

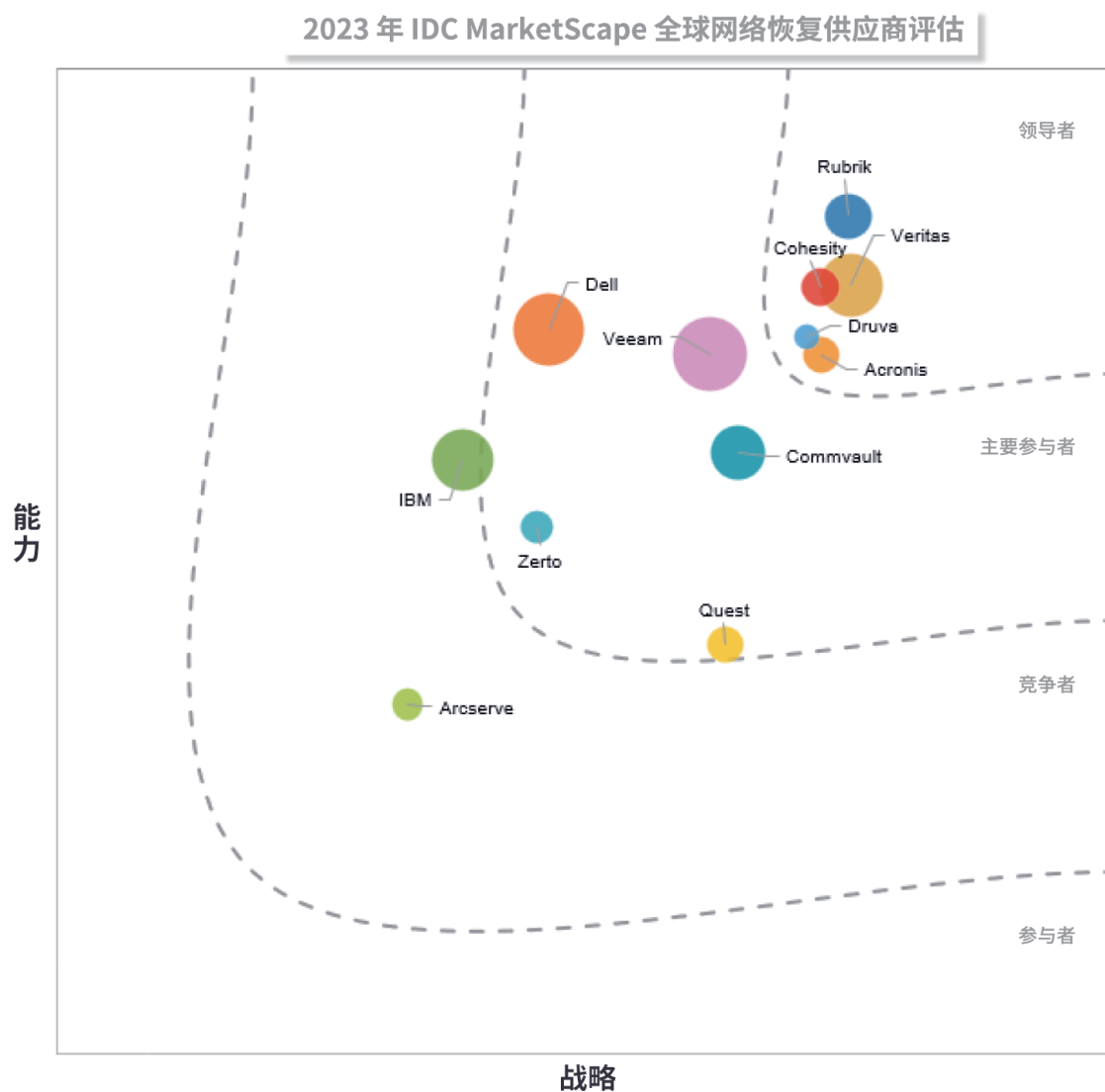
2023 年 IDC MarketScape 全球网络恢复供应商评估

Phil Goodwin Johnny Yu Greg Macatee

本篇 IDC MarketScape 节选介绍 Cohesity

IDC MarketScape 图

图 1



来源：2023 IDC

请参照附录的详细研究方法, 市场定义和评分标准。

IDC 2023年11月发布 #US49787923e

以下内容摘自 IDC 的《2023 年 IDC MarketScape 年全球网络恢复供应商评估》，文档编号US49787923。本节选包含图 1和部分内容,即 IDC 观点、IDC MarketScape供应商入选标准、基本指南、供应商综合概况、附录和进一步研究等。

IDC 观点

网络攻击是全球企业面临的最大威胁之一。无论规模、行业、地理位置或政治边界如何，网络攻击者都不放过任何企业。不幸的是，网络犯罪并没有结束的迹象，因为这对网络攻击者而言实在太有利可图了。对于受害者来说，可能遭受收入损失、永久失去客户、员工生产力下降、监管罚款和数据无法恢复，还要支付高昂的赎金。也许更糟糕的是，有些企业在受到攻击后，会面临股东诉讼或集体诉讼。

在勒索软件攻击的早期，企业依赖数据备份映像进行恢复。随着网络攻击手段变得越来越复杂和全面，攻击会清除备份映像，IT团队开始宣布对网络事件进行灾难响应。然而，灾难恢复和网络恢复之间有着重要的区别。以下表格1进行了比较。表格1不是试图捕捉这两个过程的每一步，而是为了说明单独的灾难恢复工作无法为网络事件带来良好结果。

表格 1

灾难响应与网络响应

高水准的灾难响应流程	高水准的网络响应流程
宣布灾难	检测攻击
提供恢复环境	从物理上隔离攻击，防止其进一步扩散； 根据需要关闭系统
如果需要，从上一个恢复点恢复数据	进行取证分析： <ul style="list-style-type: none">▪ 确定攻击类型▪ 确定攻击何时开始▪ 识别所有受影响的系统
按规定顺序重新启动计算服务	建立隔离沙箱： <ul style="list-style-type: none">▪ 将数据恢复到沙箱▪ 扫描数据和系统中是否存在恶意软件▪ 扫描备份中是否存在恶意软件▪ 确定上次清理的时间点，该时间点可能因文件系统或数据库而异

灾难响应与网络响应

高水准的灾难响应流程	高水准的网络响应流程
	▪ 验证恢复情况
启动应用程序故障转移	提供恢复环境： ▪ 可能需要裸机
运行完整性检查 (即,重新启动数据库并根据需要前滚日志)	将恢复环境推送到生产环境
与用户一起验证恢复情况	验证恢复情况
恢复运营	恢复运营
在适当的时候进行故障恢复	

来源: 2023 IDC

IDC首次应用NIST框架进行评估。使用NIST框架能实现网络弹性, 该框架包括五大"支柱": 识别、保护、检测、响应和恢复。从根本上说, 这些"支柱"分为两大类: 主动防御和被动恢复。企业需要它们来实现真正的网络弹性。但遗憾的是, 目前还没有一家供应商能同时提供主动防御和被动恢复。传统的数据防护功能往往侧重于响应和恢复, 而数据安全功能侧重于识别、保护和检测。无论供应商植根于数据防护, 还是数据安全, 都正在努力提供五大"支柱"的所有功能, 至少提供其中的一些功能。

IT领导人承认, 没有供应商能够完全阻止网络攻击。事实上, 大多数人都认为攻击者迟早会入侵他们的系统。此外, IDC的研究表明, 与数据加密勒索事件相比, 数据泄露勒索事件的发生频率高出约50%。原因是: 企业越来越擅长恢复加密数据, 但已泄露的数据却无法恢复; 以及企业领导者决定是否支付赎金。然而, 即使无法从外泄中恢复, 网络恢复供应商也可以提供重要的功能, 例如强大的数据加密和不可变性, 从而减少不良影响。

IDC 认为, 具有网络弹性的企业应先遵守以下三个原则:

- **绝对可靠的数据存活**
如果无法做到绝对可靠的数据存活, 企业就有可能被迫支付赎金以取回数据, 或者遭受数据丢失。IDC的研究表明, 这种情况太常见了。企业需要知道, 无论如何他们都是可以取回数据的。
- **绝对可靠的数据完整性**
与数据存活类似, 企业需要知道他们恢复的数据是准确的数据。如果做不到这一点, 网络攻击者在收到赎金后, 就会继续制造麻烦。
- **快速恢复, 数据丢失最少化**
停机时间是网络攻击者的朋友, 也是受害者的敌人。即使企业拥有干净、可恢复的数据, 漫长的恢复时间也会促使企业支付赎金。如果能够检测攻击、隔离攻击、评估损害并快速恢复运营, 就可以减轻任何损害。

由于网络响应的独特要求,IT团队正在快速实施网络响应系统,供应商也通过快速发展解决方案来响应市场和用户需求。这个充满活力的市场对IT购买者来说是件好事,因为它提供了高度差异化、激烈的竞争以及寻找最佳解决方案的机会。本 IDC MarketScape 评估了 IDC 认为最著名的 12 家网络恢复供应商。各个供应商都有独特的功能和最匹配的应用场景。此评估旨在帮助 IT 购买者区分不同的供应商,选择到最适合自身情况的供应商。

IDC MarketScape 供应商入选标准

网络恢复本身不是一种单独的功能,而是一种功能的组合。从广义上说,网络恢复从基本数据防护开始,并建立在灾难恢复的基础上。因此,它本身不是一个产品,而是一组集成的功能,用于响应勒索软件的特定目的。虽然备份或恢复声称可以在勒索软件攻击后恢复,但如前所述,仅备份或恢复本身是远远不够的。因此,IDC对备份或恢复供应商评估不感兴趣,而是对具有专门构建网络恢复功能的供应商感兴趣。

在 IDC MarketScape 中值得参考的是,供应商必须能够确保数据存活、数据完整性和快速恢复数据。不变性、加密和强大的物理隔离数据等功能是筹码。本文档各个供应商都达到了入选标准。这些解决方案中的任何一个在正确配置和管理后,都可以在勒索软件攻击时促进完整的数据恢复。

IDC应用了以下入选标准:

- 该解决方案必须是一套软件产品,不仅仅是单独的备份或恢复。
- 该解决方案必须以软件为主。允许与设备一起交付或集成,只要它们低于解决方案价格的50%(占实际售价的百分比)。
- 该解决方案必须包含专门为网络响应设计的工具或模块。
- 该解决方案必须提供 NIST 框架中“响应”和“恢复”之外的功能,至少是“识别”、“保护”或“检测”中的一个。
- 数据防护相关软件收入必须超过 1 亿美元。
- 该解决方案至少 70% 是自主研发的技术(占实际售价的百分比)。
- 该解决方案必须在全球范围内可用,即在北美、欧洲、亚太地区、中东和非洲、或至少10个不同的国家地区开展业务,并且 $\geq 20\%$ 的收入来自北美以外地区。
- 该解决方案必须解决本地、多公共云和混合云工作负载。
- 该解决方案必须满足大中小型企业的需求。
- 核心解决方案必须已于2022年1月1日全面上市,所有功能均在2023年5月30日全面上市。该时间之后发布的功能被视为规划中。

IDC的目标是促进具有足够自由度的一对一评估,使各个供应商都可以展示其独特价值,而不是将供应商限制在一种通用的评估中。

给 IT 购买者的建议

本文档中的所有供应商都支持本地、混合云和多云环境。然而，有些主要从本地的角度来实现，另一些是从云的角度来实现，还有一些是从两者的混合角度来实现。全部都具有高度可行性。因此，IT 购买者应该去考虑，哪种架构更适合他们的环境和战略方向。

网络恢复供应商通过多种方式来使自己脱颖而出。很多时候，这些都涉及权衡。一些关键的采购标准是：

- **复杂性**

IDC MarketScape 中评估的解决方案范围从简单易管理到相当复杂。毫不奇怪，复杂的解决方案可能具备更多功能。IT 购买者必须在对简单性的渴望和对强大特性功能的需求之间取得平衡。

- **解决方案的广度**

一些供应商在努力提供尽可能多的功能，另一些供应商则专注于自身擅长的特定功能。没有任何供应商可以提供一切功能，也没有任何公司需要一切功能。IT 购买者应注重自身需求，合理计划未来预期内的需求。

- **价格**

虽然价格不是本次 IDC MarketScape 的评估标准，但它无疑是每个 IT 购买者的考虑因素。本文档提到解决方案因价格而异，目标是在成本和解决方案功能之间找到平衡。

- **职权**

虽然这次评估是假设各个供应商在同一起跑线上进行，但一些 IT 购买者会放弃自认为次要的功能，选择与现有供应商继续合作。而另一些 IT 购买者不管目前与哪个供应商有合作关系，还是会坚持选择自认为最好的解决方案。最后，只有 IT 购买者才能做出权衡和选择。

本 IDC MarketScape 并非购买指南。IDC 根据自认为对网络恢复最重要的标准进行评估，IDC 的价值观和权重可能与任何特定 IT 购买者的需求不符。它的最佳用途是作为一种手段，起初是对解决方案进行区分，并制定一份候选供应商短名单，以供 IT 购买者进一步参考。在本次评估中，各个供应商在某些情况下都可能是完美的解决方案，而在其他情况下可能不太理想。IDC 建议 IT 购买者在制定候选名单时参考本文档，以缩小选择范围。在做出任何选择或采购之前，IT 购买者应进行尽职调研和 PoC。

供应商综合概况

本节选简要说明了 IDC 的主要观察结果，从而确定了供应商在 IDC MarketScape 中的位置。虽然各个供应商都根据附录中概述的每个标准进行评估，但此处描述了各个供应商的优势和挑战。

Cohesity

IDC 已将 Cohesity 评为 2023 年 IDC MarketScape 全球网络恢复领域的领导者。Cohesity 是数据防护市场上较新的供应商之一。在核心数据防护方面拥有了强大的能力,已经快速有效地转向网络弹性。Cohesity 的网络恢复产品组合包括 Data Protect (本地和作为服务)、SiteContinuity (本地和作为服务)、DataHawk 和 FortKnox,所有这些都由 Cohesity 数据云平台提供支持。Cohesity 因其数据防护或网络能力被 AWS 选为关键合作伙伴,最近又被 IBM 选为重要合作伙伴,将其纳入 IBM 的 Storage Defender 产品线。IBM 被评为 2023 年 IDC MarketScape 全球网络恢复领域的竞争者。

从一开始,Cohesity 的架构就旨在实现可扩展性。这种可扩展性不仅是为了第三方连接,也是为了更好的用户体验。Cohesity 开发和管理其解决方案的核心,也不羞于采用 Tenable、zScaler、BigID 和 Qualys 等第三方供应商技术。Cohesity 的架构不仅有助于相对快速地开发这些合作伙伴的功能,而且以一种对用户透明的无缝方式实现了这一点。

Cohesity 还创建了数据安全联盟,其中包括 CrowdStrike、Mandiant、Palo Alto Networks 和 Netskope 等供应商。该联盟使 Cohesity 能够参与更大的网络安全供应商生态系统,并采用、合作或连接关键功能。Cohesity 还向联盟成员的客户承诺,将为他们提供支持和进行交互。这包括 SIEM、SOAR、EDR、XDR、ITSM、DLP 和数据安全态势管理 (DSPM)。

Cohesity 的产品组合旨在帮助客户做好网络防御,包括漏洞扫描、早期检测、事件响应和取证分析,以协调网络恢复。它还具有基于机器学习的异常检测功能,可分析备份数据,计算异常发生的几率,并识别新的或突发的趋势。

Cohesity 的网络应急响应团队(CERT)使网络防御和恢复不仅仅局限于技术。该团队可帮助客户快速响应主动网络攻击,以保护 Cohesity 集群、取证分析、数据恢复和集群恢复。

优势

- 具备网络安全和恢复功能,同时不忘备份或恢复、灾难恢复的基本知识。
- 开发了一个集成良好、对用户友好的界面,有效地整合第三方研发的技术。
- 通过数据安全联盟的强大“上游”生态系统来发展,及利用第三方研发的技术。
- 与 AWS 和 IBM 等公司建立了强大的“下游”关系生态系统。
- 在解决方案中广泛使用零信任概念。

挑战

随着网络恢复和安全市场的快速发展,新的能力和功能也在不断推出。Cohesity 努力地保持领先地位,可惜不是每个想法都是好主意。Cohesity 必须明智地选择要追求的机会,那些能为客户提供真正价值的机会。合作关系越广,并不代表合作程度越好。Cohesity 打算继续在其数据安全联盟中添加更多合作供应商名单(在撰写本文档时,该联盟共有 22 家供应商)。其实, Cohesity 应只关注那些能带来真正附加值的合作供应商。

在以下情况可考虑 Cohesity

Cohesity主要供中大型企业考虑，但小型企业也会发现其云产品的吸引力。已经使用数据安全联盟成员产品的客户可能会发现，在某些情况下添加Cohesity会更简单。那些寻求广泛且功能强大的产品，并拥有支持和管理该产品的IT人员的企业可考虑使用Cohesity。

附录

解读 IDC MarketScape 图

IDC 将衡量标准分为两个主要类别：能力和战略。

Y轴或能力轴上的定位反映了供应商当前的能力、服务菜单、以及与客户需求的匹配程度。能力类别侧重于公司和产品的现有能力。在这一类别下，IDC分析师将关注供应商在构建或提供能力方面的表现如何，以使其能够在市场上执行所选择的战略。

X轴或战略轴上的定位表明，供应商的未来战略与客户在三到五年内的需求的匹配程度。战略类别侧重于有关未来三到五年的产品、客户群、业务和上市计划的高层决策及基本假设。

在 IDC MarketScape 图中，各个供应商标记的圆圈大小代表了在所评估的特定细分市场中的份额。在本例中，由于网络恢复是其他数据防护产品的一个用例。因此，使用 IDC 调研显示的供应商数据复制和保护软件收入作为市场份额。

IDC MarketScape 研究方法

IDC MarketScape 标准的选择、权重和供应商评分代表了 IDC 对市场和特定供应商的充分研究判断。IDC 分析师通过对市场领导者、参与者和最终用户进行结构化讨论、调查和访谈，定制了一系列标准特征，用于衡量供应商。市场权重是基于每个市场的用户访谈、购买者调研和IDC专家的意见。IDC 分析师根据各个供应商的评分、IDC MarketScape上的最终供应商排名、对供应商的详细调研和访谈、公开信息和最终用户体验，努力对各个供应商的特征、行为和能力提供准确且一致的评估。

市场定义

网络恢复能力建立在数据复制和保护软件、灾难恢复系统的基础上。IDC对相关市场组成部分的定义如下：

- 数据复制和保护 (DR&P) 软件

数据复制和保护仍是IDC跟踪的核心市场。数据复制和保护软件专注于在发生物理或逻辑错误时保护、还原和恢复数据。数据保护和恢复市场的产品包括数据保护、持续数据保护、裸机恢复、备份或恢复软件、基于主机的复制和基于阵列的复制（包括快照、镜像、克隆和远程复制）。数据保护软件包括来自许可软件和以订阅方式许可的在线数据保护服务（又称在线备份）的收入。这包括文件级和映像级备份软件、持续数据保护软件和备份报告软件。

- **数据保护即服务 (DPaaS):**

数据保护即服务是一个总括性术语, 包括备份、存档、灾难恢复和网络恢复即服务。这些是基于云的服务, 完全由服务提供商管理。大部分数据保护即服务解决方案可以解决本地、混合和多云工作负载。

- **灾难恢复和灾难恢复即服务 (DRaaS):**

灾难恢复系统包括在本地或公共云环境中重新启动整个工作负载所需的全部基础设施、流程管理和服务。灾难恢复即服务与本地和传统灾难恢复的区别在于, 灾难恢复即服务是基于云的完全托管服务。企业可以根据数据中心火灾、水管破裂和断电; 或者火车脱轨、飞机失事、恐怖事件、地震、洪水、龙卷风和飓风等区域事件来宣布灾难响应。

- **网络恢复和网络恢复即服务 (CRaaS):**

网络恢复建立在灾难恢复的基础上, 网络恢复即服务建立在灾难恢复即服务的基础上。这两种情况下的网络恢复包括所有基础设施、流程管理、分析取证和专业服务, 以帮助企业从一般恶意软件攻击和具体勒索软件攻击中恢复。为了符合网络恢复即服务的服务资格, IDC认为它必须包含灾难恢复即服务的所有组件 (即, 重新建立整个应用程序工作负载的能力), 以及卫生沙箱、取证分析和策划恢复的配置。有些供应商可能会远远超出这一范围, 提供额外的数据安全功能, 以实现增值和差异化。

进一步研究

相关研究

- IDC 于 2023 年 3 月发布的《在数据保护中实施零信任》, 文档编号 US50225723
- IDC 于 2022 年 10 月发布的《IDC 市场框架: 数据弹性》, 文档编号 US49800322
- IDC 于 2022 年 10 月发布的《网络恢复: 为什么灾难恢复不足以实现数据信任》, 文档编号 US49743422

大纲

这份IDC研究调查了全球范围内12家最著名的网络恢复供应商。各个供应商都有其独特的市场地位。此评估旨在帮助IT购买者确定适合其特定场景的候选名单, 作为采购过程或开展PoC的第一步。各个供应商的能力差异很大, 区分网络恢复解决方案对于IT购买者来说是一个挑战。如果选择了错误的解决方案, 可能会引发网络事件, 耗费时间, 损失金钱和声誉。所以, 采购决定至关重要。

IDC 基础设施系统、平台和技术集团研究副总裁 Phil Goodwin 表示: “网络恢复是网络弹性的基石。如果没有准确、快速恢复数据的能力, 企业可能逼不得已支付赎金, 以避免数据丢失和严重的业务后果。选择正确的网络恢复供应商是任何网络防御计划中的关键一步。将企业要求与供应商能力相匹配确保获得最佳成果, 而 IDC MarketScape 全球网络恢复供应商评估旨在帮助 IT 购买者实现这一目标。”

关于 IDC

国际数据公司 (IDC) 是全球著名的信息技术、电信和消费科技行业的咨询顾问、活动服务专业提供商。IDC 在全球拥有超过 1,300 名分析师, 为 110 多个国家的技术和行业发展机遇提供全球化、区域化和本地化的专业视角及服务。IDC 的分析和洞察助力IT专业人士、业务主管和投资机构制定基于事实的技术决策, 以实现关键业务目标。IDC成立于1964年, 是 IDG 旗下子公司。IDG 是全球领先的媒体出版、研究咨询和会展服务公司。

