ESG 经济性验证

Google Chronicle 安全分析平台的经济效益分析

作者：Jack Poller，高级分析师；Aviv Kaufmann，高级验证分析师

2020年8月

执行摘要

对于安全团队来说，在对本地资源的物理访问权限有限的情况下，为日益远程化的员工提供具备有效保护的基础设施从未如此重要。那些可以在云中部署其安全分析和操作的组织能够更好地继续为业务提供安全的基础设施。

ESG 证实了安全组织利用 Google Chronicle 收集和分析任何和所有安全遥测数据可以实现的节约。ESG 证实，Google 的定价模式与 Google 的规模经济相结合，可以为组织节省大量成本，同时提高他们发现高级持续威胁的可能性并提高取证调查的准确性。ESG 的建模场景预测，与基于云或本地安全分析平台的替代性基于云的或本地安全分析平台相比，大型企业组织在大规模分析安全遥测数据方面的花费可以减少 3.9 到 6 倍。由于 Google Chronicle 使用单一的全球价格并且成本不会因位置而变化，因此 TCO 优势可能会大得多。

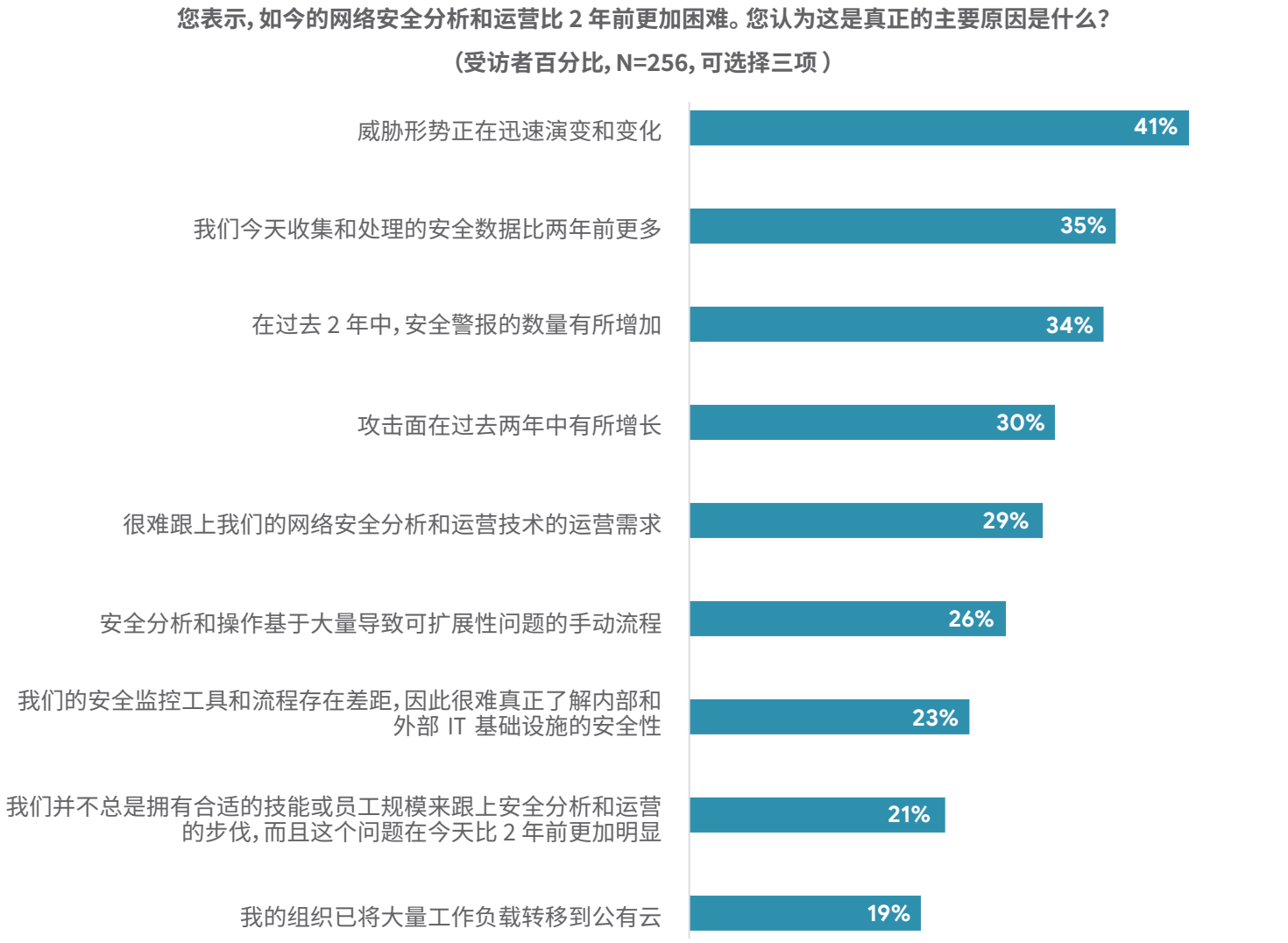
简介

此 ESG 经济性验证侧重于组织可以通过部署 Google Chronicle 来获得安全遥测的持续分析所带来的成本节约。ESG 创建了一个建模方案，该方案考虑了企业部署的 3 年期间软件、本地或云基础设施、支持和维护成本。

挑战

根据 ESG 的研究，近三分之二（63%）的组织认为，与两年前相比，如今的安全分析和运营比两年前更加困难，这是对手和 IT 变化的结果。具体而言，组织面临着不断变化的威胁形势、收集和处理更多安全数据的需求以及不断扩大的攻击面的挑战。此外，组织发现难以满足其网络安全分析和运营技术的运营需求，而手动流程会导致可扩展性问题。[1]

图 1.网络安全分析和运营困难增加的主要驱动因素



资料来源：Enterprise Strategy Group

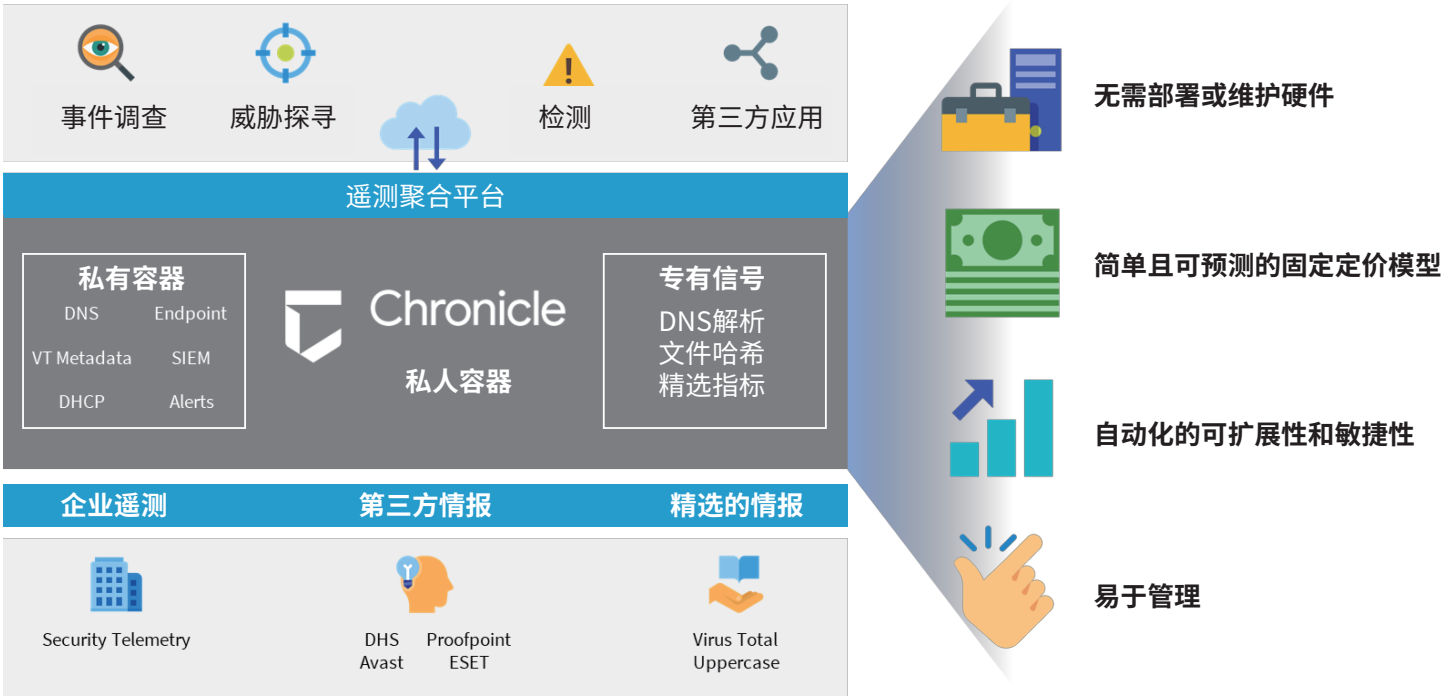
[1] 资料来源：ESG 总体调查结果：Cloud-scale Security Analytics Survey，2019 年 12 月。
本经济性验证报告中的所有 ESG 研究参考和图表均取自此调查结果集。

超过四分之三（76%）的组织表示，他们今天收集的安全数据比两年前更多，超过一半（52%）的组织将安全数据保留更长时间。四分之一（25%）通常会将安全数据保留 12 个月以上。因此，扩展安全分析和运营基础设施代表了另一个痛点。

解决方案：Google Chronicle

Google Chronicle 是一个基于 Google 核心基础设施的安全分析平台，提供无限弹性的安全遥测数据存储。借助基于员工数量的可预测固定价格模型，组织可以存储和分析所有安全数据，从而提高保真度。Chronicle 简化了管理和分析现代企业产生的大量安全遥测数据的复杂工作。自动分析引擎将来自内部和第三方公共来源的情报关联起来，以快速、自动地提取信号并检测威胁。

图 2. Google Chronicle 安全分析平台



资料来源：Enterprise Strategy Group

ESG 经济性验证

ESG 完成了 Google Chronicle 在大中型企业环境中的建模定价比较。重点放在了与典型的云或本地安全分析平台相比，组织在利用 Chronicle 的定价模型和 Google Cloud Platform 的规模经济时可以实现预期的经济节省。

ESG 的经济性验证流程是一种经过验证的方法，用于理解、验证、量化和建模产品或解决方案的经济价值主张。该流程利用 ESG 在市场和行业分析、前瞻性研究和技术/经济验证方面的核心能力。定量结果被用作一个简单经济模型的基础，该模型比较了本地和基于云的安全分析平台的预期成本。

Google Chronicle 经济性概述

ESG 的经济分析显示，Google Chronicle 通过利用 Google Cloud Platform 的资源和规模经济并为客户提供新的定价模式，为客户节省了大量资金。而传统的安全分析平台使用基于数据量的定价模型，成本增加与不断增长的安全遥测量直接相关，Google Chronicle 使用基于员工的定价 - 服务的成本主要取决于组织中的员工数量。

将成本与数据量脱钩可提高预算稳定性和可预测性，并鼓励在更长的时间范围内收集和分析所有遥测数据，确保更有可能从时间遥远的攻击指标 (IOA) 和妥协指标 (IOC) 中识别长期威胁。

ESG 分析

ESG 利用通过供应商提供的材料、公开可用的配置指南和定价以及行业经济和技术知识所收集的信息，创建了一个为期三年的 TCO/ROI 模型，该模型将 Google Chronicle 的成本和收益与两个基于云的和一个本地安全分析平台进行比较。该模型比较了在企业环境中部署每个解决方案时的预期成本，目标是量化通过 Google Chronicle 的定价模型和 Google 的规模经济实现的预期成本节约。

ESG 为两个不同规模的组织模拟了安全分析平台的部署和运营：

- 中型企业 — 15，000 名员工，每天生成 1.5 TB 的安全遥测数据
- 大型企业 — 125，000 名员工，每天生成 12.5 TB 的安全遥测数据

ESG 使用《财富》1000 强公司的平均员工增长率对员工增长进行建模，并使用来自 ESG 对首席信息安全官、网络安全经理和网络安全从业人员的研究调查的信息对安全分析数据增长率进行建模。

ESG 研究调查显示，大多数大中型企业将安全遥测数据保留 12 个月或更长时间。因此，经济模型占遥测数据保留期的 12 个月。

该模型计算并报告了在内部部署安全分析平台可能产生的预期成本，包括三年期间的硬件采购成本、电源/冷却/占地面积、支持/维护和管理成本。对于基于云的安全分析平台，该模型使用成本最低的地理区域计算并报告了软件许可和数据保留所产生的成本。

ESG 分析

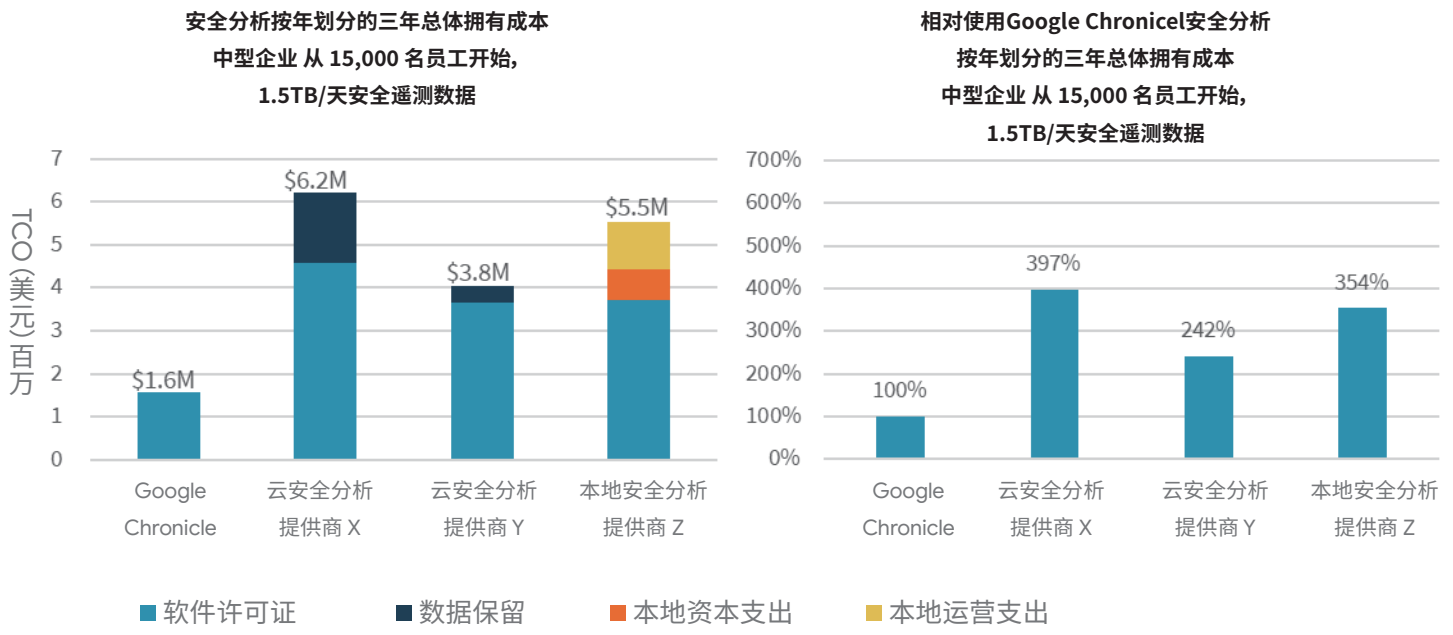
安全预算无法跟上日益增加的复杂威胁数量和不断增长的攻击面，组织继续赋予 CISO 和安全团队“用更少的资源做更多的事情”的任务。

Google Chronicle 提供了无限的可扩展性，同时消除了本地基础设施和运营开销。基于员工的定价将成本与数据量和速度分离，确保组织可以预测其成本并鼓励收集、存储和分析任何和所有安全遥测——在更长的时间范围内收集更多数据可以提高识别长期威胁的可能性 。

ESG 建模方案：中型企业

ESG 的经济模型计算了一个拥有 15,000 名员工的典型中型组织每天生成 1.5 TB 的安全分析数据，在三年内的预期成本。该模型显示，部署 Google Chronicle 的组织预计在三年内花费 1,565,000 美元（参见图3和表1）。这两个云平台的成本会高出 2.4 到 4 倍，而本地平台的成本会高出 3.5 倍。

图 3. 在中型企业中部署安全分析平台三年的预期 TCO



资料来源：Enterprise Strategy Group

表 1：在中型企业中部署安全分析平台的预期三年 TCO

	Google Chronicle	云安全分析提供商 X	云安全分析提供商 X	本地安全分析提供商 Z
本地部署资本支出	$0	$0	$0	$704，761
本地部署运营支出	$0	$0	$0	$1，105，951
软件许可证	$1，564，768	$4，584，929	$3，661，729	$3，723，750
12 个月的数据保留期	$0	$1，632，120	$374，548	（包含在资本支出中）
3 年期总计	$1，564，768	$6，217，049	$3，787，877	$3，723，750
总计占 Google 的百分比	100%	397%	242%	354%

资料来源：Enterprise Strategy Group

每个解决方案的年度支出如图 4 和表 2 所示。Google Chronicle 定价模型基于组织中的员工数量，从而产生可预测且稳定的年度支出。内置 12 个月的数据保留期后，部署 Chronicle 的组织无需为数据保留和存储制定额外的预算。整个三年的运营支出为 160 万美元。

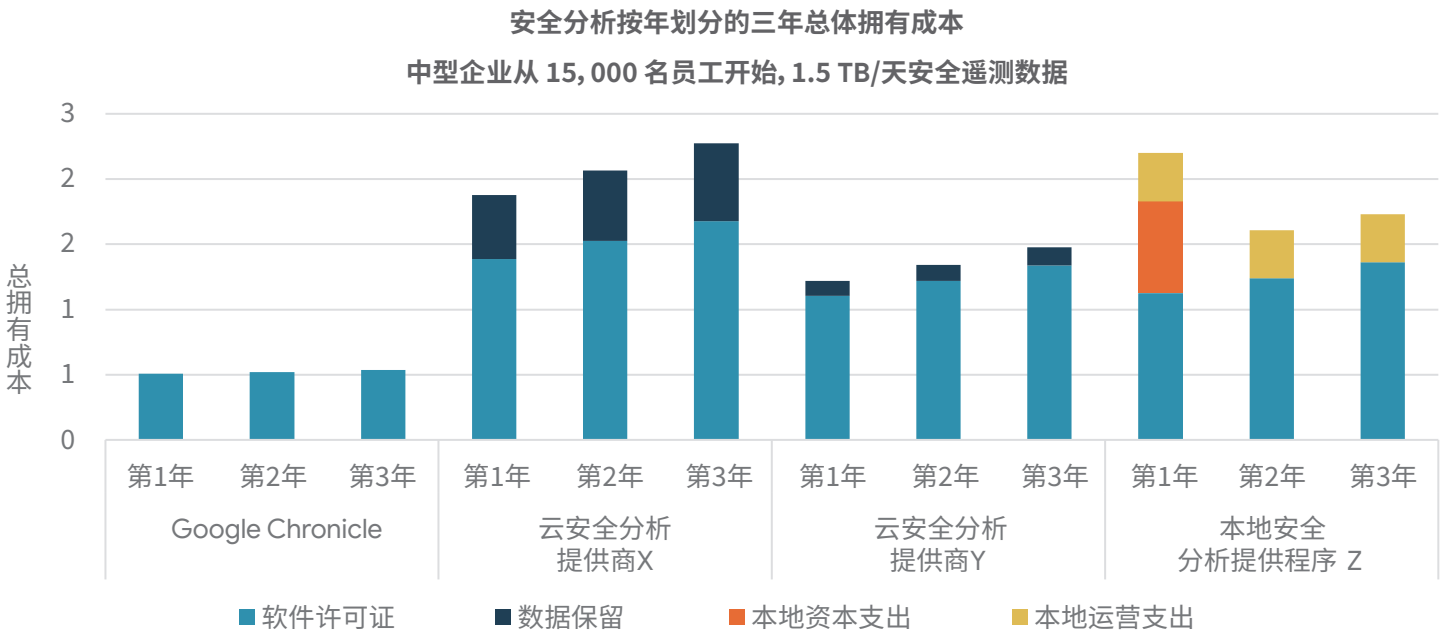
云安全分析提供商 X 的总体拥有成本基于处理的数据量和超过所包含保留期的保留数据量。提供商 X 的外部总体拥有成本为 620 万美元的运营支出。虽然提供商 X 可以利用云规模经济，但许可费比 Google Chronicle 高出 2.9 倍以上。提供商 X 仅包括 90 天的数据保留期，这要求组织为额外的存储费用制定预算。提供商 X 的数据保留率大于 Google Chronicle 的整个 TCO。

云安全分析提供商 Y 的总体拥有成本基于处理和保留的数据量。ESG 使用云服务供应商的对象存储定价对超过所包含保留期的数据保留的费用进行了保守估计。ESG 预计实际数据保留费用将超过预期。提供商 Y 的所有支出都可以归类为运营支出，并在三年内达到 380 万美元。

本地安全分析提供商 Z 的总体拥有成本包括基于所分析的大量数据的许可费。若要存储、索引和分析数据，需要本地存储和计算服务器以及必要的网络基础设施。ESG 的模型包括一个基于固态驱动器的存储系统，其大小足以保留12个月的数据。计算服务器的数量和大小基于提供商 Z 的标准指导。

提供商 Z TCO 包括第 1 年 705,000 美元的资本支出，随后几年没有额外的资本支出。基础设施运营支出包括 1 名系统管理员，负责管理存储、计算和网络集群，以及存储和计算集群的电源、冷却、占地面积、维护和支持，每年 369,000 美元。尽管第一年的资本支出支出，三年的 TCO 为 550 万美元，比云安全分析提供商 X 少 682,000 美元。

图 4.在中型企业中部署安全分析平台的预期年度 TCO



资料来源：Enterprise Strategy Group

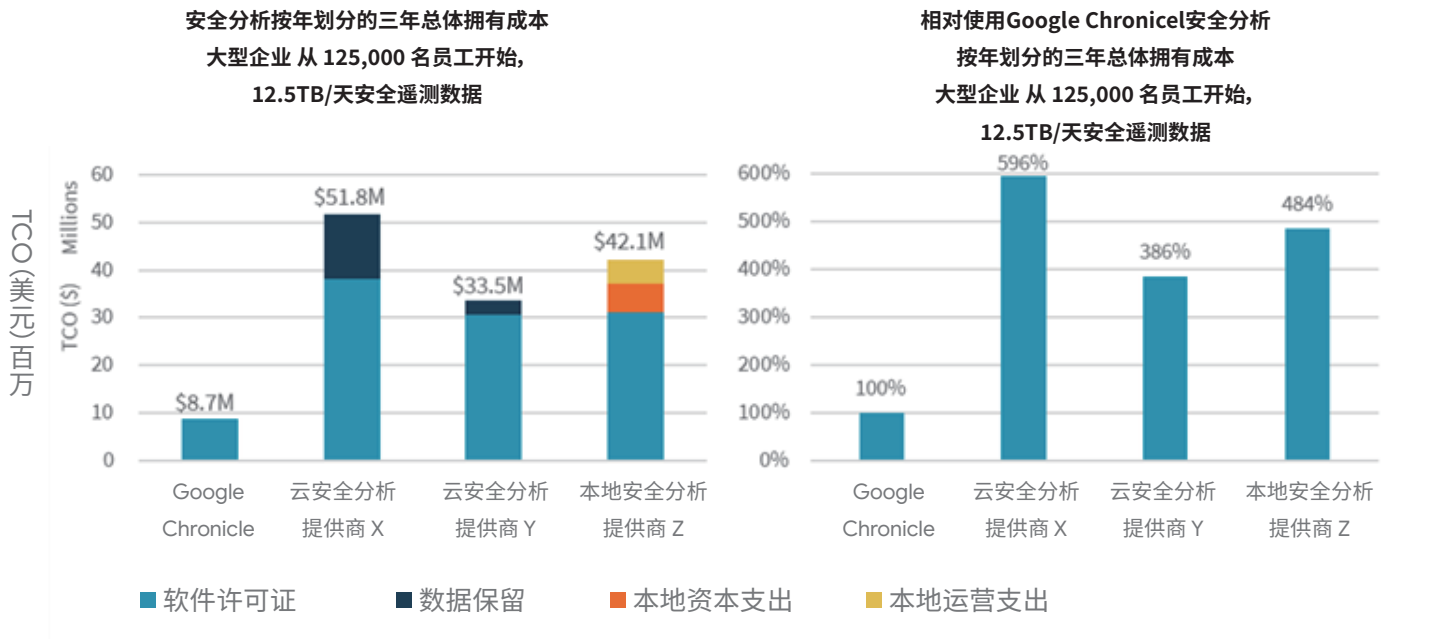
表 2：在中型企业中部署安全分析平台的预期年度 TCO

	Google Chronicle			云安全分析提供商 X			云安全分析提供商 Y			本地安全分析提供商 Z		
	第1年	第2年	第3年	第1年	第2年	第3年	第1年	第2年	第3年	第1年	第2年	第3年
本地资本支出	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$704，761	$0
本地运营支出	$0	$0	$0	$0	$0	$0	$0	$0	$0	$368，650	$368，650	$368，650
软件许可证	$506，250	$521，438	$537，081	$1，385，175	$1，523，693	$1，676，062	$1，106，262	$1，216，889	$1，338，578	$1，125，000	$1，237，500	$1，361，250
12 个月数据保留	$0	$0	$0	$493，088	$542，396	$596，636	$113，333	$124，646	$136，570	包含在资本支出中	包含在资本支出中	包含在资本支出中
全年合计	$506，250	$521，438	$537，081	$1，878，263	$2，066，089	$2，272，698	$1，219，595	$1，217，334	$1，350，948	$2，198，412	$1，606，150	$1，729，900
3 年期总计	$1，564，768			$6，217，049			$3，787，877			$5，534，462		

资料来源：Enterprise Strategy Group

ESG 的经济模型计算了一家拥有 125,000 名员工，此类大型企业未来三年预期成本每天生成 12.5 TB 安全分析数据。该模型显示，部署 Google Chronicle 的组织预计在三年内花费 8,693,000 美元（参见图5和表3）。由于 Chronicle 的替代方案是按数据量定价的，因此大型企业的差异远大于中型组织：两个云平台的成本要高出 3.9 到 6 倍，而本地平台的成本要高出 4.8 倍。

图 5.在大型企业中部署安全分析平台三年的预期 TCO



资料来源：Enterprise Strategy Group

表 3：在大型企业中部署安全分析平台的预期三年 TCO

	Google Chronicle	云安全分析提供商 X	云安全分析提供商 X	本地安全分析提供商 Z
本地资本支出	$0	$0	$0	$6，089，475
本地运营支出	$0	$0	$0	$4，992，262
软件许可证	$8，693，156	$38，207，744	$30，514，406	$31，031，250
12 个月的数据保留期	$0	$13，600，997	$3，005，286	（包含在资本支出中）
3 年期总计	$8，693，156	$51，808，741	$33，519，691	$42，112，987
总计占 Google 的百分比	100%	596%	386%	484%

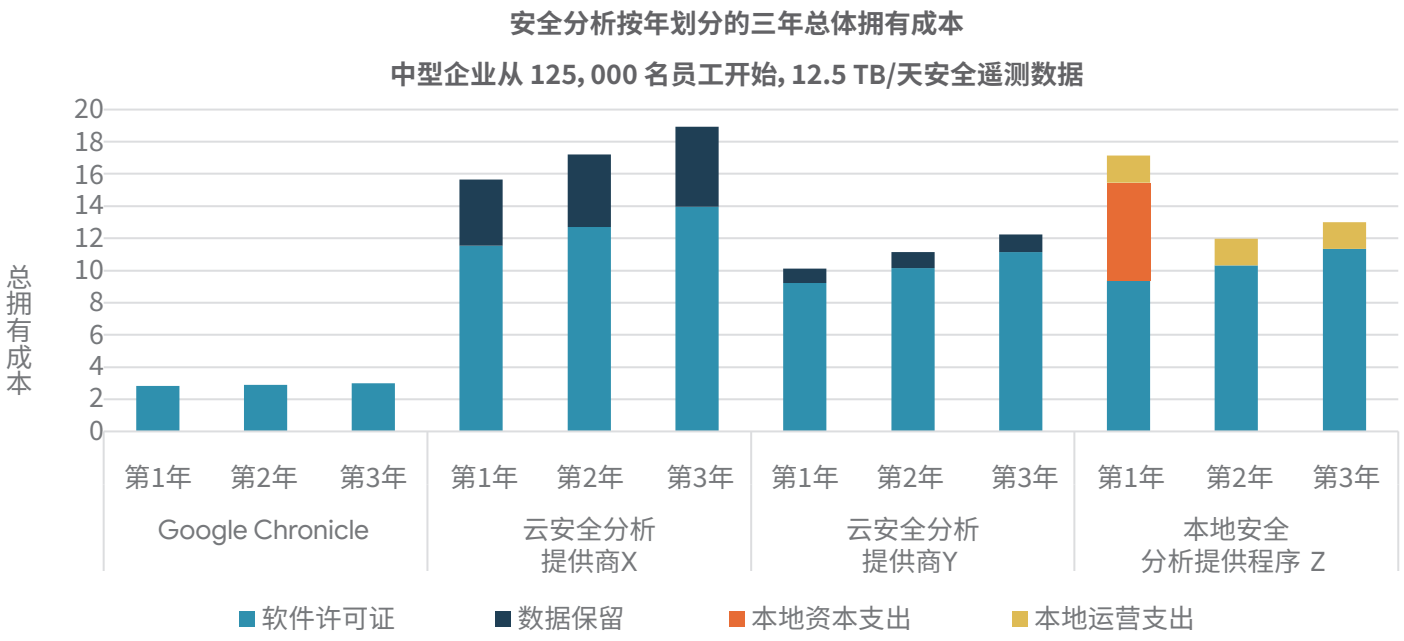
资料来源：Enterprise Strategy Group

每个解决方案的年度支出如图 6 所示。与中型企业一样，提供商 X 的数据保留支出是 Google Chronicle 总支出的 1.6 倍，占提供商 X TCO 的四分之一以上。

提供商 Y 的软件许可证是 Google Chronicle TCO 的 3.5 倍。ESG 对数据保留支出使用了保守估计。虽然数据保留率约为提供商Y TCO 的 9%，但支出占 Google Chronicle 总支出的三分之一以上。

本地安全分析提供商 Z 的支出包括用于存储、计算和网络基础设施的第一年资本支出 6,089,000 美元，以及一名系统管理员、电力、冷却、占地面积、支持和维护的基础设施运营支出每年 1,664,000 美元。三年的基础设施支出为 11,081,000 美元，是 Google Chronicle 总支出的 1.3 倍。

图 6.在中型企业中部署安全分析平台的预期年度 TCO



资料来源：Enterprise Strategy Group

更重要的事实

在更长的时间范围内收集和分析更多数据会增加发现隐蔽、移动缓慢、长期存在的威胁和攻击的可能性。根据 ESG 研究，84% 的组织表示他们将从收集、处理和分析更多数据中受益。因此，组织正在趋向于更大量的安全数据，现在超过四分之三 (76%) 收集的遥测数据比两年前更多，超过一半 (52%)保留更长时间的安全数据。四分之一 (25%)的组织将安全数据保留超过 12 个月。然而，85% 的组织表示，他们使用几个独立的安全分析工具收集、处理和分析相同的数据。80% 依赖于众多互不相连的分析引擎和单点工具；80% 的人在数据管理和微调安全分析基础设施上花费了大量时间。

传统安全分析平台的定价模型基于安全数据的数量和速度，而基于云计算的平台的定价模型则是基于地理区域。显然，这使得预测成本变得困难，并且不鼓励收集额外的遥测数据，从而降低了分析的保真度。

Google Chronicle 根据组织中的员工数量采用了新的定价模型。这种无限量数据分析引擎提供了可预测的成本，鼓励而不是限制所有安全遥测数据的收集，提高保真度并帮助组织识别高级持续性威胁(APT)。Chronicle 包括 12 个月的数据采集，帮助搜索 APT 和取证调查。

ESG 的建模 TCO 分析显示了部署 Google Chronicle 的组织如何通过利用 Google 的规模经济和定价模型，在其安全分析和运营方面节省大量成本。在三年内，中型企业在 Google Chronicle 上的支出预计将比其他基于云的平台少 2.4 到 4 倍，比本地部署少 3.5 倍。

较大的组织可能会面临更大的差异，典型的大型企业在备用云解决方案上的支出要高出 3.8 到 6 倍，而本地部署的支出要高出 4.8 倍。替代的云解决方案可能更加昂贵，因为解决方案定价取决于位置。

Google Chronicle 不会与组织现有的安全工具竞争，也不会寻求改变安全操作。相反，Chronicle 旨在通过鼓励在很长一段时间内收集和分析所有安全遥测数据、增加发现和防止隐形攻击的可能性以及提高取证调查的保真度来实施所有安全控制。如果您希望在“事半功倍”的同时简化安全运营和分析，ESG 建议您联系 Google ，看看它是否是适合您团队的安全分析平台。

Enterprise Strategy Group 是一家从事 IT 分析、研究、验证和战略的公司，致力于为全球 IT 社区提供市场资讯和可行见解。