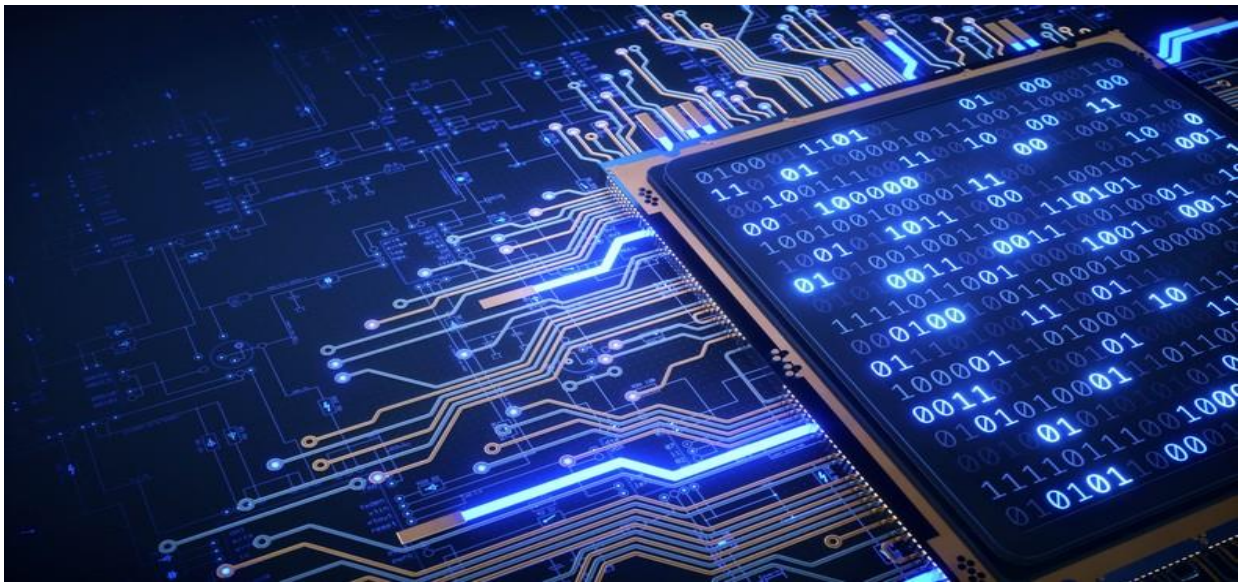


Ponemon 调研报告：关于借助 IBM Security Guardium 实现数据保护的客户洞察

赞助方：IBM

由 Ponemon Institute LLC 独立进行

发布日期：2019 年 8 月

Ponemon 调研报告：关于借助 IBM Security Guardium 实现数据保护的客户洞察

Ponemon Institute，2019 年 8 月.

第 1 部分：引言

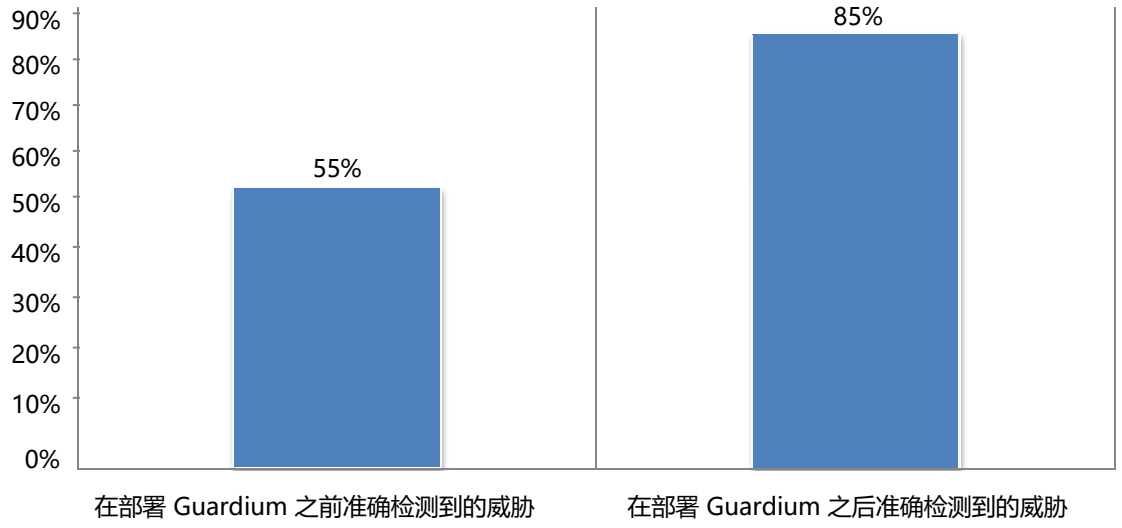
Ponemon Institute 将在本报告中公布由 IBM 赞助的 *Guardium Data Protection 解决方案客户调研*的结果。此次调研的目的是了解用户如何通过部署 Guardium 的数据保护平台来改善其组织的安全态势。通过此次调研得出的重要一点是：Guardium 的用户认为成功部署 Guardium 可降低发生数据泄露的可能性。

我们对来自使用 Guardium 监控和保护公司数据和数据库的组织中的 183 位美国 IT 和 IT 安全从业人员进行了调研。平均而言，本次调研中出现的组织使用 Guardium 保护其数据资产的时间都在三年以上。

如图 1 所示，Guardium 已帮助受访组织将检测威胁的准确率平均提高了 43%。具体而言，在部署 Guardium 之前，平均可以准确检测 55% 的威胁。部署 Guardium 之后，可以准确检测 85% 的威胁。

图 1. 在部署 Guardium 之前和之后准确检测威胁的能力对比

外推值



以下所述为此次调研的关键调研结果。

Guardium 与 SIEM 集成良好。44% 的用户已将 Guardium 与他们的 SIEM 解决方案相集成，而 63% 的用户认为这种集成对于改善威胁检测和分析而言极具价值。

组织具有更好的可视性来确定漏洞敞口。受访者认为 Guardium 的开箱即用型发现和分类模式，以及结构化/非结构化数据资产的发现和分析功能很有价值，持如此观点的受访者比例分别为 72% 和 68%。

组织能够简化威胁分析并避免可互操作性方面的问题。67% 的受访者表示有一个可用于分析数据资产威胁的 GUI 是 Guardium 最有价值的功能，而有 64% 的受访者表示确保与其他安全解决方案的异构可互操作性是 Guardium 最有价值的功能。

Guardium 能够提升跨复杂 IT 环境及在整个企业范围内管理数据风险的能力。86% 的受访者表示，使用 Guardium 跨复杂 IT 环境（如多云或混合云生态系统）管理数据风险的能力极具价值。同样，机器学习和自动化在管理整个企业范围内的数据风险方面也具有显著优势。

Guardium 的合规性快速入门 (Compliance Quick Starts) 功能可帮助组织确保与欧盟《通用数据保护条例》 (GDPR) 等法规的合规性。45% 的受访者表示其所在组织使用了合规性快速入门功能，而 81% 的受访者表示该功能极具价值。

受访者表示在识别和修复数据安全问题上所花费的时间更少。尽管只有 33% 的受访者表示他们能够减少与数据保护和合规性活动相关的人员数量，但 Guardium 确实提升了 IT 安全团队的效率。在部署 Guardium 之前，IT 安全团队在识别和修复数据安全问题上平均需要花费其 61% 的时间，而在部署之后，平均花费的时间大幅减少，在其总时间中所占的比例只有 40%。59% 的受访者表示，平均而言，部署 Guardium 使他们可以替换掉 6 个单点解决方案。

漏洞或误配置的检测和修复及数据的准确分类均得到了改善。在部署了 Guardium 之后，每年得以检测和修复的数据源漏洞或误配置平均所占的百分比从 30% 增加到 60%。类似地，得以准确分类的数据平均所占的百分比也从 49% 上升到 82%。

第 2 部分：重要调查结果

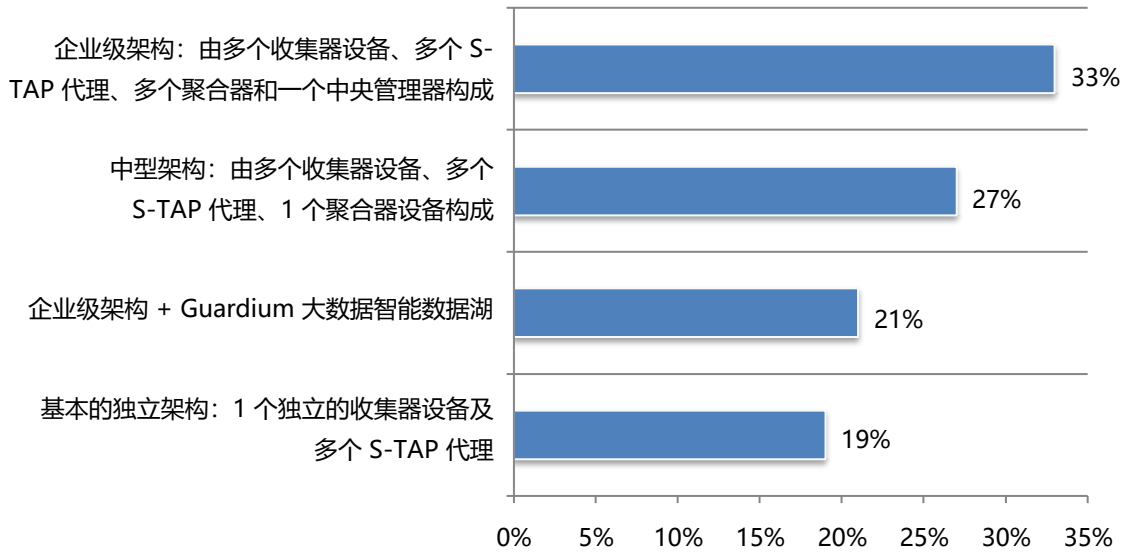
在本节中，我们针对重要调查结果进行了更深入的分析。有关经审计的完整调查结果，参见本报告的附录。此次调研涵盖了以下主题：

- 企业部署 Guardium 的方式
- 优势和价值
- 受访者对部署后运营收益的看法

企业部署 Guardium 的方式

在许多情况下，Guardium 的部署与组织的企业级架构最匹配。我们要求受访者选择与其 Guardium 的部署最匹配的架构。如图 2 所示，33% 的受访者表示与 Guardium 的部署最匹配的是他们的企业级架构（由多个收集器设备、多个 S-TAP 代理、多个聚合器和一个中央管理器构成），其次是中型架构（由多个收集器设备、多个 S-TAP 代理、1 个聚合器设备构成）。

图 2. 哪种架构与贵组织最匹配?

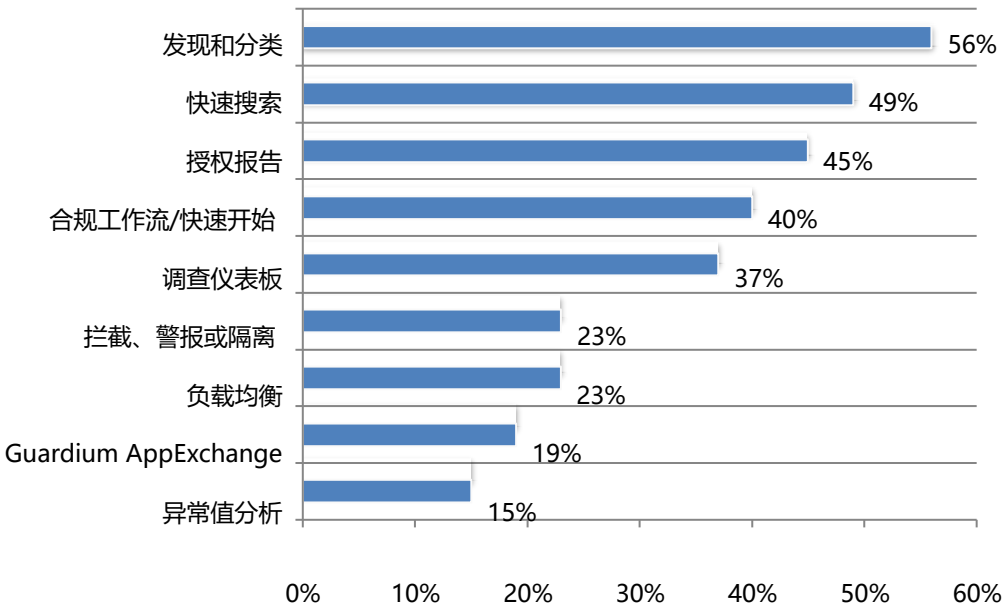


最常用的 Guardium 功能是其发现和分类功能。如图 3 所示，56% 的受访者表示他们使用了发现和分类功能，其次是快速搜索功能（占受访者的 49%）和授权报告功能（占受访者的 45%）。

平均而言，受访组织监控的人员数量占其总人数的 40%。Guardium 的许可证平均允许 342 个单独的数据库和/或数据仓库。

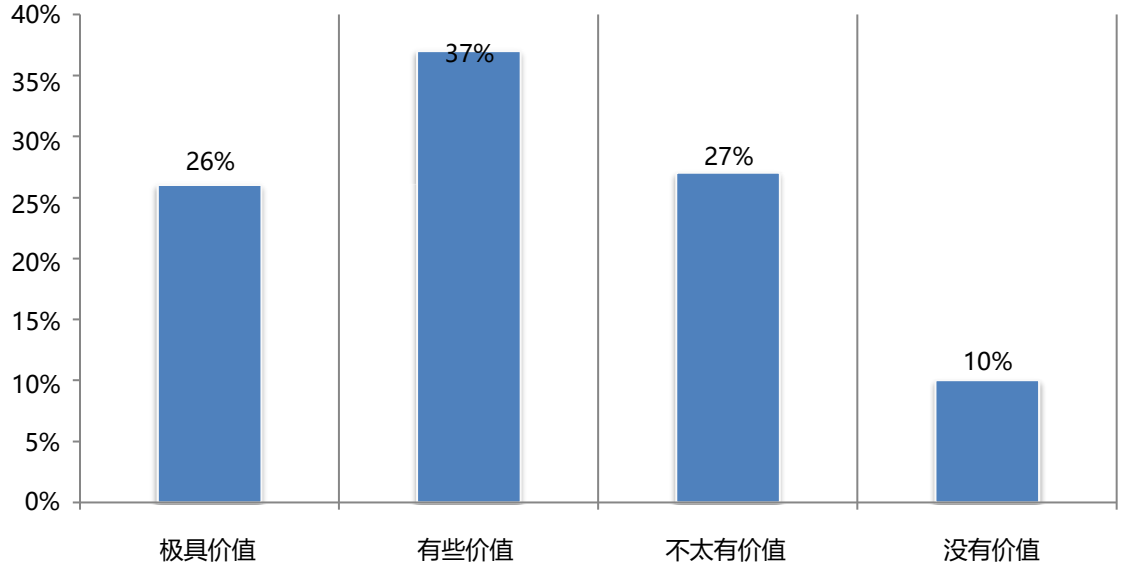
图 3. 贵组织使用了 Guardium 提供的哪些数据保护功能?

允许多选



Guardium 与 SIEM 解决方案的集成被认为具有价值。44% 的受访者表示 Guardium 已与其 SIEM 相集成。如图 4 所示，63% 的受访者肯定此集成的价值，其中 26% 的受访者表示集成极具价值，37% 的受访者表示集成有些价值。

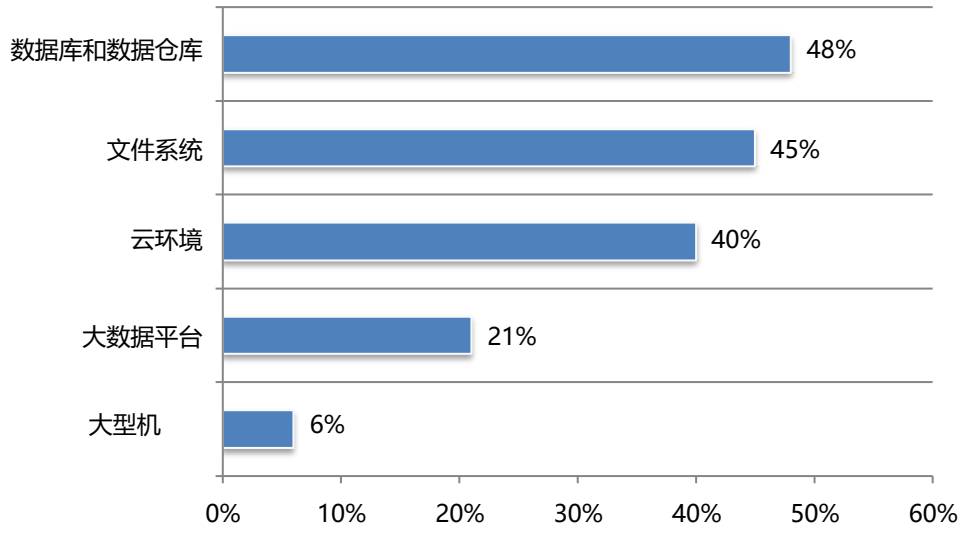
图 4. Guardium 与贵组织 SIEM 的集成的价值如何?



Guardium 的大多数数据安全平台都部署在数据库和数据仓库中。如图 5 所示，近一半（48% 的受访者）表示 Guardium 的数据安全平台部署在他们的数据库和数据仓库中，其次是部署在文件系统（45% 的受访者）和云环境（40% 的受访者）中。

图 5. Guardium 的数据安全平台部署在贵组织数据存储库中的哪个位置?

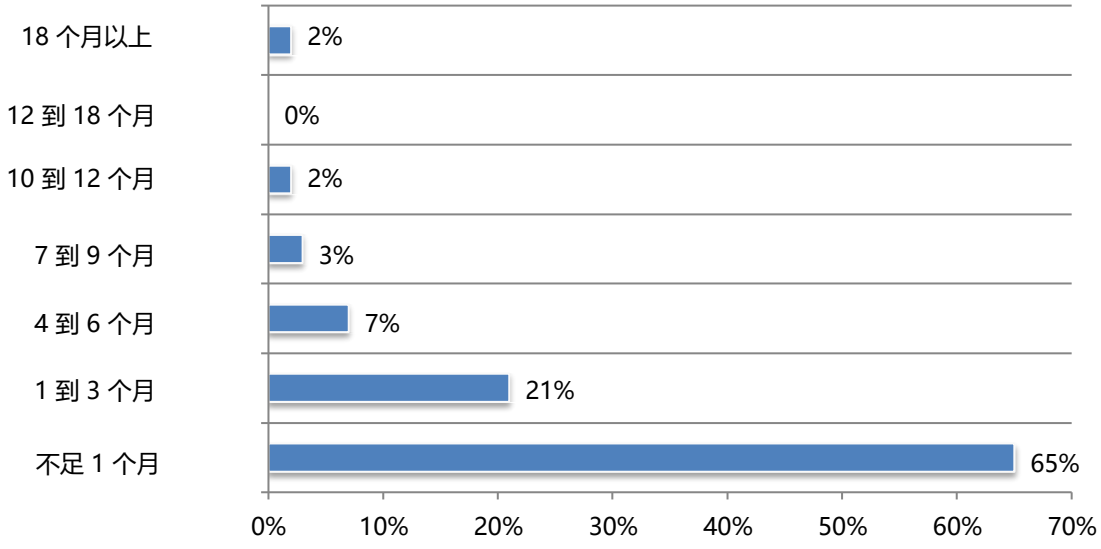
允许多选



Guardium 的优势和价值

组织正在快速从 Guardium 的部署中实现价值。如图 6 所示，大多数组织在部署 Guardium 后不到一个月的时间内就从中实现了价值。

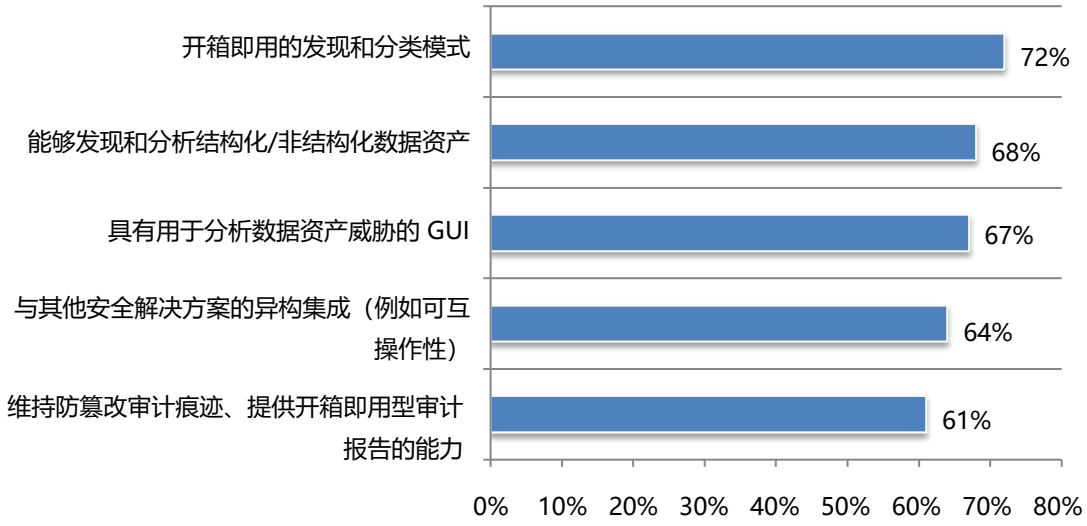
图 6. 贵组织在部署 Guardium 后多长时间从中实现了价值?



Guardium 有助于降低由于不了解组织的非结构化数据而造成的风险。我们要求受访者对 Guardium 产品功能的价值进行评分，评分范围为 1 分（= 没有价值）到 10 分（= 极具价值）。图 7 展示了表示产品功能具有高价值的回复（10 分制得分在 7 分以上）。受访者认为开箱即用型发现和分类模式，以及结构化/非结构化数据资产的发现和分析功能很有价值，持如此观点的受访者比例分别为 72% 和 68%。

图 7. Guardium 的产品功能在功能性方面的价值

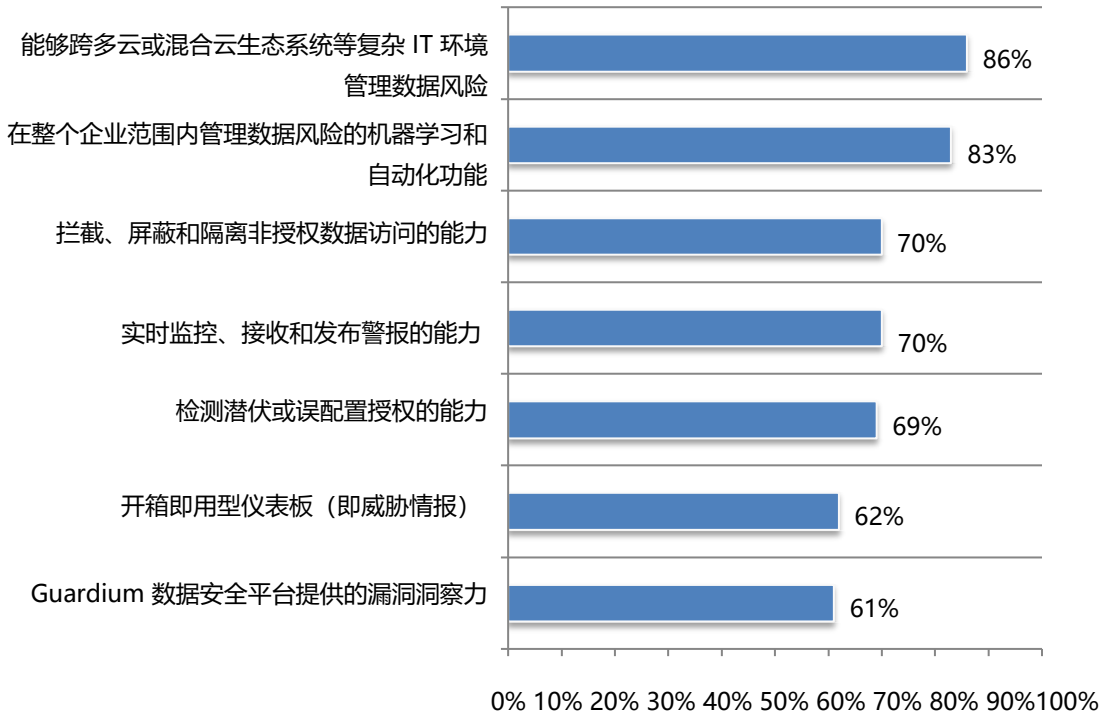
1 分（= 完全没有价值）到 10 分（= 极具价值），展示 7 分以上的受访者回复



最具价值的功能是跨复杂 IT 环境及在整个企业范围内管理数据风险的能力。如图 8 所示，有 86% 的受访者提及了跨各种复杂的 IT 环境（如多云环境或混合云生态系统）管理数据风险的能力。针对此类受访者，我们要求他们对安全相关功能的价值进行了评估。

图 8. Guardium 的产品功能在安全性方面的价值

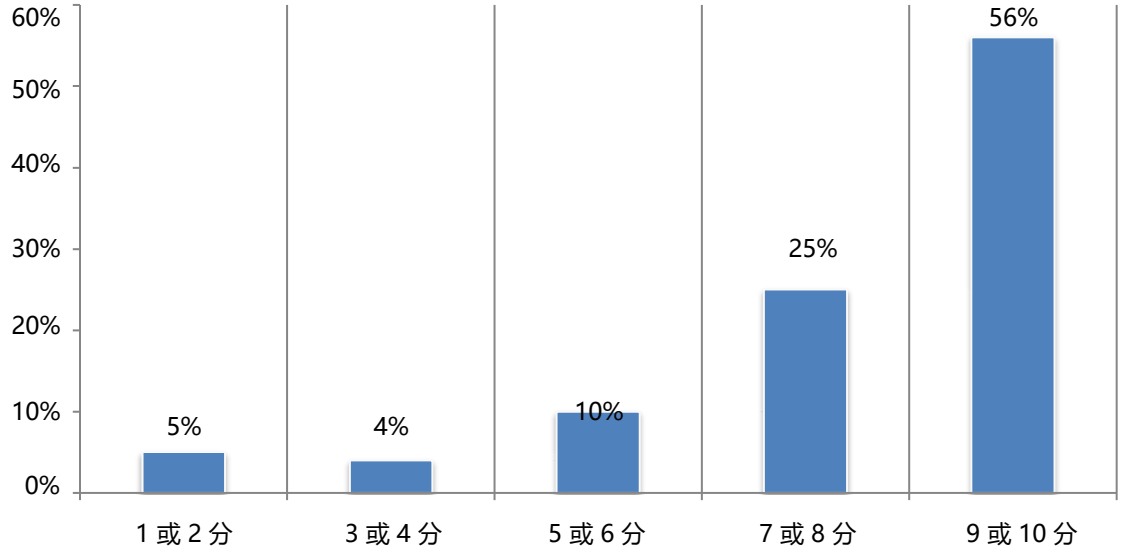
1 分（= 完全没有价值）到 10 分（= 极具价值），展示 7 分以上的受访者回复



Guardium 的合规快速入门功能被认为很有价值。组织发现他们很难确保与新法规（例如 GDPR 和《加州消费者隐私法》）的合规性。45% 的受访者表示其所在组织使用了合规性快速入门功能；如图 9 所示，81% 的受访者表示该功能极具价值（10 分制得分在 7 分以上）。

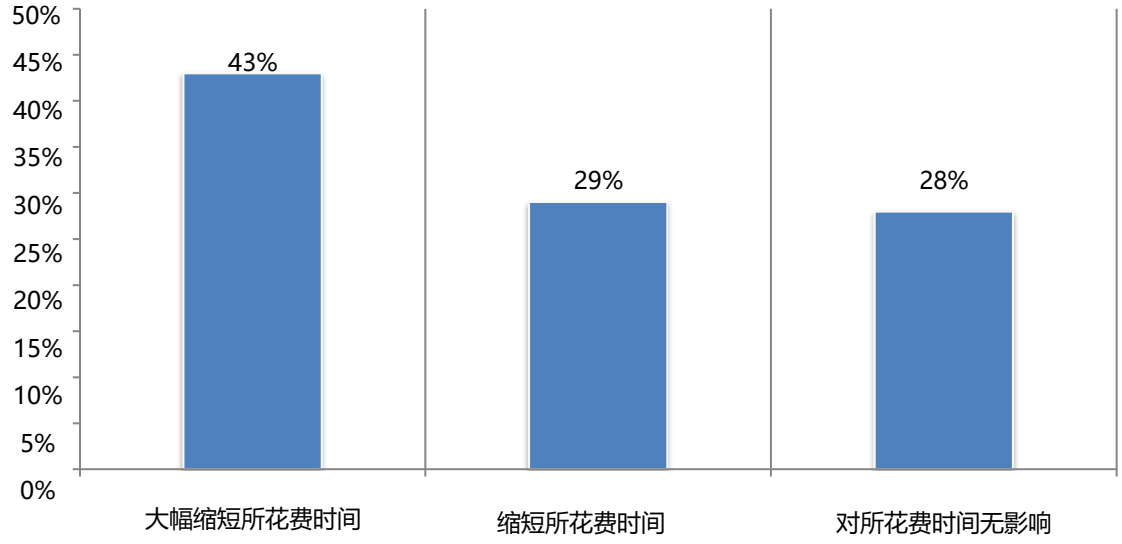
图 9. 您认为 Guardium 的合规性快速入门功能具有多大价值?

1 分（= 完全没有价值）到 10 分（= 极具价值），展示 7 分以上的受访者回复



如图 10 所示，72% 的受访者表示缩短了在合规性方面花费的时间，表示时间大幅缩短的受访者比例为 43%，表示时间有所缩短的受访者比例为 29%。

图 10. 它对合规活动所花费的时间有何影响?

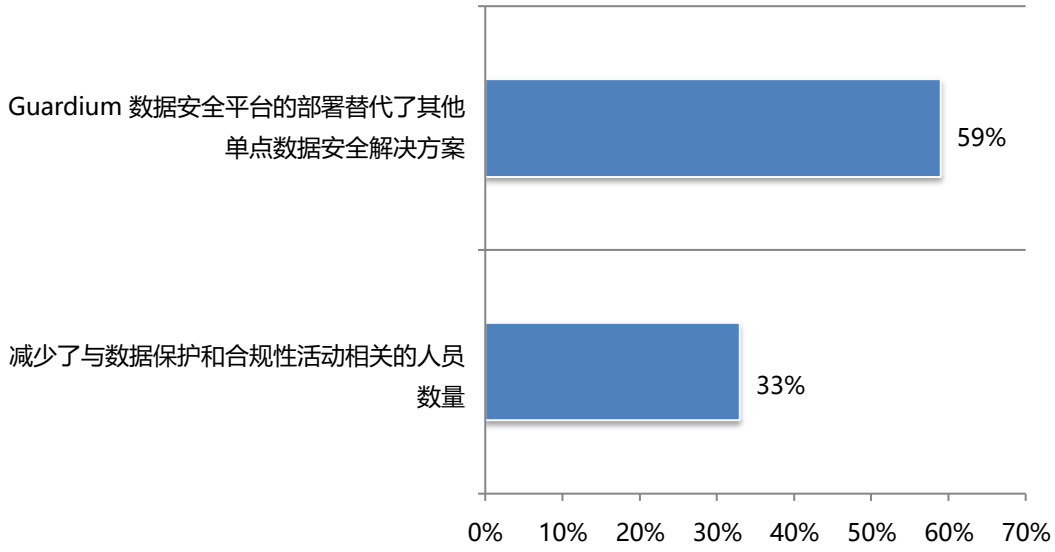


受访者对部署后运营收益的看法

Guardium 的数据安全平台减少了单点解决方案的数量，但并未减少人员数量。如图 11 所示，只有三分之一的受访者表示，Guardium 的数据安全平台有助于减少与数据保护和合规性活动相关的人员数量。不过有 59% 的受访者表示，它可以替代其他单点数据安全解决方案。平均而言，组织能够替换掉 6 个单点解决方案。

图 11. 减少人员和单点数据安全解决方案数量的能力

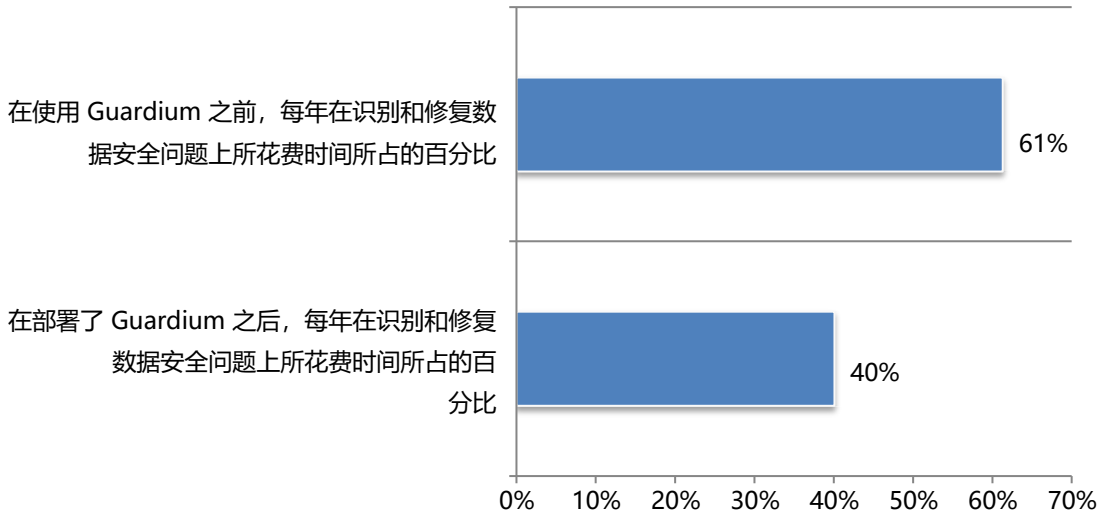
回答“是”的受访者回复



Guardium 帮助受访组织减少了每年在识别和修复数据安全问题上所花费的时间。如上所述，只有 33% 的受访者表示其组织在部署了 Guardium 之后能够减少相关人员的数量。但是，它确实提升了 IT 安全团队的效率。如图 12 所示，在使用 Guardium 之前，IT 安全团队平均每年需要在识别和修复数据安全问题方面花费其 61% 的时间。在部署了 Guardium 之后，用于此类活动的平均时间百分比为 40%。所花费的时间减少了 42%。

图 12. 每年在识别和修复数据安全问题上所花费的时间所占百分比

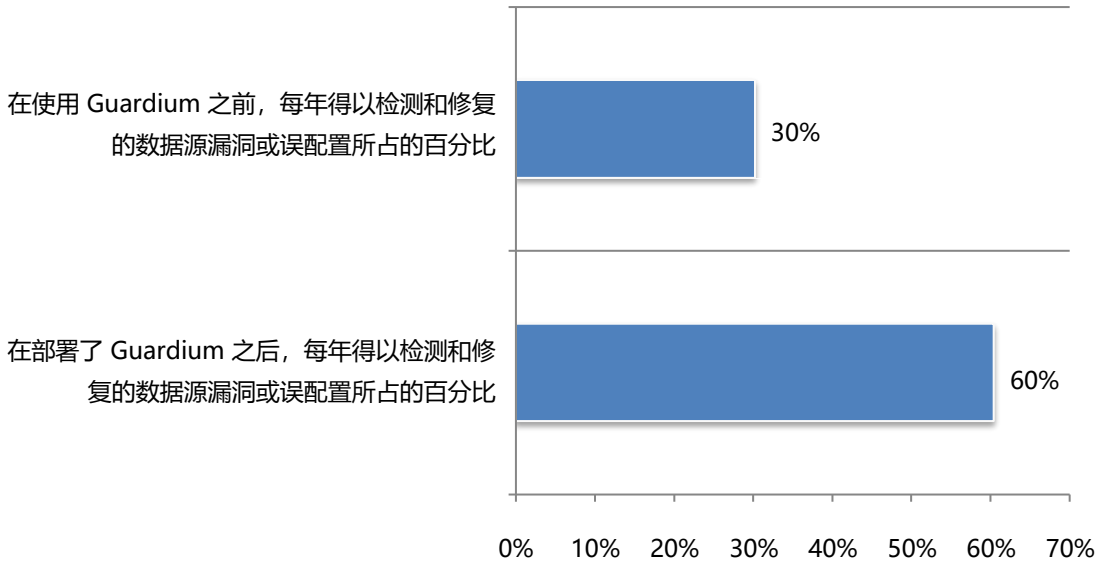
外推值



Guardium 帮助组织提高了检测和修复数据源漏洞或误配置的能力。如图 13 所示，每年平均可检测和修复 30% 的数据源漏洞或误配置。在部署 Guardium 之后，每年平均可检测到 60% 的此类漏洞或误配置。这一比例增加了 67%。

图 13. 部署前后检测到的数据源漏洞或误配置所占的百分比

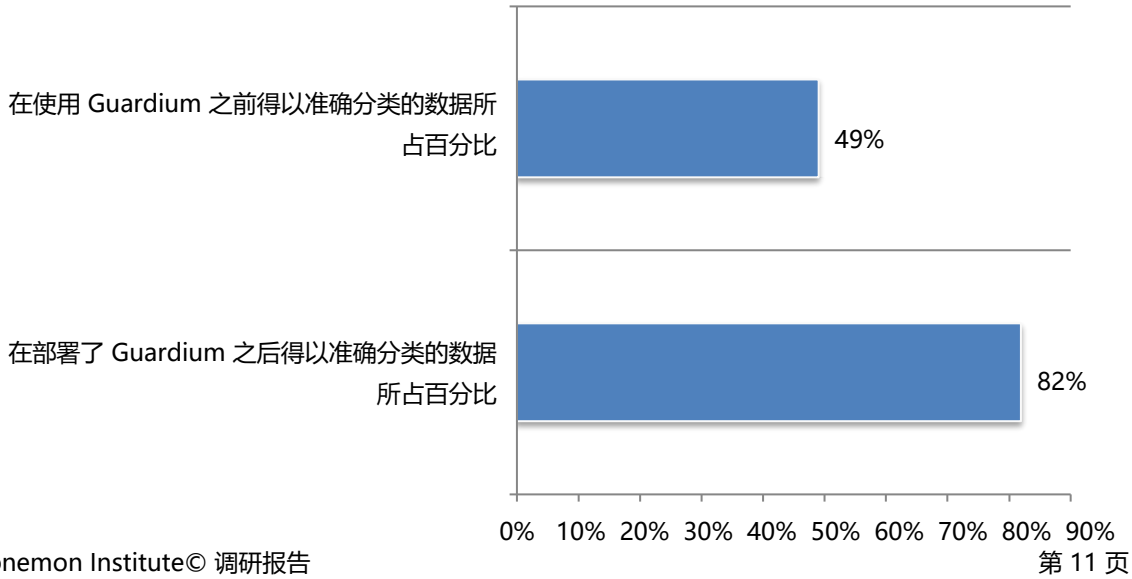
外推值



Guardium 可以提高得以准确分类的数据所占的百分比。如图 14 所示，在部署之前，平均不到一半 (49%) 的数据可以得到准确分类。在部署了 Guardium 之后，82% 的数据可以得到准确分类。这一比例增加了 50%。

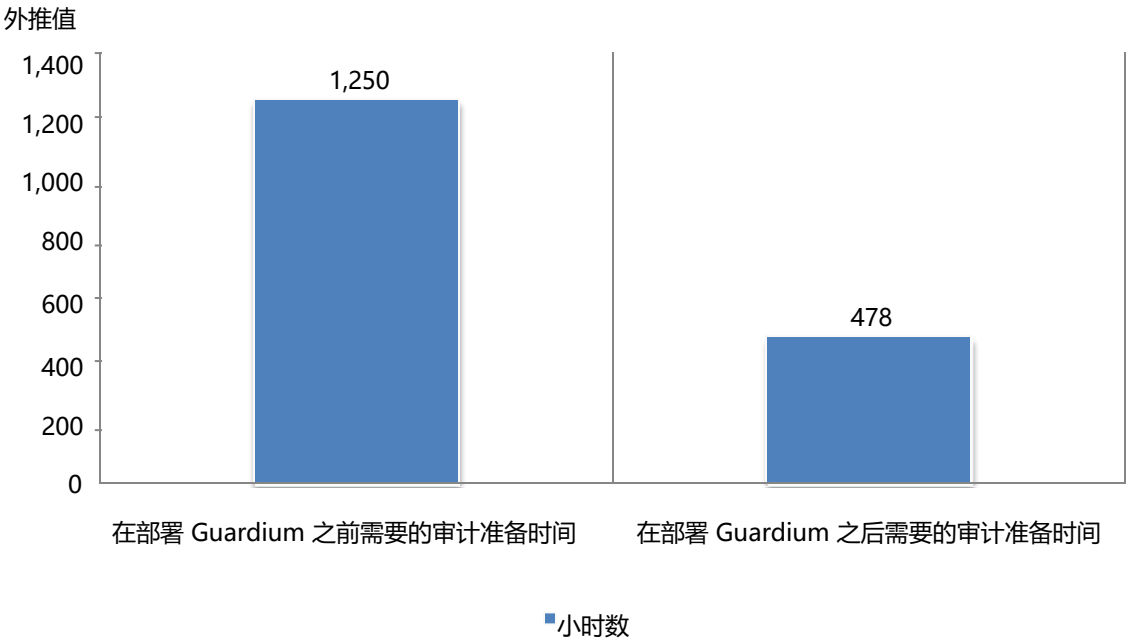
图 14. 得以准确分类的数据所占的百分比

外推值



准备审计所需的时间更少。如图 15 所示，准备审计所需的时间平均减少了 89% - 从 1,250 小时减少到 478 小时。

图 15. 部署前后需要多长时间来准备审计?



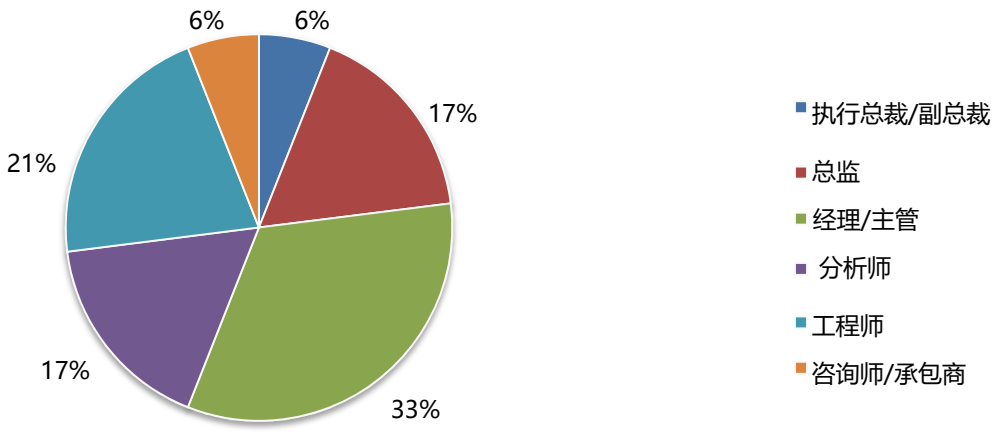
第 3 部分：方法

美国的取样范围由 18,577 位 IT 和 IT 安全从业人员组成，这些从业人员均来自使用 Guardium Intelligence 监控和保护其公司网络的组织。如表 1 所示，有 201 位受访者完成了调研，其中有 18 位受访者的回复因可靠性问题而被拒绝。最终样本由 183 位受访者组成，回复率为 1.0%。

表 1. 样本响应	频率	%
总取样范围	18,577	100.0%
总返回数量	201	1.1%
被拒或被剔除的调研数量	18 次	0.1%
最终样本数量	183	1.0%

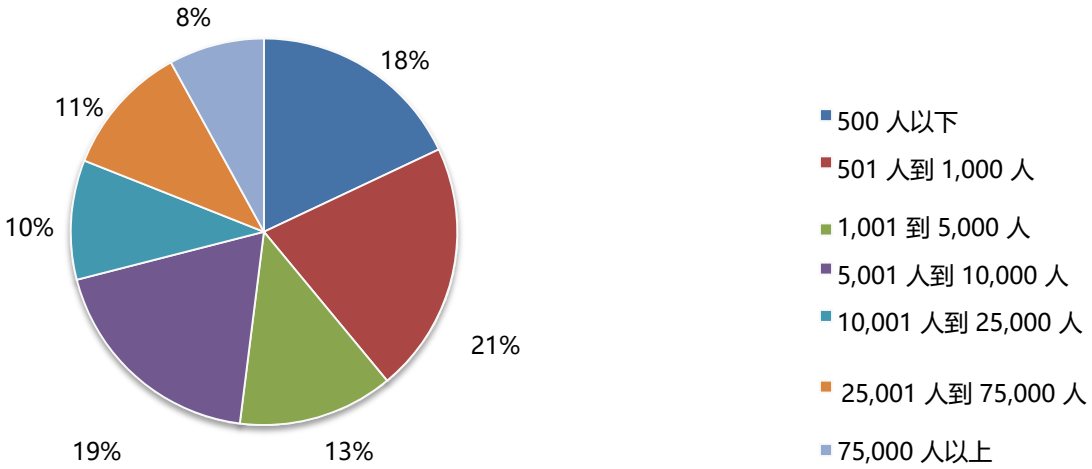
饼分图 1 显示了受访者当前所处的职位或组织级别。超过一半 (56%) 的受访者表示他们目前担任主管或更高级别的职位，而 21% 的受访者表示他们目前担任工程师的职位。

饼分图 1. 当前职位或组织级别



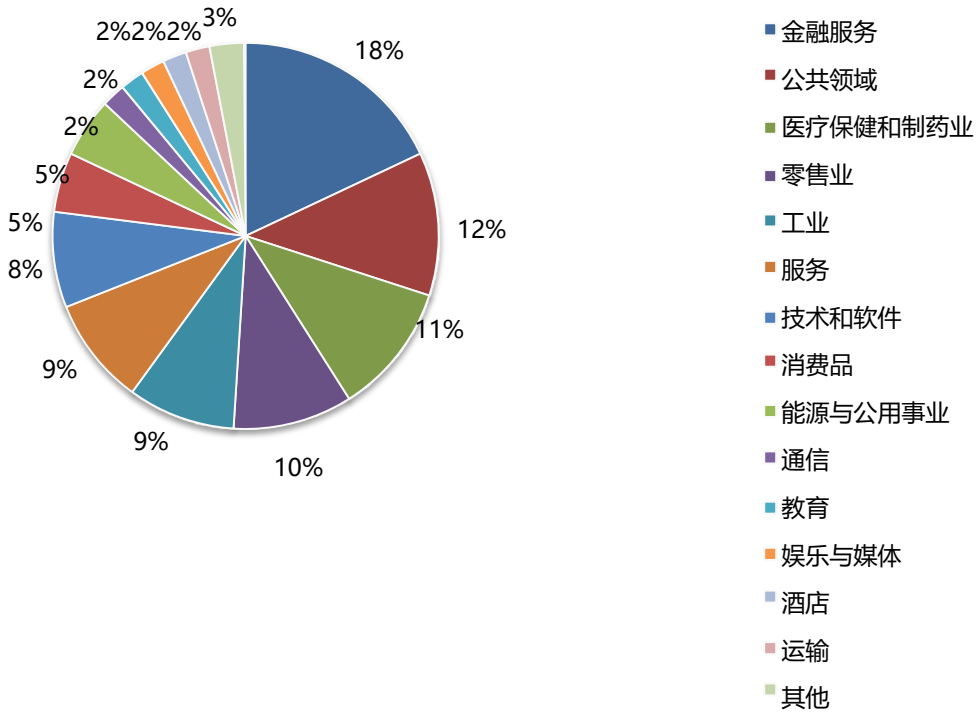
如饼分图 2 所示，61% 的受访者来自全球员工数超过 1,000 人的组织。

饼分图 2. 全球组织的全职员工数量



饼分图 3 显示了受访者所在组织的主要行业分类。从此图中可以看出，金融服务占比最大 (18%)，该行业涵盖了银行、投资管理、保险、经纪、支付、信用卡等领域；之后分别是公共领域（占受访者的 12%）、医疗保健与制药（占受访者的 11%）、零售（占受访者的 10%）、工业（占受访者的 9%）和服务（占受访者的 9%）。

饼分图 3. 主要行业分类



第 4 部分：注意事项

此调研中存在一些固有的限制事项，在根据调研结果作出结论之前，需要对这些事项加以审慎考虑。以下各项是与大多数基于 Web 的调研密切相关的特定限制事项。

无回复偏差：当前的调研结果基于一些调查结果样本。在调研中，我们将调查问卷发给具有代表性的个人样本，最终收到了大量可用的回复。尽管进行了无响应测试，但仍旧可能出现这样的情况，即：没有参与调研的个人的基本信念可能会与完成了调研的个人截然不同。

取样范围偏差：准确性基于联系信息以及受访者列表代表 IT 或 IT 安全从业人员（来自使用 Guardium Intelligence 监控和保护其公司网络的组织）的程度。我们也承认，结果可能会受到诸如媒体报道等外部事件的影响。我们也承认由于补偿主体在指定时间段内完成此次调研引起的偏差。

自报告结果：调研的质量高低取决于受访者是否给出完整、可信的回复。尽管我们可在调研过程中加入特定的制衡原则，但始终存在一种可能，即调研主体未给出准确的回答。

附录：详细调查结果

以下表格显示了此次调研中所有问题的响应频率或响应频率百分比。所有的调研响应结果于 2019 年 4 月收集。

调研响应结果	频率	%
总取样范围	18,577	100.0%
总返回数量	201	1.1%
被拒的调研数量	18	0.1%
最终样本（Guardium 用户）	183	1.0%

第 1 部分：背景

Q1. 贵组织已使用 Guardium 来保护数据资产多久的时间?	%
不足 1 年	15%
1 到 2 年	19%
3 到 4 年	35%
5 到 6 年	25%
6 年以上	6%
总计	100%
外推值	3.38

Q2. 贵组织使用哪个版本的 Guardium?	%
V9 或更早版本	9%
V10.0	12%
V10.3	16%
V10.4	23%
V10.5	23%
V10.6	17%
总计	100%

Q3. 贵组织是否使用了除 Guardium Data Protection 以外的其他 Guardium 产品?	%
Guardium Vulnerability Assessment	30%
Multi-cloud Data Encryption	27%
Guardium Data Encryption	38%
Security Key Lifecycle Manager	25%
Guardium Big Data Intelligence	21%
Data Risk Manager	16%
Guardium Analyzer	36%
总计	193%

Q4. 贵组织中 Guardium 部署的发起者是谁?	%
IT	40%
IT 安全团队	37%
数据库团队	12%
风险与合规团队	10%
其他（请注明）	1%
总计	100%

Q5. 您所监控的总人数所占百分比是多少?	%
不足 5%	4%
5% 到 10%	18%
11% 到 20%	20%
21% 到 50%	21%
51% 到 75%	19%
75% 到 90%	7%
90% 到 100%	11%
总计	100%
外推值	40%

Q6. 贵组织的 Guardium 许可证允许多少个单独的数据库和/或数据仓库使用?	%
10 个以下	4%
10 到 50 个	15%
51 到 100 个	29%
101 到 500 个	26%
501 到 1,000 个	14%
1,000 个以上	12%
总计	100%
外推值	341.5

Q7. 请选择与贵组织的 Guardium 部署最匹配的架构。	%
基本的独立架构：1 个独立的收集器设备及多个 S-TAP 代理	19%
中型架构：由多个收集器设备、多个 S-TAP 代理、1 个聚合器设备构成	27%
企业级架构：由多个收集器设备、多个 S-TAP 代理、多个聚合器和一个中央管理器构成	33%
企业级架构 + Guardium 大数据智能数据湖	21%
总计	100%

Q8. 贵组织使用 Guardium 哪些数据保护功能？请选择所有的适用项。	%
发现和分类	56%
授权报告	45%
合规工作流/快速开始	40%
调查仪表板	37%
负载均衡	23%
异常值分析	15%
快速搜索	49%
拦截、警报或隔离	23%
Guardium AppExchange	19%
总计	307%

Q9a. 贵组织是否将 Guardium 与 SIEM 解决方案相集成?	%
是	44%
否	56%
总计	100%

Q9b. 如果是，您认为这种集成具有多大价值?	%
极具价值	26%
有些价值	37%
不太有价值	27%
无价值	10%
总计	100%

Q10. 您是否是以续期的方式购买 Guardium?	%
是	49%
否	51%
总计	100%

第 2 部分：部署和用户体验

Q11. 贵组织在部署 Guardium 后多长时间从中实现了价值?	%
不足 1 个月	65%
1 到 3 个月	21%
4 到 6 个月	7%
7 到 9 个月	3%
10 到 12 个月	2%
12 到 18 个月	0%
18 个月以上	2%
总计	100%
外推值	1.96

Q12a. 在使用 Guardium 之前，贵组织能够准确检测到的数据威胁所占的百分比是多少?	%
不足 10%	9%
10% 到 25%	12%
26% 到 50%	18%
51% 到 75%	33%
76% 到 90%	15%
91% 到 100%	13%
总计	100%
外推值	55%

Q12b. 在部署了 Guardium 之后，贵组织能够准确检测到的数据威胁所占的百分比是多少?	%
不足 10%	0%
10% 到 25%	0%
26% 到 50%	7%
51% 到 75%	12%
76% 到 90%	21%
91% 到 100%	60%
总计	100%
外推值	85%

Q13. Guardium 的数据安全平台部署在贵组织数据存储库中的哪个位置? 请选择所有的适用项。	%
云环境	40%
大数据平台	21%
数据库和数据仓库	48%
文件系统	45%
大型机	6%
总计	160%

Q14a. 贵组织是否使用了 Guardium 的合规性快速入门功能?	%
是	45%
否	55%
总计	100%

Q14b. 如果是，您认为 Guardium 的合规性快速入门功能具有多大价值? 1 分 = 完全没有价值到 10 分 = 极具价值	%
1 或 2 分	5%
3 或 4 分	4%
5 或 6 分	10%
7 或 8 分	25%
9 或 10 分	56%
总计	100%
外推值	7.96

Q14c. 如果是，它对合规活动所花费的时间有何影响?	%
大幅缩短所花费时间	43%
缩短所花费时间	29%
对所花费时间无影响	28%
总计	100%

第 3 部分：Guadium 数据安全平台组件的价值

Q15. 在部署了 Guardium 之后，发生涉及超过 1000 条客户记录丢失的数据泄露的可能性降低程度如何（以预估百分比表示）？	%
没有降低	9%
降低约 10% 到 25%	20%
降低约 26% 到 50%	37%
降低约 51% 到 75%	19%
降低约 76% 到 100%	15%
总计	100%
外推值	43%

请使用 10 分制对以下 Guardium 产品功能进行评分，评分范围为 1 分（= 完全没有价值）到 10 分（= 极具价值）。

Q16. 具有用于分析数据资产威胁的 GUI	%
1 或 2 分	6%
3 或 4 分	7%
5 或 6 分	20%
7 或 8 分	32%
9 或 10 分	35%
总计	100%
外推值	7.16

Q17. 开箱即用的发现和分类模式	%
1 或 2 分	5%
3 或 4 分	8%
5 或 6 分	15%
7 或 8 分	32%
9 或 10 分	40%
总计	100%
外推值	7.38

Q18. 开箱即用型仪表板（即威胁情报）	%
1 或 2 分	6%
3 或 4 分	8%
5 或 6 分	24%
7 或 8 分	25%
9 或 10 分	37%
总计	100%
外推值	7.08

Q19. 与其他安全解决方案的异构集成（例如可互操作性）	%
1 或 2 分	2%
3 或 4 分	7%
5 或 6 分	27%
7 或 8 分	31%
9 或 10 分	33%
总计	100%
外推值	7.22

Q20. 发现和分析结构化/非结构化数据资产的能力	%
1 或 2 分	2%
3 或 4 分	6%
5 或 6 分	24%
7 或 8 分	23%
9 或 10 分	45%
总计	100%
外推值	7.56

Q21. 实时监控、接收和发布警报的能力	%
1 或 2 分	8%
3 或 4 分	7%
5 或 6 分	15%
7 或 8 分	32%
9 或 10 分	38%
总计	100%
外推值	7.20

Q22. Guardium 数据安全平台提供的漏洞洞察力	%
1 或 2 分	7%
3 或 4 分	5%
5 或 6 分	27%
7 或 8 分	23%
9 或 10 分	38%
总计	100%
外推值	7.10

Q23. 使用 Guardium 跨多云或混合云生态系统等复杂 IT 环境管理数据风险的能力	%
1 或 2 分	2%
3 或 4 分	0%
5 或 6 分	12%
7 或 8 分	33%
9 或 10 分	53%
总计	100%
外推值	8.20

Q24. Guardium 提供的在整个企业范围内管理数据风险的机器学习和自动化功能	%
1 或 2 分	4%
3 或 4 分	7%
5 或 6 分	6%
7 或 8 分	24%
9 或 10 分	59%
总计	100%
外推值	8.04

Q25. Guardium 维持防篡改审计痕迹、提供开箱即用型审计报告的能力	%
1 或 2 分	7%
3 或 4 分	11%
5 或 6 分	30%
7 或 8 分	32%
9 或 10 分	29%
总计	109%
外推值	7.30

Q26. Guardium 拦截、屏蔽和隔离非授权数据访问的能力	%
1 或 2 分	8%
3 或 4 分	12%
5 或 6 分	10%
7 或 8 分	25%
9 或 10 分	45%
总计	100%
外推值	7.24

Q27. Guardium 检测潜伏或误配置授权的能力	%
1 或 2 分	10%
3 或 4 分	11%
5 或 6 分	10%
7 或 8 分	32%
9 或 10 分	37%
总计	100%
外推值	7.00

第 4 部分：配置后的运营收益

Q28. Guardium 的数据安全平台是否帮助贵组织减少了与数据保护和合规性活动相关的人员数量?	%
是	33%
否	67%
总计	100%

Q29a. 贵组织是否能够通过部署 Guardium 数据安全平台而替换掉其他单点数据安全解决方案?	%
是	59%
否	41%
总计	100%

Q29b. 如果是，您替换了多少个单点解决方案?	%
1 到 2 个	32%
3 到 5 个	35%
6 到 10 个	20%
11 到 20 个	8%
20 个以上	5%
总计	100%
外推值	5.82

Q30a. 在使用 Guardium 之前，您的团队每年在识别和修复数据安全问题上所花费时间所占的百分比是多少?	%
不足 10%	6%
10% 到 25%	9%
26% 到 50%	18%
51% 到 75%	24%
76% 到 90%	28%
91% 到 100%	15%
总计	100%
外推值	61%

Q30b. 在部署了 Guardium 之后，您的团队每年在识别和修复数据安全问题上所花费时间所占的百分比是多少?	%
不足 10%	9%
10% 到 25%	23%
26% 到 50%	38%
51% 到 75%	20%
76% 到 90%	7%
91% 到 100%	3%
总计	100%
外推值	40%

Q31a. 在使用 Guardium 之前，贵组织每年可以检测和修复的数据源漏洞或误配置所占的百分比是多少?	%
不足 10%	14%
10% 到 25%	33%
26% 到 50%	40%
51% 到 75%	11%
76% 到 90%	2%
91% 到 100%	0%
总计	100%
外推值	30%

Q31b. 在部署了 Guardium 之后，贵组织每年可以检测和修复的数据源漏洞或误配置所占的百分比是多少?	%
不足 10%	7%
10% 到 25%	12%
26% 到 50%	16%
51% 到 75%	24%
76% 到 90%	18%
91% 到 100%	23%
总计	100%
外推值	60%

Q32a. 在使用 Guardium 之前，贵组织可以准确分类的数据所占百分比是多少?	%
不足 10%	11%
10% 到 25%	19%
26% 到 50%	20%
51% 到 75%	24%
76% 到 90%	18%
91% 到 100%	8%
总计	100%
外推值	49%

Q32b. 在部署了 Guardium 之后，贵组织可以准确分类的数据所占百分比是多少?	%
不足 10%	2%
10% 到 25%	2%
26% 到 50%	3%
51% 到 75%	12%
76% 到 90%	36%
91% 到 100%	45%
总计	100%
外推值	82%

Q33a. 在使用 Guardium 之前，贵组织每年能够准确检测/防范的数据威胁所占的百分比是多少?	%
不足 10%	12%
10% 到 25%	21%
26% 到 50%	30%
51% 到 75%	23%
76% 到 90%	9%
91% 到 100%	5%
总计	100%
外推值	42%

Q33b. 在部署了 Guardium 之后，贵组织每年能够准确检测/防范的数据威胁所占的百分比是多少?	%
不足 10%	3%
10% 到 25%	5%
26% 到 50%	5%
51% 到 75%	14%
76% 到 90%	29%
91% 到 100%	44%
总计	100%
外推值	78%

Q34a. 在使用 Guardium 之前，贵组织准备审计需要多长时间?	%
100 个小时以下	13%
100 到 250 个小时	16%
251 到 500 个小时	24%
501 到 1,000 个小时	26%
1,001 到 5,000 个小时	11%
5,000 个小时以上	10%
总计	100%
外推值	1,250

Q34b. 在部署了 Guardium 之后，贵组织准备审计需要多长时间?	%
100 个小时以下	32%
100 到 250 个小时	28%
251 到 500 个小时	18%
501 到 1,000 个小时	14%
1,001 到 5,000 个小时	8%
5,000 个小时以上	0%
总计	100%
外推值	478

第 5 部分：解决方案评估洞察

Q35. 您是如何听说 Guardium 的?	%
口碑相传	35%
分析师报告/电话拜访	43%
第三方市场	21%
IBM 网站	19%
IBM 业务合作伙伴	16%
营销手册	44%
其他（请注明）	2%
总计	180%

Q36. 贵组织为何要购买 Guardium，而不是竞争对手的产品？请选择所有的适用项。	%
IBM 在数据安全和合规市场上是值得信赖的领导者	53%
内置专业知识（即 GDPR 加速器、PCI/DSS 加速器）	45%
有助于改善数据、数据所有权和数据活动的可视性	59%
能够发现、理解和分类敏感数据	63%
可以帮助我们获得之前无法获得的新数据洞察力	41%
能够监控特权用户、拦截非授权访问	39%
满足合规报告和审计要求	57%
支持企业可扩展性	43%
集成功能方面的优势	35%
自动化功能方面的优势	46%
通过单个控制台支持集中化/管理	50%
覆盖多个不同的数据平台、数据库和数据仓库	28%
不会对数据库/数据仓库的性能带来不利影响	46%
总体拥有成本低	28%
可通过单个解决方案满足多个用例/需求	30%
总计	663%

请使用 10 分制（从 1 分 =完全不满意到 10 分 = 非常满意）对以下陈述进行评分。

Q37. 贵组织对 Guardium 数据安全平台的满意程度如何？1 分 = 完全不满意到 10 分 = 非常满意	%
1 或 2 分	0%
3 或 4 分	5%
5 或 6 分	12%
7 或 8 分	28%
9 或 10 分	55%
总计	100%
外推值	8.16

第 6 部分：人员统计

D1. 哪一项最能描述您在贵组织中的职位？	%
执行总裁/副总裁	6%
总监	17%
经理/主管	33%
分析师	17%
工程师	21%
咨询师/承包商	6%
其他（请注明）	0%
总计	100%

D2. 作为全球性组织，贵组织的全职员工数量有多少?	%
500 人以下	18%
501 到 1,000 人	21%
1,001 到 5,000 人	13%
5,001 到 10,000 人	19%
10,001 到 25,000 人	10%
25,001 到 75,000 人	11%
75,000 人以上	8%
总计	100%

D3. 哪一项最能描述贵组织的主要行业分类?	%
农业与食品服务	1%
通信	2%
消费品	5%
国防与航天	1%
教育	2%
能源与公用事业	5%
娱乐与媒体	2%
金融服务	18%
医疗保健与制药	11%
酒店	2%
工业	9%
公共领域	12%
零售	10%
服务	9%
技术和软件	8%
运输	2%
其他（请注明）	1%
总计	100%

如有任何疑问，请联系 research@ponemon.org 或拨打 800.887.3118。

Ponemon Institute

推动可靠的信息管理

Ponemon Institute 致力于进行独立调研和培训，旨在推动企业和政府中可靠的信息和隐私管理实践。我们的使命是对可能影响人员和组织敏感信息的管理和安全性的关键问题进行高质量的实证调研。

我们遵守严格的数据保密、隐私和有道德调研标准。我们不会从个人收集任何个人识别信息（或在业务调研中出现的公司识别信息）。此外，我们还执行严格的质量标准，确保不会向当事人提出不相关或不适当的问题。