灰犀牛和避风港计划

刘庆宇
数据保护首席架构师
戴尔科技集团

2021-3-27

黑天鹅还是灰犀牛

早在公

天鹅比

much lik

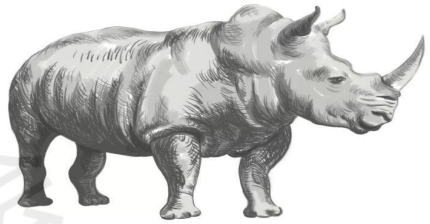
012年希腊金融危机后发

“黑天鹅”这一术语是美国经济学家纳西姆·尼古拉斯

，而是一系列预警和明显征兆（a series of and visible evidence）之后爆发出来的问题。灰犀2001年创造的。

袭击时，极具爆发力，且不可阻挡

灰犀牛正在来的路上



2015

2016

2017

2018

2019

2020

TeslaCrypt 勒索软件瞄准的是主要游戏平台的玩家们

Chimera2015-9月份首次出现，但已经推出了勒索软件服务商业模式，从中收取客户50%的利润。比较有趣的是，他们招募的勒索软件运营人员主要是他们的受害者

RAnsom32赎金高达13比特币

Locky登上了多家报纸头条。威胁行为人马上发现，感染医疗保健必备设施的相关系统会带来巨大收益，因为多家医院都立即支付了赎金

SamSam包含了一个信道，可供攻击者通过一个 .onion 网站与受害者直接实时联系。Petya如果其索要的431美元赎金未在7天之内收到，赎金金额还会翻倍。

Maktu 是第一款利用Crypter(加壳器)加密自身源代码的勒索软件Jigsaw《电锯惊魂》系列电影里的Jigsaw角色。如果150美元的赎金未被支付，它将会每60分钟删除一份文件。另外，如果受害者试图终止该进程，或者重启机器，它就会马上删除1000份文件

CryptXXX 散布最严重的最新勒索软件变体。：反沙箱技术、鼠标活动监测、定制C2通信协议、Tor赎金支付。

ZCryptor 有自繁殖技术，能感染外部设备和网络中的其他系统，加密每台机器和共享硬盘。

Ransomware-as-a-Service（RaaS）的兴起
IBM：2016 年勒索软件增长 60 倍，赎金规模 10 亿美元
赛门铁克 个人消费者仍然是勒索软件的主要攻击目标（57%）。但长期趋势表明，以企业为攻击目标的勒索软件正在缓慢且稳步地增长。

WannaCry勒索病毒全球大爆发，至少150个国家、30万名用户中招，造成损失达80亿美元，已经影响到金融，能源，医疗等众多行业，造成严重的危机管理问题。
5月12日：全球近74个国家受到严重攻击
24小时内监测到的WNCRY敲诈者蠕虫攻击次数超过10W+

台积电芯片制造基地遭遇“勒索病毒”，损失超过11亿
波音位于南卡罗来纳州查尔斯顿的生产工厂遭到了WannaCry勒索软件的网络攻击。这可以说是近日2018年以来，被媒体曝出来的首例WannaCry勒索病毒攻击案例。
2018年1月，GandGrab勒索家族首次出现

GandCrab 狂赚20亿美元金盆洗手
加拿大两大银行支付赎金
国内多家医疗政府被勒索
CyberEdge 2019年，选择支付赎金的受害者比例是45%，2018年则是39%。

波音/本田/佳能/佳明/德国AG SOFTWARE/研华/富士康/智利银行/阿根廷电信/企业旅行社CWT/在线教育巨头K12.....

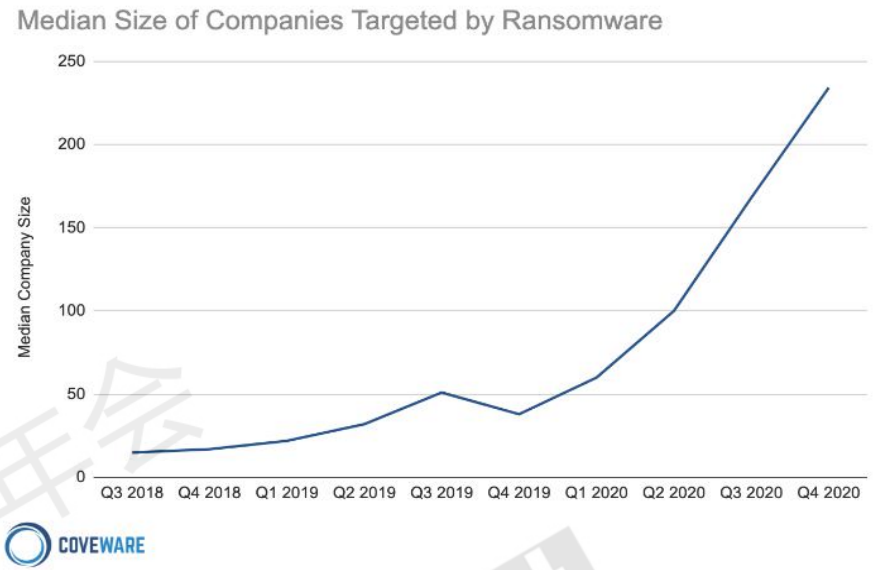
Ryuk
RagnarLocker
DoppelPayme
.....

勒索病毒的发展趋势

2016 比特币均价 $700

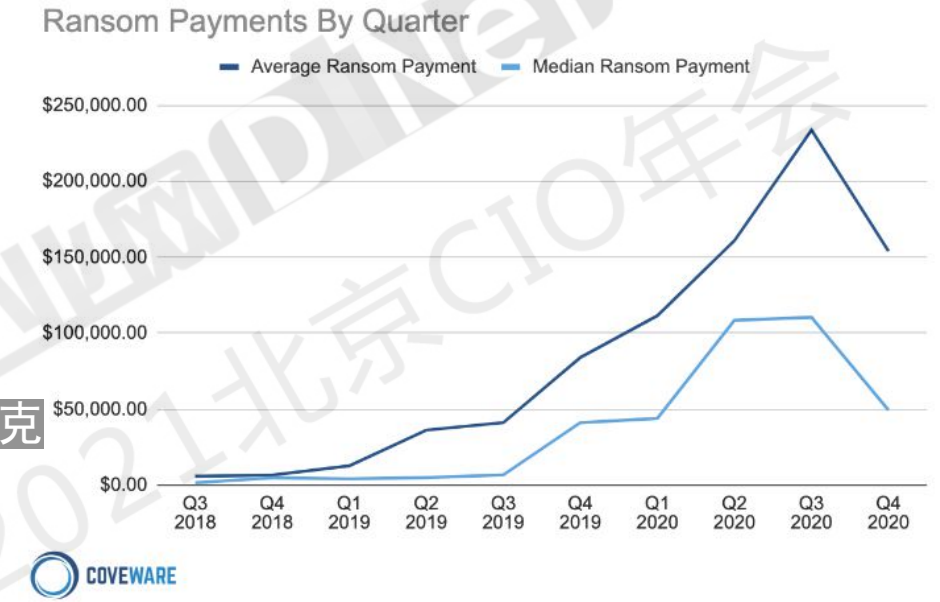
2020 Q4 比特币均价 $20000

28倍



从2015年年末至今，勒索软件的平均赎金增长超过2倍，从294美元增长至679美元。2020 Q4达到15万美元

220倍



Palo Alto: 机构平均支付赎金从 2019 年的 115123 美元增加到 2020 年的 312493 美元，同比增长 171%。网络犯罪分子已经变得越来越贪婪。

如果你想避免出现黑天鹅事件，就要先处理好灰犀牛事件------米歇尔·渥克

安全公司给出的建议

安全体系不能100%防住勒索病毒

传统备份成为勒索病毒绕不开的一道坎

勒索方证实，他们于11月29日袭击了富士康在北美的工厂，但并未袭击整个公司。

作为此攻击的一部分，威胁人称，已加密了约1,200台服务器，并删除了20-30 TB的备份。

BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White

FIREEYE Products Mandiant Solutions Customers

Threat Research

Unauthorized Access of FireEye Red Team Tools

December 08, 2020 | by FireEye

FIREEYE TOOLS RED TEAM

Overview

A highly sophisticated state-sponsored adversary stole FireEye Red Team tools. Because we believe that an adversary possesses these tools, and we do not know whether the attacker intends to use the stolen tools themselves or publicly disclose them, FireEye is releasing hundreds of countermeasures with this blog post to enable the broader security community to protect themselves against these tools. We have incorporated the countermeasures in our FireEye products—and shared these countermeasures with partners, government agencies—to significantly limit the ability of the bad actor to exploit the Red Team tools.

You can find a list of the countermeasures on the FireEye GitHub repository found HERE.

Red Team Tools and Techniques

GARMIN

Garmin官方微博

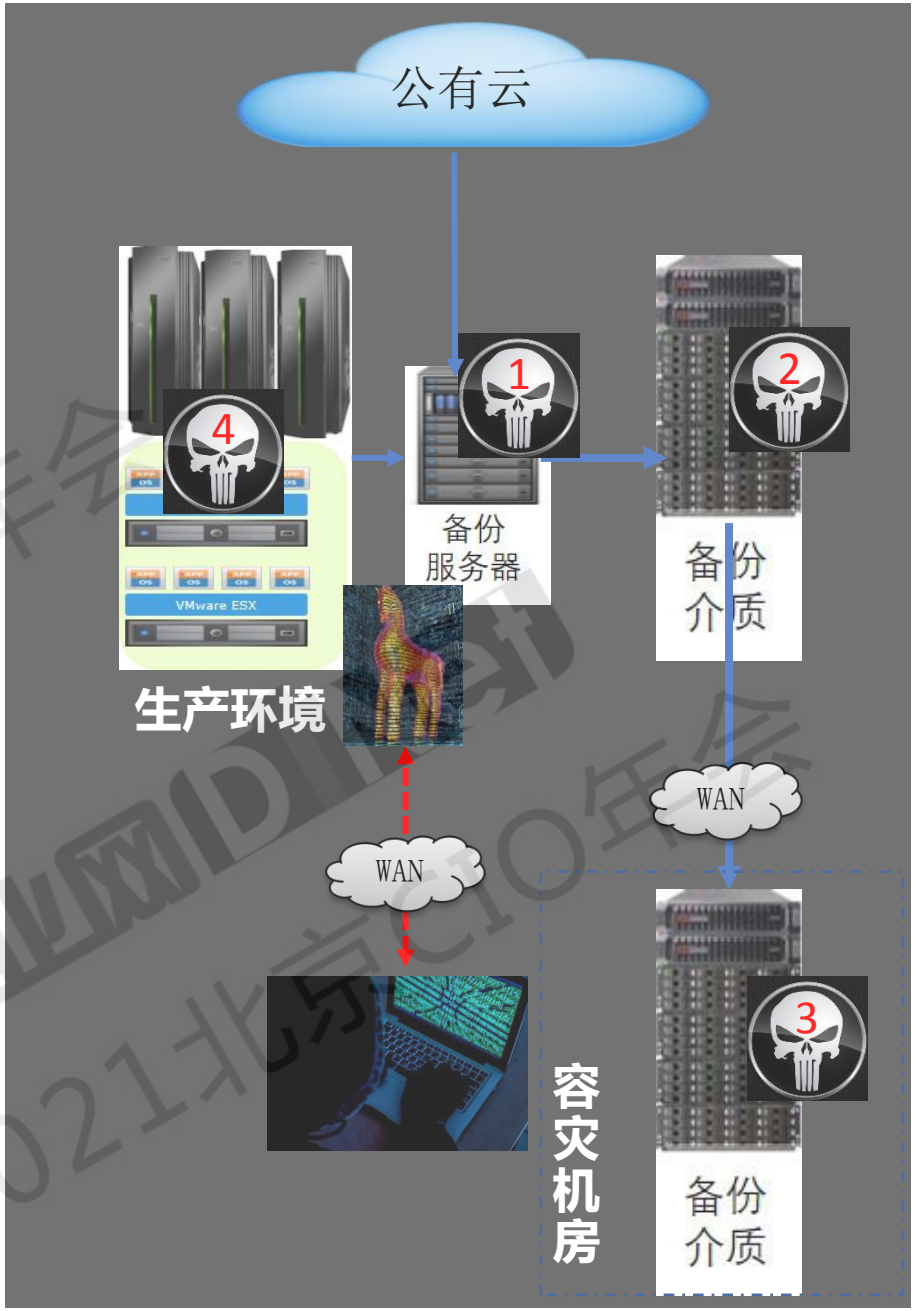
7月28日 18:42 来自 微博 weibo.com

Garmin 系统和服务相关公告

尊敬的用户您好：

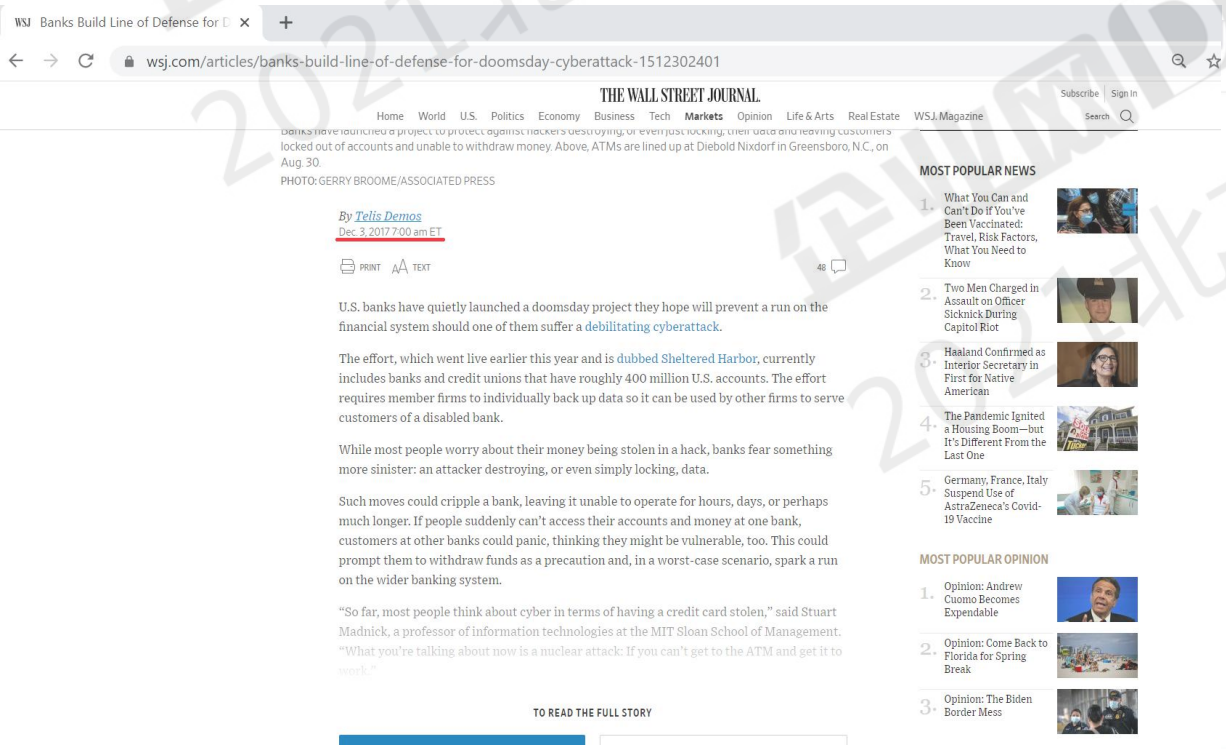
我们诚挚地宣布，目前暂停运作的 Garmin 系统和服务，包括 Garmin Connect 国际服务器相关服务等，已陆续恢复运行。由于目前我们仍在处理部分数据资料，因此某些功能暂时仍然不可用。我们真诚地感谢所有用户的耐心配合与理解！

2020年7月23日，我们受到了网络攻击，导致我们许多在线服务受到了影响，包括网站功能、客户服务支持、终端应用程序和公司通讯等。Garmin 高度重视数据安全与客户服务，因此我们当下立即评估了攻击的性质、危害的范围并紧急开启了应对措施。

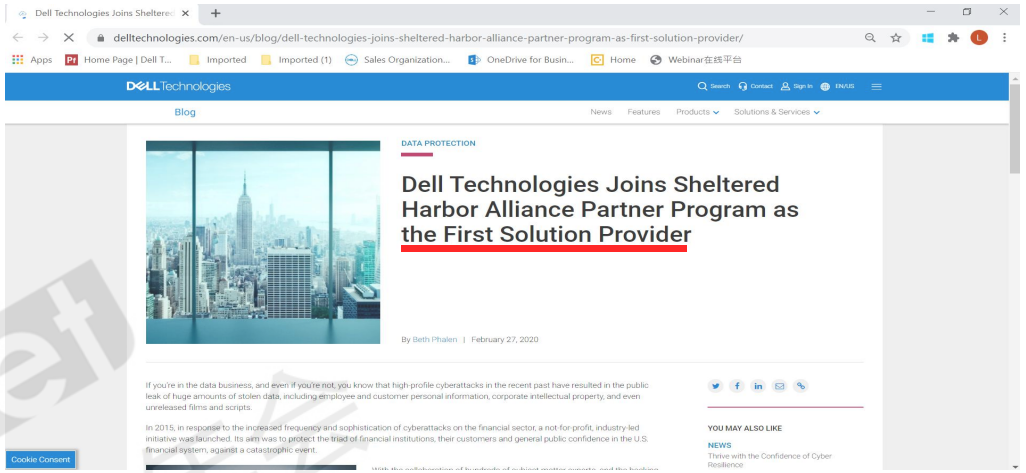


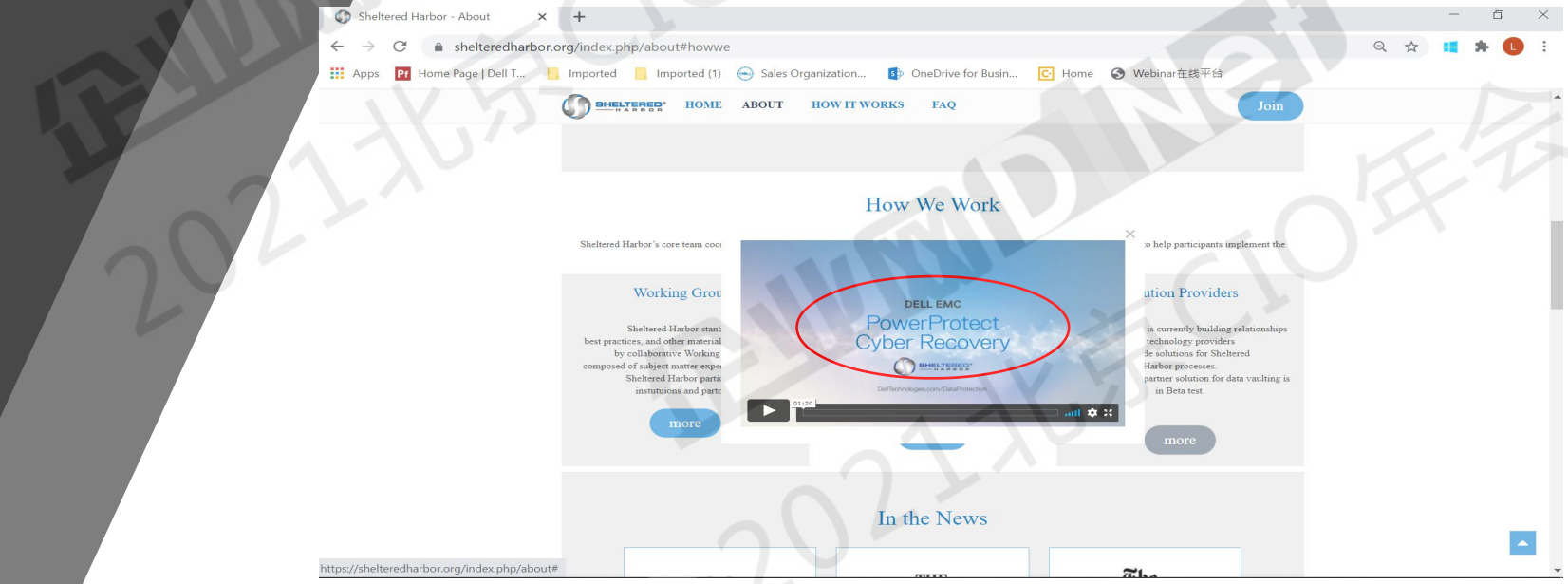
人们不去做一件事的原因之一就是，他们觉得自己没有那么大的力量改变事物

-------米歇尔•渥克

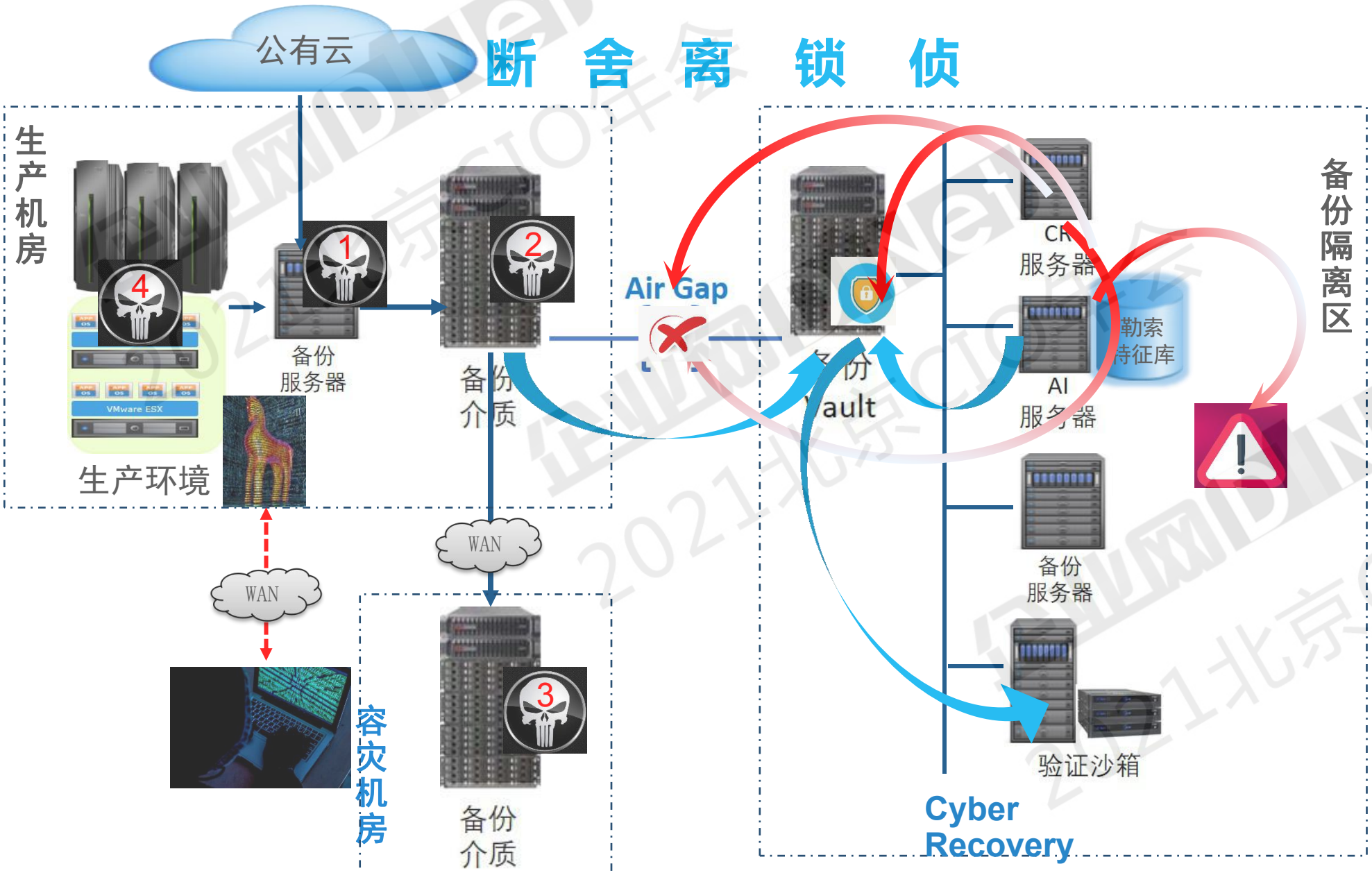


DELLEMC 成为避风港计划第一个 也是 唯一 入选的解决方案供应商





流程是功能实现的保障

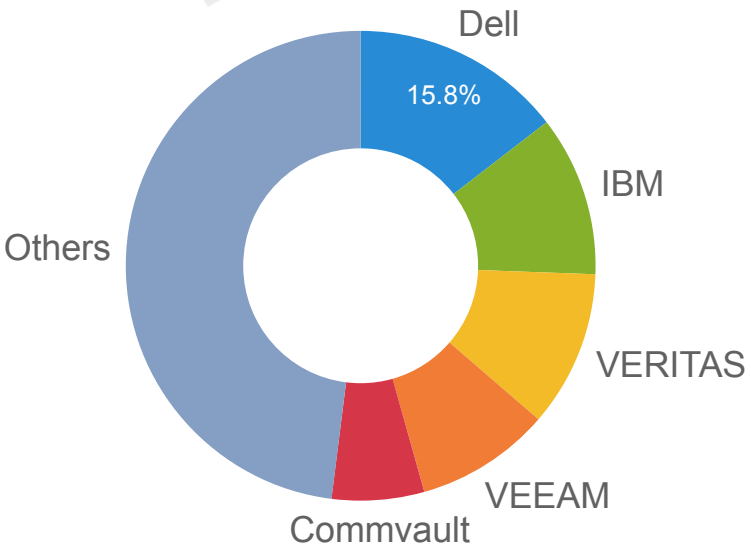


1. 打开Air Gap
2. 数据复制到隔离区
3. 断开Air Gap
4. 数据加锁
5. 读取数据并分析
6. 异常告警
7. 恢复验证

DELLEMC – 数据保护领域领导者

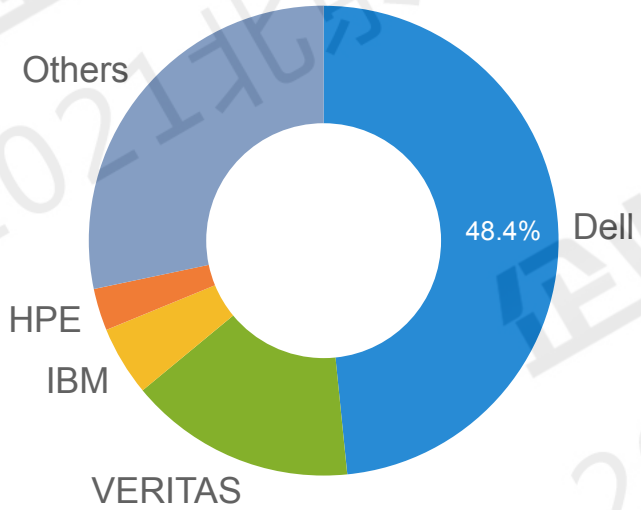
20年 Gartner魔力象限领导者

软件全球市场份额第一 @15.8%



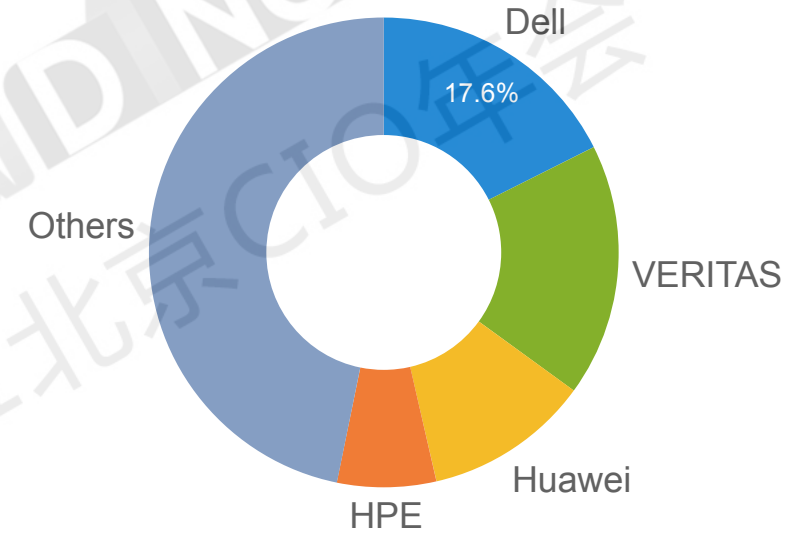
来源： IDC 2020Q2 Storage SW QView, Sept 2020；

PBBA全球市场份额第一 @48.4%



来源： IDC 2020Q2 PBBA Tracker, Sept 8 2020

PBBA大中国区市场份额第一 @17.6%



来源： IDC 2020Q2 PBBA Tracker, Sept 8 2020

在中国，为中国

戴尔科技集团中国研发集团

- 新产品开发
- 新技术研究

92	483	25000
大学院校	跨国企业研发中心	高科技公司

- 新产品开发
- 新技术研究
- 技术支持

64	575	9206
大学院校	跨国企业研发中心	高科技公司

- 软件测试 系统测试
- 方案验证

52	206	3000
大学院校	跨国企业研发中心	高科技公司

数据来源: 2019年《中国科技统计年鉴》

DELL Technologies
戴 尔 科 技 集 团

一. 承认危机的存在。

二. 定义灰犀牛式危机事件的性质。

三. 不要静立不动。

四. 不要浪费危机。

五. 站在顺风处。最好的领导会在危险尚未靠近的时候就采取行动。

当危险只远在天边，人们就需要提前制订一系列的计划。

六. 成为发现灰犀牛式危机的人，成为控制灰犀牛式危机的人。

米歇尔·渥克

刘庆宇 13910654989 Qingyu.liu@dell.com