DELL Technologies
戴 尔 科 技 集 团

白皮书

利用机器学习分析检测勒索软件导致的
数据损坏

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

由 Index Engines 提供支持

实时网络安全解决方案旨在抵御攻击，但这些解决方案并非万无一失，每天依然在发生企业数据遭到破坏的情况。CyberSense 在这些实时解决方案之外再添一层保护，可以及时地发现攻击成功侵入数据中心时所造成的损坏。

CyberSense 可帮助您恢复正常业务运营

2022年6月

 © 2022 Dell Inc. 或其子公司。

目录

 © 2022 Dell Inc. 或其子公司。

为何选择 CyberSense？为什么是现在？

66%

的组织在2021年受到勒索软件的攻击[1]

只有实时安全保护还不够

勒索软件正在绕开现有的安全保护产品，并且攻击次数不断增长

20天

的平均停机时间发生在2021年的勒索软件攻击之后，而2020年为15天[2]

停机时间不断增加

组织在遭受攻击后很难进行恢复

***Sabbath* 勒索软件团伙的目标是关键基础架构、备份[3]**

备份不可靠

备份和备份数据很容易遭到新的勒索软件变体的破坏

组织在实时防病毒产品和数据中心安全应用程序上投入了大量资金。随着时间的推移，许多组织又在其数据中心内添加了数十个这样的内联应用程序，但是勒索软件攻击及其导致的停机却呈上升趋势。

如何攻击？网络罪犯通过升级变种的攻击，使其变得更加复杂诡诈，以此来绕开现有安全保护。以前，他们依靠非常基本的变种来加密文件、附加扩展名，或其它能被安全工具检测到的明显操作。2021 年，攻击涉及更加复杂的损坏，包括部分加密、实际击键更改以及隐藏在文件和数据库中的更难检测到的内容更改。

而且，他们会攻击关键数据资产，包括：

- 核心基础架构，包括 Active Directory、DNS 和 LDAP
- 生产数据库，包括 Oracle、DB2、SQL、IRIS 和 SharePoint
- 用户文件，包括合同、财务文档以及知识产权
- 备份，加密和损坏备份映像

他们这样做的目的是什么？答案就是，尽可能加大恢复的难度，乘机勒索更高的赎金。

[1] Sophos《2022 勒索软件现状》：https://www.sophos.com/zh-cn/content/state-of-ransomware

[2] Statista《Average duration of downtime after a ransomware attack from 1st quarter 2020 to 4th quarter 2021》：https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/

[3] https://securityintelligence.com/news/sabbath-ransomware-critical-infrastructure-backups/

 © 2022 Dell Inc. 或其子公司。

CyberSense: 现有安全解决方案被突破后的最后一道防线

大多数组织都部署了数十种安全工具（例如防火墙）来抵御网络攻击并保护其数据。最常用的工具之一就是防病毒软件。防病毒软件在生产环境中运行，而后者便是勒索软件的主要攻击面。防病毒软件的设计原理是在创建或更改程序和文件时对它们进行实时扫描，并将它们与已知的病毒特征码进行比较。集成了病毒扫描功能的备份软件，可以成为抵御网络攻击的另一层保护。通过在生产环境中扫描备份内容来寻找恶意软件，可以提供额外的防御，但是备份仍然直接位于网络攻击的攻击面上。

防病毒软件是必不可少，但并非 100% 有效。如果没有检测到恶意软件怎么办？许多攻击都是手动干预的实际击键。因此，数据未被损坏，而且防病毒软件对攻击一无所知。网络罪犯花费大量资源来开发绕过这些安全工具的技术，并重点攻击生产备份环境，包括具有集成式病毒扫描的备份环境。需要最后一道防线来检测何时发生损坏，诊断相关活动，并推进还原过程。

CyberSense 并不能取代现有的实时安全应用程序或病毒扫描，而是对这些应用程序形成有效补充，并与戴尔 PowerProtect Cyber Recovery 数据避风港全面集成。在 Cyber Recovery 数据避风港存储区中，CyberSense 提供 PB 级备份映像扫描，旨在检查数据的完整性，并检测加密、大量删除和数据损坏等可疑行为。CyberSense 会不断检查您的数据，寻找勒索软件破坏的迹象，并在破坏开始时发出警报。当发生攻击时，CyberSense 会提供攻击后取证报告来诊断损害，并报告已知良好的最新文件，帮助快速恢复。

CyberSense 的核心是分析和机器学习。CyberSense 通过查看您的数据在一段时间内的观测结果来生成数以千计的分析结果，然后将它们馈送给功能强大的机器学习演算法来确定数据是正常还是可疑。当发现数据被损坏时，会为其加上标记。然后，提供有关这些损坏文件的报告，并随附已知良好的最新备份拷贝。它知道损坏的数据位于何处，已知良好的数据最新版本位于何处，以及数据在哪个备份集中，因此能够简化恢复过程。

使用 CyberSense，组织可以免受网络罪犯摆布。他们可以利用现有的灾难恢复资源，快速地将业务恢复到稳定状态。要实现放心无忧的检测和恢复，CyberSense 是您的不二之选。

利用 CyberSense 可以:

- 验证数据完整性
- 确保数据完好，让您安心无忧
- 在检测到损坏迹象时发出警报
- 报告已知良好的最新备份，以便进行还原

 © 2022 Dell Inc. 或其子公司。

CyberSense 的优势

CyberSense 是同类产品中罕有的能够对所有受保护的数据部署完整内容分析的解决方案。唯有如此，您才能确保数据完整性，防止网络罪犯绕开您的数据安全工具，隐藏行迹并偷偷损坏您的数据。要了解不法分子如何损坏数据，您首先需要了解文件的结构。

文件包含三个主要组成部分：

- **元数据：** 文档属性，包括文件大小、扩展名和名称。
- **标题：** 内容标题，其中包含真实文件类型和文档结构。
- **内容：** 文件内容或数据库中页面的内容。

如果基本类型的恶意软件能够得逞，网络罪犯一开始就会如此部署。基本类型的攻击集中在影响文件元数据的损坏上。相关更改包括附加 .wcry 或 .locky 文件扩展名，或由于文件损坏导致文件大小发生较大变化。这些基本类型的损坏很容易被检测到。如果供应商只对元数据进行分析，就只能发现影响文件属性的明显损坏迹象。当这些攻击被检测到时，网络罪犯将继续发起更高级的攻击类型。高级攻击的重点是偷偷损坏文件或数据库页面的内部。这些攻击很难被检测到。它们包括损坏文件或数据库的标题或内容的恶意软件。其他类型的损坏会更改文件结构，并对文件或数据库页面的内部内容进行全部或部分加密，以避免被检测到。

如果仅对元数据进行分析，这两种类型的高级损坏都很难被检测到。甚至有些勒索软件（例如 JigSaw）会在文件名后面加上一个有效的文件扩展名（例如 .fun）来造成混淆。元数据扫描将检测到这是一个有效的扩展名，并导致漏报。而 CyberSense 内容分析会读取标题，并检测到文件类型不准确。

为弥补分析上的不足，只基于元数据进行分析的供应商引入阈值来获得文件更改情况的概要视图。当文件更改数量（例如大小）或删除数量超过日常的正常范围时，阈值分析即会发出警报。阈值和元数据属性可以根据经验推测可疑行为，并发送警报。这样容易导致误报。

CyberSense 利用超过 200 项基于完整内容的分析，这些分析可指示由于勒索软件攻击导致的损坏类型。其他解决方案基于元数据，而不是完整内容。因此，它们只有基于元数据的依据，最多涵盖约 12 项分析属性，而 CyberSense 有超过 200 项分析。这种全面的洞察力消除了对可疑行为的不确定性，在查找因攻击导致的损坏方面，诊断可信度达到 99.5%[1]。

如果数据库对于您的业务至关重要，那么 CyberSense 是您的不二之选

 © 2022 Dell Inc. 或其子公司。

[1]基于戴尔在 2022 年 6 月对公开数据进行的分析。实际结果可能有所不同。

强大的机器学习

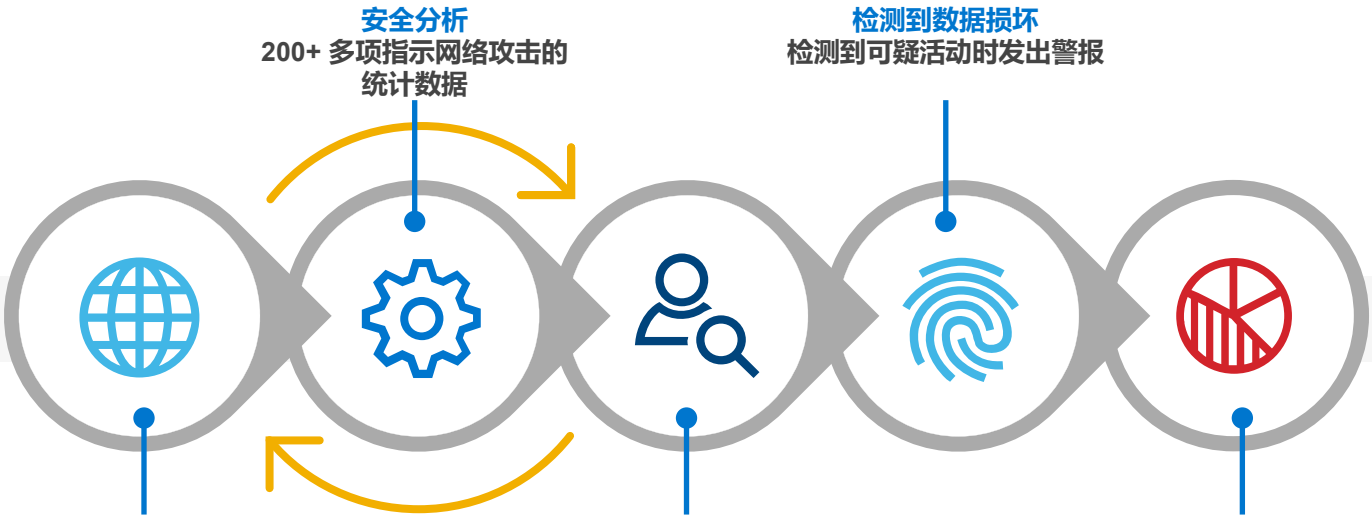
超过 200 项分析
一段时间内的数据观测结果
利用数以千计的恶意软件进行训练

- **检测异常模式**
- **区分用户活动与勒索软件破坏活动**
- **更大限度地减少误报和漏报**

功能强大且具有确定性的机器学习是 CyberSense 的“心脏”和“大脑”。CyberSense 将超过 200 项分析（是同类产品的 20 倍）与随时间推移，通过更多的观察而越来越智能的数据观测结合在一起。此外，机器学习基于数以千计的恶意软件感染进行训练，能发现异常行为模式，并区分用户活动与勒索软件行为，同时更大限度地减少误报和漏报。

机器学习利用 CyberSense 实验室的研究成果得到了进一步的训练，其中包括新的攻击变种。此外，机器学习会根据来自现有 CyberSense 客户端的真实数据进行更新。具体过程为：通过一个安全的数据二极管从 Cyber Recovery 数据避风港存储区导出 CyberSense 分析，然后将它们发送给 CyberSense 开发团队。这些分析被用于进一步训练机器学习模型，然后将产生的更新提供给所有 CyberSense 客户端。

以下是将数据同步到存储区后，CyberSense 工作流的编排。



1. **全面索引:** 在内容级别为备份映像创建索引
2. **安全分析:** 超过 200 项分析，指示针对每个映像收集的损坏迹象
3. **机器学习:** 利用分析，将当前备份与先前的备份进行比较
4. **重复执行:** 如果未发现损坏，对每个新的备份映像副本重复执行先前的步骤
5. **检测到损坏:** 如果检测到损坏，则向控制面板发送警报
6. **攻击后取证:** 报告有关人员、事件、位置和时间的详细信息，以帮助进行恢复

 © 2022 Dell Inc. 或其子公司。

CyberSense 对比其他解决方案

许多其他备份供应商在其产品中添加了某种类型的元数据分析功能。理论上听起来可行，而且在使用时看起来很简单，但它们会导致漏报和误报，带来错觉。用户可能会开始忽略它们，并将它们视为“正常”现象。事实证明，在面对当今的高级攻击时，这些分析并不可靠。

CyberSense: 完整内容分析

超过 200 项分析，在文件、数据库和核心基础架构中查找损坏迹象

其他解决方案: 元数据分析

元数据分析至多包含约 12 项分析，并且仅限于对文件的分析。数据库等其他关键数据资产并未包括在内

CyberSense：高级机器学习

针对数以千计的恶意软件和特洛伊木马进行了训练，以检测预示勒索软件攻击的异常模式

其他解决方案：（未经）训练过的猜测

使用基本分析和阈值来确定是否发生了异常行为

CyberSense: 全面洞见

利用深度分析来训练机器学习模型，在损坏检测方面达到 99.5%[1] 的可信度

其他解决方案: 有限的洞见

元数据分析加阈值所提供的洞见较为低级，很容易被绕开，并产生漏报

 © 2022 Dell Inc. 或其子公司。

[1]基于戴尔在 2022 年 6 月对公开数据进行的分析。实际结果可能有所不同。

我们能够发现其他解决方案无法识别的许多新型攻击。以下便是轻型分析工具无法检测到的灰色区域的一些变体：

- **缓慢损坏：** 隐藏在阈值“雷达”下
- **附加文件扩展名：** 需要读取文件标题来确认
- **部分加密：** 微妙地损坏文件内容
- **大量删除/创建：** 文件数量不变

通过 CyberSense，您可以分析备份以及一段时间内的数据变化，每一次观察，每一次备份，都是对数据的一次了解。挑战在于确定哪些更改是正常的用户活动，哪些更改是勒索软件破坏的迹象。

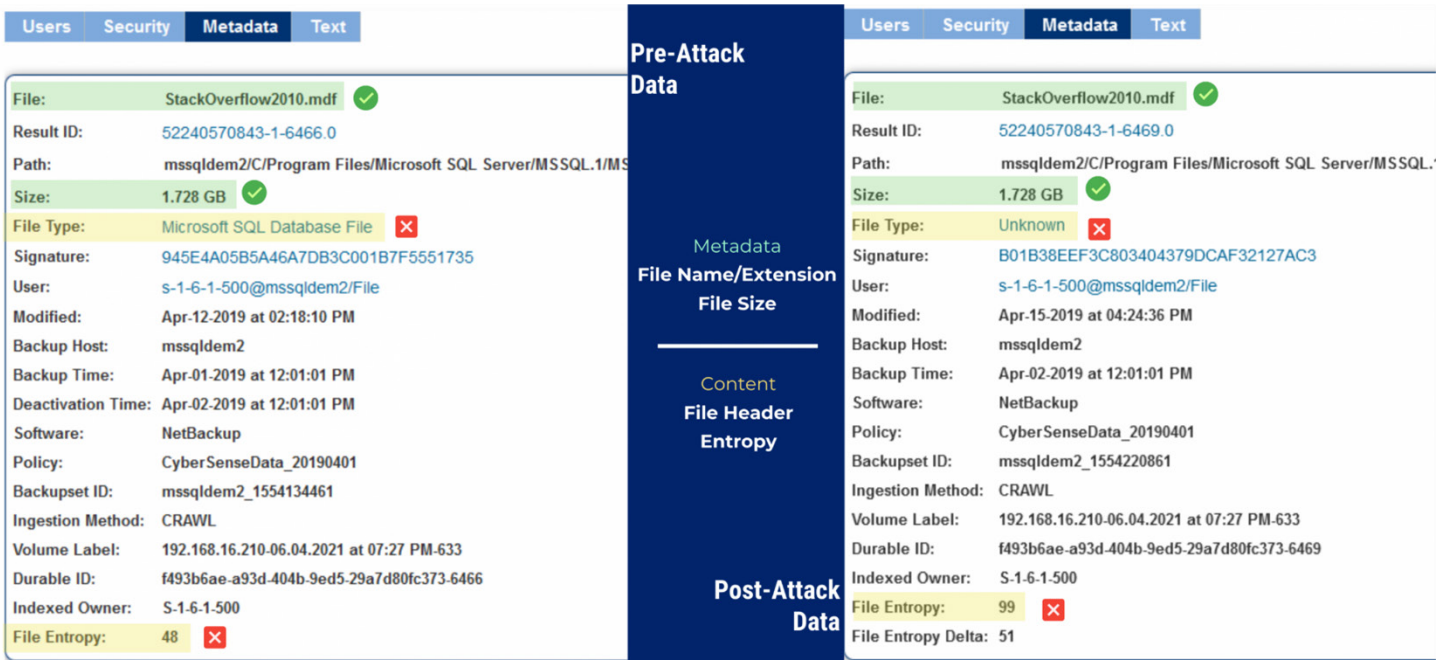
用户在日常活动中以及网络罪犯在进行恶意活动时都会添加、删除或加密文件。正确地区分它们是一项挑战。很明显，附加诸如 .encrypted 等文件扩展名是网络攻击行为。创建一系列文件显然是正常用户行为。然而，让网络罪犯得以藏匿的灰色区域很广，他们在那里进行的更改难以被检测到，也很难确定是正常用户行为还是恶意损坏。新的勒索软件变体将此灰色区域作为主要目标，因为它们更加难以被检测到。而使用 CyberSense 的完整内容分析、智能和机器学习来检查数据，甚至可以在文件更改的灰色区域检测出损坏。

我们怎么知道 CyberSense 在检测由于勒索软件或网络攻击造成的损坏方面具有如此高的准确度？我们利用最新恶意软件和特洛伊木马对 CyberSense 进行持续测试。在测试中使用了 2000 多万个备份集，看看 CyberSense 能否发现损坏。在学术研究和诸如 VirusTotal 等其他来源中发现新变体时，我们会下载并执行这些变体，在对数据造成损坏后，使用 CyberSense 进行测试。除了这些测试之外，CyberSense 还从终端用户安装群获取大量分析，以验证损坏警报的可信度。这些方法结合在一起，在检测现有和新的勒索软件变体造成的损坏方面达到了 99.5%[1] 的准确度。使用其他解决方案，或许能够检测到明显的用户数据损坏迹象。但是，在网络罪犯隐藏踪迹的灰色区域，它们很难（而且往往无法）发现深藏的损坏，这对检测构成了挑战并导致误报，更麻烦的是，还会出现漏报的情况。

 © 2022 Dell Inc. 或其子公司。

[1]基于戴尔在 2022 年 6 月对公开数据进行的分析。实际结果可能会有所不同。

CyberSense 的实际应用



攻击后恢复

AlphaLocker 勒索软件就是高级损坏的一个示例。该勒索软件会对文件内容进行加密，同时保留原始元数据。在上图中，您可以看到文件攻击前和攻击后版本的示例。

在检查文件信息时，您可以看到以绿色突出显示的文件名和大小在攻击前后保持不变。基本元数据分析工具会看到这些属性，并推断文件依然完整。

使用 CyberSense 基于内容的分析进行更加深入的检查，会发现以黄色突出显示的文件类型现在已损坏，并且熵值增加到 99，表示存在加密。CyberSense 中的机器学习会识别到该文件无法键入内容，并且对内部结构进行验证得到的熵值较高，随后便会生成警报。

目前，市场上有许多勒索软件可以避开那些只包含基本元数据分析的工具，例如，JigSaw 和 CyrpMIC。这两种类型的勒索软件不会更改元数据，而主要损坏文件或数据库页面的内部内容。

除了检测由于勒索软件导致的数据损坏，确保恶意软件在恢复过程中不会还原也至关重要。在执行恢复时，CyberSense 可以搜索相关备份集以确定文件或目录是否存在。在还原备份之前，可以使用文件签名、文件名或目录/路径对备份执行搜索。如果检测到勒索软件，可以删除这些文件或目录，防止造成进一步的损坏。

 © 2022 Dell Inc. 或其子公司。

了解

何时 发生了攻击

具体 攻击情况

谁 是攻击的对象

如何 恢复

当发生攻击时，至关重要的是进行诊断并从攻击中恢复，尽快使业务运营恢复到稳定状态。当备份数据同步到存储区时，会为其创建索引以确定是否检测到损坏。如果检测到损坏，系统将发出警报，以便贵组织可以快速开始恢复过程，并尽可能缩短业务停机时间。

尽可能缩短业务停机时间

了解何时发生了攻击
在备份周期中检测是否出现损坏

具体攻击情况
攻击的对象、具体情况、位置和时间

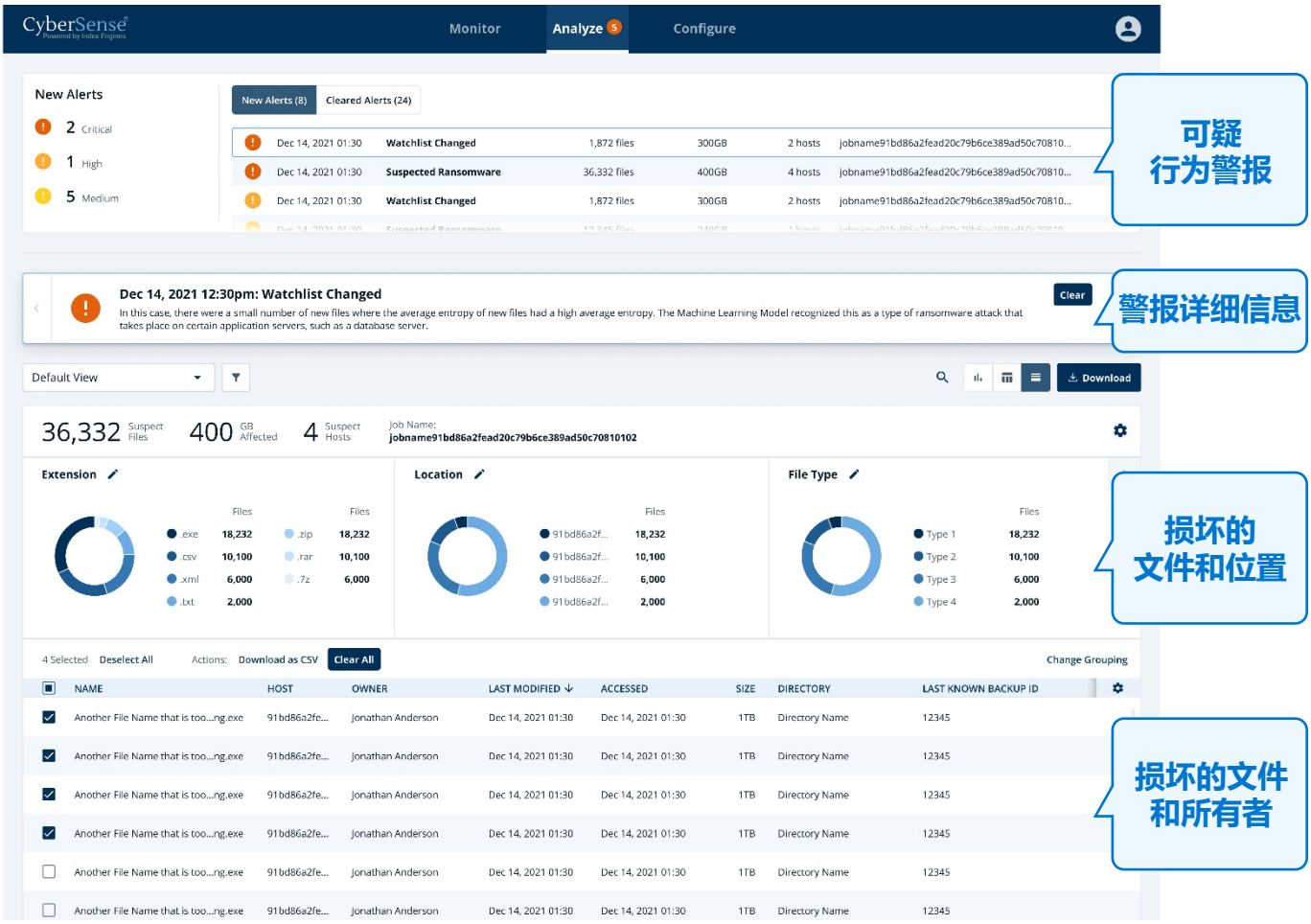
如何恢复
列出可以快速恢复的攻击前干净备份数据版本

CyberSense 将提供以下洞见：

- 谁受到影响，以及对哪些服务器造成了多大程度的损害
- 遭受攻击的内容，按路径、所有者和部门列出文件
- 攻击来源所在的位置，包括受到攻击的用户帐户和相关勒索软件
- 被损坏文件的干净可恢复的最新备份版本

 © 2022 Dell Inc. 或其子公司。

利用 CyberSense 的全面报告功能，可使攻击无处遁形。您将获得用于确定安全可靠的行动方案所需的全部详细信息。在下面的 “Analyze” 控制面板中，您会看到可疑行为警报、警报详细信息、损坏文件所有者等信息。该控制面板提供了关键数据完整性的全面视图，可帮助您尽快恢复业务运营。

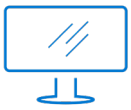


总结

组织需要层层保护来实现网络弹性。防病毒软件作为其中的一层保护，在检测病毒特征码方面非常有效。但是，未使用病毒特征码的网络攻击可能会被漏掉，并导致严重的业务中断。因此，除了防病毒应用程序之外，还需要 CyberSense 的完整内容分析、机器学习和异常模式识别检测，才能有效地抵御网络攻击。适用于戴尔 PowerProtect Cyber Recovery 数据避风港的 CyberSense 作为最后一道防线，可以简化遭受网络攻击后的恢复过程。**检测、诊断、恢复** — CyberSense 让您安心无忧。

无需支付高昂的赎金！
不再任由网络罪犯摆布！

CyberSense 助您快速恢复业务运营 .



详细了解 适用于戴尔 PowerProtect Cyber Recovery 数据避风港的 CyberSense

联系 Dell Technologies 专家

详细了解 戴尔 PowerProtect Cyber Recovery 数据避风港

版权所有©2022 Dell Inc.或其子公司。保留所有权利。戴尔、戴尔标志、Dell Technologies, Dell, EMC, Dell EMC 和其他商标是 Dell Inc. 或其子公司的商标。其他商标权益归属其商标所有者所有。本案例分析仅供参考。如有更改，恕不另行通知。戴尔对本案例分析不作任何明示或暗示的担保。