

保护敏感数据

适用于 Vertica 的 Micro Focus® Voltage SecureData

适用于 Vertica 解决方案快速的 Voltage SecureData

Voltage SecureData 是一种全面的数据保护框架，可保护在各种设备、操作系统、数据库和应用程序中捕获、处理和存储的数据。Voltage SecureData 可作为 Vertica + Voltage 插件用于 Vertica。

Vertica 分析平台

Vertica 是一种极快的 SQL 分析数据库，使企业能够在几秒或几分钟（而不是数小时或数天）的时间内从大数据中访问和获取有意义的见解。通过全套高级分析和数据库机器学习提供无与伦比的速度和扩展能力，Vertica 能够为全球大多数数据驱动型企业提供支持。

Vertica 可以就地部署在您自己的数据中心、私有云或公共云中，包括 Amazon、Azure 和 Google 云平台。这种统一的 Vertica 引擎可以在 Apache Hadoop 上进行本地部署。Hadoop 上的 Vertica SQL 可以加速数据探索和 SQL 分析，同时可在组织首选的 Hadoop 发行版上以本机方式运行。

挑战：保护敏感数据

与任何企业数据架构部署一样，您面临着许多安全性和合规性方面的挑战，尤其是在跨多个节点自动复制数据、处理多种类型的数据，或者允许具有不同分析需求的多用户进行访问时。

有时，安全性选项没有以最优方式实施。对于缺乏适当的安全实施，最常提到的原

因是：由于具有复杂、繁琐和侵入性的性质，管理会干扰和拖慢业务。

保护用于分析的使用中的数据

Vertica + Voltage 插件提供了您期望企业系统具备的易于配置的数据安全功能。身份验证和授权只是开始。借助用于 Vertica 的 Voltage 插件，敏感信息的私密性将在整个企业的 IT 基础设施（从通过业务分析应用程序捕获信息到后端数据存储）中受到端到端的保护。这种以数据为中心的方法可满足大数据分析解决方案（如 Vertica）的安全需求。

通过 Voltage SecureData 保留格式的加密和令牌化技术，保护可以应用于数据字段和子字段级别。这将保留数字、符号、字母和数字关系（例如日期和工资范围）等原始数据的特征。此外，它还会在分布式数据集之间保持参照完整性，因此联接的数据表可以继续正常运行。Voltage SecureData 保护静态数据、移动和使用中的数据，因此大多数分析可以在其受保护的表单中基于去识别化数据执行。数据专家无需访问实时支付卡、个人或受保护的健康信息即可提供商业见解。

解决方案亮点

Voltage SecureData 采用经过验证且以数据为中心的独特方法来保护 Vertica 中的敏感数据。它还有助于显著降低合规审计的范围，例如支付卡行业 (PCI) 和美国健康保险便携与责任法案 (HIPAA)。Voltage SecureData 需要去除数据的身份信息，使其尽可能接近其源，从而将敏感数据

元素转换为可用但不可识别的、保留其格式、行为和含义的等效数据元素。这种数据保护形式可用于后续应用程序、分析引擎、数据传输和数据存储，并可为特定应用程序和需要它的用户轻松、安全地重新识别身份。

Vertica + Voltage 插件的优势

- 能够保护数据，使其尽可能接近其源。
- 支持加密、令牌化和数据屏蔽保护技术。
- 数据可以去识别化状态用于许多应用程序。
- 在需要时，能够安全地重新识别数据（仅授权用户和应用程序可进行此操作）。
- 显著减少与 PCI 合规性相关的审计范围和成本
- 符合安全性证明和安全性标准的保护技术。
- 高性能、高可扩展性，而且可与大数据速度完美匹配。
- 广泛的平台和应用程序支持 — Vertica 内部和外部。
- 支持面向欧盟数据主体的新 GDPR（一般数据保护法规）法规中的加密和假名化指导。

来自源的安全性

Voltage SecureData 加密和令牌化保护可在源数据进入大数据分析环境之前应用于源数据。它还可以在提取、转换和加载 (ETL) 传输到定位区或将数据传输到

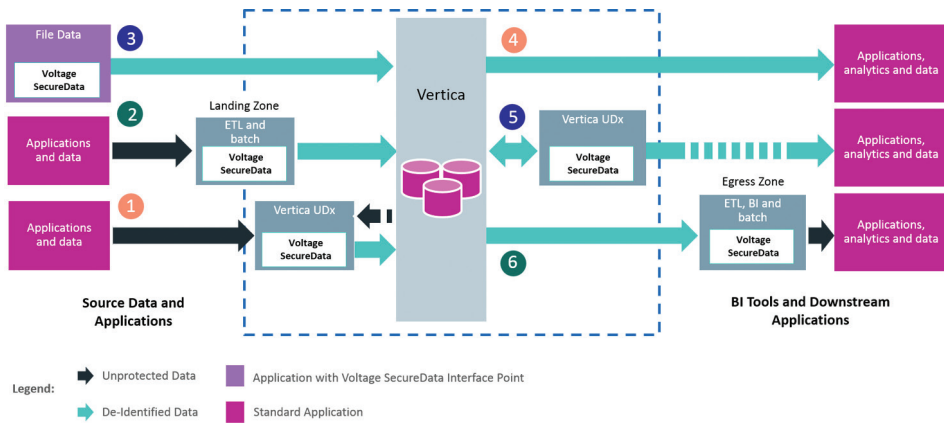


图 1. 用于在 Vertica 分析平台中保护数据的选项

Vertica 分析程序的过程中进行。安全数据进入 Vertica 之后，可以去识别化状态进行额外的处理和分析，而无需进一步与 Voltage SecureData 系统进行交互。如果需要，在 Vertica 上运行的分析程序可以通过适当的身份验证和授权级别，利用 Voltage SecureData 高速解密和去令牌化接口来安全地访问明文。

如果需要将已处理的数据顺利导出到下游流程，例如，要执行诸如客户邮件之类的操作，则在 Vertica 中有多个选项可用于安全地重新识别数据。

工作原理

下面列出了六个使用 Voltage SecureData 保护 Vertica 大数据分析环境中的敏感数据的具体选项：

- **选项 1:** 在 Vertica 数据加载过程中通过 Vertica 的用户定义的扩展 (UDx) 应用数据保护
- **选项 2:** 应用接近应用程序的数据保护
- **选项 3:** 为批量文件加载应用数据保护

- **选项 4:** 在 Vertica 中使用去识别化数据
- **选项 5:** 使用来自 Vertica 的重新识别的数据
- **选项 6:** 在 Vertica 外部 (ETL/BI/Batch) 导出数据并重新识别

关于 Voltage SecureData

Voltage SecureData 推动了以数据为中心的安全和加密解决方案的领先地位。凭借超过 80 项专利和 51 年的专业知识，我们为全球众多高端品牌提供保护，并消除静态、使用中和移动中的敏感数据的违规影响。我们的解决方案提供高级加密、令牌化和密钥管理，可保护企业应用程序、数据处理 IT、云、支付生态系统、任务关键型事务、存储和大数据平台中的敏感数据。Voltage SecureData 解决了业界最大的挑战之一，即如何简化在最复杂的使用情形中的敏感数据保护。

如需了解更多信息，请访问以下链接
www.microfocus.com/securedata
www.vertica.com

联系我们：
www.microfocus.com