2011 年 5 月 6 日

Forrester Wave™： 数据库审计与实时防护，2011 年第二季度

作者：Noel Yuhanna

适用于应用程序开发与交付专业人员

FORRESTER® 为领先公司带来成功的每一天

2005 年 5 月 6 日

Forrester Wave™： 数据库审计与实时防护，2011 年第二季度

IBM、Imperva 和 Sentrigo 位居榜首，Application Security、Oracle 和 Fortinet 紧随其后

作者：Noel Yuhanna
Stephanie Balaouras 和 Adam Knoll

执行摘要

经过 Forrester 的数据库审计与实时防护供应商的 147 项标准评估，我们发现市场中充斥着大量的成熟产品。IBM、Imperva 和 Sentrigo 处于领先地位，因为它们具备强大的用户活动审计、策略管理、实时防护和应用支持能力并制定了各种前瞻性战略。Application Security、Oracle 和 Fortinet 表现非常强势，其产品的报告、实时检测和防护及用户活动审计功能仅略微弱于处于领先地位的供应商产品功能。然而，我们评估的所有产品均为成熟的数据库审计与实时防护解决方案。鉴于此，应用开发和交付专业人员不应仅局限于选择基于传统审计功能的数据库审计与实时防护产品，而应将他们的决策着眼于更加前沿的功能之上，如攻击活动实时阻止、特权用户监控、深度分析和集中资源库。

目录

备注及资源

Forrester 公司于 2010 年 10 月开展了产品评估，并与 20 家供应商和用户公司进行了访谈，以评估 Application Security、Fortinet、IBM、Imperva、Oracle 和 Sentrigo 几家公司的数据库审计和实时保护产品。

相关调研文档

“制定企业数据库安全计划”2010 年 7 月 29 日

“您的 2010 企业数据库安全战略”2009 年 9 月 28 日

“市场概况：数据库安全性” 2009 年 2 月 27 日

© 2011, Forrester Research, Inc. 保留所有权利。Forrester、Forrester Wave、RoleView、Technographics、TechRankings 和 Total Economic Impact 是 Forrester Research, Inc.的商标。所有其他商标均为其各自公司的财产。未经事先书面许可，严禁以任何形式复制或共享本文档内容。若要购买本文档的再版本，请发送电子邮件至 clientsupport@ forrester.com。有关其他复制

和使用信息，请参阅 Forrester 引用政策，网址为 www.forrester.com。信息基于最佳可用资源。意见反映当时的判断，可能随时变更，恕不另行通知。

数据库审计与实时防护采用范围不断扩大

数据库审计已经成为所有企业满足各种监管合规和安全要求的关键因素。数据库审计重点回答以下数据访问问题，如： “谁获取了信用卡号码？”；“何时有人更改客户地址？”；“更改之前的内容是什么？”；以及“采用哪种应用程序访问敏感数据？” 虽然数十年来，数据库审计的根本方法并未发生改变，但现在的工作重点发生了转变，即跨越成千上万的数据库进行更深入细致的数据审计分析和集中审计管理、综合审计报告、角色分离和实时防护。此外，审计数据库管理员和其他特权用户的需求持续提升，特别是审计员和安全组人员迫切需要明确敏感数据，以便满足《格雷姆-里奇-比利雷法案》(GLBA)、《健康保险流通及责任法案》(HIPAA)、《支付卡行业数据安全标准》(PCI DSS) 及《萨班斯-奥克斯利法案》(SOX) 等各种监管合规要求。实时阻断攻击已经成为所有组织的关键任务，尤其是因为这些攻击已逐渐变得错综复杂且难以检测。一旦黑客攻破应用程序和数据库，他只需要花费不到 20 秒钟的时间即可完成敏感信息查询和检索。由于个人用户无法检测到此类攻击，所以实时数据库防护就变得非常关键。

此次 Forrester Wave™ 评估的数据库审计与实时防护产品可帮助组织：

- **满足监管合规要求。**数据库审计是一种最佳实践，所有处理敏感数据（如信用卡号码、社会保险号码、个人身份信息 (PII)、个人健康信息 (PHI) 或任何其他公司的机密数据）的企业均应进行部署。如果您处理的任何合规要求与 PCI、HIPAA、GLBA、SOX 有关，则必须对处理敏感数据的数据库启用数据库审计。如今，大多数审计人员重点强调启动数据库审计跟踪每一项与敏感数据相关的活动。
- **保护数据库免受攻击和数据窃取的侵扰。**如今，大多数企业均在企业环境中处理数以百计的数据库，并且很多数据库均包含公司机密数据。实时手动检测可疑数据库活动和阻止数据访问实施起来非常困难。数据库审计与实时防护解决方案能够实时主动监控数据库访问、向数据库管理员 (DBA) 和安全专家发出警报，并阻止连接和会话。
- **制定更加完善的数据安全策略。**制定成功的数据安全战略过程中的一个重要环节就是数据库审计与实时防护，以及静态数据加密、数据屏蔽、授权管理和漏洞评估。[1]

©2011, Forrester Research, Inc. 禁止复制

数据库审计市场成熟而稳固

当触及安全防护时，数据库智能不足以区分用户和黑客，或确定数据本质上是否敏感。除帮助企业满足监管合规要求外，数据库审计与实时防护解决方案还能够增强数据库本身的安全性。三年前，企业纷纷开展审计并保护少数几个包含敏感数据的重要数据库。如今，随着许多组织采用提供集中式管理、角色分离、策略管理、高性能、数据发现及分类和简化管理功能的企业数据库审计与实时防护解决方案，工作重点业已转向保护整个企业成百上千的数据库。

Forrester 公司估计，数据库安全市场（包括新的许可、支持和服务）市值约 6.5 亿美元，随着越来越多的企业开始考虑采用企业级审计战略，预计到 2015 年市场将翻一番达 13 亿美元。现在，顶级的数据库审计与实时防护供应商有：Application Security、Fortinet、IBM、Imperva、Oracle 和 Sentrigo。[2] 数据库安全市场发展成熟，但多年来随着收购仍得到有效巩固，其中收购案例有： McAfee 收购 Sentrigo、Fortinet 收购 IPLocks、Netezza 收购 Tizor Systems、IBM 收购 Netezza、IBM收购 Guardium 及 Oracle 收购 Secerno。一些大型供应商甚至试图独闯数据库安全市场，但表现不佳，最终不得不叫停产品线。其中包括 Symantec Database Security 和 Quest Software InTrust 数据库产品。

企业数据库审计与实时防护市场分为以下两个主要部分：

- **本机数据库管理系统（DBMSes）提供基本的审计功能。**每款主流 DBMS 产品（包括 IBM、Ingres、MarkLogic、Microsoft、Oracle 和 Sybase 提供的产品）均提供本机审计功能，以便对访问和更改进行基本审计跟踪。尽管这些功能对于小型和不太复杂的实施非常有效，但是一旦涉及到报告、角色分离、实时防护和大型数据库支持，就显得力不从心了。Forrester 认为，DBMS 供应商在未来数年里将继续增加更先进的本机数据审计功能，以此缩小其产品与各主要第三方供应商产品之间的差距。

- **第三方供应商提供全面的审计解决方案。**如今，共有十几家厂家提供数据库审计与实时防护解决方案。这其中有几家大型供应商，如Fortinet、IBM、Oracle 等，而其他公司都是刚刚起步，如 Application Security、Imperva 和 Sentrigo。这些供应商主要提供两种类型的架构： 1) 基于网络的设备，及 2) 基于软件的设备。现在大多采用基于软件的架构类型；这些解决方案要么无代理，要么是基于代理，均从数据库共享内存、数据库日志和程序连接上读取审计信息。无论架构如何，第三方供应商解决方案均重点强调简化、角色分离、策略管理、集中管理及合规报告。

© 2011, Forrester Research, Inc. 禁止复制

数据库审计与实时防护评价概述

为了评估数据库审计与实时防护市场的状况，以及了解供应商之间如何相互较量，Forrester 对六家顶级数据库审计与实时防护供应商的优势和劣势进行了评估。

评估标准： 当前的产品、战略以及市场地位

在回顾过往研究、用户需求评估以及供应商和专家访谈之后，我们制定了一套全面的评价标准。我们采用 147 项标准对供应商进行了评估，将它们分为三个高级组别：

- **目前的产品。**为了评估产品实力，我们评估目前提供的产品标准的八个高级类别： 数据库审计、用户和应用程序审计、审计策略、审计存储库、报告和分析、实时防护、架构和可管理性。
- **战略。**我们审查了每个供应商的战略，并思考了旨在满足未来客户需求的产品定位计划改进。同时，我们还审查了可用于为公司产品提供支持的财务资源、进入市场的定价以及企业战略定位。
- **市场地位。**为了奠定产品的市场地位，我们整合了每个供应商的用户群、财务绩效、服务、员工、技术合作伙伴及国际地位相关信息。

接受评估的第三方供应商具备可靠的部署和企业级解决方案

Forrester 对六家第三方供应商进行了评估，其中包括： Application Security、Fortinet、IBM、Imperva、Oracle 和 Sentrigo。每家供应商均具有以下特点（见图 1）：

- **企业级数据库审计解决方案。**我们仅评估那些已经认识到需要加大对数据库审计需求的支持力度的第三方供应商，这些供应商特别关注能够提供本机 DBMS 审计功能以外的高性能和可扩展性、报告、策略管理及易用性。产品必须于 2010 年 8 月 15 日前上市。
- **审计过程可见性。**我们只评估那些客户在去年的 Forrester 调查中至少提及 10 次以上的第三方数据库审计与实时防护供应商。
- **可靠的客户基础。**我们评估的第三方供应商均具备 100 家以上的企业客户基础。所有接受评估的供应商都符合这一标准。

©2011, Forrester Research, Inc. 禁止复制

图 1 接受评估的供应商： 产品信息和选择标准

供应商	接受评估的产品	接受评估的产品版本	版本发布日期
Application Security	DbProtect	版本 6.1	2010 年 6 月
Fortinet	FortiDB	版本 4.1	2010 年 7 月
IBM	InfoSphere Guardium	版本 7.0	2008 年 7 月
Imperva	SecureSphere Data Security Suite	版本 8.0	2010 年 7 月
Oracle	Audit Vault	版本 10.2.3	2008 年 6 月
Sentrigo	Hedgehog Enterprise	版本 4.0	2010 年 8 月

供应商选择标准
产品提供全方位的企业级数据库审计解决方案，可帮助满足各项监管合规要求，并保护数据防止其遭到窃取，包括产品合规报告、角色分离、实时数据防护、审计跟踪存储、审计进程和步骤自动化。
产品在过去一年的调查中被 Forrester 客户提及 10 次或 10 次以上。
产品必须具有 100 家或 100 家以上的企业客户群。
产品必须于 2010 年 8 月 15 日前上市。

来源：Forrester Research, Inc.

绝大多数数据库审计供应商现在均提供全方位解决方案

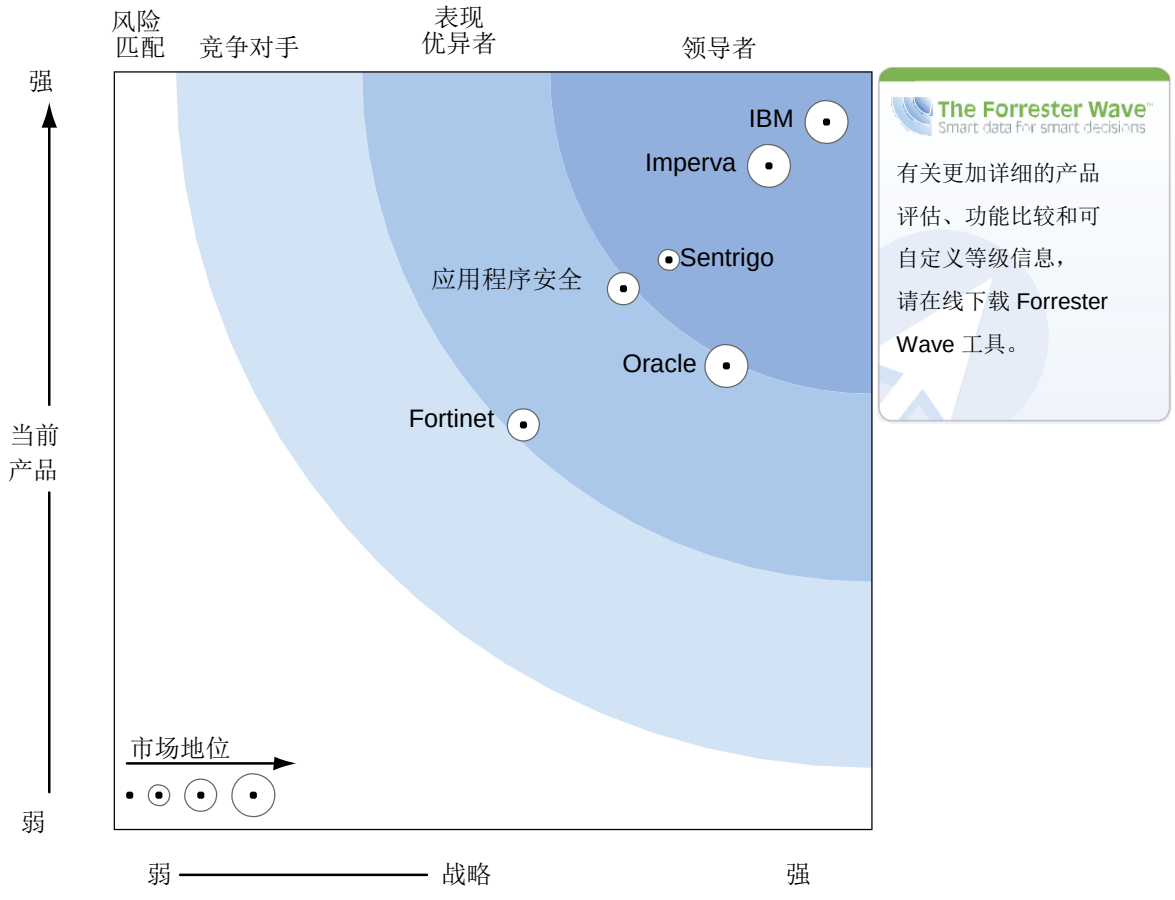
这项评估揭示了以下市场（见图二）：

- **IBM、Imperva 和 Sentrigo 处于领导地位。**这些供应商为绝大多数数据库审计特点和功能提供强大的支持，以满足所有企业审计要求。IBM InfoSphere Guardium 可支持审计和实时防护解决方案中几乎所有的功能。InfoSphere Guardium 则可为数据库访问审计、应用程序审计、策略管理、审计存储库和实时防护提供强大的支持。Imperva 的 SecureSphere Data Security Suite 可提供强大的实时防护、报告和分析、用户活动审计及策略管理功能。Sentrigo Hedgehog Enterprise 的强项在于审计策略、性能、易用性、合规报告和策略管理。
- **Application Security、Oracle 和 Fortinet 提供具有竞争力的选项。**Application Security DbProtect 表现非常出色，该厂商在多年来主要关注漏洞评估。DbProtect 在审计策略、合规报告、易用性、性能、集中存储库、用户和特权用户审计方面拥有良

好性能。Oracle 每年仍继续加大其对安全防护的重视，他们在审计保管库和数据库保管库产品方面表现优越，通过收购 Secerno 正在弥补其数据库防火墙功能的不足。Oracle 的强项在于数据审计、审计存储库和访问、通知和警报，以及用户活动和特权用户审计。2008 年收购 IPLocks 之后，Fortinet FortiDB 进入数据库安全市场。几年来 Fortinet 都做得非常好，为企业提供了低成本的解决方案，以支持所有中小规模的审计要求。

这项数据库审计与实时保护市场评估仅仅是一个开端。我们鼓励读者查看详细的产品评估，并采用该标准通过 Forrester Wave 提供的 Excel 表格供应商比较工具满足他们的独特需求。

图 2 Forrester Wave™： 数据库审计与实时防护，2011 年第二季度



来源：Forrester Research, Inc.

©2011, Forrester Research, Inc. 禁止复制

图 2 Forrester Wave™： 数据库审计与实时防护，2011 年第二季度（续）

	Forrester's Weighting	应用安全性	Fortinet	IBM	Imperva	Oracle	Sentrigo
当前产品	50%	3.57	2.67	4.67	4.38	3.06	3.76
数据库审计	10%	3.81	3.51	4.88	4.40	3.92	4.12
用户和应用程序审计	15%	3.08	2.56	4.68	4.44	2.68	3.56
审计策略	10%	3.90	3.30	5.00	4.60	3.20	4.60
审计存储库	10%	3.80	3.24	5.00	4.04	4.52	4.28
报告和分析	10%	4.46	3.44	4.76	4.64	3.40	3.56
实时防护	15%	2.70	1.10	4.80	4.80	2.20	4.20
架构	15%	3.57	3.00	4.19	4.15	3.17	2.94
可管理性	15%	3.80	2.15	4.40	4.04	2.29	3.35
战略	50%	3.36	2.70	4.70	4.32	4.04	3.66
产品策略	60%	2.80	2.50	4.50	4.40	3.40	3.30
企业战略	40%	4.20	3.00	5.00	4.20	5.00	4.20
成本	0%	0.00	0.00	0.00	0.00	0.00	0.00
市场地位	0%	3.69	3.49	4.92	4.18	4.88	2.64
用户群体	20%	3.00	2.00	5.00	5.00	5.00	2.00
收入	10%	2.60	4.00	4.20	2.40	3.80	2.60
服务	20%	3.60	5.00	5.00	2.90	5.00	2.20
员工	20%	4.05	4.25	5.00	4.30	5.00	2.40
技术合作伙伴	20%	5.00	1.70	5.00	5.00	5.00	3.68
国际地位	10%	3.00	5.00	5.00	5.00	5.00	3.20

所有评分都是基于 0（弱）到 5（强）的标准进行。

来源：Forrester Research, Inc.

供应商资料

领导者： IBM、Imperva 和 Sentrigo

- **IBM 收购 Guardium 有助于其进入领导者行列。**IBM 在 2007 年第四季度 Forrester Wave 关于数据库审计和实时防护市场的评估中表现出色，其中我们对 IBM Consul InSight 和 IBM DB2 Audit Management Expert (AME)进行了评估。然而，IBM 在 2009 年收购 Guardium 后使局面完全改变，使得 IBM 在该市场领域中迈进了领导者的行列。IBM InfoSphere Guardium 展现着在支持超大型异构环境方面的领导地位，持续实现高性能和可扩展性、简化管理，并进行实时数据库防护。IBM 一如既往地注重创新和延伸 Guardium 产品，

© 2011, Forrester Research, Inc. 禁止复制

以便与 InfoSphere Discovery 和 InfoSphere Optim 等其他 IBM 产品集成。如今，IBM InfoSphere Guardium 已在许多大型企业和数百个任务关键型数据库中成功部署。此外，IBM 还提供全面的专业服务，以此为拥有复杂环境的客户以及在执行企业数据库安全方面需要协助的客户提供帮助。

- **Imperva 紧跟 IBM 之后。**Imperva 多年来表现一直非常出色，尽管如今还有几个更大的巨头与之竞争，如 Fortinet、IBM 和 Oracle。Imperva 作为领导者具备和可扩展的高性能数据库审计解决方案，因此在我们评估的很多方面都获得了高分。Imperva 在审计和合规报告、事务和查询审计、实时发现、用户级别和特权用户审计、策略定义、合规策略、通知和警报以及实时保护方面均可提供强大的支持。Imperva 还拥有强大的产品和企业战略，其强劲的市场地位在未来几年中将助其进一步强化发展。Imperva 是在数据库审计领域持续保持着最强劲发展势头的厂商之一。除数据库安全外，Imperva 也提供 Web 应用程序和文件安全解决方案。Forrester 认为，Imperva 在未来几年中很有可能成为大型安全供应商的收购目标。

- **Sentrigo 表现非常优异，在领导者群体占据一席之地。**在该 Forrester Wave 发布的不久前，McAfee 收购了 Sentrigo。Sentrigo Hedgehog Enterprise 产品现更名为 McAfee Database Activity Monitoring，而 Sentrigo Hedgehog DBscanner 产品现更名为 McAfee Vulnerability Manager for Databases。Sentrigo 成立于 2006 年，公司提供多种数据库安全解决方案，包括数据库审计、漏洞评估、数据发现、虚拟修补程序及实时防护。Sentrigo 在审计策略、易用性、实时攻击检测、端到端分析及合规报告方面取得了非常好的成绩。Sentrigo 还具有强大的产品远景、承诺及合作伙伴。虽然 Sentrigo 没有像 IBM 和 Imperva 那样多的客户群体，但也有一些非常大的财富1000 强企业采用其产品为数百个关键数据库提供支持。

表现优异者： Application Security、Oracle 和 Fortinet

- **Application Security 依托极具吸引力的价格提供可行性审计解决方案。**Application Security 成立于10多年前，在数据库漏洞评估领域处于领先地位，并且继续在延伸其 DbProtect 产品，以支持数据库审计和实时防护。然而，Application Security 近年来面临 IBM、Imperva 和 Oracle 等众多厂家的激烈竞争。Application Security 在我们的全面评估中表现抢眼，是不折不扣的佼佼者。它在用户活动监控、合规报告、深度分析、实时攻击检测和性能方面取得了非常高的分数。

- **Oracle 提供超越审计范围的全方位数据库安全解决方案。**Oracle 是提供最全面数据库安全解决方案的厂家；Oracle 解决方案包括数据库审计、数据屏蔽、漏洞评估、数据发现、标签安全性、静态数据加密、授权管理及补丁管理。Oracle 在我们的评估中表现良好，并且持续致力于提供安全解决方案。此外，Oracle 是唯一一家在数据库级

©2011, Forrester Research, Inc. 禁止复制

别为 DBA 上的敏感数据提供保护解决方案的厂商（Oracle Database Vault 产品）。Oracle 最近发布了其数据库防火墙产品，可提供实时防护、强大的用户和审计访问功能；该产品是 Oracle Audit Vault 和 Database Vault 产品线的一个很好补充。由于我们的生产评估截止日期定为 2010 年 8 月 15 日，所以我们没有对 Oracle 数据库防火墙产品进行评估。

- **Fortinet 公司以低成本提供可行的数据库安全解决方案。**Fortinet 于 2008 年收购了 IPLocks，从而进入了数据库安全市场。总体而言，Fortinet 自收购以后表现良好，现在 Fortinet 已经拥有 100 多位客户，其中一半以上是全球财富500 强公司。虽然 Fortinet 公司核心焦点是网络安全设备和统一威胁管理 (UTM)，但同时也依然保持对数据库安全的高度重视。Fortinet 的强大功能在于其将本机数据库安全、报告、主动报警、自定义策略、用户级别及事务级审计融为一体。随着各供应商地位的进一步巩固，Fortinet 很可能面临激烈的竞争。Fortinet 需要坚持专注和创新，以保持其竞争力。

补充材料在线资源

图 2 的在线版本是基于 Excel 的供应商比较工具，可提供详细的产品评估和可自定义排名。

本 Forrester Wave 使用的数据源

Forrester 结合使用两大数据源评估每项解决方案的优势和劣势：

- **产品演示。**我们 要求各供应商对其产品功能进行演示。我们利用这些产品演示结果验证每个供应商产品功能细节。
- **客户咨询呼叫。**为了验证产品和供应商资格，Forrester 还要求与每位供应商的两名当前客户进行咨询访谈。

Forrester Wave 调查方法

我们进行初步研究以制定满足我们的标准的供应商清单，以便在市场中进行评估。随后，我们从初步圈定的供应商中缩小范围确定最终名单。我们基于以下标准选择这些供应商： 1) 产品适合度；2) 客户成功案例；以及 3) Forrester 客户需求。排除客户参考有限的供应商，以及不符合我们的评估范围的产品。

在考察以往的研究、用户需求评估及供应商和专家评审后，我们确立最初的评估标准。为了依据我们的这套标准评估各供应商及其产品，我们会通过采用实验室评估、问卷调查、演示

© 2011, Forrester Research, Inc. 禁止复制

和/或客户讨论相结合的方式，收集产品资格详细信息。我们会将评估结果发给供应商供其审核，并会相应调整评估结果，以便对供应商产品和战略进行最准确的评价。

我们会设置默认权重体现我们对大型用户企业需求的分析结果和/或 Forrester Wave 文档中列举的其他方案，然后根据明确界定的标准对各供应商进行打分。这些默认权重仅作为起点使用，我们鼓励读者通过基于 Excel 的工具采用适应其各自需求的权重进行评估。最终得分将会根据当前产品、战略和市场地位生成图表，描述实际市场状况。Forrester 将会随着产品功能和供应商战略的演进定期更新供应商评估结果。

尾注

1 有关制定全方位数据库安全战略的更多研究，请参阅“您的企业数据库安全战略”报告（2009 年 9 月 28 日）。

2 在本期 Forrester Wave 发布之时，McAfee 收购了 Sentrigo。

©2011, Forrester Research, Inc. 禁止复制

FORRESTER®

让领先公司每天都获得成功

总部

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139
USA 电话： +1 617.613.6000
传真： +1 617.613.5000
电子邮件：forrester@forrester.com 纳斯达克代号：FORR
www.forrester.com

调研和销售处

Forrester 在全球超过 27 个城市设有研究中心和销售办事处，包括阿姆斯特丹、马萨诸塞州剑桥、达拉斯、迪拜、加利福尼亚福斯特城、法兰克福、伦敦、马德里、悉尼、特拉维夫和多伦多。

要获得全球办公地点的完整列表，请访问 www.forrester.com/about。

有关打印件或电子重印的信息，请通过以下方式联系客户支持：致电 +1 866.367.7378、+1 617.613.5730 或发送电子邮件至 clientsupport@forrester.com。我们将会向学术机构和非营利性机构提供数量折扣和优惠价格。

Forrester Research, Inc. (纳斯达克： FORR）是一家为全球业务和技术领先企业提供实用性和前瞻性建议的独立研究公司。Forrester 与大型企业中 19 个关键角色的专业人员合作，提供专利研究、客户洞察、咨询、活动以及点对点的执行方案。超过 27 年来，Forrester 一直在为 IT、市场营销和技术行业的领袖们带来成功的每一天。如需更多信息，请访问 www.forrester.com 。