CHISTOR DATA Cyber Recovery 防勒索数据保护方案

针对勒索软件为关键数据提供富有弹性的现代保护

概述

为了降低网络攻击造成的业务风险，并制定更具网络弹性的数据保护方法，您可以对恢复和业务连续性战略进行现代化和自动化改造，并利用新的智能工具来检测和抵御网络威胁。DATA Cyber Recovery 防勒索数据保护方案为您的数据提供有效的保护方案。

DATA Cyber Recovery 防勒索数据保护方案提供经验证的智能保护，可隔离关键数据、识别可疑活动、加快数据恢复，助您以更智能的方式恢复关键数据，从而快速恢复正常的业务运营。

不可变性、隔离和智能

不可变性

BD 备份存储是 DATA Cyber Recovery 防勒索数据保护方案的基础。它采用多层零信任安全性，可以提供不可变的备份副本，以确保数据的完整性和机密性。硬件信任根、安全启动、加密、保留锁、基于角色的访问和多因素身份验证等功能可助您确保数据的可恢复性。

隔离

DATA Cyber Recovery 防勒索数据保护方案存储区是隔离的环境，具有多层保护，可提供应对网络攻击（甚至包括内部威胁）的抗风险能力。其自动数据隔离功能可将关键备份数据（包括开放

系统和大型机）安全地复制（同步）到物理隔离的存储区中，远离生产攻击面，绝不会将管理路径暴露给威胁行为者。接下来，一个不可变副本将自动创建，以防止数据被修改。由于专用的管理、网络和服务独立于生产环境，因此需要单独的安全凭证和多因素身份验证才能访问数据以进行恢复和测试操作。

智能

DATA Cyber Recovery 防勒索数据保护方案是集成了 CyberSense 的解决方案，可针对网络威胁进行更智能的恢复。所有这些都在 DATA Cyber Recovery 防勒索数据保护方案存储区的安全环境中进行。CyberSense 超越了纯粹的元数据解决方案，通过完整内容分析，它可以检测攻击后的数据损坏情况，准确率达 99.99%，并且促进智能、快速恢复。CyberSense 利用不可变的数据备份来观察数据在不同时间的变化，并利用基于 AI 的机器学习来检测遭到勒索软件攻击的损坏迹象。

CyberSense 可检测核心基础架构（包括 Active Directory、DNS 等）、用户文件和数据库中由复杂攻击导致的批量删除、完全和部分加密以及其他可疑更改。您可以创建自定义的阈值警报。如果检测到数据损坏的迹象，警报控制面板和攻击后取证报告可帮助快速诊断攻击的规模和影响，包括识别可用于恢复关键系统的干净数据副本。自定义规则和恶意软件签名搜索有助于实现定制操作并授权组织主动防御网络威胁。

部署选项

混合云和多云环境中的部署

关键数据可能存在于企业中的许多不同位置，可能在本地，可能托管在不同的数据中心内，也可能位于全球的多个云和区域。当需要从网络攻击中进行恢复时，无论数据位于何处，都必须确保安全且无损。

DATA Cyber Recovery 防勒索数据保护方案可通过 AWS、Microsoft Azure 等公有云市场获取和购买，以快速保护云中 DATA Cyber Recovery 防勒索数据保护方案存储区中的数据。DATA Cyber Recovery 防勒索数据保护方案可在生产系统与公有云中的 DATA Cyber Recovery 防勒索数据保护

方案存储区之间自动执行关键数据同步。与基于云的标准备份解决方案不同，对管理接口的访问被网络控制措施锁定，需要单独的安全凭据和多因素身份验证才能访问。跨多个云散布和复制数据的做法可能会导致安全和合规风险、潜在的同步问题以及更高的资源成本。这种做法还会降低您对各种环境的了解程度，导致无法充分抵御不断变化的网络威胁。

在 BD 全闪存备份节点中部署

随着关键数据的持续增长，快速高效地从网络事件中恢复的能力对于确保业务连续性和网络弹性至关重要。那些正在扩展关键数据管理的组织必须能够很好地从隔离的恢复环境检索数据。BD 全闪存备份节点提供经过简化、节能且经济实惠的网络恢复解决方案，具有增强的 CyberSense 分析和快速恢复功能，可满足组织 SLA 要求。通过减少使用的硬件、空间和能源，组织可以加快数据访问速度，提高运营效率并确保数据完整性，最终缩短停机时间并降低总体维护成本。

恢复业务运营

恢复和修正

DATA Cyber Recovery 防勒索数据保护方案可提供自动化还原和恢复流程，使业务关键型系统能够快速、可靠地恢复正常运行。恢复融入事件响应流程之中。发生事件后，事件响应团队将通过分析生产环境找出根本原因。CyberSense 提供攻击后取证报告，以便了解攻击的深度和广度，并提供损坏之前最后良好备份集的列表。然后，当准备好执行生产环境的恢复时，DATA Cyber Recovery 防勒索数据保护方案会提供执行实际数据恢复所需的管理工具和技术。

优势

网络攻击的意图在于损害您的宝贵数据，包括您的备份。保护您的关键数据并以有保障的完整性来恢复数据，是在攻击后恢复正常业务运营的关键。

网络弹性解决方案包括以下组件：

- 数据不可变性：创建不可更改的数据副本，通过多层安全和控制保持数据完整性和机密性

- 自动数据隔离：自动将不可更改的数据副本从生产备份环境隔离到具有更高限制访问权限的安全数字存储区
- 智能分析：使用基于 AI 的机器学习和完整内容索引编制进行的自动化完整性检查，以及在安全存储区内进行的强大分析，用以确定数据是否受到恶意软件的影响
- 恢复和修正：使用动态还原过程和您现有的灾难恢复程序在事件发生后执行恢复操作的工作流和工具
- 解决方案规划和设计：提供专家指导，帮助选择关键数据集、应用程序和其他重要资产，以确定 RTO 和 RPO 并简化恢复

CyberSense

CyberSense 是基于 AI 的分析和取证工具，助力检测和诊断网络攻击并更智能地实现恢复。随着网络攻击频率的持续上升和网络犯罪分子的弹性越来越强，传统的安全工具在保护数据免受网络攻击方面已无法满足要求。

CyberSense 可检测攻击发生后的数据损坏情况，并有助于实现智能而快速的恢复。作为全球数千家组织的最后一道防线和第一道恢复线，CyberSense 可确保组织数据资产的完整性，保障数据不会受到恶意损坏，让客户放心无忧。

CyberSense 可扫描 DATA Cyber Recovery 防勒索数据保护方案存储区中的数据备份，以观察数据如何随时间变化。然后，它利用机器学习和 AI 来检测指示勒索软件攻击的损坏迹象。它会将该数据与 200 多项内容分析进行比较以发现损坏的数据，其准确率高达 99.99%，可帮助您保护业务关键型基础架构和内容。CyberSense 可检测核心基础架构（包括 Active Directory、DNS 等）、文件存储库、文件系统和关键数据库中由复杂攻击导致的批量删除、加密和其他可疑更改。

当发生可疑行为时，CyberSense 会提供攻击后取证报告，以诊断网络攻击的影响范围。检测到数据损坏时，CyberSense 可提供最后一批已知完好的备份数据集的列表，以支持快速、有序的恢复，帮助您尽可能减少业务中断和数据丢失，从而降低网络恢复成本。

DATA Cyber Recovery 防勒索数据保护方案工作流

CyberSense 与 DATA Cyber Recovery 防勒索数据保护方案无缝集成，能够主动监视文件和数据库，并通过分析数据的完整性来检测勒索软件造成的损坏。将数据复制到 DATA Cyber Recovery 防勒索数据保护方案存储区并应用保留锁后，CyberSense 会自动发起对备份数据的全面扫描，从而创建文件、数据库和核心基础架构的时间点观察结果。CyberSense 可细致地跟踪文件在不同时间发生的变化，即使是面对最复杂的网络威胁，也能有效地发现数据损坏。

完整内容分析

CyberSense 是一款出色的产品，可对所有受保护数据进行完整内容索引编制和分析。CyberSense 深度 AI 分析贯穿整个数据，并以 99.99%的准确率生成概率决策，以确定数据是否具有完整性或是否被勒索软件破坏。此功能使 CyberSense 从众多解决方案中脱颖而出，因为其他解决方案只能大概了解数据，并使用分析寻找基于元数据的明显损坏迹象。元数据级别的损坏不难检测；例如，将文件扩展名更改为 .encrypted 或大幅更改文件大小。但这些类型的攻击并不能代表当今网络犯罪分子所使用的复杂攻击。

CyberSense 超越了纯粹的元数据解决方案，并使用完整内容分析来检测数据损坏。它会审核文件和数据库以查找指示攻击的更改，包括全部或部分文件损坏。传统分析会错过这些威胁，从而导致误判。用户可以根据文件中的更改、添加的文件或删除的文件来设置自定义阈值警报。您还可以实施自定义规则和恶意软件签名，以便对备份中的恶意软件进行前向和后向检测。

支持的数据类型

CyberSense 可针对各种数据类型生成分析，包括 DNS、LDAP、Active Directory 等核心基础架构，文档、合同、知识产权等非结构化文件，以及 Oracle、DB2、SQL、PostgreSQL、Epic Caché 等数据库。