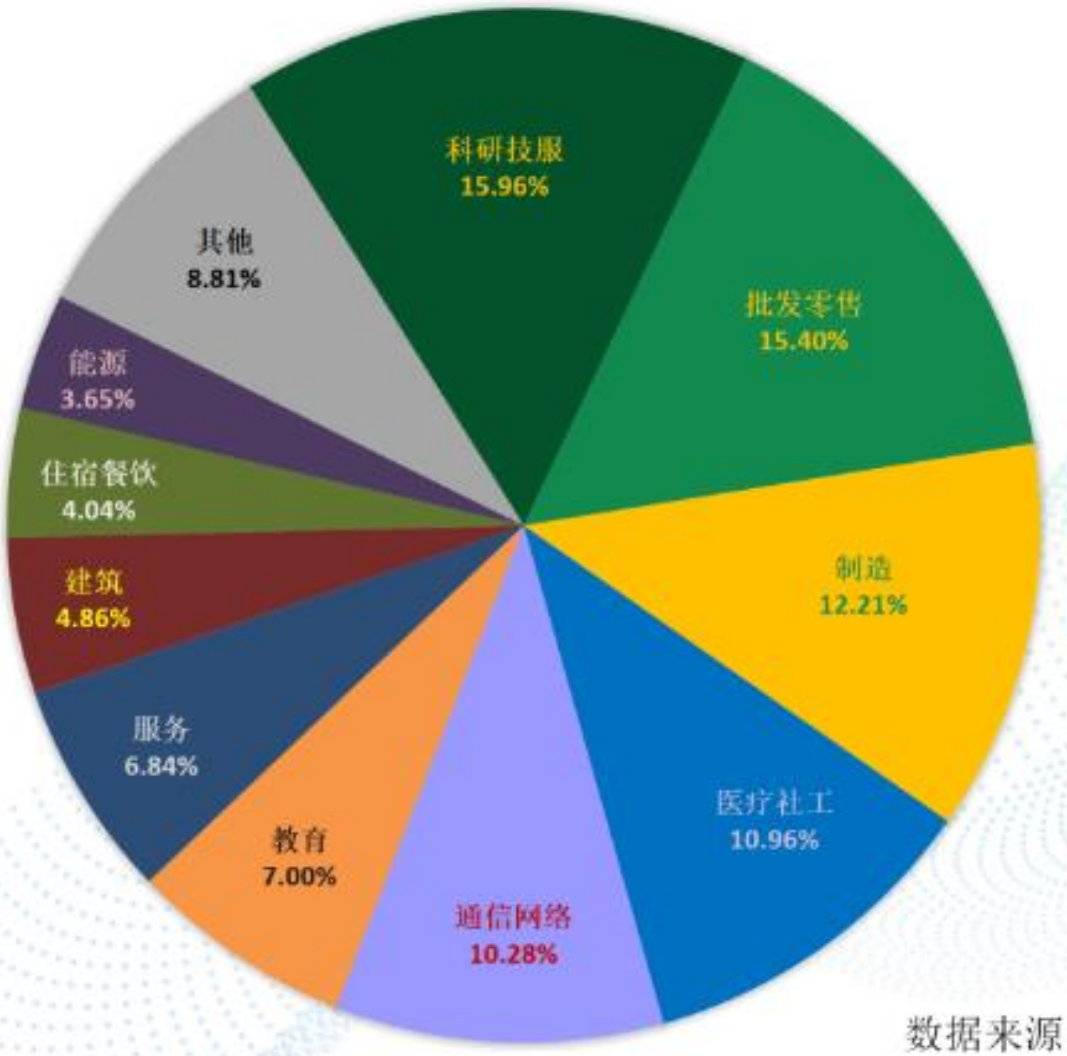
Dell数据防勒索解决方案助力企业数字化发展

李文伟 | 解决方案顾问
Wenwei_L@dell.com
13386539266

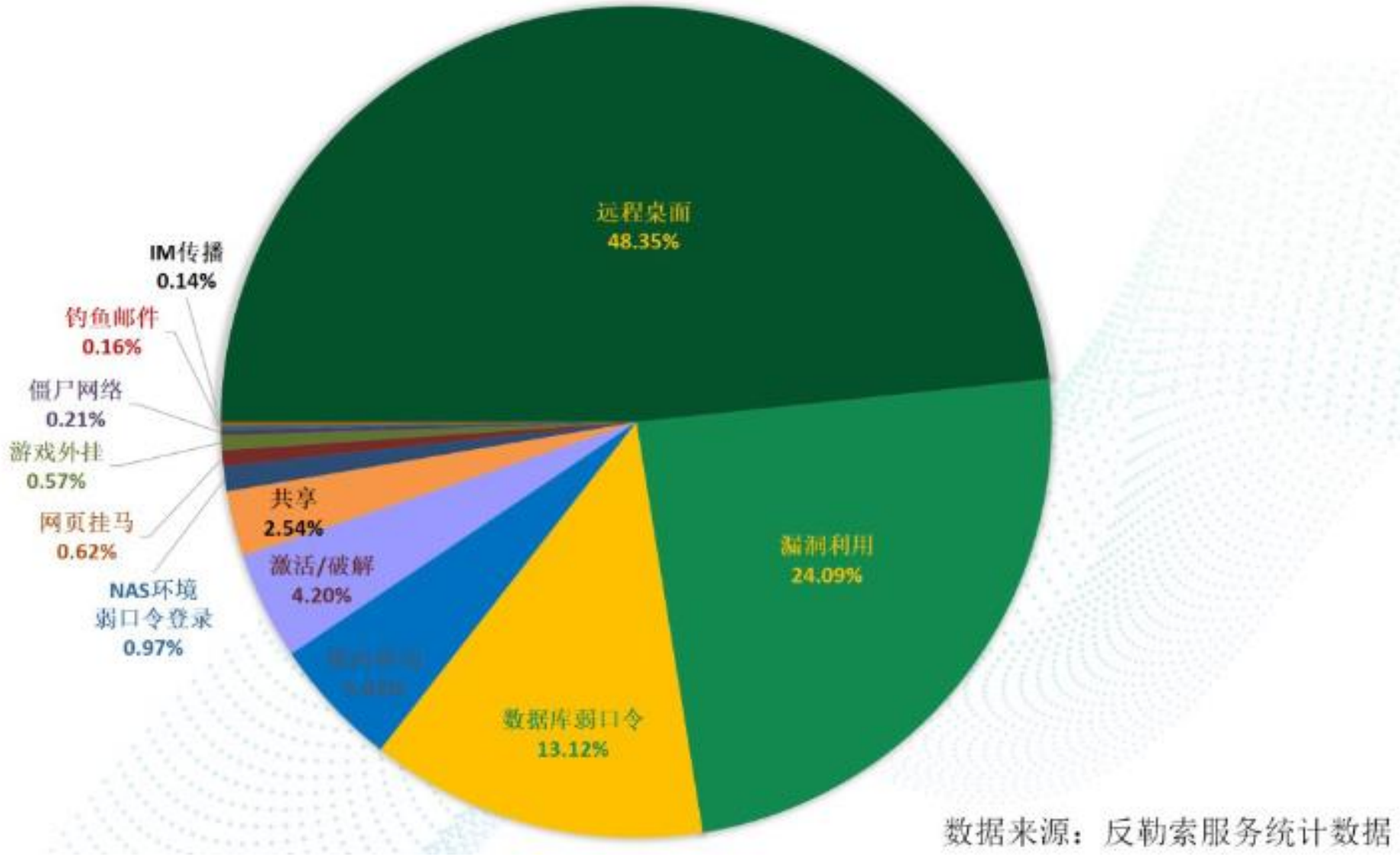
DELL Technologies
戴 尔 科 技 集 团

2023国内被勒索行业分布



数据来源：反勒索服务统计数据

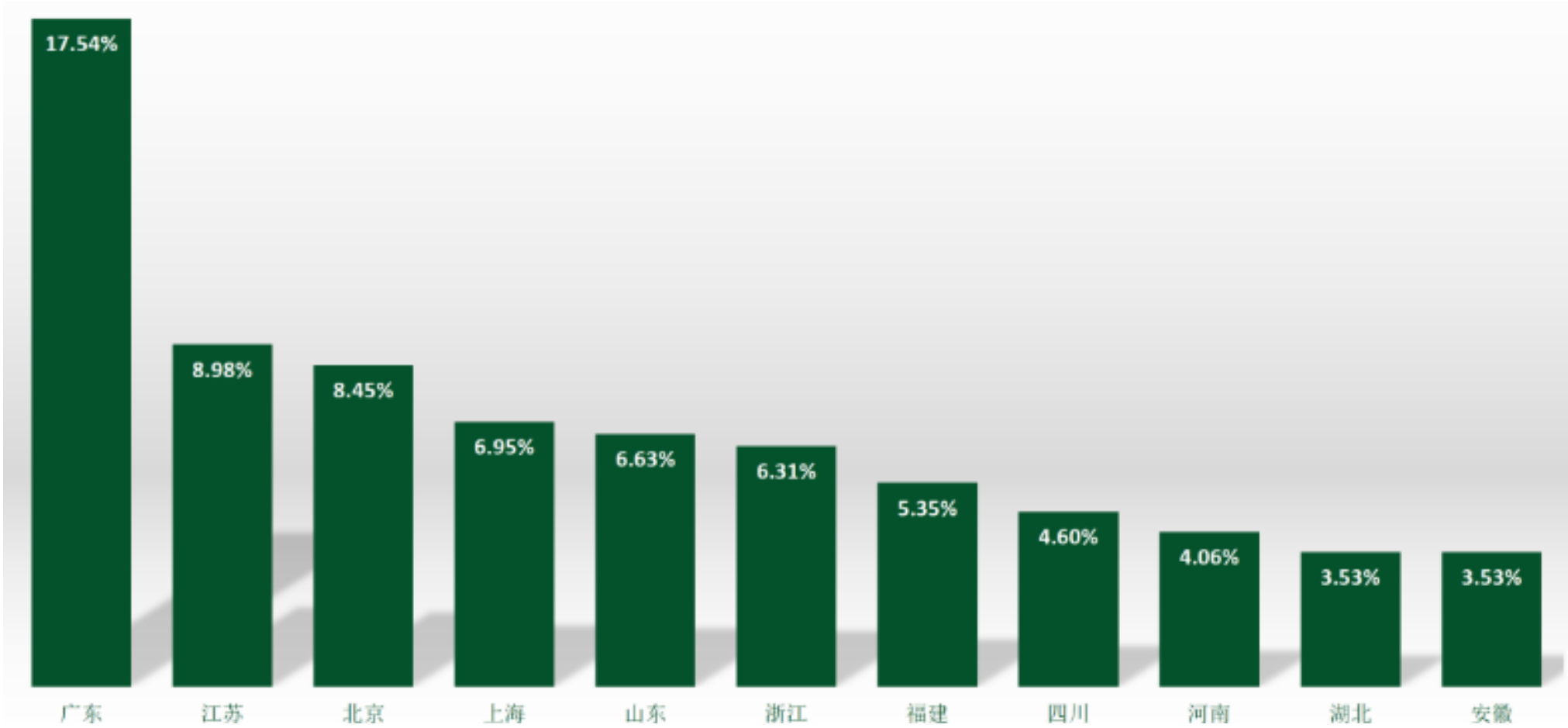
2023勒索入侵方式



数据来源：反勒索服务统计数据

2023国内勒索病毒活跃TOP10

2023国内勒索区域分布TOP10



2024 AI黑客.....

勒索攻击是毁灭性的

公司关闭

KNP物流公司

- 2023 6月遭受勒索攻击
- **英国物流公司**
- 700 名员工失业

销售额下降

Clorox

- 2023 8月被攻击
- 销售额下降20%
- 首席安全官CISO被解雇

耗费时间

达拉斯市, 德州

- 2023 5月被攻击
- 用5周时间恢复90%业务
- $8.5M 用于恢复

损害名誉

MGM 米高梅酒店

- 2023 9月被攻击
- 全球性德新闻
- 导致 1 亿美元损失、数据被盗

案例：某公司中勒索病毒后快速建立备份+容灾+数据避风港数据保护

没有重视！

2019年12月15日

1台服务器被勒索用备份软件恢复

备份软件服务器被加密

备份存储DD完好无损

2020年1月15日

50台被勒索

Windows & Linux

个人筹集50W

2020年1月16日

每台 7.5W 解锁

打包375W → 50W

2020年1月18日

转账 5W

不予处理

我们介入

2020年1月19日

协调资源

齐心协力

2020年1月20日

专业工程师入场

7小时恢复备份服务器

2020年1月21日

凌晨1点开始恢复数据

2020年1月22日

所有数据成功恢复

DD的可靠性获得了客户的认可和赞赏

交流改进方案 DR + CR

解答客户疑惑

排除磁带库

设计数据保险库架构

POC

CR 功能实现

建立备份，灾备和数据保险库

DELL Technologies 戴尔科技集团

没有完美的安全方案


防火墙
安全策略
数字签名
防病毒
职责分工
充分的防御
入侵检测
风险管理
漏洞扫描
访问控制
网络监控
变更配置管理
灾难恢复计划
网络安全准入
基于角色的配置


剩余风险
Residual Risk
风险敞口大
新业务形态多
约束风险
Constraints
勒索病毒变种快
攻击越来越频繁
安全产品的有效性
安全基因缺乏
APT攻击
0 Day攻击
社会工程攻击

从网络安全走向网络韧性

传统安全关注点

Dell的关注点

网络安全

一种过程、能力或状态

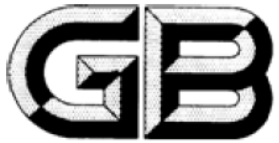
- 保护信息和通信系统及其包含的信息免受和/或防止损害
- 未经授权的使用、修改或利用

网络韧性

- 遭遇打击、破坏的时候,资源使用者所具备的预测承受恢复和适应的能力
- 重点是当网络攻击发生时，如何将数据损失和财务影响最小化的同时，恢复组织的正常运营。

新国标：信息系统灾难恢复规范

ICS 35.030
CCS L 80



中华人民共和国国家标准

GB/T 20988—202X

代替 GB/T代替 GB/T 20988—2007/GB/T 30285—2013

网络安全技术 信息系统灾难恢复规范

Cybersecurity technology—Disaster recovery specifications for information systems

A.3 第3级 电子传输和部分设备支持

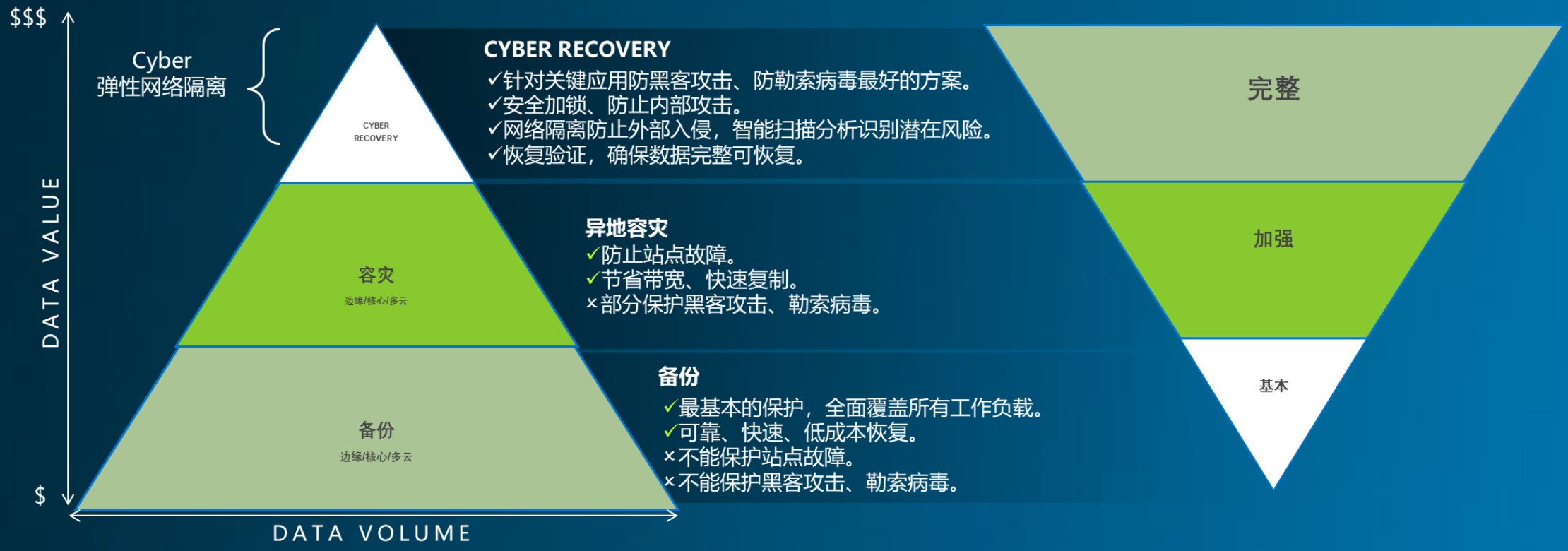
第3级灾难恢复能力应具有技术和管理支持如表A.3所示。

表A.3 第 3 级——电子传输和部分设备支持

要素	准则
数据备份容灾系统	a)完全数据备份至少每天一次，至少保留1个月冗余数据； b)备份存储场外存放或者本地存放，异地备份或者本地备份要使用专属的备份存储； c)生产中心和灾难恢复中心，重要系统数据周期性同步，实现小时级到天级RPO； d)副本数据不可修改和防泄漏机制，保护备份数据加密和不被非法篡改，保障数据完整性； e)支持防勒索功能，建立安全的隔离区用于数据存储，防止备份数据被非法访问； f)当生产中心发生灾难，灾难恢复中心能够在24小时内拉起应用，接管业务。 注：可借助数据备份系统提供一定程度的容灾保护。
备用数据处理系统	a)配备灾难恢复所需的部分数据处理设备； b)备用数据处理系统独立于生产系统运行。
备用网络系统	配备部分通信线路和相应的网络设备。
备用基础设施	a)有符合介质存放条件的场地； b)有满足信息系统和关键业务功能恢复运作要求的场地。
专业技术支持能力	在灾难恢复中心有专职的计算机机房运行管理人员。
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。
注：“—”表示不作要求	

Dell数据保护最佳实践 -- 三位一体 (BR+DR+CR)

所有的数据都要备份BR+重要的数据要容灾DR+核心的数据要隔离保护CR



传统备份软件的防勒索是不是够用？

勒索软件趋势	传统备份软件	数据避风港
备份数据已经成为黑客的主要目标	备份系统是一个共享系统	AirGap隔离机制，避免黑客发现“避风港”数据
锁定组织数据强制勒索赎金	没有对数据完整性进行全面验证。不验证数据库	全面验证数据完整性，包括文档、数据库和核心基础设施.
新的复杂变体	使用元数据和阈值检测明显的损坏	基于内容的深度取证分析 内部数据以检测隐藏的腐败
使用人工智能开发新方法	输入到 AI 引擎的数据点有限	200+点输入到AI引擎进行检测数据的损坏，可信度为99.5%。

原生的零信任数据保护储存--DataDomain

数据保护的基石，持续的零信任架构强化，确保备份数据的安全性

PowerProtect DD
(Data Domain)

多因子认证 (MFA) – RSA
- 网页操作接口、命令行接口、安全官、以及 iDRAC

双角色验证 (2017)
管理员与安全官
- 敏感与破坏性指令 (95+)

DIA Data Invulnerability Architecture
- 持续检查已储存数据的写入– 自我修复
- 确保数据的正确性及**可还原性**

传输协议- DDBoost
- 经加密、安全、经验证、非开放
- 现代化、数字化，促进**资料可移动性**

操作系统- DDOS
- 安全强化的操作系统，限制存取
- 在单用户模式下无法重启

文件系统– DDFS
- 哈希化容器– 恶意代码无辨识

安全AD / LDAP 认证整合

根据角色控管存取
- 管理者、受限管理者、操作者、安全官

端至端加密
- 传输中数据: TLS 1.2 256位
- 静态数据: RSA BSAFE FIPS 140-2 验证的加密函式库

不变性
Retention Lock Compliance Mode(2012)
Cohasset Associates (2013)
- SEC 17a-4(f) 合规性
- FDA 21 Part II
- Sarbanes-Oxley Act

安全系统时钟
NTP 时钟窜改控制 (2019)
- 变更、漂移、同步化、数字签名

本地或外部密钥管理 (KMIP)

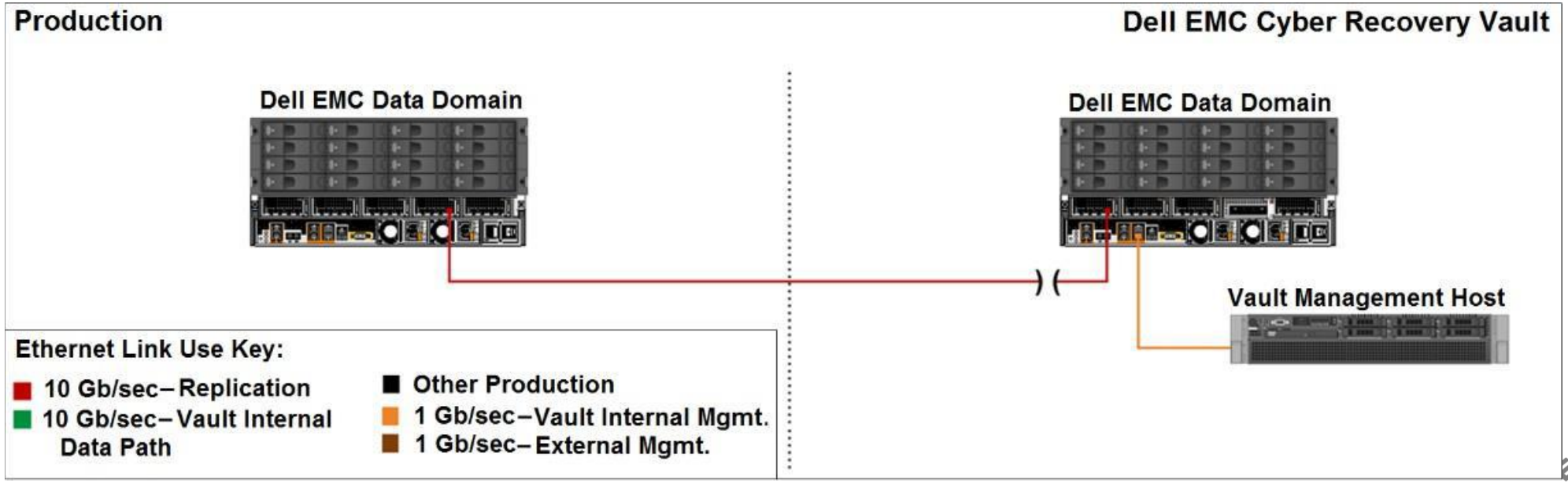
安全日志记录SIEM / SOAR

整合式熄灯管理硬型化 (iDRAC)

安全远程支持服务 (Call Home)

“AirGap”的本质

- 数据有复制时连通，没有复制的时候断开，数据处于“隔离状态”
- 真正的AirGap是：让生产端不能发现“隔离数据”的存在。
- 所有的管理操作都在Vault区实现，外面无感知
- 生产的备份服务器上index/catalog没有记录这份数据，黑客突破了你的备份数据也发现不了这份数据的存在。



数据防篡改（WORM）

- Retention Lock 提供备份文件不可变的能力
- 在设定的期间内，避免数据被窜改或删除
  - DD Retention Lock Governance
  - DD Retention Lock Compliance

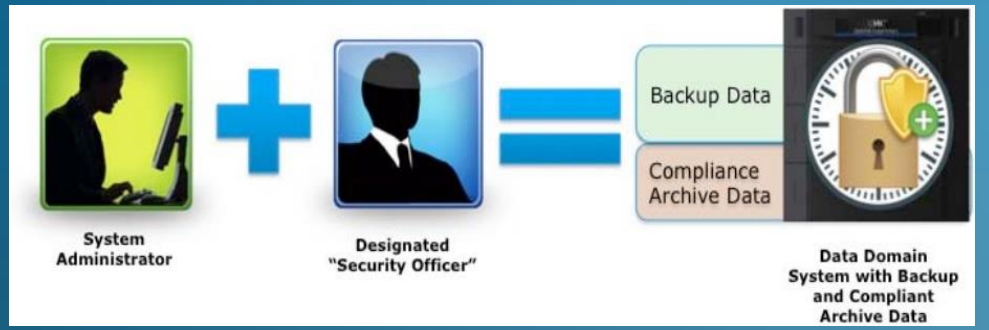
- Compliance Edition 符合下列美国及国际上通用的法规标准
  - US: SEC 17a-4f, CFTC, SOX, FDA, IRS
  - International: ISO Standard 15489-1, MoREQ

- Compliance Edition 强认证
  - 必须设定安全管理员
  - 高级别及重启操作必须有安全管理员的授权，并进行双重认证
  - 系统时间的高级控制，防止系统时钟被篡改
  - 即使DELL Support也不能覆盖已设定合规锁的保留期

系统时钟攻击

iDRAC攻击

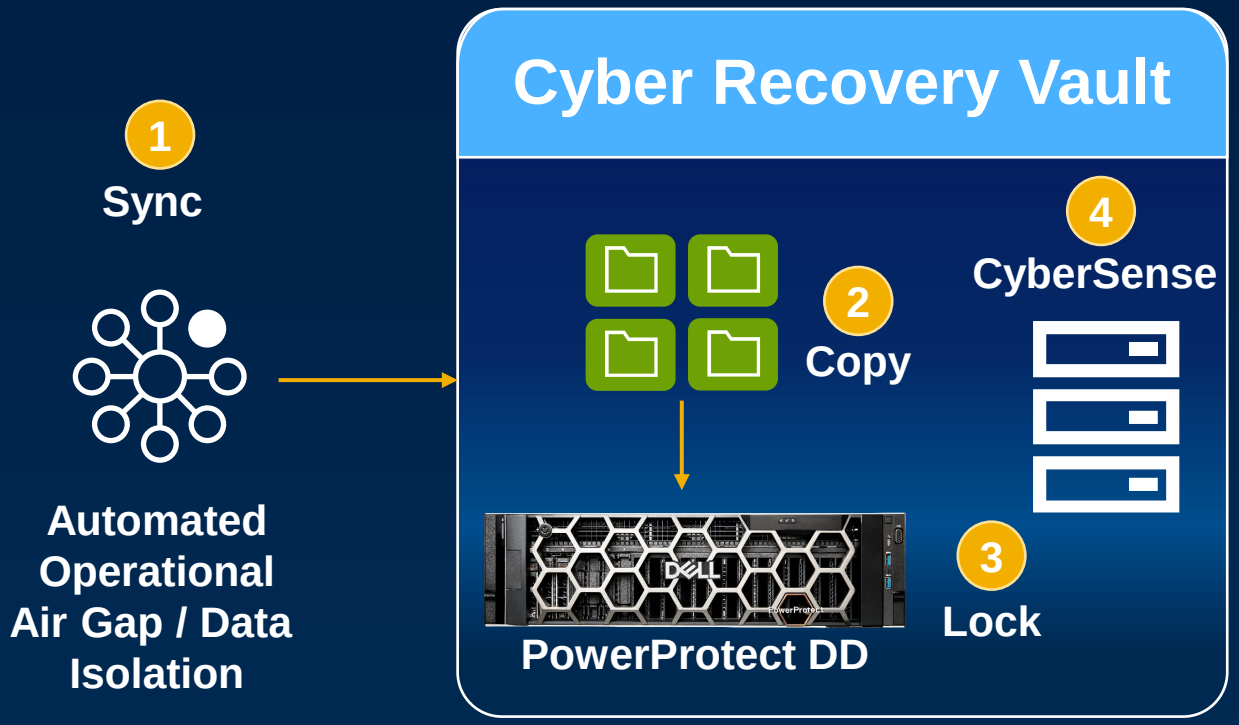
双因素认证

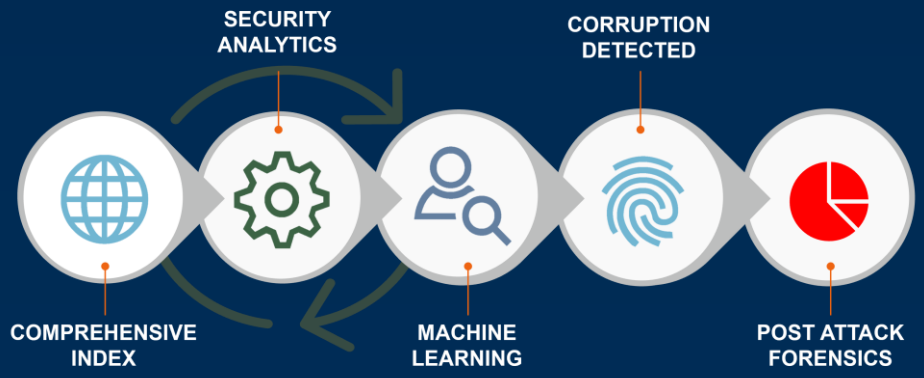


DELL Technologies
戴 尔 科 技 集 团

数据智能分析

CyberSense®
Powered by Index Engines





全方位的资料检索统计
安全性分析
机器学习
数据损坏检测
攻击后鉴识报告
最后干净的备份拷贝

Cyber Vault

- Air-Gap 离线数据保护库
- Air-Gap & Sync 自动化由Vault内部控制
- 账号及权限与生产环境分离
- 网络与生产环境分离

PowerProtect DD Capabilities

- Retention Lock Compliance
- End to End Encryption
- Dual Role Authorization
- Multi-Factor Authentication
- Secure System Clock
- NTP Clock Tamper Controls
- Key Management
- Custom System DDOS
- DD File System Hardened
- DDBoost
- Data Invulnerability Architect (DIA)
- Integrated Lights Out Mgt Hardening (iDRAC)
- Secure AD/LDAP Authentication
- Secure Remote support
- Role Based Access

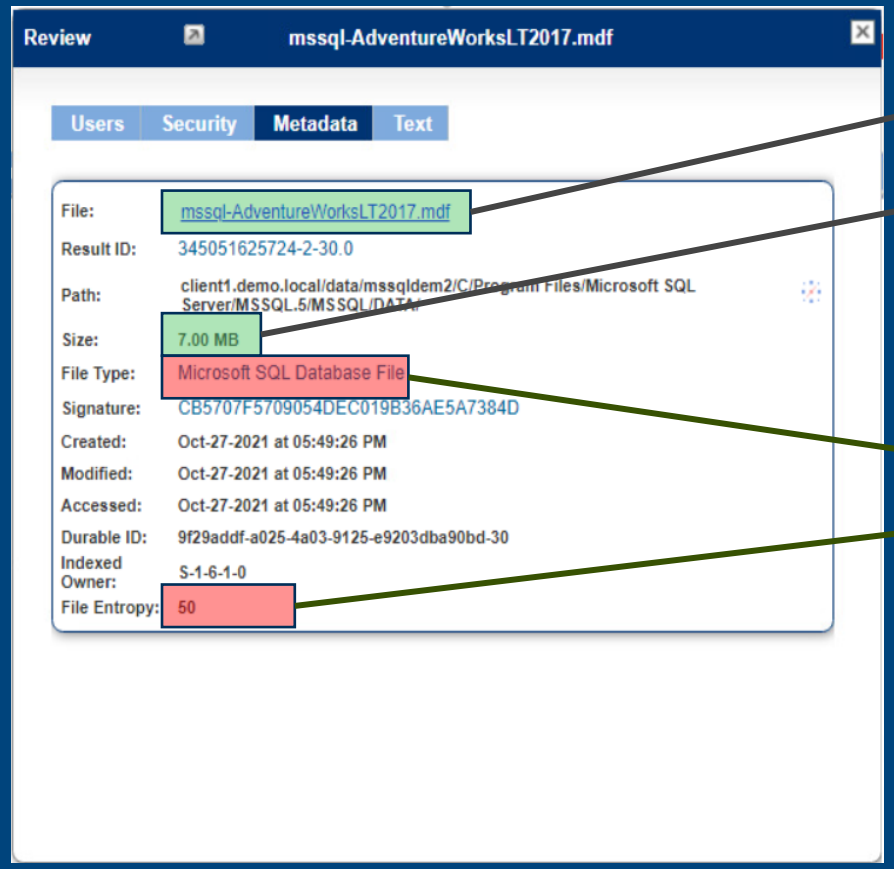
DELL Technologies

比较元数据与内容分析

AlphaLocker – 强机密保持原文件名

01 攻击前版本
最后的良好版本

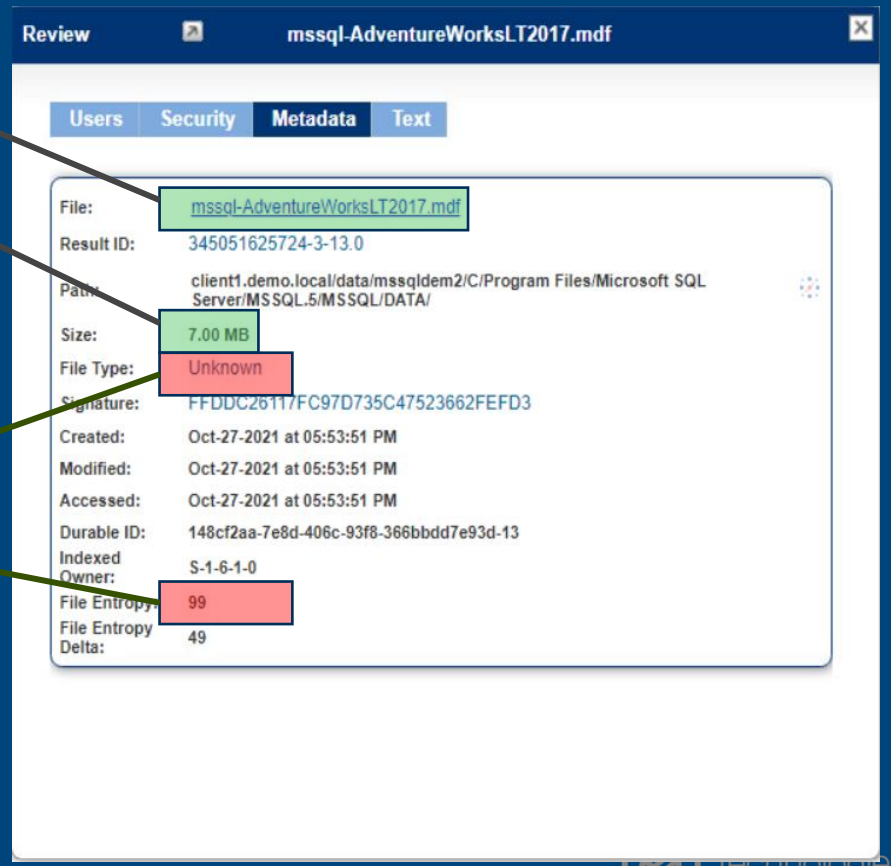
02 攻击后版本
损坏的文件



Meta Data
Filename, extension, filesize

Content

Entropy, fileheader, file structure, daily changes



CyberSense是市面上唯一支持对Database内部隐藏损害进行数据完整性分析扫描的产品

Metadata元数据检测:

Types the file and validates the extension

SAP Hana, Oracle, SQL, DB2, Epic, Iris, etc.

Integrity完整性检测:

Validates structure based on the type of database

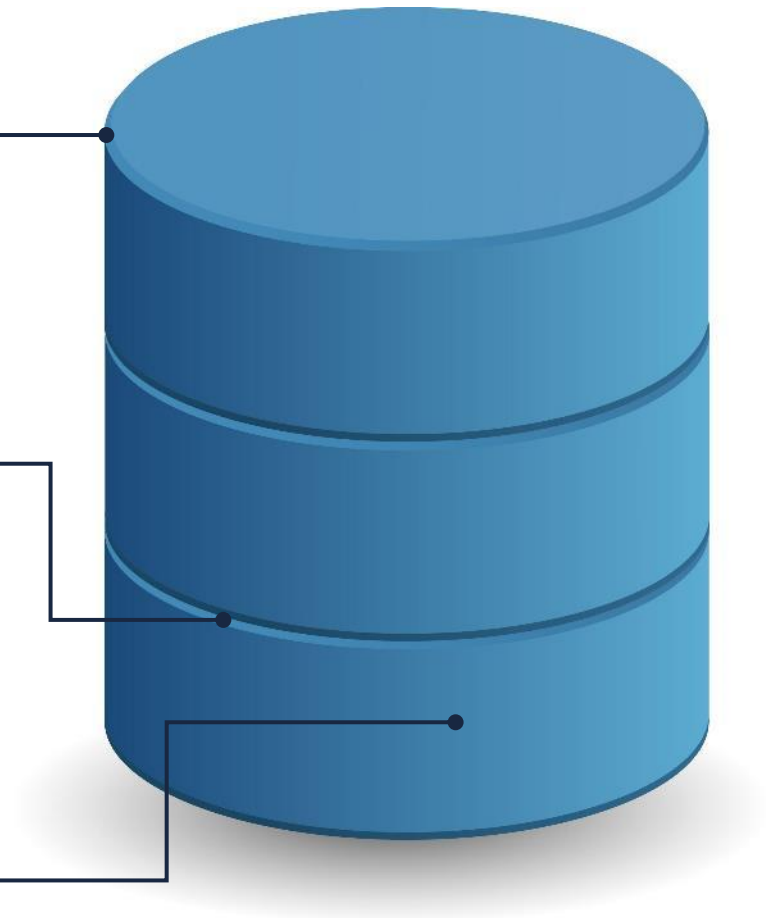
Validates page signatures in the allocation map; validates header; and more

Content内容检测:

Validates page headers. Identifies pages found corrupted/encrypted

比较页面熵、相似度

和以前版本的签名进行比较

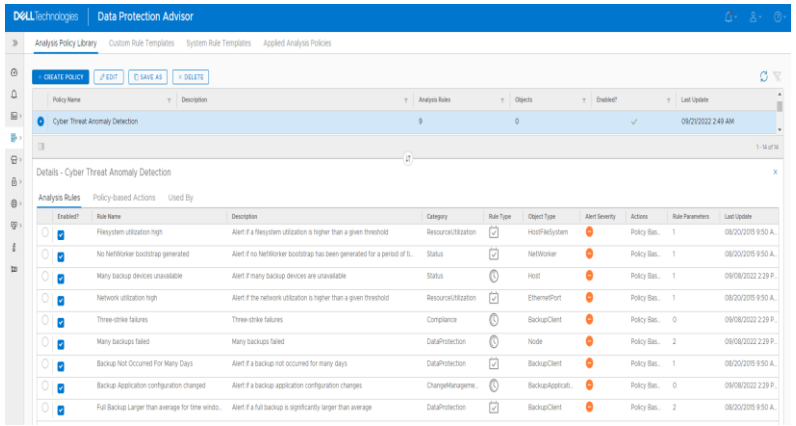


CyberSense®
Powered by Index Engines

数据保护系统前端实时监测+Vault智能侦测

检测异常数据和更改

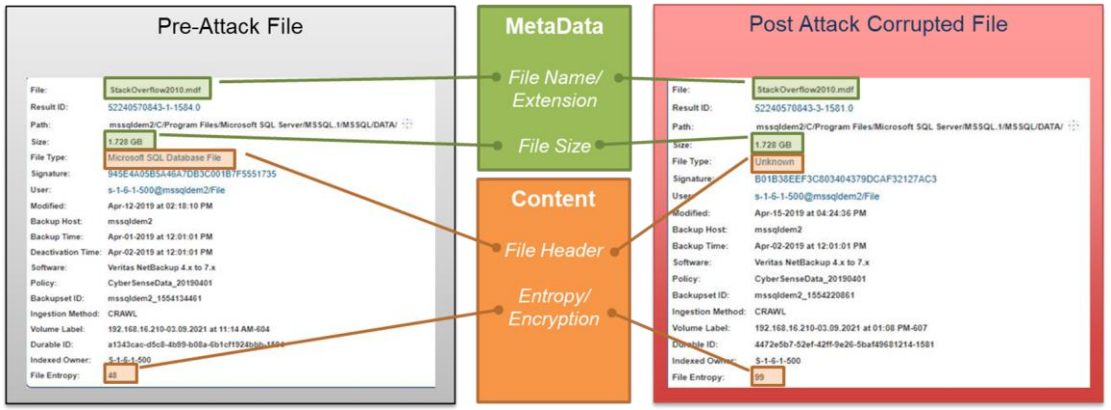
Dell Data Protection Advisor
(Dell数据保护顾问)



- 监控数据保护系统的更改、检测客户端数据的异常变化
- 监控不正常的客户端网络活动、实时触发警报
- 将警报导出到企业安全系统

智能侦测数据是否被破坏

CyberSense提供智能分析

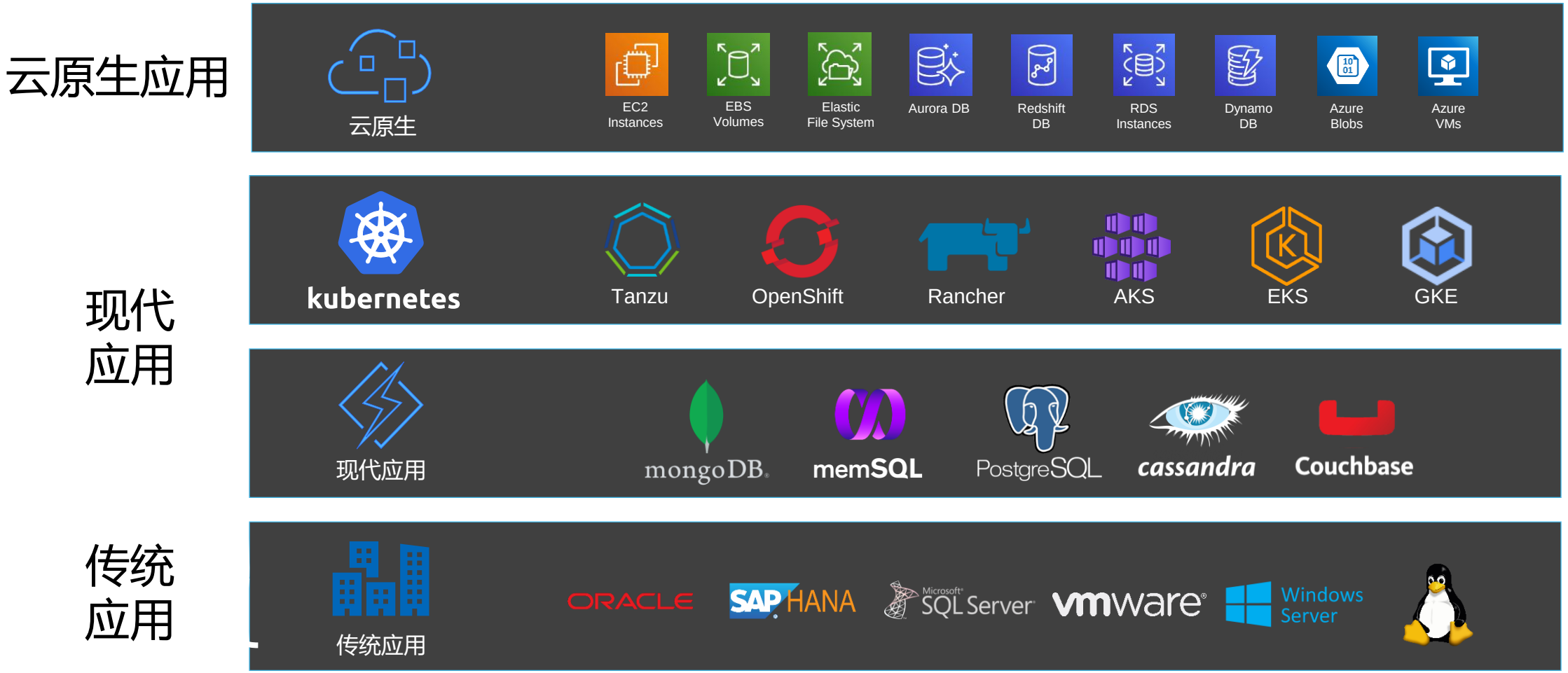


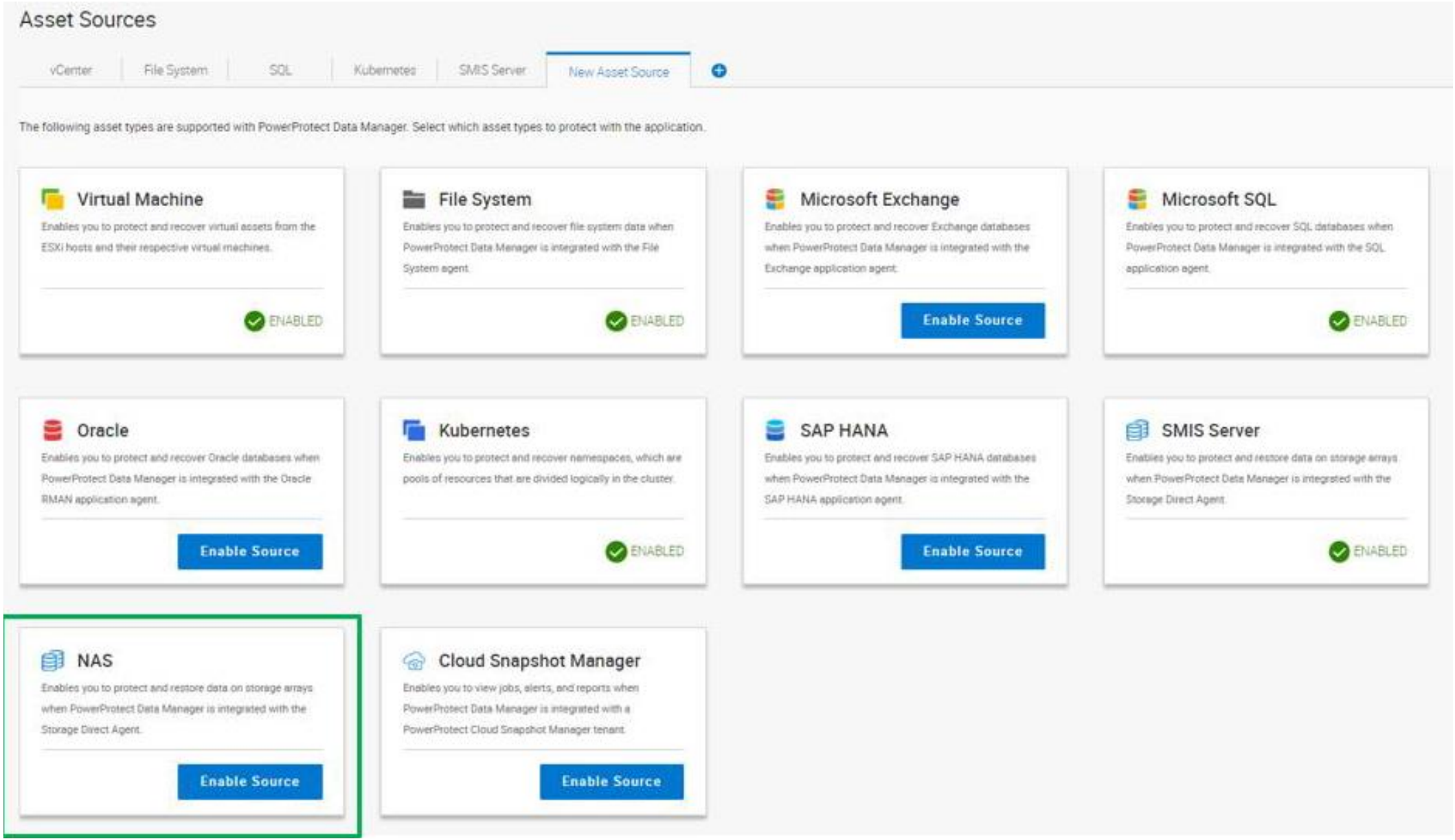
- 元数据+全内容分析
- 可检测复杂的网络攻击
- 99.5% 正确率
- 报告最近的完整备份拷贝
- 支持文件、虚机、数据库等

DELL Technologies
戴 尔 科 技 集 团

灵活轻量的软件

PowerProtect Data Manager:简称PPDM，其实就是一个打包的OVA，所以安装只需要导入即可，无需更多的环境准备和备份程序的安装




Asset Sources
vCenter
File System
SQL
Kubernetes
SMIS Server
New Asset Source
The following asset types are supported with PowerProtect Data Manager. Select which asset types to protect with the application.
Virtual Machine
Enables you to protect and recover virtual assets from the ESXi hosts and their respective virtual machines.
ENABLED
File System
Enables you to protect and recover file system data when PowerProtect Data Manager is integrated with the File System agent.
ENABLED
Microsoft Exchange
Enables you to protect and recover Exchange databases when PowerProtect Data Manager is integrated with the Exchange application agent.
Enable Source
Microsoft SQL
Enables you to protect and recover SQL databases when PowerProtect Data Manager is integrated with the SQL application agent.
ENABLED
Oracle
Enables you to protect and recover Oracle databases when PowerProtect Data Manager is integrated with the Oracle RMAN application agent.
Enable Source
Kubernetes
Enables you to protect and recover namespaces, which are pools of resources that are divided logically in the cluster.
ENABLED
SAP HANA
Enables you to protect and recover SAP HANA databases when PowerProtect Data Manager is integrated with the SAP HANA application agent.
Enable Source
SMIS Server
Enables you to protect and restore data on storage arrays when PowerProtect Data Manager is integrated with the Storage Direct Agent.
ENABLED
NAS
Enables you to protect and restore data on storage arrays when PowerProtect Data Manager is integrated with the Storage Direct Agent.
Enable Source
Cloud Snapshot Manager
Enables you to view jobs, alerts, and reports when PowerProtect Data Manager is integrated with a PowerProtect Cloud Snapshot Manager tenant.
Enable Source

DELL Technologies Cyber Recovery 数据避风港和数据保护表现出色

2015	支持自定义部署的“独立”恢复解决方案
2018 年	推出 PowerProtect Cyber Recovery 数据避风港解决方案
2019 年	成为 Sheltered Harbor 联盟合作伙伴计划的技术供应商
2020 年	PowerProtect Cyber Recovery 数据避风港成为率先获得认可的 Sheltered Harbor 解决方案
2021 年	推出 Dell PowerProtect 具有多云数据服务的 Cyber Recovery 数据避风港
2021 年	推出适用于 AWS 的 PowerProtect Cyber Recovery 数据避风港
2022 年	推出适用于 Azure 的 PowerProtect Cyber Recovery 数据避风港
2022 年	推出适用于 Google Cloud 的 PowerProtect Cyber Recovery 数据避风港

#1

数据保护设备和软件[1]

2000+ **全球Cyber Recovery 数据避风港客户**

150+ **大中华区 Cyber Recovery 数据避风港客户**

[1] 基于 IDC 2022 年第 2 季度专用备份设备 (PBBA) 跟踪报告中的综合收入，涵盖 2022 年第 2 季度存储软件和云服务跟踪报告中的部分存储软件细分市场

DELL Technologies

什么是数据避风港

戴尔科技数据避风港Cyber Recovery | 守护企业数据安全的最后一道防线

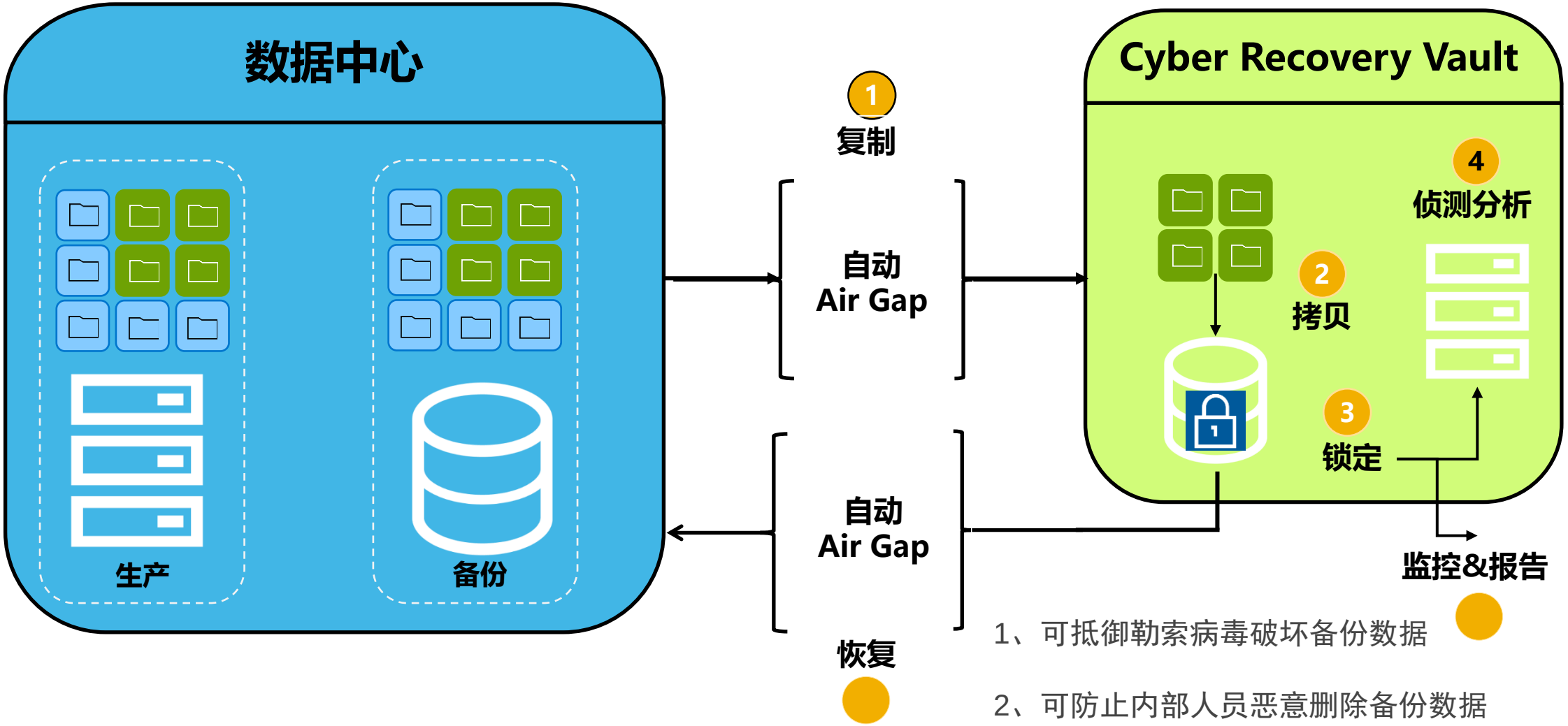
DELL Technologies

全球组织的最佳实践建议

很明显，隔离(AIR GAP)是网络弹性的主要设计原则和最佳实践

Gartner	THE WHITE HOUSE WASHINGTON	Hong Kong Monetary Authority	CNCERT/CC 国家互联网应急中心
“创建隔离恢复环境 通过灾难恢复计划的IRE部分进行勒索软件恢复，并将其包括在未来的灾难恢复测试中。	确保备份没有连接到业务网络。	“安全的第三级数据备份应该断开……以便它能够抵御有针对性的网络攻击……或来自恶意内部人士的威胁。”	**要备份重要数据和系统。**重要的文件、数据和业务系统要定期进行备份，**并采取隔离措施。**
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA	SHELTERED HARBOR	IDC ANALYZE THE FUTURE	GDPR
保持离线、加密的数据备份至关重要。	数据保险库要求跟生产隔离，并要求上锁	网络弹性可以超越更基本的不变性概念，包括数据隔离。	数据机密性、完整性、可用性和高弹性。

安全可靠的整体
PowerProtect Cyber Recovery



1、可抵御勒索病毒破坏备份数据

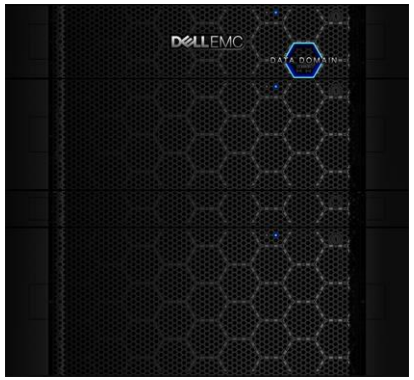
2、可防止内部人员恶意删除备份数据

超高安全的备份架构

ERP　PLM　SCM　……　CRM

文件　数据库　虚拟机

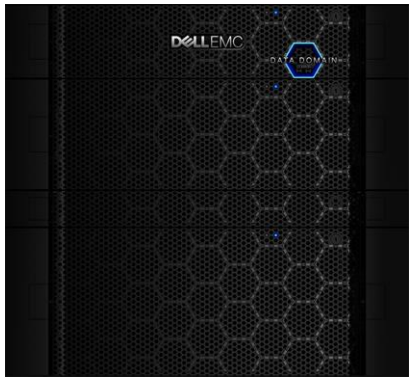
DDBoost　备份软件



一级备份设备
Data Domain

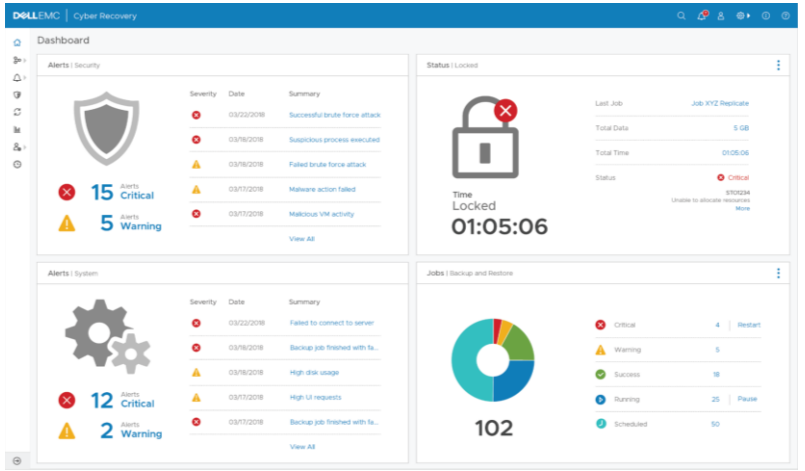
空气开关

只当复制时开启



二级隔离方案
Cyber Recovery

检测前导出



安全检测区
Cyber Sence

1、超高消重比
2、高安全性DDOS，符合FIPS 140标准
3、Retention Lock数据锁定
4、数据传输为DDBoost私有协议
5、具备硬件级冗余

1、单独隔离区域，保证运维绝对安全
2、不可更改存储卷，保证存储卷绝对安全
3、空气开关只在复制时单向开启，保证网络绝对安全

1、日常检测恶意代码
2、做恢复演练，保证备份成功率

DELL Technologies


DELL Technologies