VERITAS

VERITAS ALTA™

云中数据异常检测

监控云数据和用户活动的单一出色工具

异常检测是一种强大的预警系统，旨在跟踪云数据和用户行为，根据发现的异常活动或奇怪行为及时发出警报。从本质上说，它有助于企业及时发现隐患。如今，检测这些异常是保证数据安全的重要措施，因为异常可能表明存在安全漏洞、软硬件问题、客户需求变化或需要立即处理的一系列难题。它的原理是使用统一流程在一组数据中查找异常点或模式。任何偏离既定基线（在预定的容差范围内）的行为都被视为异常。活动监控功能以一组既定的参数和智能指标为基准，对需要立即注意的异常活动向客户发出警报。收到警报后的客户可通过实时更新的管理面板轻松了解当前状况。异常示例包括异常的文件写入活动，这些活动可能表明存在渗透攻击（但也可能是检测到已知的勒索软件文件扩展名），文件访问模式、流量路径改变，甚至不同于常见模式的活动异常激增。及时发出异常通知有利于客户立即采取措施解决问题或减轻影响，为客户争取了宝贵的时间。它的价值体现在让客户及时发现问题或缓解风险影响，快速隔离相应区域，防止入侵造成破坏性损害、停机或其他相关问题。

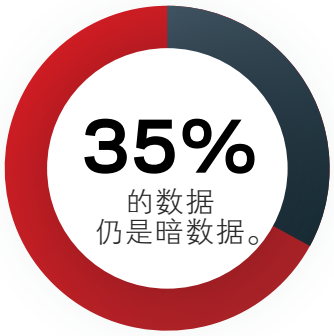
数据守望塔的力量

随着云数据的规模和体量呈爆炸式增长，用户对异常检测的需求也与日俱增，在网络威胁和勒索软件愈演愈烈的局面下，大家都希望检测功能像守望塔一样能够守护所有云数据。一直以来，网络不法分子以各种意想不到的手段盗取系统和数据的访问权限。他们入侵系统后开始加密数据，疯狂地下载数据，然后赶紧逃之夭夭，以免被发现。面对这种情况，异常检测就能立即发出警报，帮助您及时采取应对措施。

云是 2022 年网络罪犯的头号勒索软件攻击载体[1]，如今的网络不法分子经常借鉴一些有组织犯罪攻略中的战术，玩放长线钓大鱼的战略游戏。他们还完善了网络侦察技术。一款名为休眠勒索软件或睡眠勒索软件就是这类反侦察战术的典型代表，在当今的数字世界里屡见不鲜。这意味着，一旦犯罪分子撕开了访问口，就会采取蛰伏战略，保持隐蔽状态。为什么？因为他们的首要任务是观察、学习和在云环境中移动，努力找出平台中的弱点并利用漏洞，同时还要等待最佳攻击时间。在这种情况下，企业若能趁早发现，就能掌握先机解决隐患，采取措施防止出现破坏性影响。

为攫取巨额暴利，实现收益最大化，不法分子总是想着尽可能制造最大力度的破坏，就像做生意一样，他们关心的都是投资回报率。一些报告表明，勒索软件可能休眠长达 18 个月之久。他们也深知，破坏力度取决于多个因素，譬如时机和范围。他们希望受害者别无选择，只能乖乖支付赎金。不过，入侵和攻击同时发生的时代早已一去不复返。攻击手段越来越狡猾就意味着，他们通常比您更了解您的系统。因此，他们会发起一系列精心设计的事件来中断和禁用关键系统，以期实现巨额回报，今后这种可能性越来越高。

跨云数据可见性



不过异常检测实施可以先放一放，企业的当务之急是先确保自己了解所有数据的位置，确保环境中没有潜藏任何暗数据。Veritas《企业 IT 安全脆弱性报告》[2]指出，35% 的数据仍是暗数据。这个数字高得惊人。我们建议企业立即着手调查自己拥有的数据及其存储位置。

Veritas 解决方案以综合性视图显示所有云平台、物理环境和虚拟环境中的全部数据，还以视图显示您的存储空间、计算容量、所有的主数据保护解决方案和交叉报告，这样就可确保系统不会出现任何漏洞。在当今的威胁态势下，这个功能尤为重要，因为网络犯罪分子正是希望您不要详细盘点所有应用程序和数据，或在某些领域对数据的安全保护和/或监督不到位。

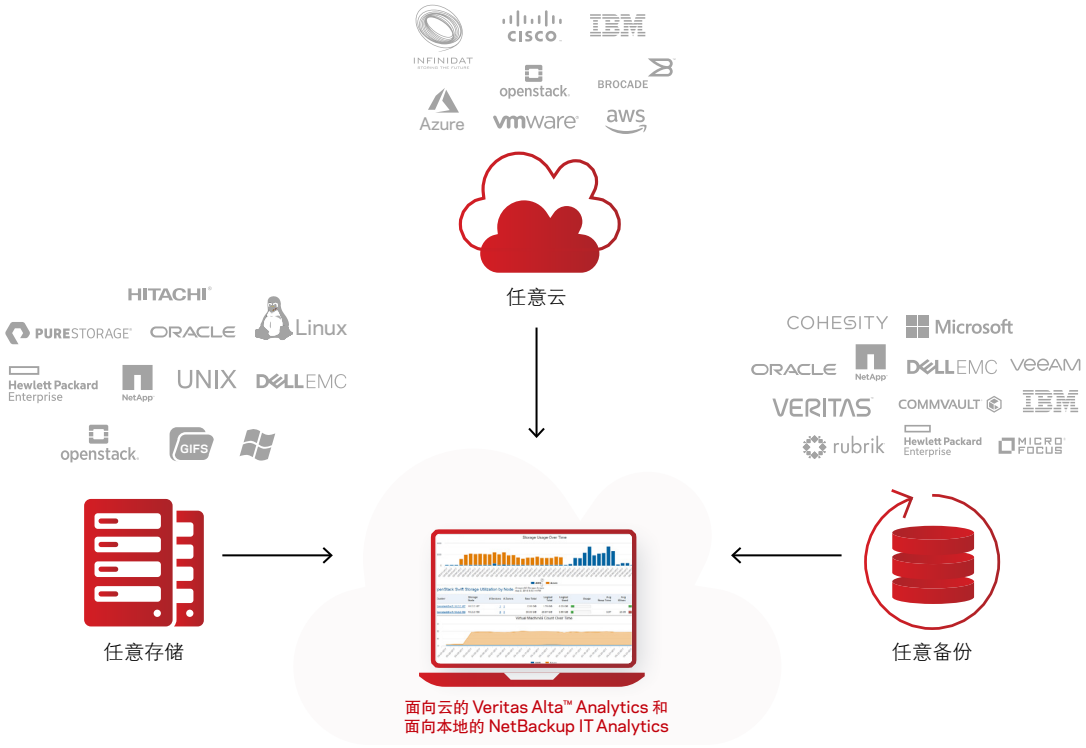


图 1：统一 IT 基础架构可覆盖所有数据，无论数据位于何处

除了照亮环境中的暗数据，Veritas 解决方案还能提供涵盖本地、云、数据保护和存储的全面洞察、警报和报告。借助这份洞察见解，您就能在面对网络攻击时做出明智决策。报告选项可帮助您了解备份环境，从而有助于企业：

- 发现基础架构中的所有主机或虚拟机，并将它们与面向云的 Veritas Alta™ Data Protection 和面向本地的 NetBackup 共同保护的虚拟机进行比较
- 将未纳入备份范围或最近未备份的主机标记为潜在风险。
- 检测可能遭到勒索软件感染的文件，了解它们的大小以及在环境中的位置。
- 访问交互式图表，查看生成的风险记录视图

以人工智能为支持，跨云检测异常

数据可见性到位后，下一步就是实施基于人工智能的异常检测。面向云的 Veritas Alta™ Data Protection 和面向本地的 NetBackup 可检测整个环境中的异常数据和用户活动，并近乎实时地提醒您注意可疑异常。该技术旨在挖掘大量数据，自动执行监控和报告，就环境内正在进行中的活动提供可操作洞察。

您可以将“异常检测”设想为一个测谎仪测试。参加测谎仪测试时，考官将从预筛选开始，他们会提出问一系列问题，确定构成正常基线的参数。撒谎时，预计**血压、脉搏、呼吸和皮肤电导率**等生理指标会波动，超出既定的正常参数范围。同样，面向云的 Veritas Alta™ Data Protection 和面向本地 NetBackup 将利用基于人工智能的检测引擎，根据一段时间内的备份作业元数据模式计算正常状态的参数，并自动调整以自定义备份策略。

捕获超出既定常态模式的事件，并近乎实时地发出通知。根据严重性为观测到的异常分配分数，该分数是根据观测的群集距离值计算得出的。距离越远，分数越严重。这旨在帮助管理员确定哪些洞察是可操作的，有助于减少误报。

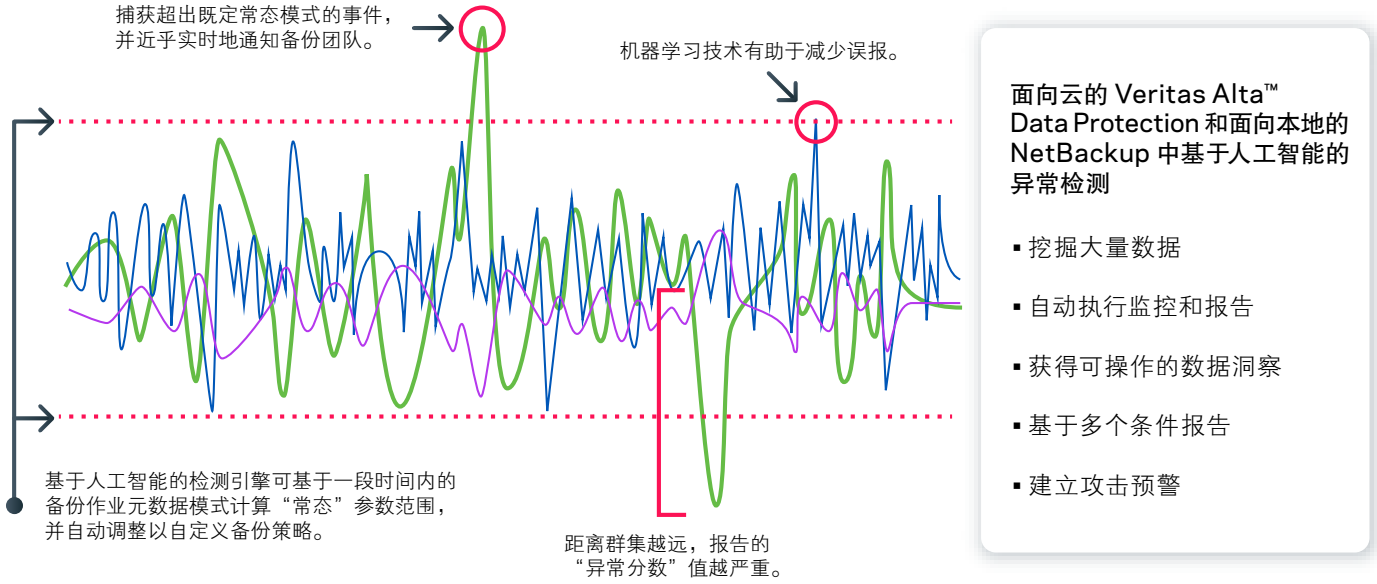


图 2. 了解异常检测

总而言之，基于人工智能的异常检测引擎可帮助您挖掘大量数据，自动执行监控和报告，获得可操作洞察，基于各种条件进行异常报告，更重要的是，可建立攻击预警。通过监控所有设备并对任何攻击建立预警，管理员可以随时查看数据并提供异常相关的建议，随时掌握最新问题。例如，Veritas 人工智能支持的异常检测可无缝集成到主服务器中，从而能够检测异常的观测值，也就是将那些不属于集群的观测值视为异常值。此功能有助于管理员深入调查异常，找出问题所在。它可以挖掘大量数据，提出应对勒索软件事件的可操作洞察，并指出管理员应注意的环境变更。这些解决方案可帮助您识别攻击正在进行或可能即将开始的迹象，有利于您立即采取措施遏制影响。

该工具智能化程度高，可比较历史备份与新备份，并识别异常，例如作业持续时间的显著变化、映像大小变化和/或策略配置更改，以此识别潜在的误报。人工智能引擎可监控文件或文件组，无论文件是在块磁盘还是云中的对象存储中，都能及时了解文件字符发生变更（向下至元数据级别），所有这些都无需后处理。只有 Veritas 解决方案可以扫描和监控所有系统，摆脱任何系统限制，覆盖包括第三方备份产品在内的所有云平台。我们的人工智能/机器学习引擎可在任何服务器上运行。这种级别的覆盖范围有助于消除盲点。

恶意软件扫描

Veritas 解决方案可检测多种类型的恶意软件（如加密型和渗漏型），还提供自动扫描和按需扫描；自动恶意软件扫描功能将消除对人工操作的依赖，允许人工智能/机器学习技术自动扫描恶意软件。较高的异常分数值会自动触发人工智能/机器学习恶意软件扫描。扫描涵盖非结构化数据、Windows、Linux 和 VMware 数据，这个范围至关重要，因为恶意软件通常由主目录进入企业环境，而这些都是大型非结构化数据的存在位置。

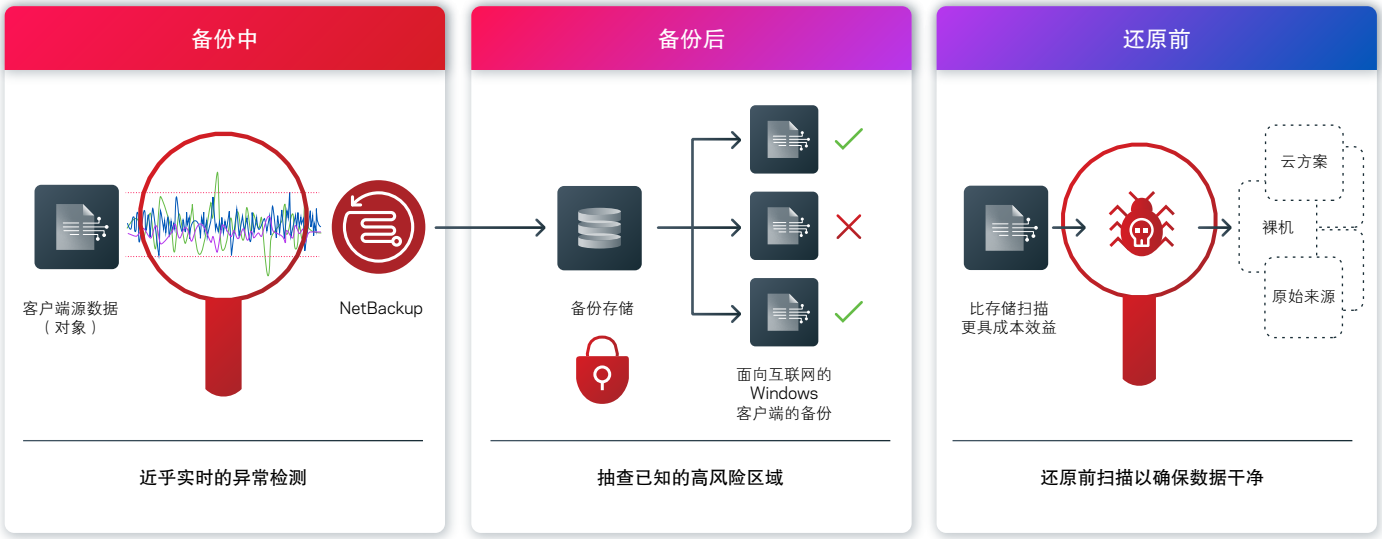


图 3：恶意软件扫描概述

不仅如此，恢复前，备份数据也会经过扫描，确保使用了最新的恶意软件特征码。若备份遭到感染，扫描后会用清晰的图标和警告提示，确保恢复的所有数据是干净的，未遭到感染。这种做法通常称为恢复到上次已知干净的副本。

Veritas 从设计源头保证安全

Veritas 可通过面向云的 Veritas Alta™ Analytics 和面向本地 NetBackup IT Analytics 交付统一的数据可见性、异常检测和恶意软件扫描。下图是管理面板示例。

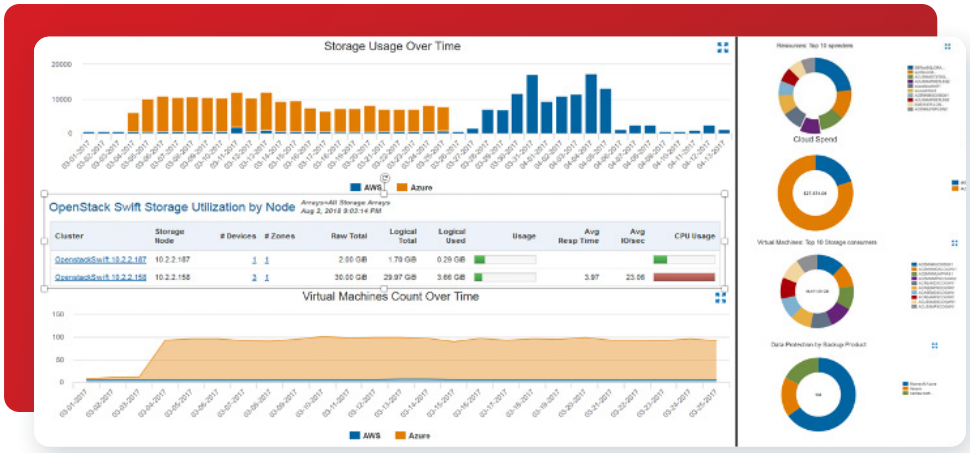


图 4.NetBackup IT Analytics 管理面板示例，显示一段时间的存储使用情况。

Veritas Analytics 属性：

- **全面：**Veritas 单一解决方案通过集成式控制台识别数据资产，面向云的 Veritas Alta™ Analytics 和面向本地 NetBackup IT Analytics 支持当今企业常用的所有服务器、存储、管理程序、数据库和应用程序平台。
- **可扩展：**集中式管理提供无代理数据收集器，从本地和云环境收集约 30,000 个不重复数据点，包括应用程序、云、数据保护、主机、网络、存储、虚拟化和非结构化数据。
- **创新：**专利算法采用了五项自主设计专利，结合云平台领域的更新，可深入分析这些数据点并提出针对性建议，以期提高性能、韧性和利用率。这个分析虽然由机器主导，但要基于人工设置的策略，运用大数据提出可操作的解决方案，帮助改进措施效率，最大限度降低风险，预测故障并简化审计和合规流程。
- **成熟可靠：**十多年来，NetBackup IT Analytics（如今包括面向云的 Veritas Alta™ Analytics）一直凭借久经客户验证的可扩展性和可靠性引领市场，整合并分析整个企业的数据。

Veritas Analytics 关键功能：

- **集成式控制台可提供如下洞察：**
  - 本地和云备份、计算和存储
  - 云和本地容量、成本和使用量
- **成本分摊：**
  - 按用户定义的组分摊成本，如应用程序、部门和成本中心
  - 备份和云、计算和存储等资源的使用情况
- **容量规划：**
  - 基于云成本和使用率规划预算
  - 基于使用率规划介质/存储容量

通过面向云的 Veritas Alta™ Analytics 和面向本地 NetBackup IT Analytics，最大限度发挥云平台的价值

在 Veritas，我们发现企业迁移到云的原因有很多：小型企业看重减少维护数据中心和/或灾难恢复站点开销的优势；中型企业看重在高度可扩展硬件上构建的异地数据存储，不但可随时随地访问，还能运用即时云恢复；大型企业则发现工作负载入云可实现高度可用性和经济实惠优势，同时为关键任务工作负载腾出昂贵的数据中心空间。有时，企业也需要临时空间来处理工作负载，与其在数据中心搭建新的磁盘架构，不如运用云提供商的空间，避免另花成本购买数据中心硬件。云订阅模式带来可扩展、易于使用的模型，是这些临时项目的完美选择。

如今，数据入云大趋势背后的核心诉求是降低企业相关成本。云模型非常灵活敏捷，不仅能满足企业的需求，还能轻松快速地向服务器添加磁盘，而不必采购硬件及其配套的机架和堆栈。云还有利于企业避免投入成本和时间替换或升级数据中心的软硬件。这些都是云服务提供商统统满足的要求，因而企业丝毫感觉不到这类需求的存在。无论企业出于何种原因决定迁移入云，面向云的 Veritas Alta™ Analytics 和面向本地的 NetBackup IT Analytics 都能确保企业始终合规，与本地环境相比，成本效益更高。

Veritas 带来基于人工智能的数据守望塔，让您全面掌控不断扩张的云数据。选择 Veritas，您就能通过单一面板实现所有企业数据的可见性，始终了解自己数据的存储位置，无论数据位于何处。它还能轻松扩展，为 PB 级容量带来一流保护性能，通过便捷的自助服务为 IT 即服务铺平道路。Veritas 的分析解决方案带来数据完全可见性技术、智能异常检测和恶意软件扫描，消除一切不确定性。

跳出云原生工具和单点产品思维，以网络安全和数据保护为重心，构建统一数据管理战略。

Veritas 可赋予您全面掌控云的能力。

1. https://www.esg-global.com/ransomware
2. https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf

关于 Veritas

Veritas Technologies 是多云数据管理领域的领导者。超过八万家企业级客户，包括 95% 的全球财富 100 强企业，均依靠 Veritas 确保其数据的保护、可恢复性和合规性。Veritas 在规模化的可靠性方面享有盛誉，可为企业提供抵御勒索软件等网络攻击威胁所需的弹性。Veritas 通过统一的平台，支持超过 800 种数据源，100 多种操作系统，1400 多种存储设备以及 60 多类云平台。在云级技术的支持下，Veritas 现正在实践其自治数据管理战略，在提供更大价值的同时，降低运营成本。欲了解更多详细信息，请访问 www.veritas.com/zh/cn/ 或关注 Veritas 官方微信平台：VERITAS_CHINA（VERITAS 中文社区）。

北京市朝阳区东大桥路 9 号
侨福芳草地大厦 A 座 10 层
04-05 单元 100020
咨询服务热线：400-120-4816
www.veritas.com/zh/cn

关于全球联系信息，请访问：
veritas.com/company/contact

V1627 12/22