DELL Technologies

解决方案简述

适用于 Dell PowerProtect Cyber Recovery 数据避风港的 CyberSense®

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

Cybersense 的优势

CyberSense® 与 Dell PowerProtect Cyber Recovery 数据避风港存储区解决方案全面集成。

- 自动定期扫描备份数据以验证数据完整性并在检测到可疑行为时发出警报。
- 直接扫描来自 Dell Avamar、NetWorker、Commvault、NetBackup 和 PowerProtect Data Manager 的备份映像中的内容，而无需解冻数据。
- 在每次数据扫描时提供深入的完整内容分析，以检测极复杂的勒索软件攻击。
- 针对 YARA 规则和恶意软件签名的自定义警报，以检测勒索软件或内部不良行为者的已知行为。
- 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，推动实现更智能、更快速的恢复。

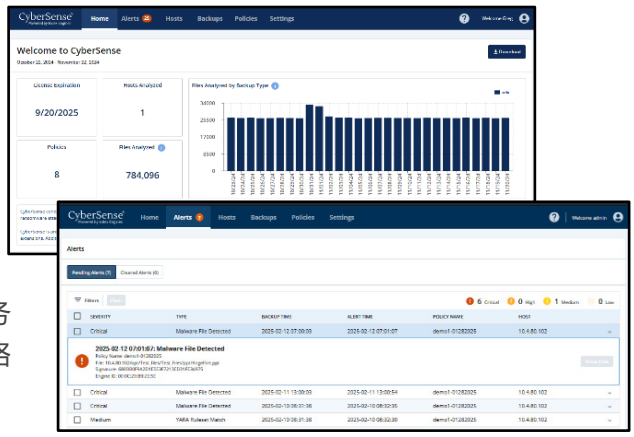
CyberSense 与其他数据分析方法不同，它可以让您更加信任备份数据的完整性，并在攻击发生后快速恢复。

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（包括核心基础架构、数据库和关键文档）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 Cyber Recovery 数据避风港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。



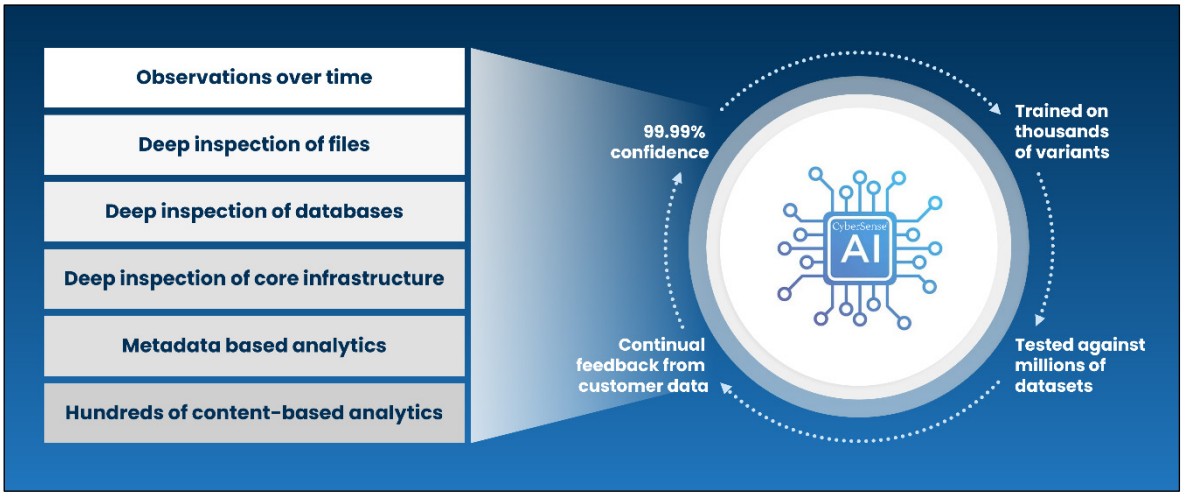
Cyber Recovery 数据避风港工作流

CyberSense 与戴尔 PowerProtect Cyber Recovery 数据避风港无缝集成，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 Cyber Recovery 数据避风港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。

© 2025 Dell Inc. 或其子公司。

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 YARA 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。

摘要

CyberSense 与 Dell PowerProtect Cyber Recovery 数据避风港全面集成，可分析您的存储区数据并检测损害和损坏的行为指标。您可以通过 CyberSense 主动了解正在发生的网络攻击的影响范围，推动实施快速诊断和恢复计划，从而减少业务中断以及由此产生的巨额费用。

详细了解 Dell PowerProtect Cyber Recovery 数据避风港

联系 Dell Technologies 专家

详细了解 CyberSense

加入 #PowerProtect 对话

* 基于 Index Engines 委托撰写的一份 ESG 报告：《Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption》。2024 年 6 月

© 2025 Dell Inc. 或其子公司。保留所有权利。Dell 和其他商标是 Dell Inc. 或其子公司的商标。其他商标可能是其各自所有者的商标。