戴尔科技集团
防勒索解决方案介绍

戴尔资深高级客户经理
黄浩林 18602080399

DELL Technologies
戴 尔 科 技 集 团

勒索病毒

对各行业的危害分析

DELL Technologies
戴 尔 科 技 集 团

网络攻击来势汹汹

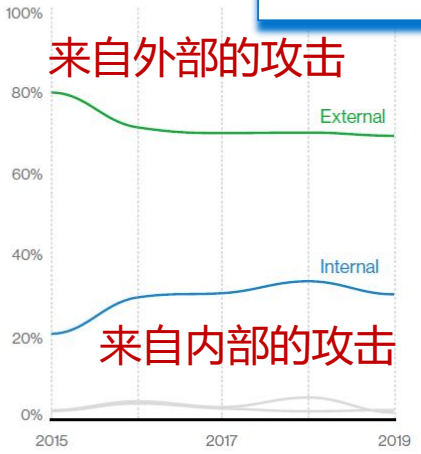
黑客攻击　勒索病毒　内部攻击

勒索钱财为动机

有组织的犯罪

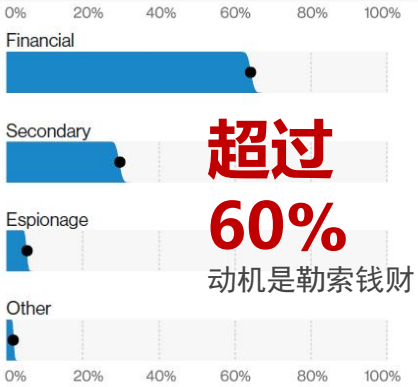
网络犯罪被称为历史上最大的财富转移， 埃森哲预测，未来5年，全球将有**$5.2万亿美元**资产面临网络犯罪的风险。

Figure 7. Actors over time in

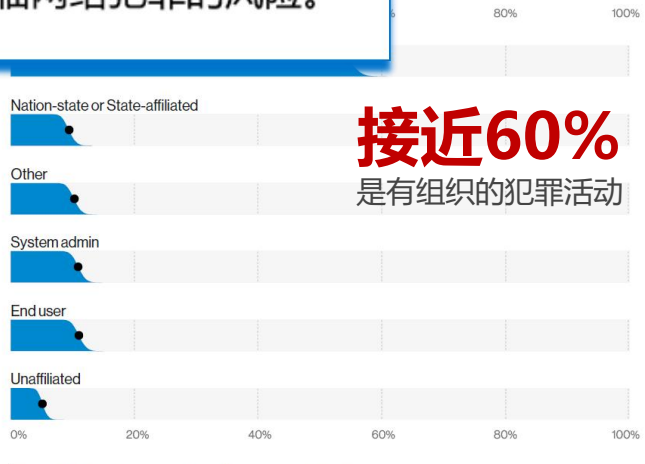


来自外部的攻击

来自内部的攻击



超过60%
动机是勒索钱财



接近60%
是有组织的犯罪活动

Figure 10. Top Actor varieties in breaches (n = 977)

数据来源：VERIZON公司的《**Data Breach Investigations Report 2020**》

国内外医院遭受勒索病毒攻击个别案例

国内

2017年5月	“永恒之蓝”勒索软件对成都市传染病医院等部分医院造成影响
2018年2月	湖南省某三甲专科医院也被爆疑似遭遇勒索病毒
2018年2月	上海某公立医院系统被黑，黑客勒索价值2亿元以太币

国外

2017年5月	英国全民医疗体系属下48个机构受到勒索病毒冲击
2017年5月	日本在国内确认了2起，分别为某综合医院和个人电脑感染病毒
2017年6月	美国最大制药商之一的默克（Merck）公司和宾夕法尼亚州西部经营两家医院的医疗网络机构——Heritage Valley 健康系统也成为新勒索病毒攻击的牺牲品。

具体案例： 湖北某医院遭受勒索病毒攻击

重庆晨报（记者牛泰）2月23日上午，湖北襄阳南漳县人民医院系统被植入升级版勒索病毒后陷入瘫痪，黑客要求支付比特币才能恢复正常。24日上午11时，该院回复上游新闻称，患者看病已不受影响，公安部门已介入调查。

多名知情人向上游新闻记者介绍，23日上午上班后，住院部医生发现，原来只能联内网的电脑可以上外网了；药剂师发现，因系统瘫痪录入在电脑中的药价等数据不见了；还有医生发现，存储在电脑中的病例也消失了。

南漳县人民医院办公室值班人员介绍，系统瘫痪后，他们联系技术人员前来修理，并向南漳公安局报警；另一方面，医生克服困难，就诊秩序没受太大影响。

上游新闻记者了解到，2017年勒索病毒全球爆发。23日上午，南漳县人民医院电脑系统被植入了“升级版勒索病毒”，黑客要求医院支付比特币，才能恢复正常。

目前，医院已建立了一个新系统，但之前的数据尚未恢复。

“这次被勒索的比特币换算成人民币，在30万元左右。”一知情人告诉上游新闻记者。

- 时间: 2018年2月
- 涉及范围: 医院系统瘫痪，取号、办卡、挂号、收费、诊疗等业务受到影响。
- 勒索赎金: 攻击者要求院方必须在六小时内为每台感染终端支付1个比特币赎金，约合每台终端解锁需要支付人民币66000余元。

DELL Technologies
戴 尔 科 技 集 团

遭遇勒索病毒攻击的后果：经济及连带损失>=赎金23X

至2021年，预测全球遭遇勒索病毒攻击损失讲高达$200亿美金

34%遭遇攻击的企业需要一个星期甚至更多时间来恢复数据

停机时间200%YOY
损失是赎金的23X

勒索攻击每11秒发生一次，21% YOY 增长

Source Information:

1. Source: Accenture “The Cost of Cybercrime Study” 2019
2. Source: Marsh & Microsoft “Global Cyber Risk Perception Study” 2019
3. Source: Cybersecurity Ventures “Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021” 2019
4. Source: Datto’s “Global State of the Channel Ransomware Report” 2019
5. Source: Kaspersky Lab survey

遭遇勒索病毒攻击的后果：对管理者及公 司的声誉损失

XX（信息技术部）

2020 年 6 月 27 日，由于你在工作期间未能遵守公司规定，安全意识差，作为公司信息技术部技术人员为对自己的办公电脑设置安全防范措施，造成其办公电脑中毒、收到攻击，从而导致公司整个网络系统瘫坏、停止运营长达 5 天以及公司重要数据丢失，严重影响公司的运营以及给公司造成重大损失（已超 20 万元人名币）。你的行为属于严重的渎职，违反公司的规章制度。对于前述情况，公司已经通知工会，向工会通知拟解除与你的劳动合同，工会无不同意见。

现公司根据公司《人力资源管理制度》以及《劳动合同法》第三十九条的规定，决定自 2020 年 7 月 24 日起解除与你的劳动合同关系。

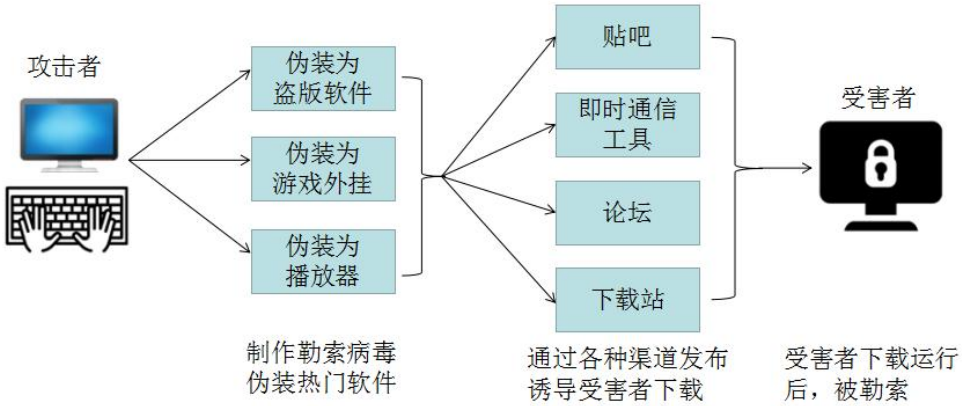
- 影响个人职业生涯
- 个人及医院受到行政处罚的可能
- 影响医院口碑、负面舆情

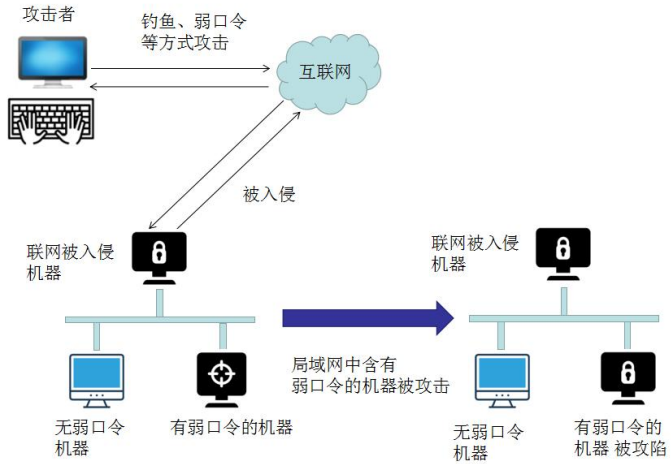
如何构筑数据安全的最后一道防线

DELL Technologies
戴 尔 科 技 集 团

杀毒软件、防火墙等不能防范勒索病毒

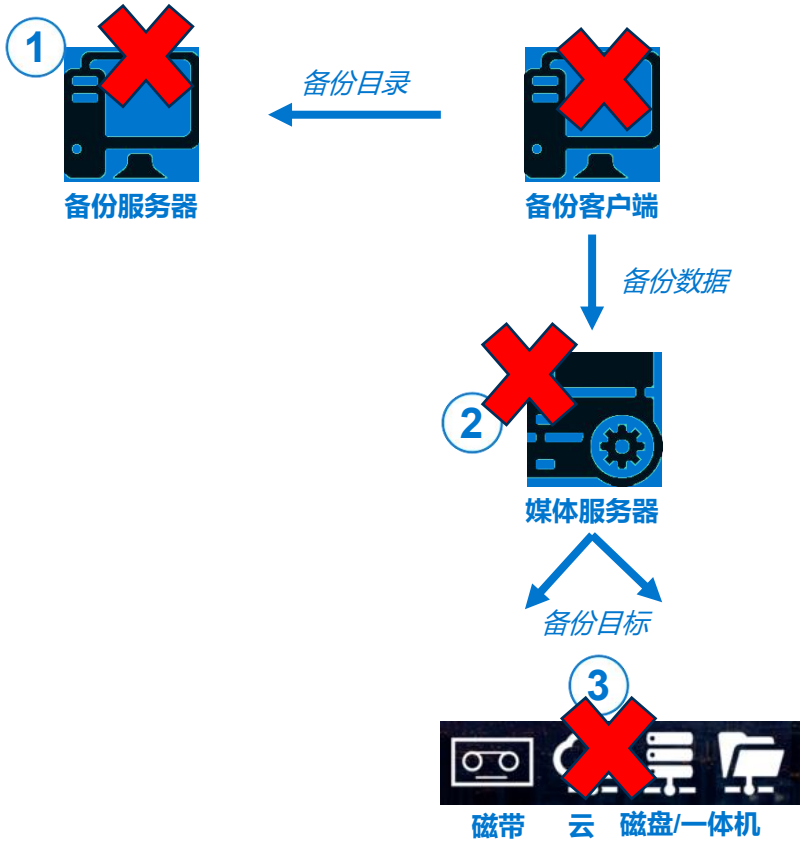
1. 杀毒软件、防火墙都不能彻底解决钓鱼、木马、弱口令、U盘接入等方式攻击
2. 勒索病毒变种快，杀毒软件无法拦截
3. 勒索病毒采用高强度加密算法，一旦数据被勒索加密，无法破解秘钥





通用备份系统不足以保护数据安全

通用备份系统各组件容易受到网络攻击：备份服务器、媒体服务器和备份目标



1. **备份服务器（含恢复所需的备份目录信息）：**以备份主服务器为攻击目标并使其感染病毒，从而导致加密/擦除备份目录
2. **媒体服务器：**以媒体服务器上安装的所有文件系统为攻击目标，将其加密/擦除
3. **备份目标：**
   - **磁盘/重复数据消除一体机：**以媒体服务器上的文件系统为攻击目标，将其加密/擦除。
   - **磁带：**如果在攻击前已从环境中移除威胁，则可提供更好的机会从破坏性事件中恢复。 但是，如果备份目录被劫持或销毁，则从磁带进行恢复将愈发困难。
   - **云：**由于依赖互联网，固有的安全性较低，使数据、备份和目录暴露在外。

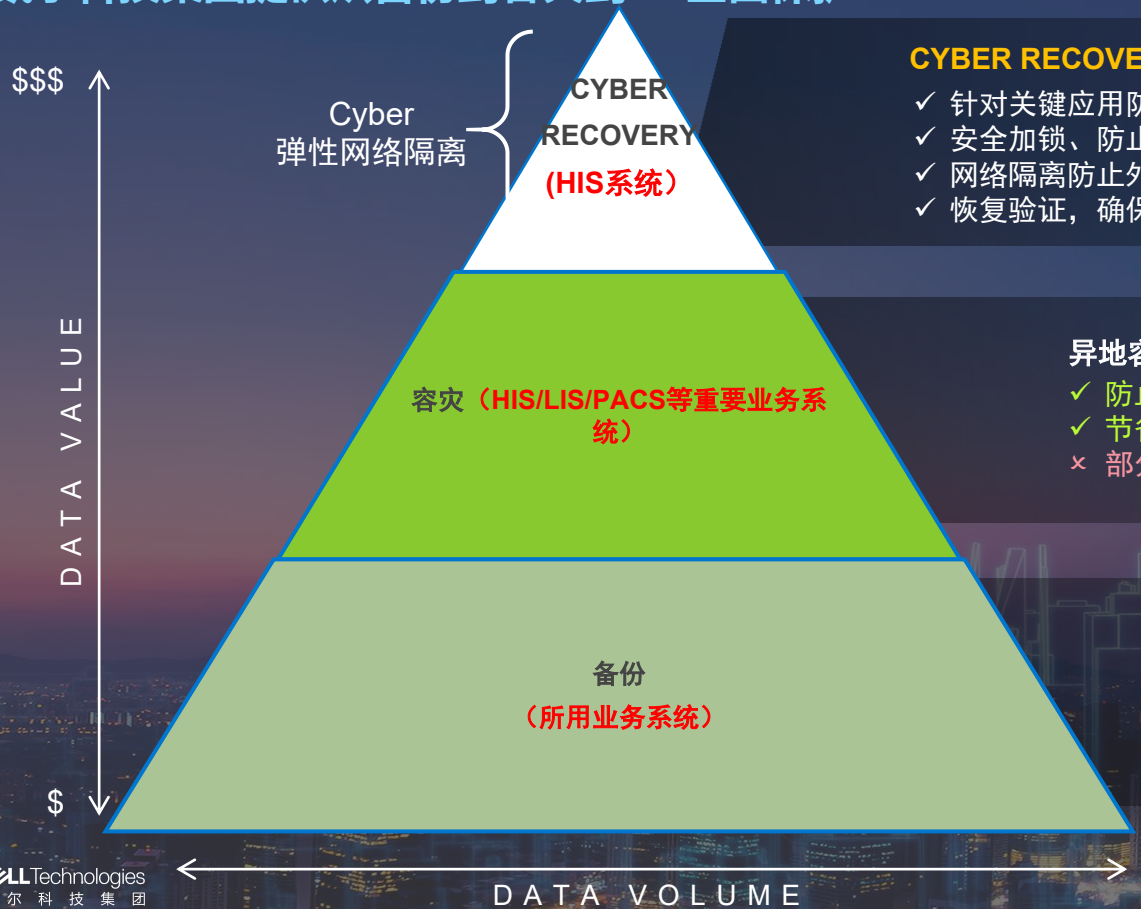
防盗门思维 – 只能防范正面攻击

保险柜的启发 – 对重要数据构建vault区（保险箱）

“不怕贼偷，就怕贼惦记”　　——防盗门也有失灵的时候

数据保护需要更安全

戴尔科技集团提供从备份到容灾到CR全面保护



CYBER RECOVERY

- ✓ 针对关键应用防黑客攻击、防勒索病毒最好的方案。
- ✓ 安全加锁、防止内部攻击。
- ✓ 网络隔离防止外部入侵，智能扫描分析识别潜在风险。
- ✓ 恢复验证，确保数据完整可恢复。

异地容灾

- ✓ 防止站点故障。
- ✓ 节省带宽、快速复制。
- × 部分保护黑客攻击、勒索病毒。

备份

- ✓ 最基本的保护，全面覆盖所有工作负载。
- ✓ 可靠、快速、低成本恢复。
- × 不能保护站点故障。
- × 不能保护黑客攻击、勒索病毒。

DELL Technologies
戴 尔 科 技 集 团

保证数据安全第一步：优化数据备份架构

远离容易攻击的系统，尽量避免备份数据成为容易攻击的脆弱点！

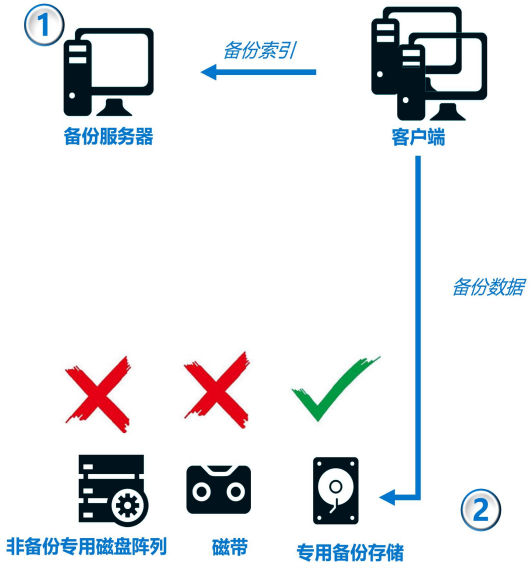
优化您的备份架构 – 尽量避免被攻击的可能性

① **备份服务器：**

- 远离主流的被攻击平台
- 备份索引目录需要自动备份

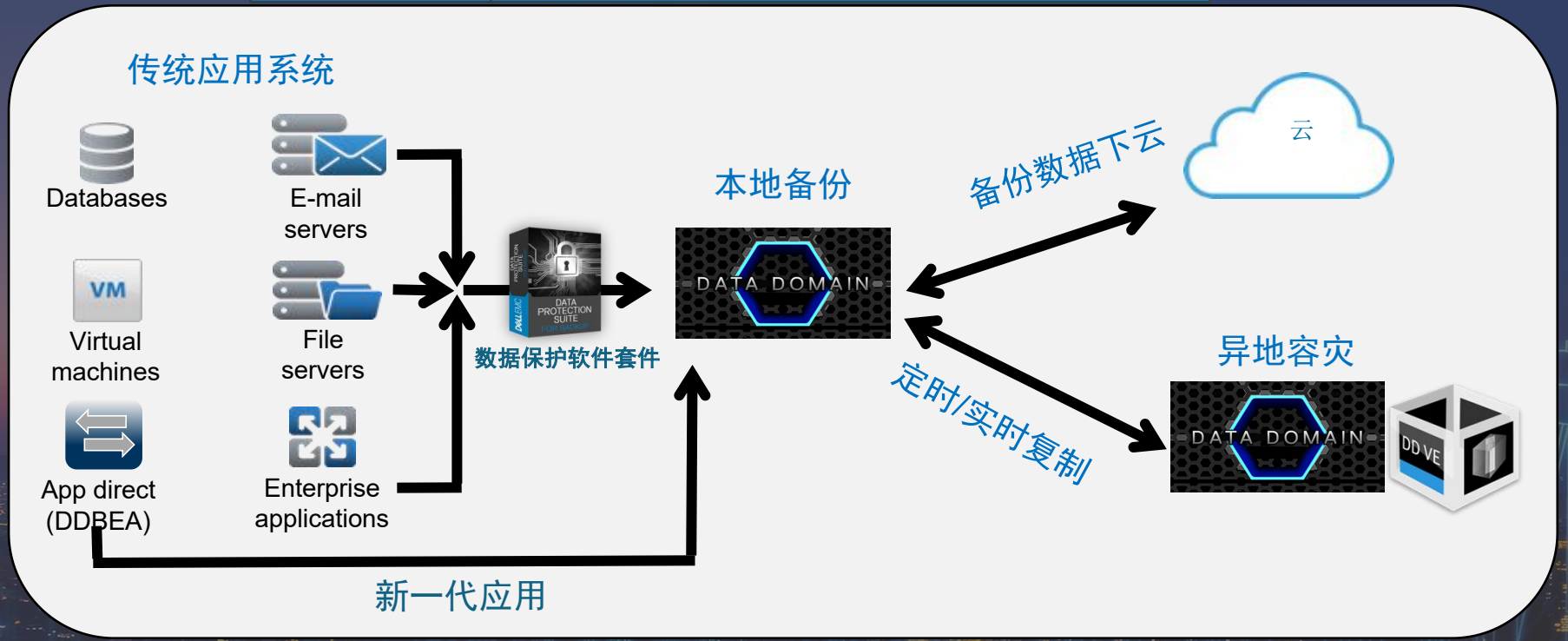
② **备份资料存储设备：**

- 尽量采用专用的备份设备
- 传输通道加密
- 备份资料加密
- 备份资料防篡改
- 快速还原的机制



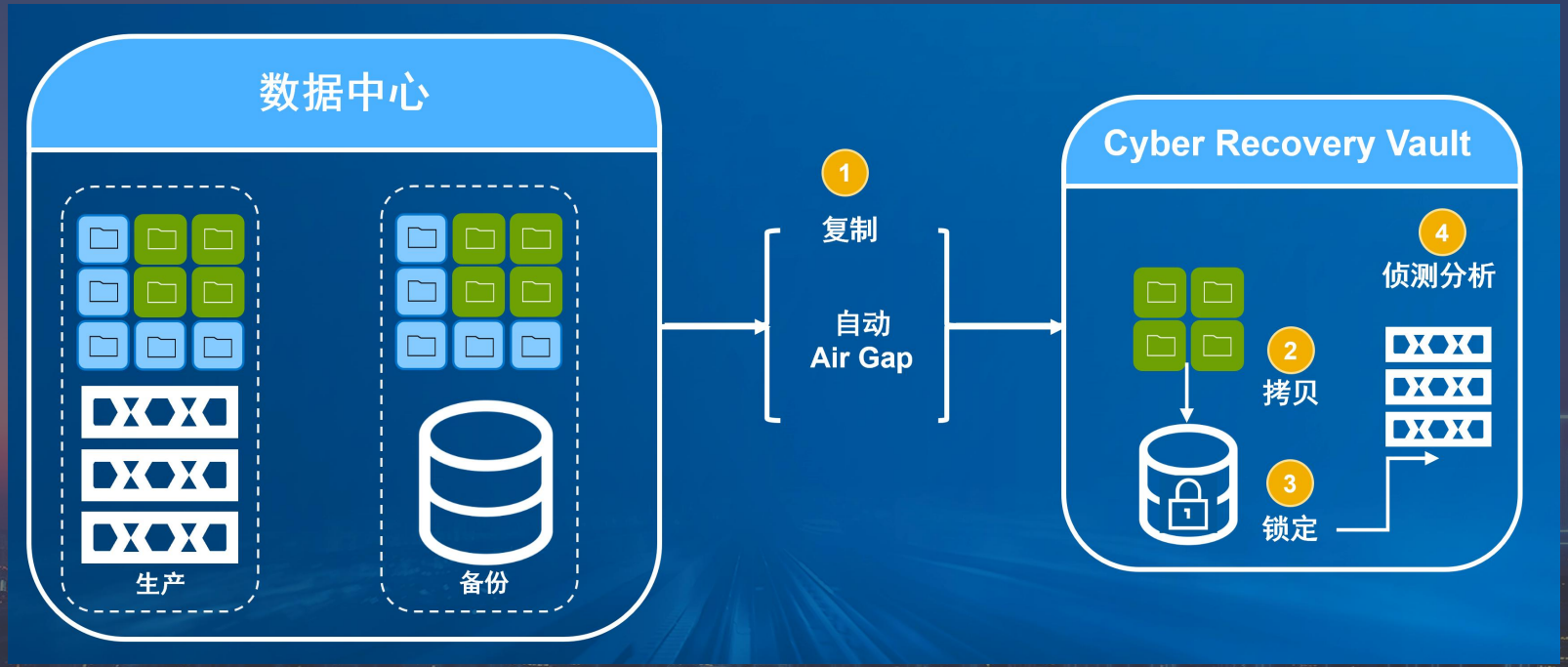
保证数据安全第二步：建立满足等保2.0要求数据级容灾

级别	要求
一级	本地备份与恢复
二级	本地备份与恢复+**异地定时备份**
三级	本地备份与恢复+异地数据实时备份+**本地业务高可用**
四级	本地备份与恢复+异地数据实时备份+本地业务高可用+**异地业务高可用**

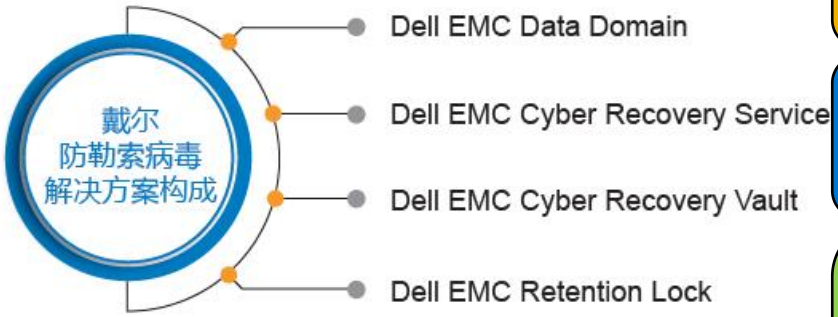


保证数据安全第三步：建立Cyber Recovery Vault（避风港）

对于重要的业务数据，除了备份+容灾保护外，还需建立Cyber Recovery Vault避风港



Dell 集团高度重视网络安全

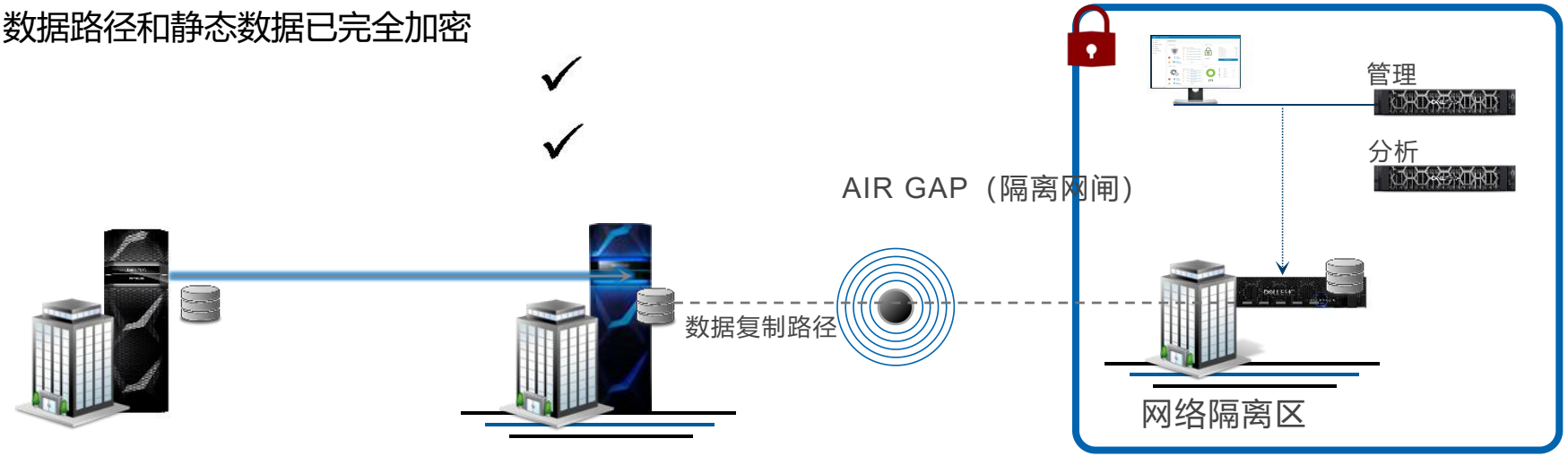


- 好
  - 备份数据加锁（Retention Lock），不可变副本
  - 提升的安全凭证
- 更好
  - 内部保护（Insider Protection）
  - 支持多个备份软件供应商
- **最好**
  - 自动的隔离网闸（Air Gap）
  - 基于完整内容分析和智能机器学习
  - 强大的恢复能力
  - 避风港（Sheltered Harbor）计划

勒索病毒防范解决方案概览

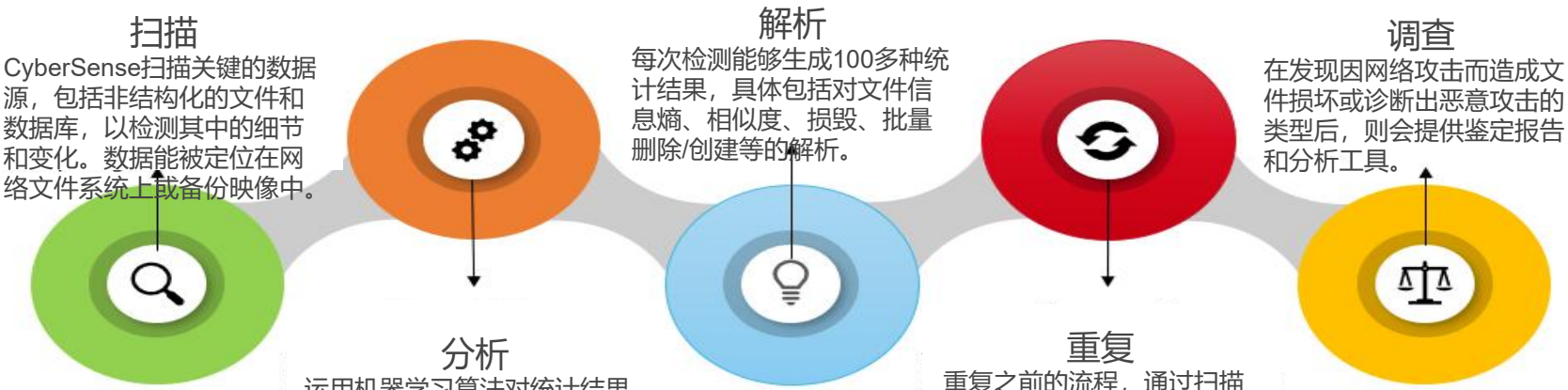
网络恢复架构和工作流程

- 受保护的存储和网络隔离区相互认证
- 除了复制周期外，实施全面的Air Gap
- 数据路径和静态数据已完全加密

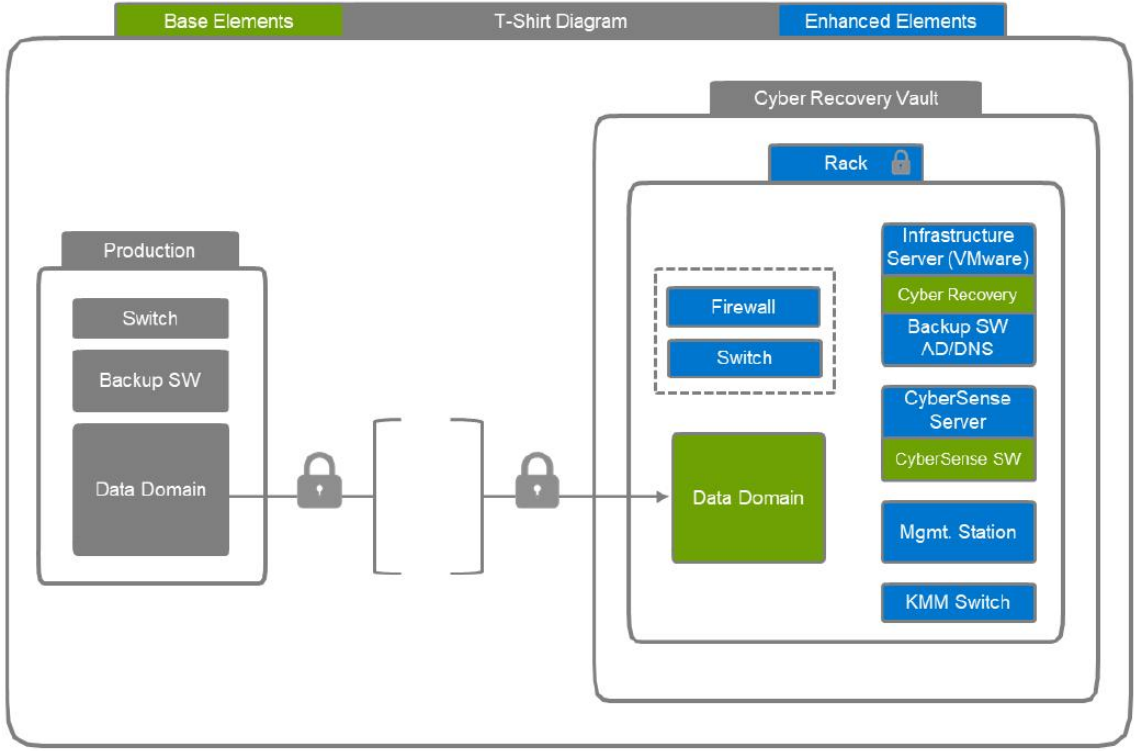


隔离网络恢复技术介绍

- CyberSense与数据保护软件配合使用，可分析备份中的数据，以识别在不知情的情况下被勒索软件破坏的文件和数据库。
- CyberSense利用基于完整内容的分析和机器学习的组合，来检测是否发生了攻击。CyberSense分析的内容涵盖所有常见的攻击目标，包括熵变（entropy change）、已知的勒索软件的变种、数据的损坏和删除，以及100多种其他统计数据。
- CyberSense会通过机器学习技术分析统计信息，以确定是否已经发生数据损坏。



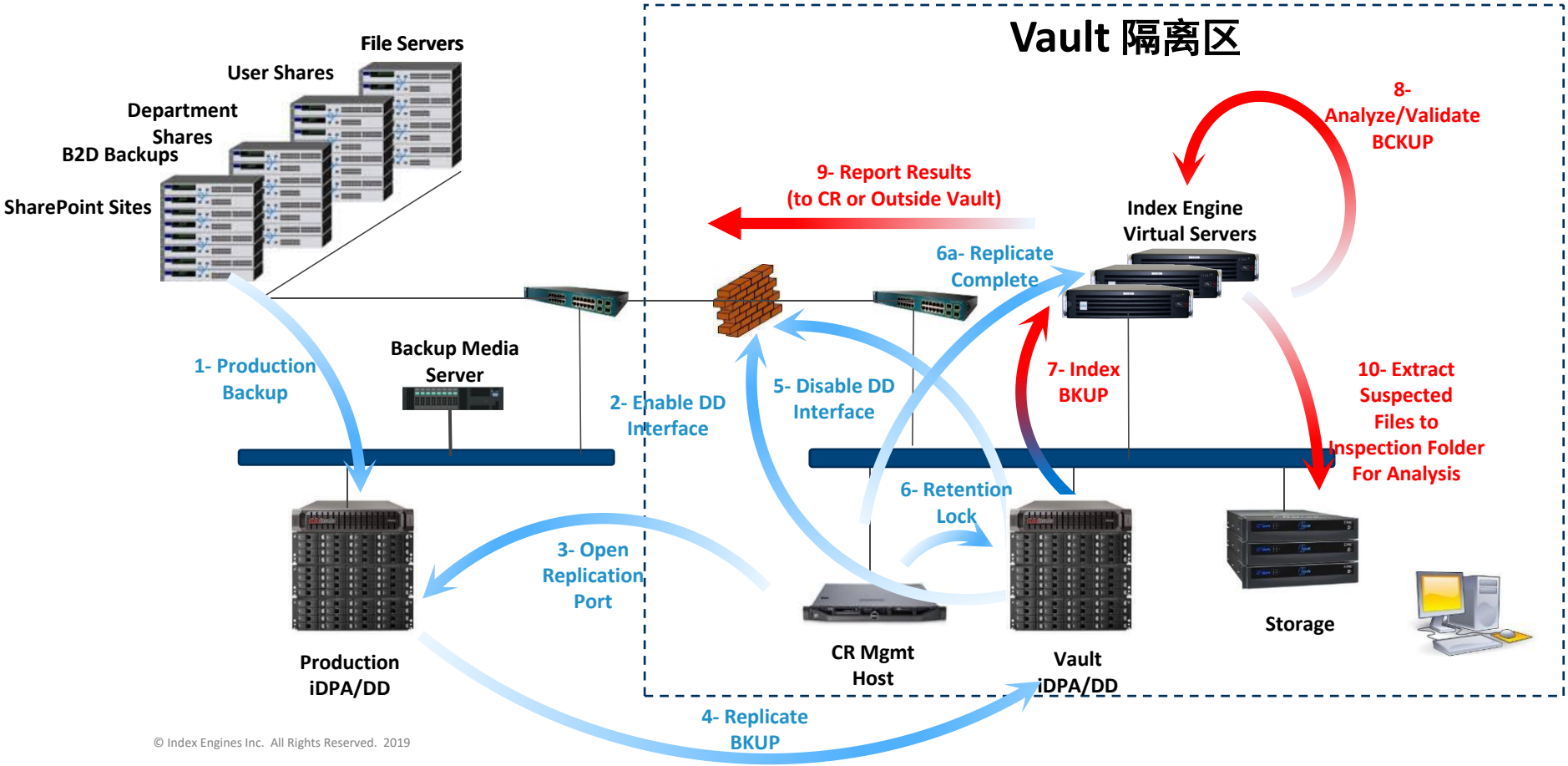
CR T-shirt Solution 组件概览



- 绿色部分为CR T-shirt solution的基本组件，是构成CR所需最小配置
- 蓝色部分为CR T-shirt solution的增强组件，是构成CR客户可通过DELL购买的组件
- CR T-shirt solution只包含Vault区组件，不包含Production 站点的组件

DELL Technologies
戴 尔 科 技 集 团

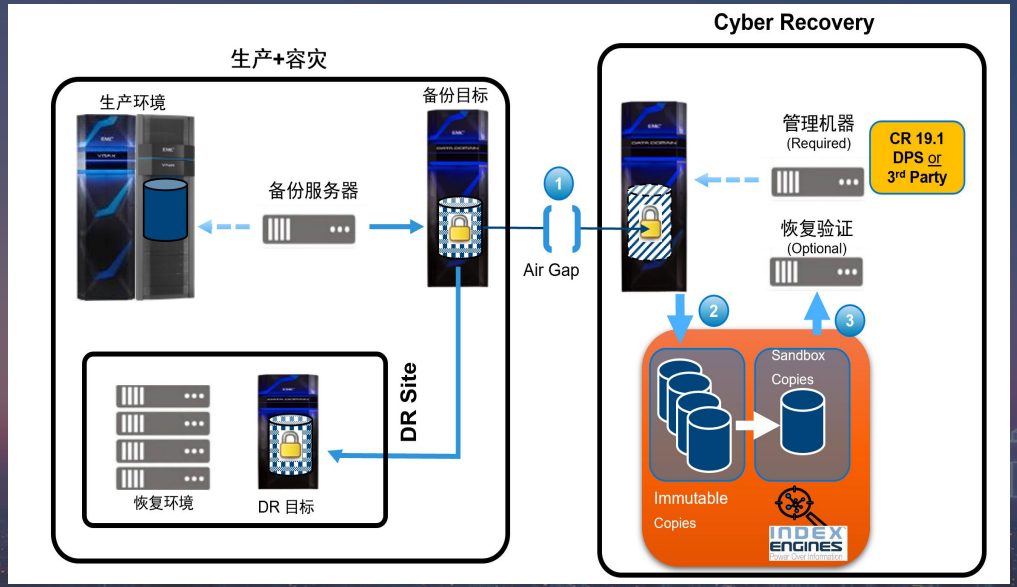
Cyber Recovery + CyberSense 工作流程



确保数据安全的多重数据保护方案：备份+容灾+CR避风港

第一步
- 本地备份
- 异地容灾

第三步
- 数据上锁，生成不可篡改版本
- 在沙箱内扫描侦测数据是否被感染破坏



方案主要特点和优势

断：
断开备份主机及备份储存媒体，避免备份主机及备份数据同时遭绑架勒索

舍：
舍去大量数据，透过专利去重复技术，舍去高达60倍的储存空间需求

离：
离开风险，建构安全备份平台

锁：
锁住备份数据，无法恶意窜改

侦：
使用 AI/ML 技术对恶意软件（包括勒索软件）进行扫描、分析、侦测，并提供即时报警

第二步
- 重要数据复制CR保险库
- 设置弹性网络隔离降低入侵风险

第四步
- 对完整数据进行恢复验证

DELL

CR 解决方案价值

DELL Technologies
戴 尔 科 技 集 团

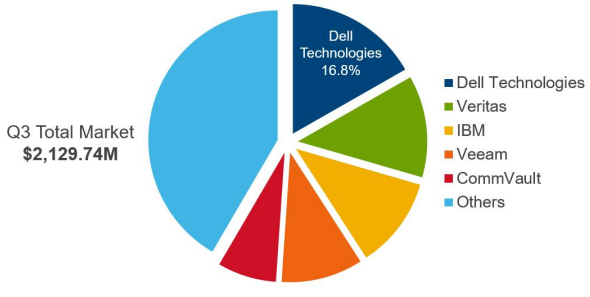
戴尔CYBER RECOVERY 方案价值

- Dell EMC Cyber Recovery 是业内唯一能够针对勒索病毒自动启动有效防御和恢复机制的解决方案。最大程度减少遭受网络攻击的损失。
- Dell EMC Retention Lock 创建不可删除、不可篡改的副本，防止勒索病毒攻击，阻止病毒对数据的加密。
- Dell EMC Cyber Recovery Vault 通过Air Gap 技术建立独立的、隔离的、不可窜改、不可删除的数据隔离区（Data Vault），将数据隔离和业务连续性的优势相结合，最大程度减弱网络攻击带来的影响，提高数据安全。
- 通过进行数据恢复的训练和测试、备份数据的数据验证和分析，确保工作人员熟悉流程，让企业面对最严重的网络攻击情况下对业务的连续性抱有信心。
- 还能够利用人工智能（AI）和机器学习（ML），运用40 多种推断方法来对受保护的数据进行广泛的扫描，分析和持续验证，进一步确保资料本身安全。

DELLEMC 数据保护领域的 4个第一

Data Protection Software

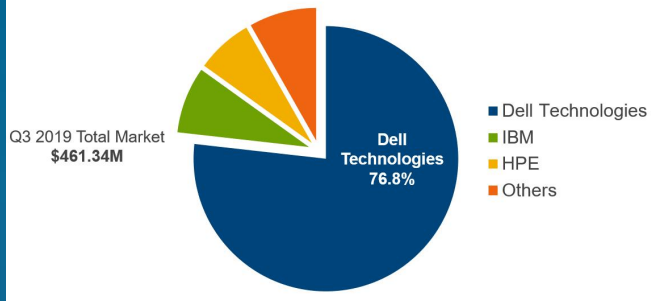
Q3 2019 Total Revenue



Source: IDC Quarterly Storage Software and Cloud Services Qview, 3Q19

Purpose Built Backup Appliances

Q3 2019 Total Revenue Target Systems

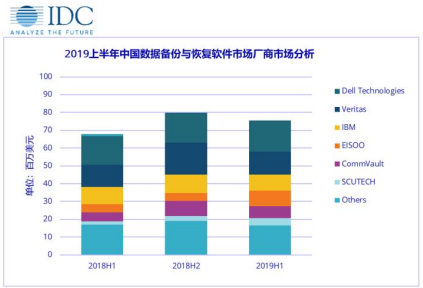


Source: IDC Quarterly Purpose Built Backup Appliance Tracker, Q3 2019

2019年上半年中国备份与恢复软件份额

从数据备份与恢复软件市场来看，2019年上半年，数据备份与恢复软件占数据备份与恢复系统总市场的48.7%，较去年同期略微上升。

从软件供应商表现来看，戴尔2018全年和2019上半年出货量均排名第一。2019上半年，戴尔出货量占数据备份与恢复软件市场的份额为23.3%，排在第二的是Veritas，占有率为17.0%，其次为IBM和爱数。



来源：IDC中国，2019

2019年上半年中国备份一体机份额

从数据备份与恢复一体机市场来看，2019年上半年，数据备份与恢复一体机占数据备份与恢复系统总市场的51.3%。

从数据备份与恢复一体机供应商表现来看，戴尔2018全年和2019上半年出货量亦排名第一。2018年，戴尔出货量占数据备份与恢复一体机市场份额为16.8%；排在第二的是鼎甲，占有率为15.0%。

2019上半年，戴尔出货量占数据备份与恢复一体机市场的份额为15.7%，排在第二的是爱数，占有率为11.2%；排名第三为H3C，其出货量在2019上半年度较去年同期实现了高速的增长。

来源：IDC中国，2019

对医疗行业用户的价值

- 省钱：
  - 免遭天价勒索
  - 降低删库跑路带来的经济损失

- 省心：
  - 提供入门、进阶、终极多层次解决方案，可以分期部署也可以一步到位
  - 基于机器学习算法侦测网络攻击，及时报警
  - 快速地从网络攻击中恢复

- 放心：
  - 规避职务风险
  - 全球300+客户案例和5年以上的实践经验

常见问题应对

- 我们有灾备了，不需要CR
  - 如果您的备份系统也被勒索了，您如何恢复？CR帮助您打造备份的隔离区，使得备份受感染的几率大大降低。当数据被入侵时可以迅速用“干净”的数据恢复生产
- 如果数据被恶意软件入侵，复制到隔离区，隔离区也被“污染”了
  - 驻留在Data Domain隔离区里的备份数据是不可更改的，确保总有干净的数据。数据被复制到CR隔离区后，恶意软件无法正常执行或处理计算指令，只能处于休眠状态
- 我有磁带机了，不需要CR
  - 磁带可靠性低，无容错能力
  - 无重删功能，大数据量的备份导致磁带数量激增难以保管
  - 无法分析受损数据
- 我现在用的不是DELL EMC的备份软件，也可以搭建数据避风港吗？
  - 可以的。数据避风港方案可以用DELL EMC的DD与其他厂商的备份软件搭建，我们的工程师可以和您具体说明


DELL Technologies
戴 尔 科 技 集 团