COHESITY

Cyberworld

# 如何架设绿色现代化及安全永续的数据管理策略

Linda Hui and Michael Chung

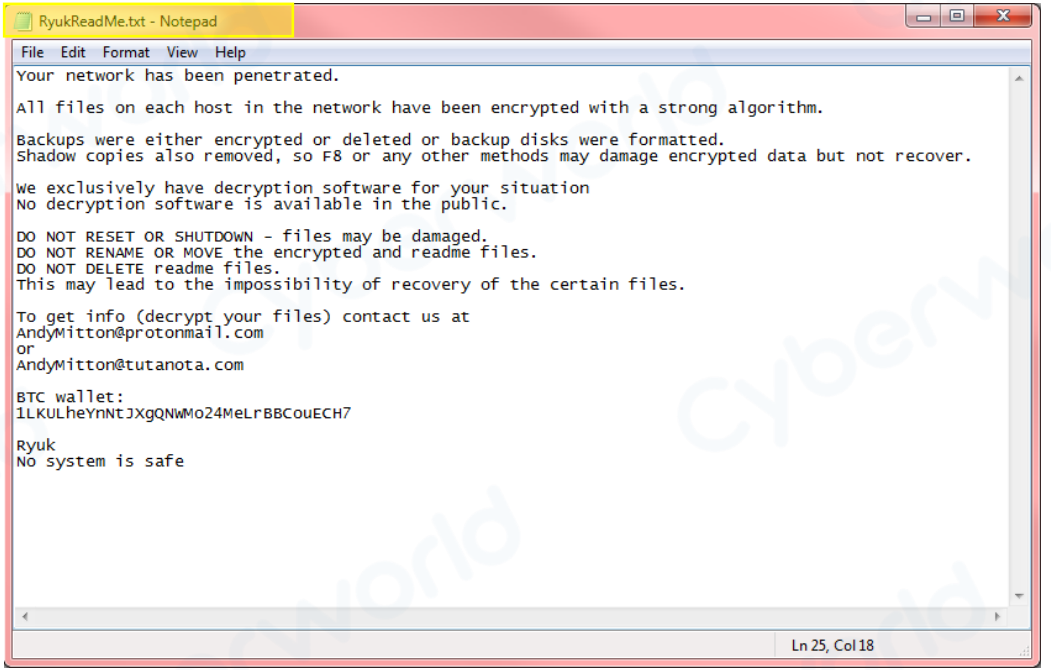
*“陛下，有坏消息，它是网络攻击。”*

*“Bad news, Your Majesty—it’s a cyberattack.”*

## 您还在使用老旧的方法吗?

# Ryuk

- 双击开始：网络钓鱼攻击利用 EOL 服务器和 DC。
- Ryuk 勒索软件运行 13 小时未被发现，传播速度非常快。
- 任何连接到 Windows 的东西都会受到影响。
- 562 台服务器和 2,000 多个终端设备。
- EPIC（医疗记录 App）停止运行 23 天。
- 实时的 SmartFiles 视图被加密。
- 没有预先警报。
- 一切被转移到纸上。
- 财务瘫痪。




您的网络已被入侵。

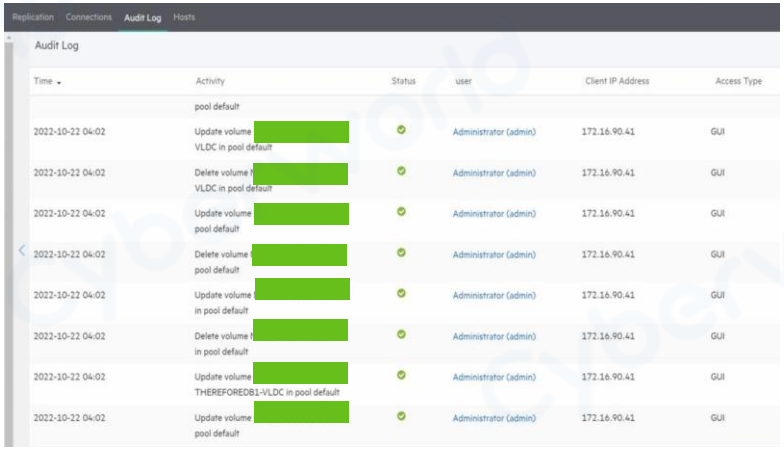
每个主机上的所有文件都已加密。

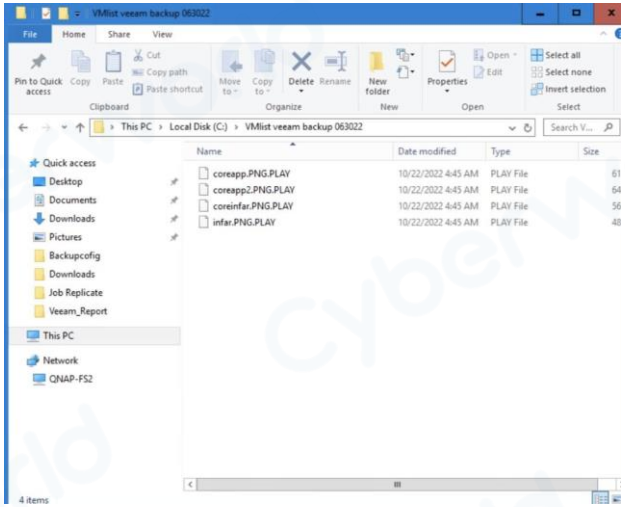
我们独有解密软件。

不要重置/关闭/重命名/删除。

# 锁定位与备份噩梦


2023年2月8日




**Hanada 医院遭遇勒索软件攻击**

**5 天内无法访问记录，用1年时间恢复所有数据**

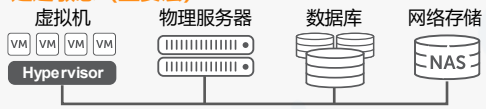
https://www.youtube.com/watch?v=XaVkzX7NjmA

# 过去与现在

## 传统备份

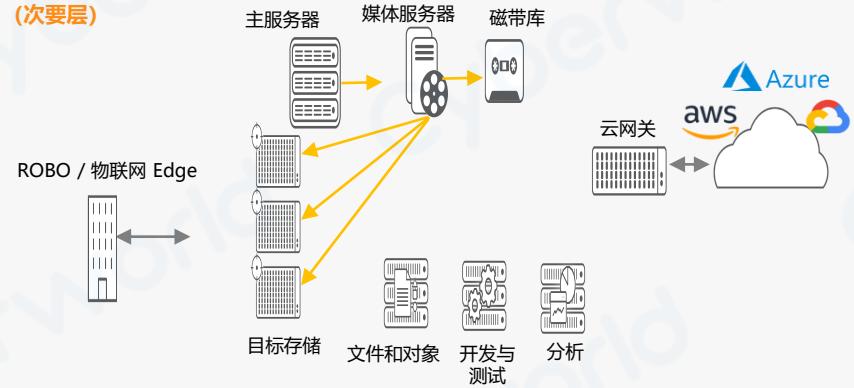
碎片化 | 效率低 | 暗数据

延迟敏感（主要层）




海量数据碎片化
- 孤立的基础设备
- 孤立的控制
- 孤立的情报

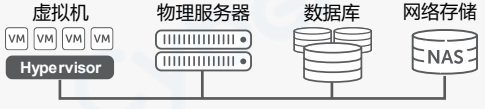
非延迟敏感（次要层）




Veritas：1983，数据域：2001

## 现代网络规模备份

延迟敏感（主要层）




重新定义数据管理
- 单一的平台
- 单一的用户界面
- 运行 Apps

备份与恢复


Cohesity：2013 （云、大量文件、安全性）

# 灵活的部署方式

- **Cohesity的数据平台是一个软件定义平台**
  - **能运行物理系统（数据平台）**
    - Cohesity 商品系统（Cohesity 品牌 OEM 系统）
    - 来自HPE、Cisco、Dell 或 Fujitsu 的合格系统
  - **能在多个不同的管理程序上作为虚拟机运行**
    (Edge 或虚拟版本的数据平台)
    - 两种不同的类型 —— ROBO 站点的 Edge 、核心数据中心的集群（虚拟版本）
  - **能在 AWS、Azure 或 GCP 云数据平台上原生地运行**

# 数据管理平台

- 现代化数据管理平台
- 分层平台架构
  - **可部署的应用程序和服务**
    - 由 Cohesity MarketPlace 提供支持
    - 快速部署可扩展和增强数据管理功能的容器化解决方案
  - **单一管理界面**
    - Helios 提供简易全局管理
    - SPOG 提供暗站点联合管理
  - **Cohesity 数据平台**
    - 数据管理的软件定义、网络规模平台
    - 专为处理广泛的工作负载而构建
      (数据保护、文件与对象、开发与测试、云)

# 许多用例，从任何或所有组合开始

差异化


**集成备份与恢复**

**淘汰传统**备份软件

**备份目标存储***

**重用传统**备份软件

**大数据和分布式数据库备份**

支持最广泛的 Hadoop 和 NoSQL 数据库

**ICP / 私有 / 混合**

**多云数据管理**

存档、容灾、分层、XaaS

**综合网络安全**

反勒索软件、网络扫描、防病毒

**横向拓展 NAS**

智能文件和对象存储

**利用备份和非结构化数据做更多事情**

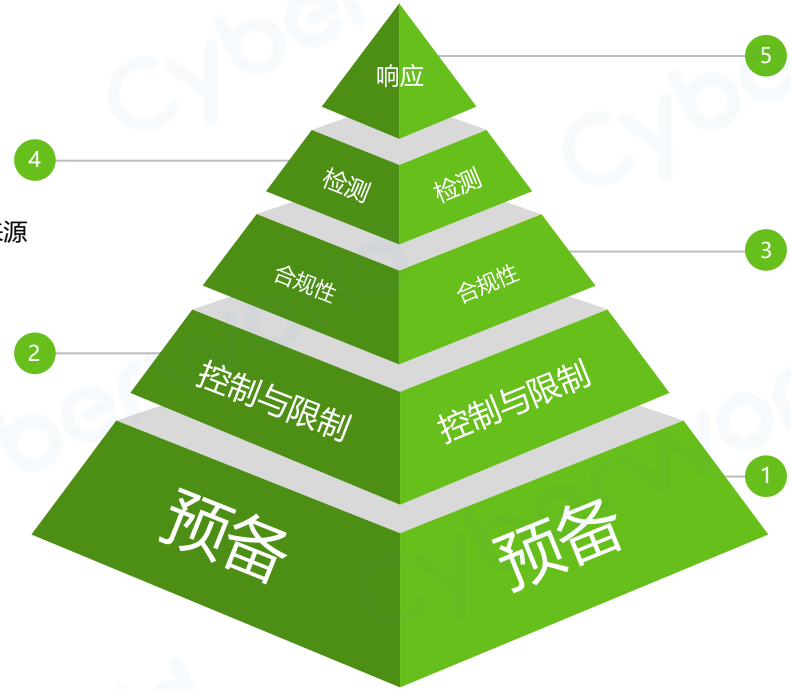
将计算引入数据

**灵活开发与测试**

开发者的即时数据访问

# Cohesity 的安全架构

标绿色部分是差异化功能




## 检测

- 勒索软件异常检测
- 深度可视化：受影响的对象与来源

## 预备: 控制与限制

- 多重身份认证
- 安全的 API 访问
- 精细的 RBAC
- 没有服务后门
- 安全的 App 生态系统
- 主动监察
  - 审计
  - 活动目录精细比较
  - 漏洞扫描

## 响应

- 基于机器学习的完整快照推荐
- 即时批量恢复

## 合规

- FIPS-140-2, CFTC 1.31(c)-(d), 通用标准, PCI-DSS, SOC
- SEC 17a-4(f) 数据锁（WORM 合规性）

## 预备: 平台保护

- 设计安全
- 不可变的文件系统
- 动态加密和静态加密
- Air Gap
- 测试可恢复性

# 安全永续的数据管理策略

# SHELTERED HARBOR 与传统容灾对比

## Sheltered Harbor 是对任何金融机构弹性策略的补充和增强

| | SHELTERED HARBOR | 容灾 |
|---|---|---|
| **灾难的性质** | **有针对性的网络攻击、网络事件、因扩展系统中断导致完全无法访问可信的关键数据** | 停电、技术故障、火灾、洪水 |
| **重点** | **当主要和备用系统长时间停机时，通过实现持续的客户账户和资金访问来维护公众信心** | 恢复一切如常 |
| **范围** | **关键客户服务**对于维护公众信心至关重要 | 所有关键的应用程序和基础设施 |
| **数据量** | **有限的 — 以MB或GB为单位** | 所有数据 — 综合而言 |
| **恢复时间** | **数小时** | 极端事件可能需要几天或几周的时间 |

# 不断发展的 SHELTERED HARBOR 合作伙伴生态系统

## 我们继续扩展生态系统，以提供广泛的选项来支持行业

### 服务提供商社区

- 公司在其组织内实施 Sheltered Harbor 存储和数据恢复标准，通过独立审计（最初和之后每年一次）证明其遵守情况，促进其客户和潜在客户参与 Sheltered Harbor，协助注册并为他们提供必要的服务以实现他们的目标参与和实施 Sheltered Harbor 标准。

Broadridge · COCC collaborative to the core · CSI · FIS · fiserv. · jack henry & ASSOCIATES INC. · UFS thrive. together.

### 联盟伙伴社区

| 顾问：咨询服务 | 解决方案提供商 | 保障：审计和合规性 | 营销： “品牌大使” |
|---|---|---|---|
| • 公司促进Sheltered Harbor的参与，并通过规划、实施和独立控制准备评估和审查支持参与者，这是Sheltered Harbor认证所必需的。 | • 公司促进 Sheltered Harbor 的参与，并为参与者提供经过 Sheltered Harbor 验证的交钥匙数据存储解决方案、实施和服务，以加快采用工作。 | • Sheltered Harbor合格评估公司促进参与，为参与者提供独立的控制准备评估、审查和证明服务，以完成他们的Sheltered Harbor认证。 | • 公司创造Sheltered Harbor意识，促进其金融部门客户和潜在客户的参与和采用。 |
| Capgemini · EY · pwc · RSM | cobalt IRON · COHESITY · DELL Technologies · VERITAS | Grant Thornton · pwc · schellman | ASPG ADVANCED SOFTWARE PRODUCTS GROUP INC. |

# 来自 FBI 的避免勒索软件提示

- 避免暴露于勒索软件（或任何类型的恶意软件）的最佳方法是成为一名谨慎而认真的计算机用户。恶意软件分发者变得越来越精明，您需要小心下载和点击的内容。
- 使操作系统、软件和应用程序保持最新状态。
- 确保将防病毒和反恶意软件解决方案设置为自动更新并运行定期扫描。
- 定期备份数据并仔细检查这些备份是否已完成。
- 保护您的备份。确保他们没有连接到他们正在备份的计算机和网络。
- 制定持续性计划，以防您的企业或组织成为勒索软件攻击的受害者。

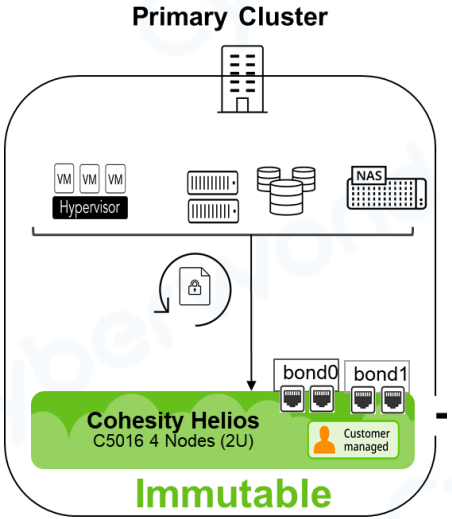
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

# 安全数据备份的特点

1. **不可变性** – 存储的数据在保留期间不应更改或删除。
2. **抗毁性** – 数据可恢复。
3. **Air-gapped** – 逻辑上或物理上断开连接以维护黄金源数据。
4. **安全** – 预防性（访问控制）、检测性（日志或警报）。
5. **受控** – 摄入 STDB 内容完整、准确、干净。
6. **可验证** – 在整个生命周期中验证数据。
7. **保障** – 适当的控制和流程以减少误报调用。
8. **异构** – 不同于生产环境。
9. **高性能** – 应该支持大规模并行处理和即时数据。

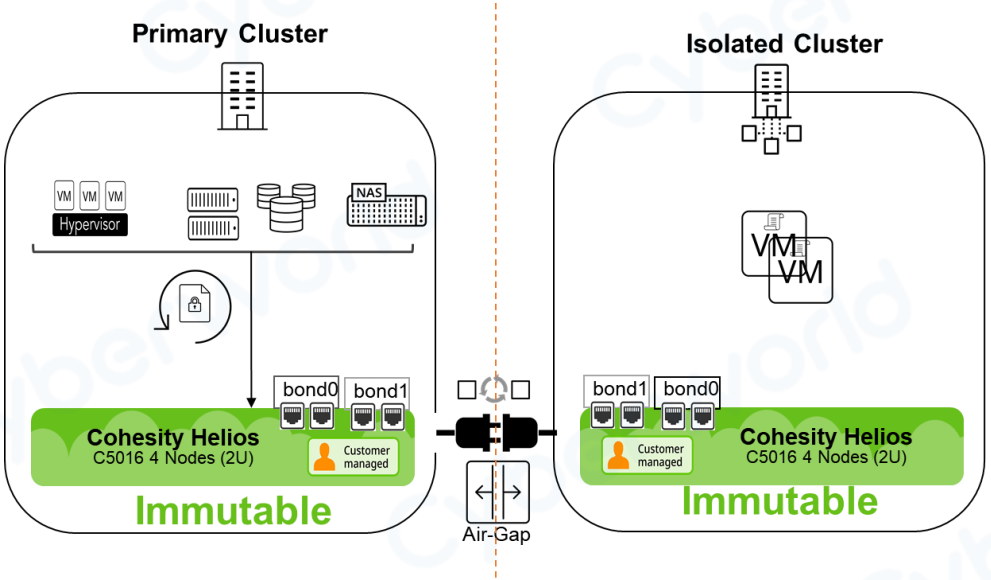
# 进程的第一步

- 不可变性
- 抗毁性
- 高性能
- 异构



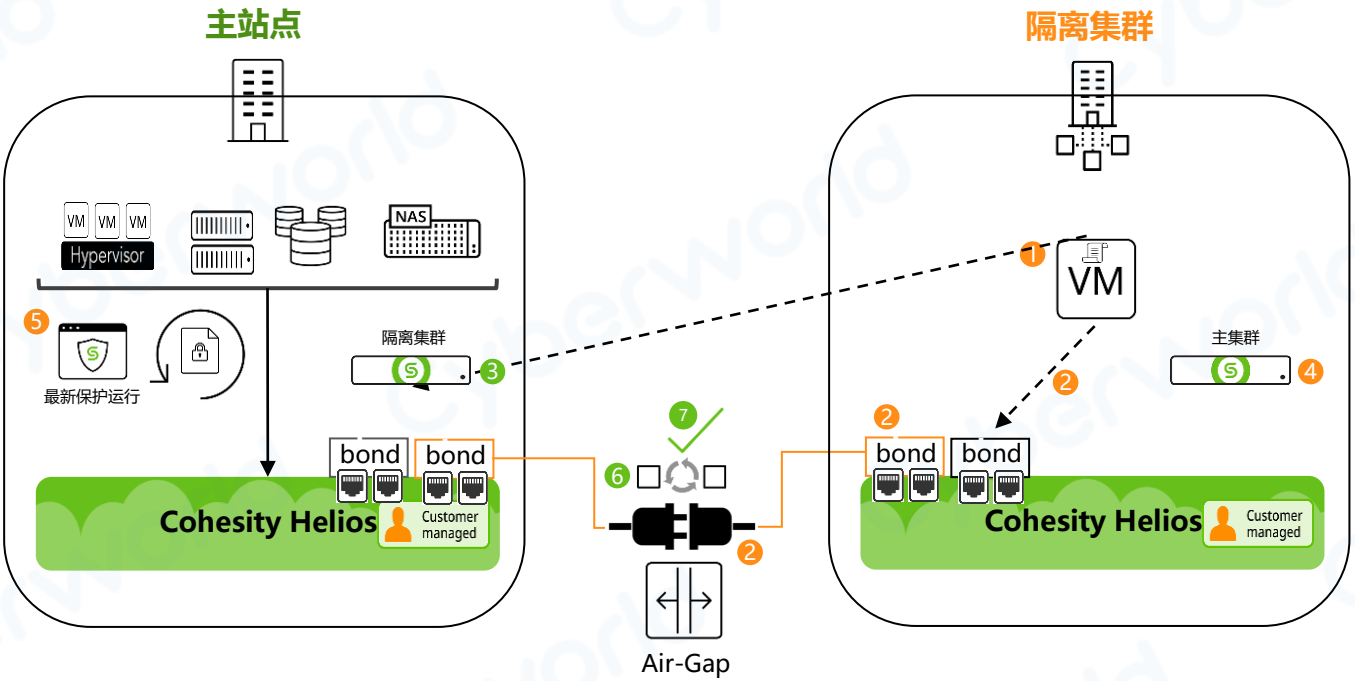
# 完成进程

- 不可变性
- 抗毁性
- 高性能
- 异构



# 数据隔离实施(STDB) Isolation

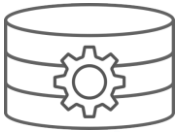
## 工作流程




1. 在与主集群通信的管理 VM 上启用接口
2. 在隔离集群上的 bond1 上启用复制防火墙端口
3. 将隔离集群注册为主集群上的远程目标
4. 将主集群注册为隔离集群上的远程目标
5. 在所选保护作业的主集群上收集最新的成功保护运行
6. 执行按需复制以保护从主集群到隔离集群的运行
7. 轮询主集群上复制作业的完成状态
8. 完成后，从两个（主集群和隔离集群）注销远程集群
9. 禁用隔离集群 (bond1) 上的复制防火墙端口
10. 禁用与主集群通信的管理 VM 上的接口

# Cohesity Immutable不可变性





数据操作

- **不覆写**，新的或更新的数据总是写入可用空间（分布式写时重定向）。
- 即使是特权用户也永远无法更改不可变数据。
- 为输入或输出操作克隆不可变数据（例如，恢复）。

**不覆写**

数据一致性

- 跨集群分布的数据的**严格一致性**，包括外部目标。
- 用于静态数据一致性的数据和元数据校验和。
- 两阶段提交以确保传输中数据的一致性（读后读，写后读）。

**一致性**

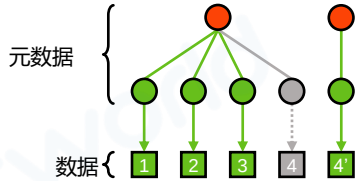
数据安全

- Cohesity 管理的所有数据加密（静态或动态）。
- 使用**数据锁策略**，即使是管理员也无法更改保留或删除恢复点。
- 无限期保留的**合法保留。**
- 基于角色的访问控制 (RBAC)。

**安全性**

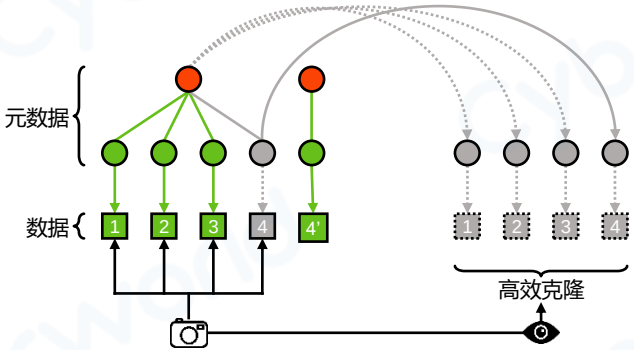
# 不可变性的数据操作

## 不覆写




- 新版本的 4 写为 4 ‘ 以释放集群中的空间。
- 活动文件系统更新为引用 1、2、3 和 4’ 。
- 如果没有对 4 的活动引用，它会一直保留到垃圾回收为止。

## 快照和克隆



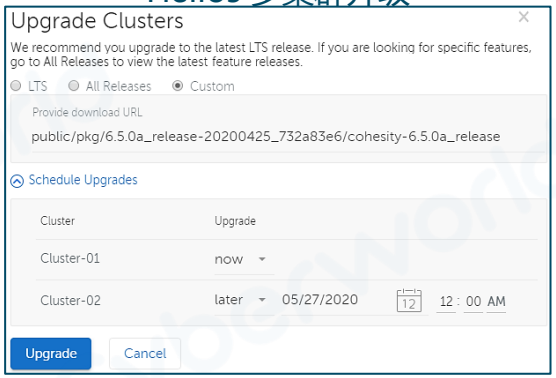

- 4 是不可变的，因为它被快照引用。
- 4 ‘ 是不可变的，因为它被活动文件系统引用。
- 1、2、3 是不可变的，因为它们被活动文件系统和快照引用。
- 数据被有效地克隆以用于恢复操作或副本。

# 无中断升级(软件)

- 直接从集群 UI、REST API 升级，或通过 Helios 多集群升级
- 在集群中的所有节点上滚动升级
- 所有节点必须在同一个 数据平台版本上

1. 下载软件包
2. 升级前检查
3. 将软件部署到备用分区
4. 停止服务
   (athena, groot, magneto, bridge_proxy, smb2_proxy, smb_proxy, alerts, stats)
5. 切换和重启服务
6. 移动到集群中的下一个节点

Helios 多集群升级




一次升级多个集群
每个集群进行精细调度

# 集群容错

- 一个集群同时能承受多少个故障?

### 机架

- 集群最多可同时承受 2 个机架故障


### 机箱

- 集群最多可同时承受 2 个机箱故障

### 节点

- 集群最多可以承受 2 个同时发生的节点故障

### HDD

- 集群最多可同时承受 3 个 HDD 故障

### SSD

- 集群最多可同时承受 2 个 SSD 故障

### 网络

- VIP 节点故障切换到集群中的其他可用节点

### 启动装置

- 集群不受引导设备故障的影响（存储在由持久硬盘支持的单独闪存分区上）

### 电源

- 集群中的每个节点可以承受集群中每个节点 1 个 PSU 故障（每个节点都有冗余 PSU）

### 风机

- 集群可以承受集群中每个节点 1 个风扇故障 +1 个额外故障（N+1 冗余）

集群弹性具有最低配置要求，必须满足这些要求才能维持最大数量的故障

# 高性能 – Instant Mass Recovery

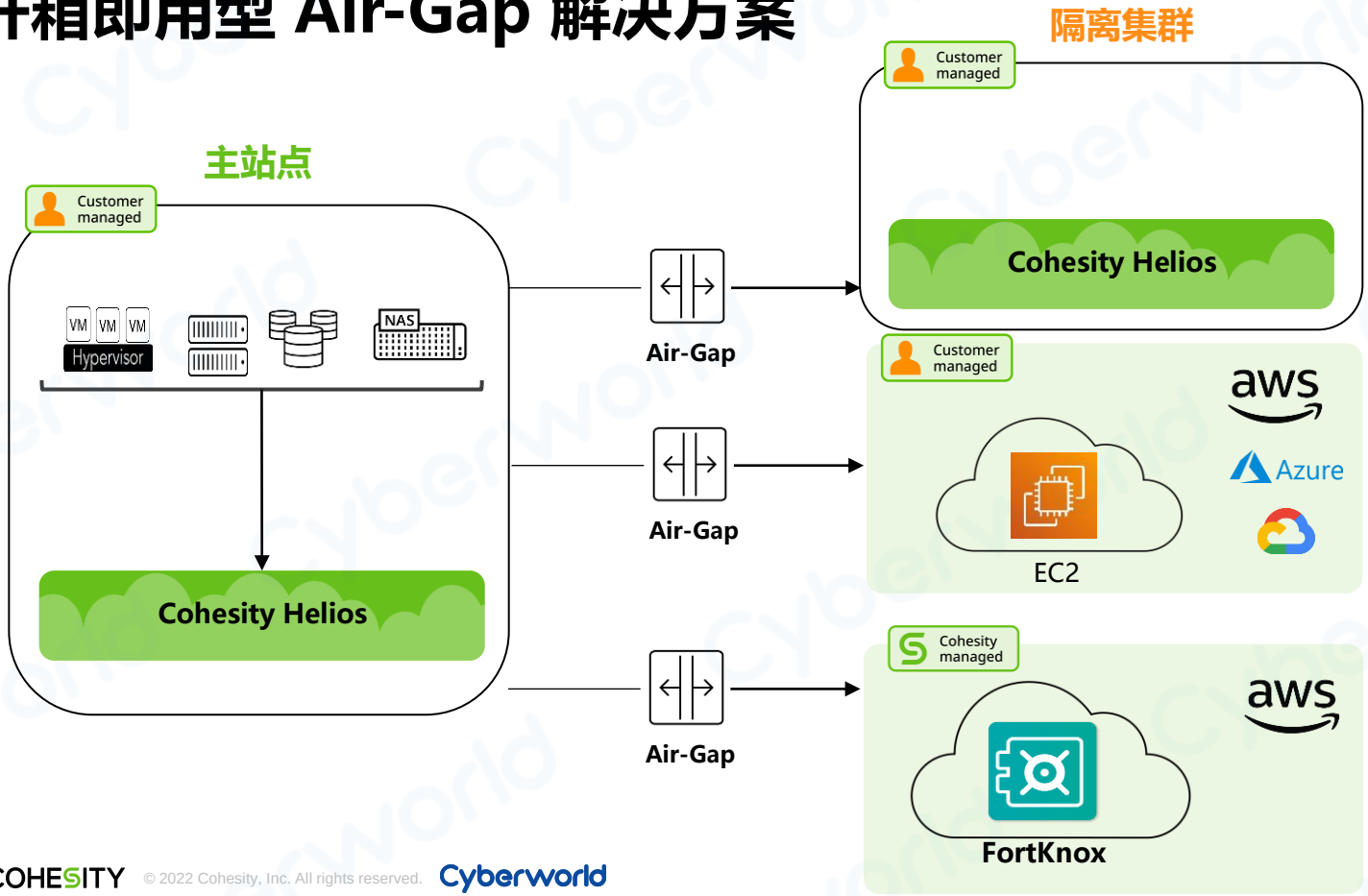
| 场景 | VM 数量 | 业务影响 | 风险性 | 即时恢复时间 | 目标恢复时间 | Cohesity POC 结果 |
|---|---|---|---|---|---|---|
| **删除或损坏的文件** | 1 | 低 | 高 | 基于文件计数的变量 | 基于文件计数的变量 | 具有灵活恢复选项的全局搜索<br>**< 1 分钟** |
| **单个 VM 损坏** | 1 | 低 | 中等 | 1-2 小时 | <10 分钟 | 即时恢复 VM<br>**< 1 分钟** |
| **存储卷损坏** | 30-50 | 中等 | 低 | 3 小时以上 | <10分钟 | 即时恢复50个 VM<br>**< 3 分钟** |
| **存储阵列损坏** | 300-1,200 | 高 | 低 | 8 小时 | 8 小时 | 即时恢复1,000个 VM<br>**39 分钟** |
| **应用升级回滚** | 1-50 | 中等 | 高 | 30 分钟 | <10分钟 | 即时恢复50个 VM<br>**< 3 分钟** |
| **操作系统补丁出错** | 300-1,000 | 高 | 低 | 5 天 | 28 小时<br>< 1 小时 | 即时恢复250个随机选择的 VM<br>**< 7 分钟** |
| **大规模恶意软件攻击** | 1,000-16,000 | 高 | 低 | 4 周 | < 24 小时 | 2,200个虚拟机已启动并可用<br>**47 分钟**<br>回到主存储=4小时 |

# 3-2-1备份策略

# 3-2-1备份策略+离境备份

- Three data copies 三份数据
- Two types of storage 两种不同储存
- One off-site location 一份脱机/离境备份

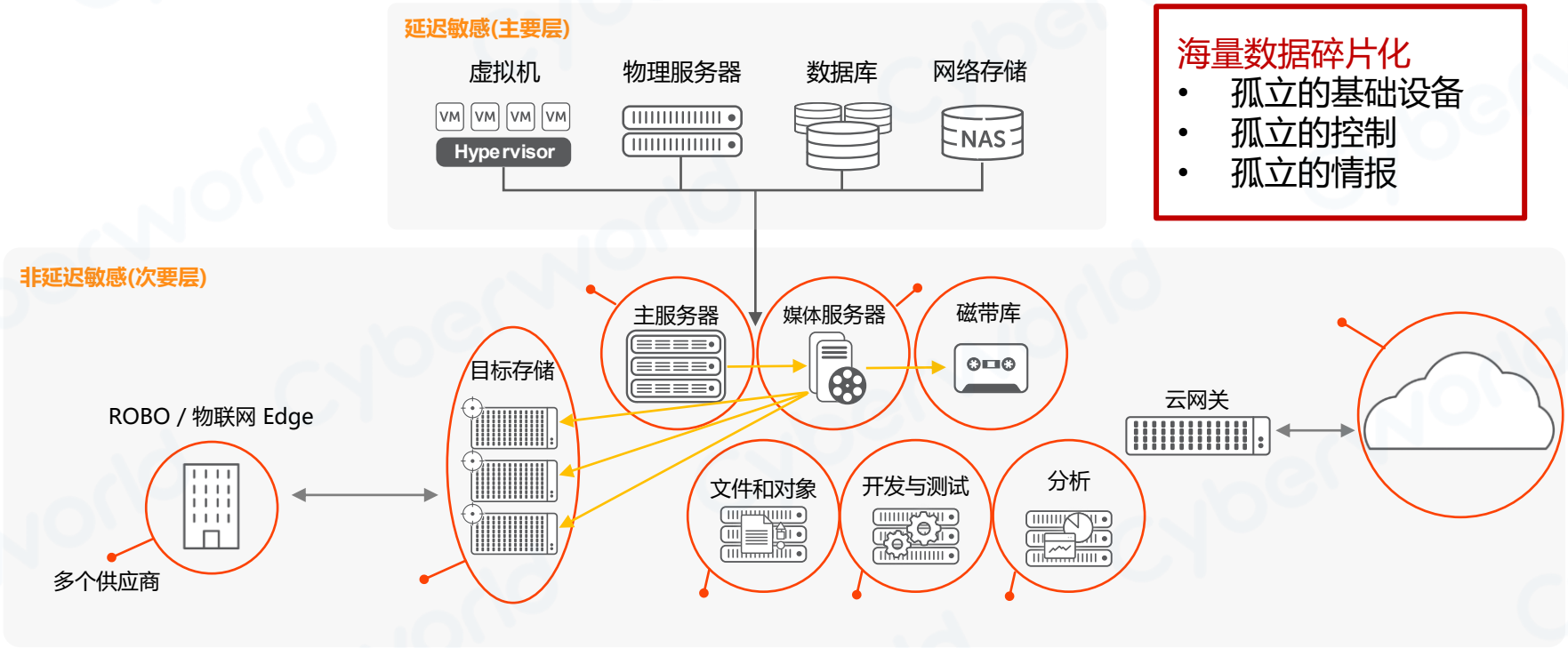
# 开箱即用型 Air-Gap 解决方案



# 永续的数据管理

# 数据管理非常复杂

## 碎片化 | 效率低 | 暗数据

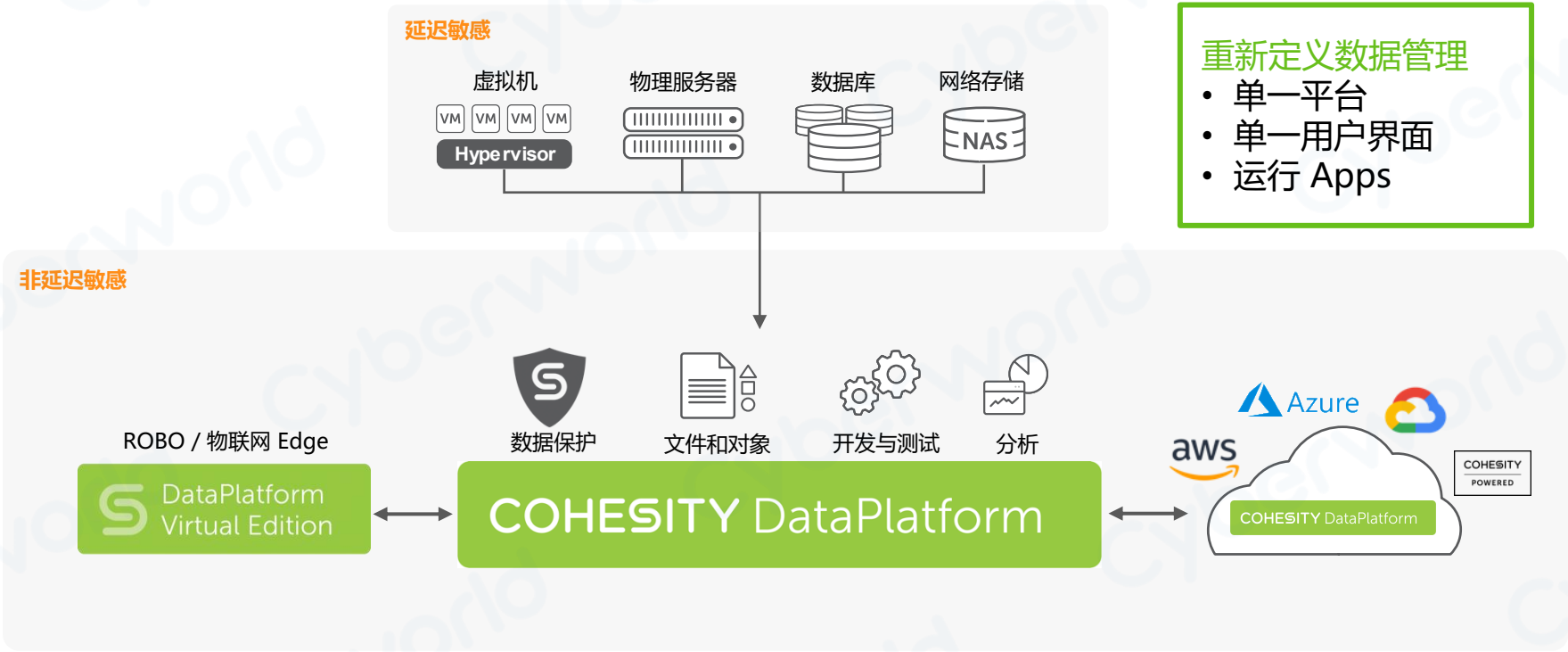



海量数据碎片化

- 孤立的基础设备
- 孤立的控制
- 孤立的情报

# Cohesity 简易数据管理

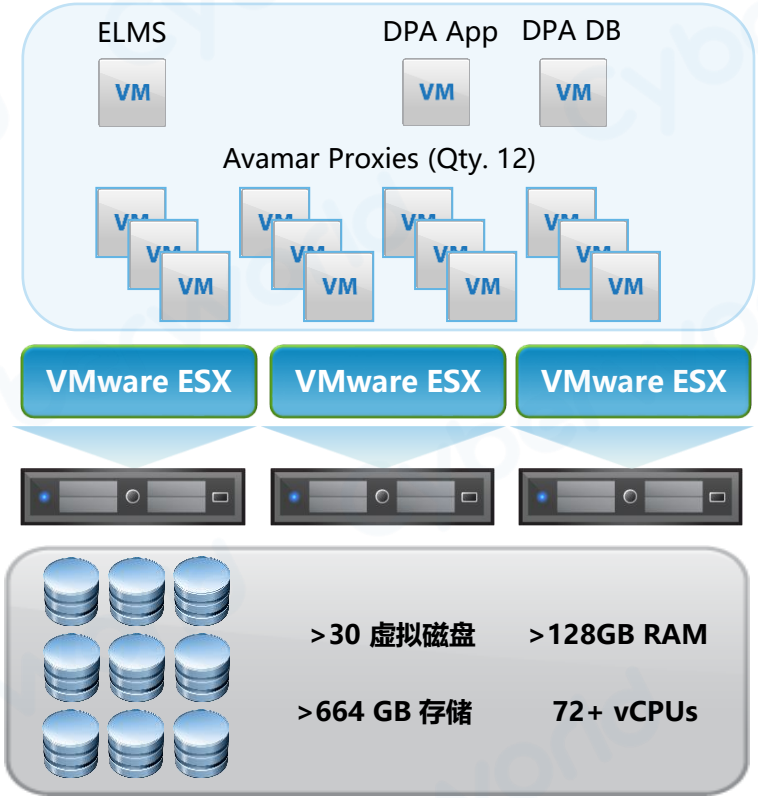
## 单一平台| 单一用户界面| 运行 APPS




重新定义数据管理

- 单一平台
- 单一用户界面
- 运行 Apps

# 现有客户环境

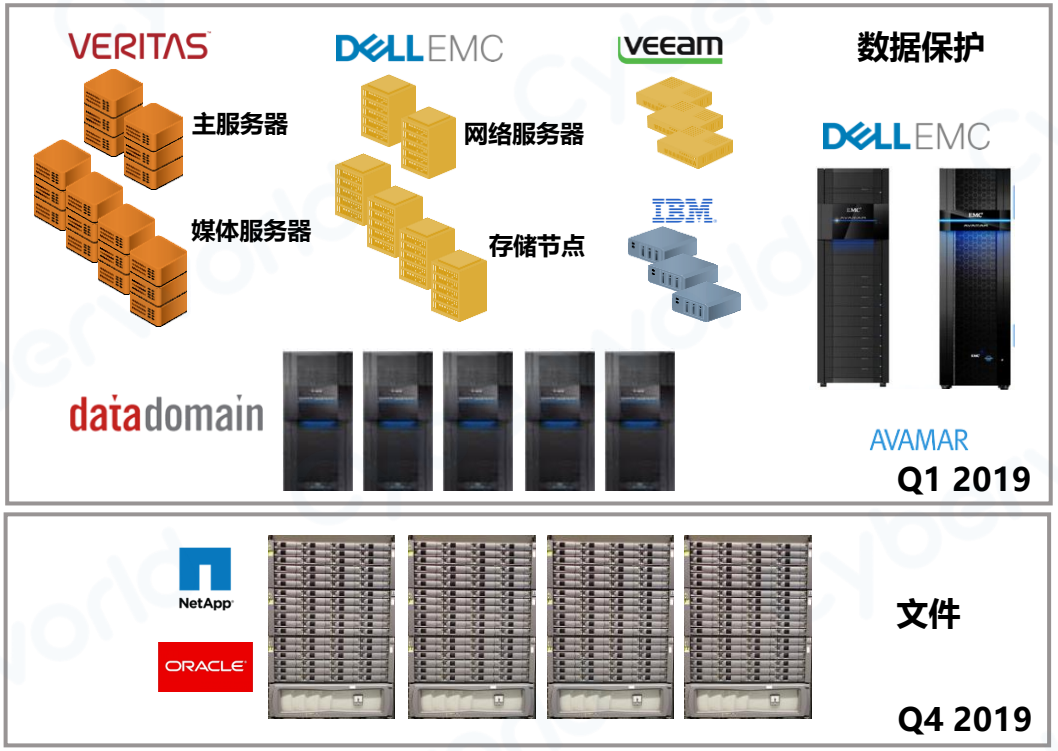





**数据保护套件企业版**

- Avamar
- NetWorker
- ProtectPoint
- DD Boost for Enterprise Apps
- RecoverPoint for VMs
- AppSync
- Data Protection Advisor
- SourceOne for email, files and Microsoft Sharepoint
- CloudBoost
- DP Search
- eCDM
- eCDA
- MSM/CLP

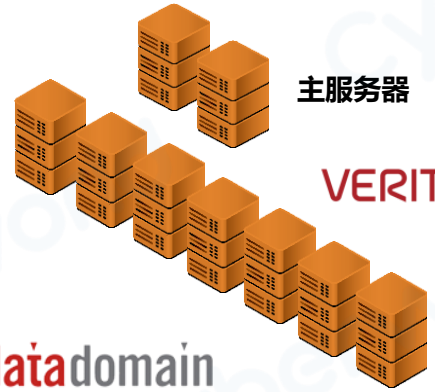
# 雄厚的企业采用 — 全球性信用卡公司




# 雄厚的企业采用 — 领先的全球性投资银行

媒体服务器

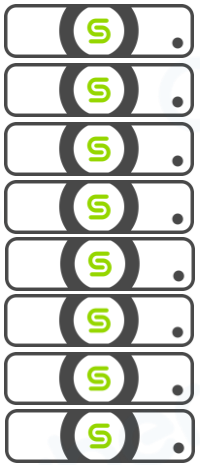
主服务器




datadomain

ORACLE

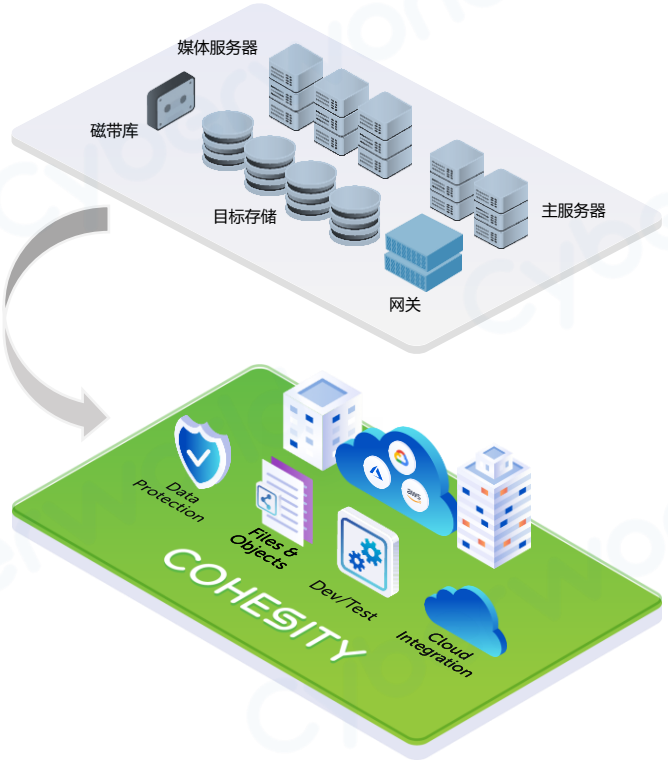
COHESITY



ORACLE

# 总结三点 3i

- 不可变性 Immutable
- 隔离性 Isolation
- 即时批量恢复 Instant Mass Recovery



COHESITY

Cyberworld

# 广州科明大同科技有限公司

## Cohesity 的中国区总代理商

COHESITY
AUTHORIZED DISTRIBUTOR

欢迎业务联系


官方网站：www.cyberworld.com.cn

广州公司：广州市天河区林和西路157号保利中汇A座2912室

上海办事处：上海市黄浦区淮海中路138号3楼WeWork 03N129

北京办事处：北京市朝阳区霄云路40号国航世纪大厦3层150室


cohesity.com