织提供对全局 IT 活动的实时可见性，以缓解安全威胁、改善安全操作，并在整个物理、虚拟和云环境中自动实行策略控制。它降低了传统安全信息和事件管理 (SIEM) 的复杂性和采用 SIEM 的门槛，使得所有组织均可获得安全智能。NetIQ Sentinel 7 还通过合并实时智能、异常检测和用户活动监控功能提供提前警告机制和更准确的 IT 活动评估，为组织提供更高效的 SIEM 解决方案。

NetIQ Sentinel 7 提供业内唯一的身份管理无缝集成，可在所有环境中将用户与特定活动绑定。因此，它使各组织可以轻松地识别关键风险、显著缩短响应时间，并在威胁和安全漏洞影响业务之前快速进行补救。通过其实时智能，Sentinel 使组织能够防御高级威胁的出现、改善安全操作以及不间断地执行策略。

解决方案
安全管理

产品
NetIQ® Sentinel™ 7

NetIQ

“即便我们每天遇到多达 35 件严重安全事件，Sentinel 也能使我们能够尽早发现和尽快解决，从而确保这些事件丝毫不会影响活动的进行”

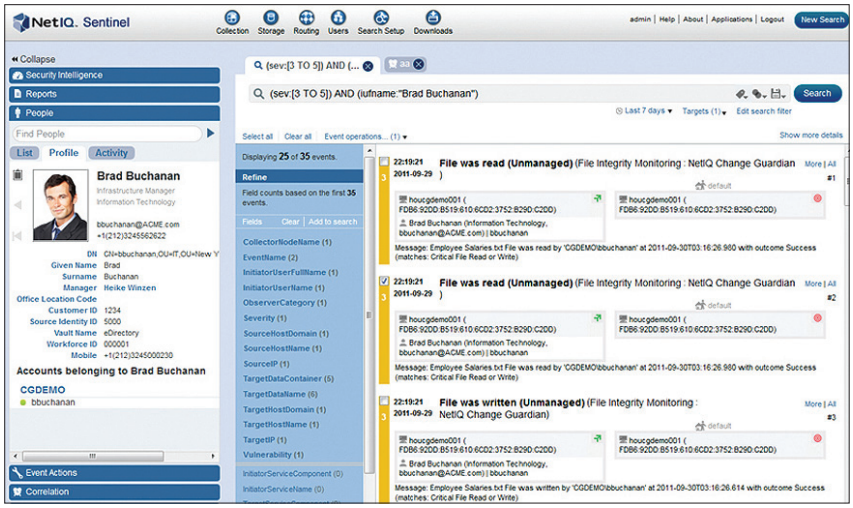
Vladan Todorovic，
青年奥运会的技术与
IT 安全经理 Atos Origin

功能和特性

- **异常检测** — 确定事件是真正的问题还是需要调查的潜在问题通常很难。通过 NetIQ Sentinel 异常检测，您可以自动确定组织环境中不一致的地方，而无需制定需要您确切知道查找内容的关联规则。实施 Sentinel 后，便对组织的特定环境设定了基线，使您可以立即提供更强的智能和更快的异常活动检测。您可以将趋势与基线进行比较，以查看历史活动模式，从而快速开发典型 IT 活动 - 或正常状态 - 的模型，使您可以轻松发现新的、潜在的不利趋势。要增强这些功能，您可以进一步调整您的环境基线和相应的异常事件检测。NetIQ Sentinel 还可向您显示您的安全和合规性状况如何随时间改变。

- **灵活的部署选项** — NetIQ Sentinel 作为所有主要超级管理程序（包括 VMware、HyperV 和 XEN）上的软设备（通过标准化国际组织 [ISO] 映像）以及 SUSE® Linux Enterprise Server 和 Red Hat Enterprise Server 上的可安装软件提供。NetIQ Sentinel 部署和许可模型非常灵活，使您可以在整个组织中部署 SIEM 和日志管理以满足其特定使用需求。Sentinel 采用灵活的搜索和事件转发机制，使部署体系结构可以适应您的环境，甚至是高度分布式部署。

- **高性能储存体系结构** — NetIQ Sentinel 采用基于文件的高效事件储存层，该存储层针对长期事件存档进行了优化。事件存储提供 10:1 的压缩，完全支持快速、使用索引的搜索。NetIQ Sentinel 还可让您选择将部分或全部企业事件数据同步或移动到传统的关系数据库。搜索功能显著增强，可减少查找数据和生成报告的时间。Sentinel 储存体系结构不再需要第三方数据库许可，从而降低贵组织的总拥有成本。



NetIQ Sentinel 7 通过使用身份管理提供了行业领先的用户活动监控功能，可在整个系统中将用户绑定到特定操作。

- **图形规则构建器** — NetIQ Sentinel 允许您直接根据在您的环境中收集的事件快速构建事件关联规则 — 无需管理员进行大量培训，也无需学习专有脚本编写语言。此外，您还可以在部署规则前对其进行测试，以减少误报警报、提高事件关联，并最终交付更完善的攻击检测功能。这样可以显著延长您组织的价值实现时间，同时降低总拥有成本。
- **身份增强功能** — 通过与 NetIQ® Identity Manager 的现成集成，NetIQ Sentinel 提供业内唯一的无缝身份管理集成，将用户与整个企业中的特定活动绑定。使用用户和管理员的唯一身份信息丰富安全数据，可显著提高用户系统访问的“用户、时间和地点”信息的透明度。此外，通过将身份信息包括到事件数据中，NetIQ Sentinel 可以智能地保护您免遭内部威胁，并提供可操作性更强的补救机制。NetIQ Sentinel 还包括与 Microsoft Active Directory 的身份集成，而且不久之后还将包括与其他身份管理产品的集成。
- **简化过滤、搜索和报告** — NetIQ Sentinel 简化了 IT 基础设施事件的收集工作，以自动执行乏味的合规性审计和报告功能，并显著降低了查找和准备审计员所要求的数据的复杂性、时间和成本。这有助于您的组织快速遵守政府法规和行业规定。
- **已增强和扩展的报告包** — NetIQ Sentinel 通过其数据聚合和标准化功能、预构建报告和可自定义策略以及快速搜索功能简化了报告工作。您只需简单地按下按钮，即可生成实时搜索结果报告，从而能够即时报告所需的数据，无需烦琐地修改限制性的预构建模板。
- **单个统一解决方案** — NetIQ Sentinel 在单个统一的解决方案中将日志管理与 SIEM 结合。

“没有至少 10,000 名人员，不可能与网络安全活动的急剧增长保持同步。Sentinel 使我们的中央监控团队能够全面了解安全事件，因此我们可以立即对最关键的事件采取行动。”

Keith Rohwer,
NCDOC 研究、开发、测试与评估主管

NetIQ

要进一步了解
NetIQ Sentinel 7
或要开始体验，请访问
www.netiq.com/sentinel7。

主要优势

与战术性的 SIEM 解决方案（比较简单，但并不是专为提供真正的安全智能而设计）和传统的 SIEM 解决方案（功能强大，但需要大量的技能和自定义，并且难以适应不断变化的环境）不同，NetIQ Sentinel 7 在安全智能方面提供了最高的价值，因为其简单性和强大的功能帮助解决了“我是否安全？”这一问题。

- 虚拟软件设备封装能够实现快速方便的部署。与基于硬件的产品不同，虚拟设备易于扩展，便于应对增长和附加的容量。
- 身份增强功能为安全事件提供了丰富的环境，可为检测和防止基于内部的威胁提供更深入的了解。
- 通过图形规则构建界面和容量规划来简化管理。管理员在实施期间可以快速制定关联规则，并根据业务需求的改变进行轻松维护和更新，从而降低总拥有成本。
- 安全智能仪表板一经安装即可开始监控组织的安全性，能够实现一天内的数值记录。
- 直观的数据搜索功能使安全管理员能够轻松找到所需数据，并迅速将搜索结果转变成报告。

NetIQ 中国
北京朝阳区东三环中路7号财富中心写字楼A座3603
免费咨询电话：400 6900 962
info@netiq.com
www.netiq.com
http://community.netiq.com

有关我们在
北美洲、欧洲、
中东、非洲、亚太地区
和拉丁美洲的办事处完整列表，
请访问：**www.netiq.com/contacts**。

跟随我们：

PB595001SENT CN A4 PO 6/12 F
577-CN1002-002 DS 05/12