Lenovo NetApp

向勒索经济SAY NO

解读新常态下的数据安全

丽达 联想凌拓产品经理
朱海光 VERITAS资深系统工程师

2020.8.26

Agenda

- ➔ 我们遇到的挑战
- ➔ 联想凌拓对于数据安全的见解
- ➔ 联想凌拓在数据安全方面的合作伙伴华睿泰
- ➔ 华睿泰对于数据安全的见解
- ➔ 我们一起帮助客户实现数据安全

Lenovo NetApp

“勒索软件网络攻击已经是一门大生意，事实上，研究预计每11秒就有一家企业被网络犯罪分子攻击，到2021年，这些攻击造成的损失成本将达到200亿美元左右。”

新浪财经 美股 > 正文

行情 简称/代码/拼音

本田：全球业务网络被勒索软件攻击 部分产线被迫停工

2020年06月11日 11:39 新浪财经综合 新浪财经APP

安装新浪财经客户端第一时间接收最全面的市场资讯→【下载地址】

原标题：本田官方发声：全球业务网络被勒索软件攻击 部分产线被迫停工 来源：驱动之家

如果公司遭到了勒索病毒的攻击，由于该病毒独特的加密机制，被攻击方除了缴纳赎金之外，往往没有更好的解决办法。而当下，本田汽车(25.59, 0.71, 2.85%)就遇到了这件麻烦事。

我的電腦出了什麼問題?
您的一些重要文件被我加密保存了。
照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因
這和一般文件追儘有本質上的區別。
您大可在網上找我恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢

有沒有恢復這些文檔的方法?
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的
但這是收費的，也不能無限期的推遲。

但想要恢復全部文檔，需要付款點費用。
是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對妳不利。
最好3天之內付款費用，過了三天費用就會翻倍。
還有，一個禮拜之內未付款，將會永遠恢復不了。

我們只會接受比特幣。首先，您需要支付解密服務費。
請發送0.05個的比特幣到該比特幣地址: 1NXTgfGprVktuokv3ZLhGCPCjcKjXbswAM
發送以後，請復制本軟件上的本機KEY和您付款給我們比特幣的時間發送到我們的郵箱地址Wanna
我們收到比特幣以後就會把您的解密密碼發送到您的郵箱。您拿到密碼以後，在本軟件上輸入密

聯系方式: WannaRenemal@goat.si

我強烈建議，為了避免不必要的麻煩，恢復工作結束之前，請不要關閉或者刪除該軟件，並且暫

佳明遭勒索病毒攻击：被曝向黑客支付数百万美元“赎金”

2020年08月04日 19:39 1152 次阅读 稿源：快科技 0 条评论

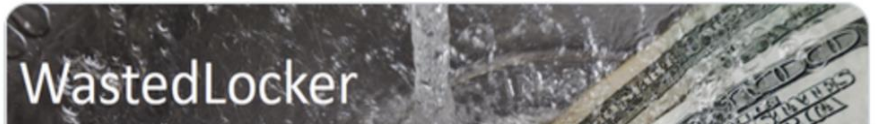
日前，知名可穿戴设备、GPS设备厂商Garmin（佳明）确认，其网络遭遇攻击，致使运营和产品服务出现问题。据外媒报道，佳明此次遭遇的是勒索病毒攻击，黑客一开始索要的赎金高达1000万美元。

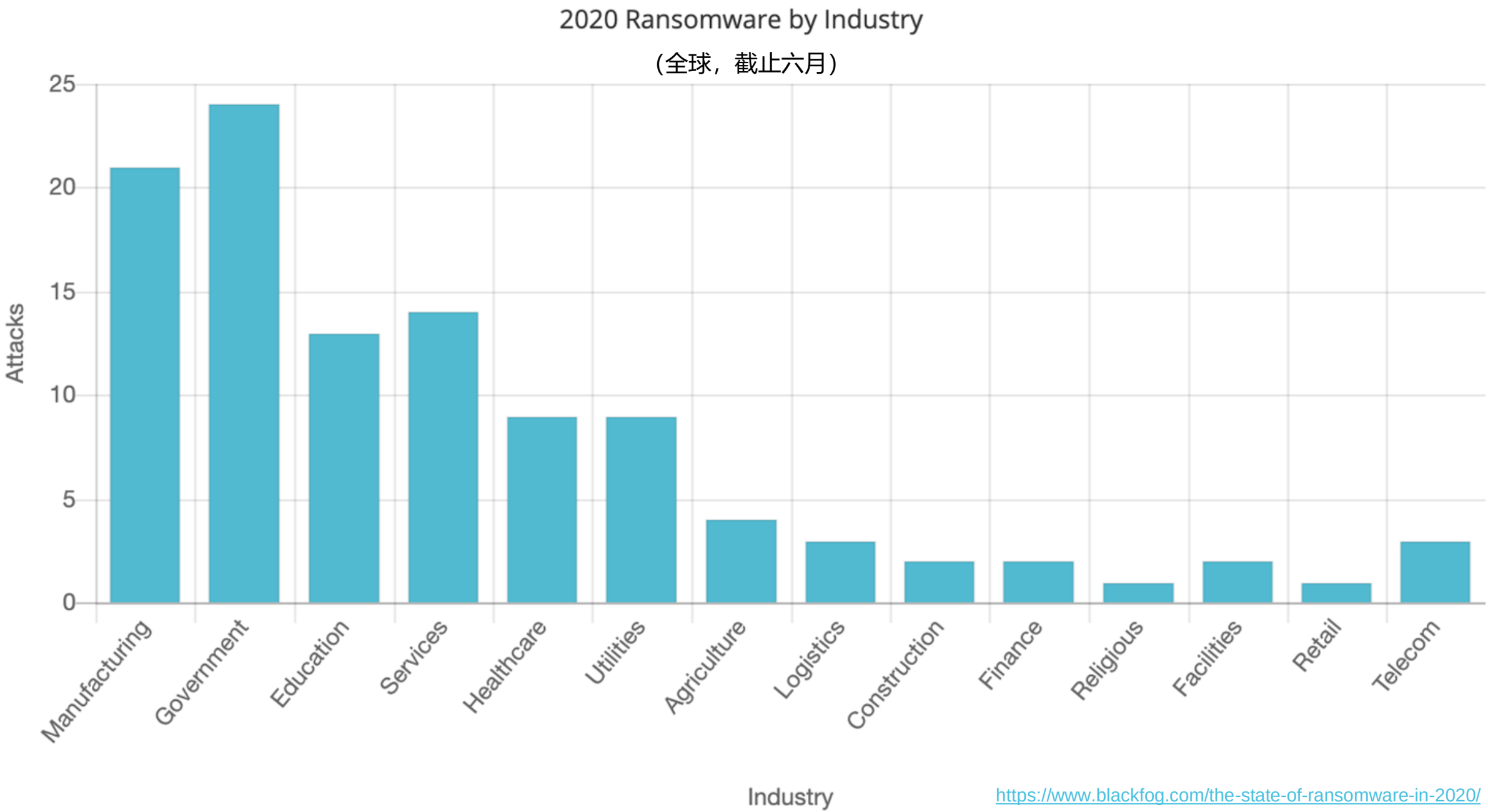
访问：

阿里云福利专场 云服务器ECS低至102元/年

Arete Incident Response
@Arete_Advisors

WastedLocker is a new variant of #ransomware that was initially reported in May and is rumored to have come from the "Evil Corp" group. In this insight, we discuss the four main reasons why Arete experts determined this theory to be inconclusive. (bit.ly/3f18Mly)





https://www.blackfog.com/the-state-of-ransomware-in-2020/

联想凌拓是谁?
我们如何看待勒索病毒?

联想凌拓

智能数据管理
解决方案及服务

致力于加速企业实现数字化转型

Lenovo
NetApp

我们的优势

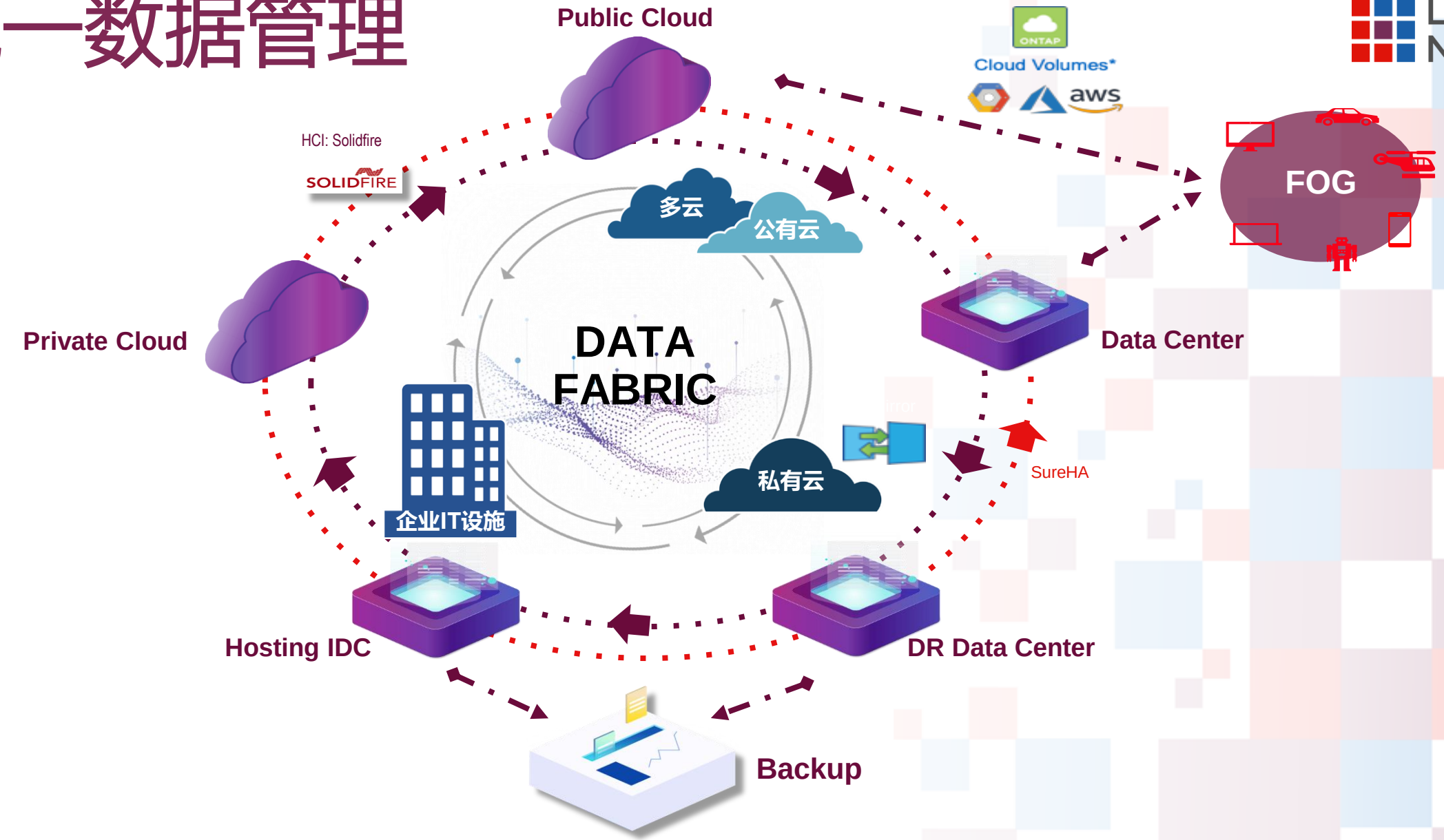
Lenovo NetApp

最大化的一站式
全方位解决方案

双品牌策略

本地优化

统一数据管理



勒索病毒是如何被感染的?

人事部的小王收到一封题为“简历”附件“职位应聘”的邮件。

他的电脑瞬间被锁，并弹出一个对话框需要支付比特币才能解锁。

抄起电话，小王立刻打给IT的小明，小明随即确定小王的电脑成为了勒索病毒的遇害者。

挂了电话之后，小明意识到更可怕的事情发生了，公司的主文件服务器也受到感染。并且杀毒软件无法删除病毒!

大多数勒索软件的攻击都是在文件遭到入侵破坏时发生的，因此您的文件共享是组织中最易受攻击的部分。文件共享是最终用户与数据中心进行直接接触的地方，大多数勒索软件都是利用与最终用户的交互从前门进行攻击的。只要您的组织中有人收到恶意的电子邮件并点击了它，Bang！您的文件共享就被感染了，左边是一则典型勒索病毒入侵的过程演示。

如果您遭受到这样的入侵，您的选择只有:

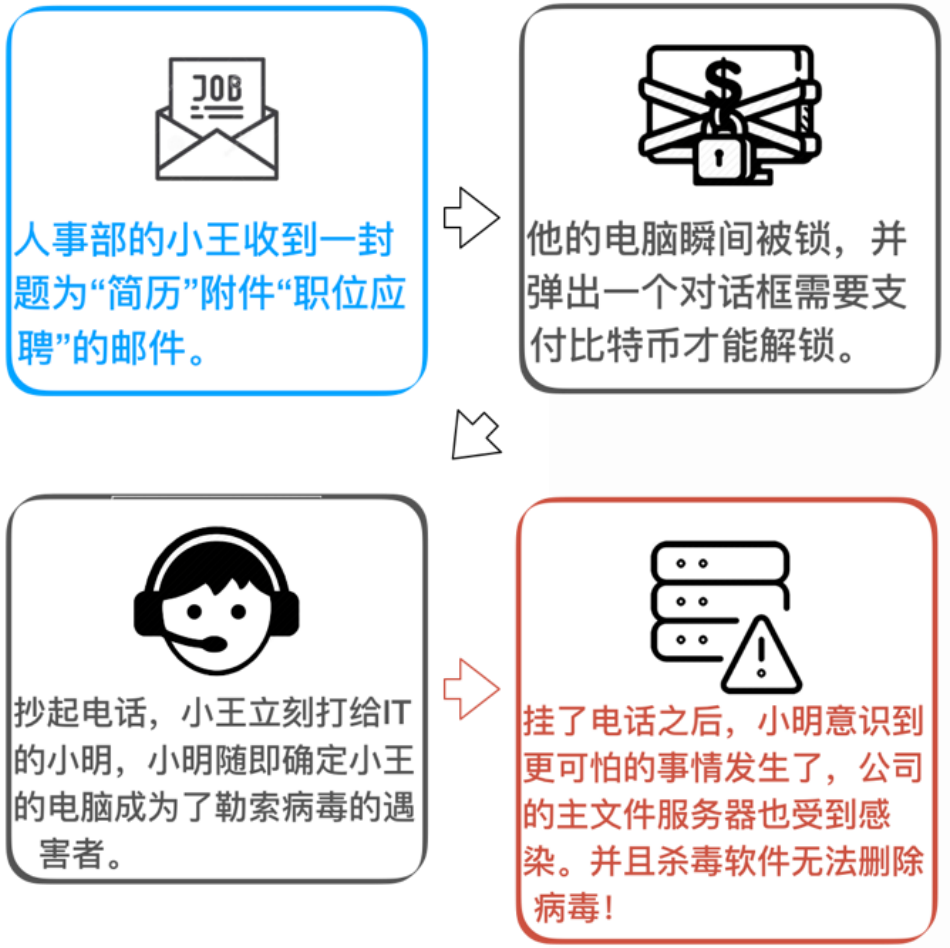
支付赎金 还是? 冒着企业崩溃的风险

防护和应对措施是解决勒索病毒的两大法宝

桌面

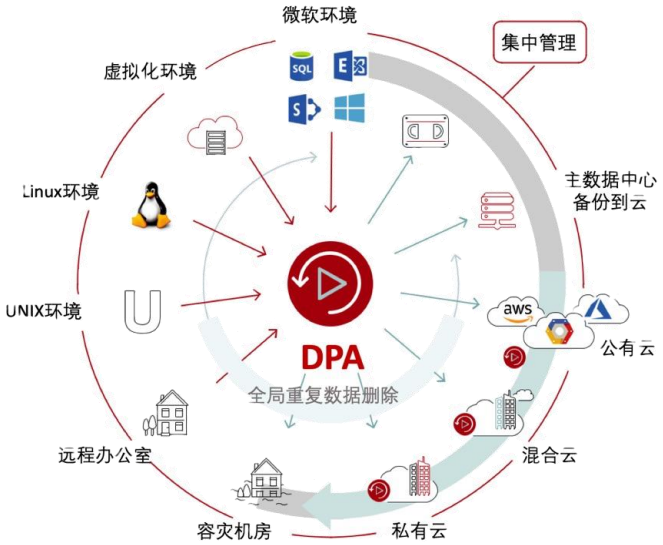
防护

服务器



应对

联想凌拓防勒索病毒解决方案



DPA备份一体机

应用保护

TS系列磁带产品

离线保护

- 备份系统
- 长期归档数据

*.*locked
*.*kraken
*.*crypto
*.*cry
*.exx

黑名单

.pdf
.xls
.doc
.jpg
.giv

白名单

Pattern:
SMB...
SMB...
SMB...
SMB...

深度学习

Crypto Spike

文件保护

- 黑白名单拦截勒索病毒
- 深度学习防范可疑用户（疑似感染病毒用户）
- 基于用户或文件类型快速恢复单个/多个文件

CIFS/NFS

服务器端

（应用系统、数据库、虚拟化等）

客户端

（终端客户，Windows/Linux）

ECX

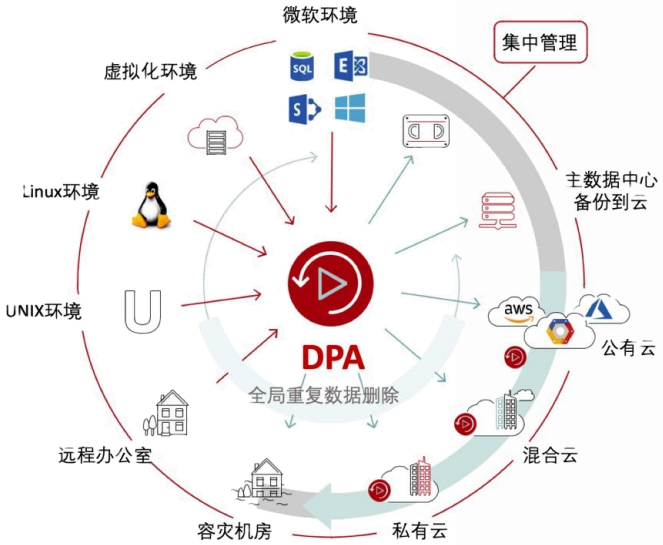
快速应用保护

- 基于Ontap快照快速恢复应用 Oracle, Vmware, SQL

保护/物理链接

链接

联想与Veritas一直以来致力于帮助客户实现数据安全



The truth in information.

传统应对之道（一）

这是杀毒软件问题，只是系统安全加固并重视数据备份

勒索病毒是安全问题，安全问题就找安全厂商

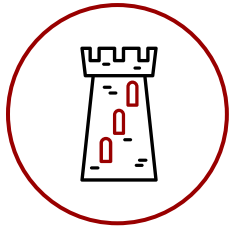
安全厂商建议：
1、及时更新杀软病毒库
2、及时进行数据备份

传统应对之道（二）

1、Windows 平台是勒索病毒主要攻击目标。直接删除备份文件
2、无效备份策略导致数据无法恢复

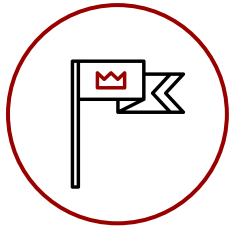
VERITAS

Veritas 防御勒索软件小贴士



防止

- 加固设备
- 可靠的备份
- 数据保护



检测

- 数据管理
- 第三方安全工具

恢复

- 可恢复
- DR 编排

VERITAS

Veritas 驾驭数据安全

数据安全 ⇨ 数据管理的延伸

数据洞察

- 数据优化
- 数据合规

数据保护

- 持续数据保护
- 可恢复性

高可用

- 应用可用
- 24/7 业务连续

BE 勒索病毒防御（一）

- 当未经授权的进程试图修改备份数据时，保护备份数据不受外部攻击
- 保护Backup Exec磁盘存储不被未授权或非Backup Exec进程写入
- 只允许从Backup Exec受信任进程写入Backup Exec磁盘存储

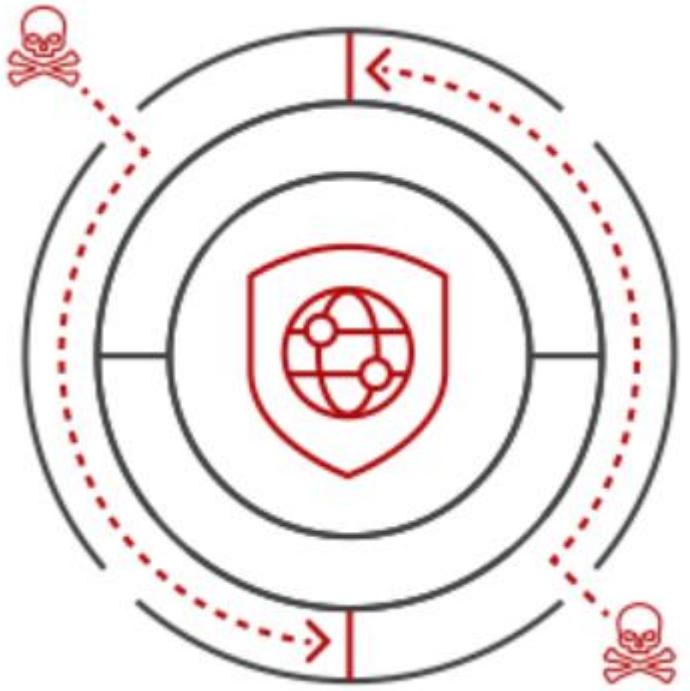
BE 勒索病毒防御（二）

通过两种方式保护基于磁盘存储的数据

免受勒索软件攻击:

- 仅允许受信任的Backup Exec进程写入基于磁盘的存储（在Backup Exec 20.4中引入）
- 防止外部代码执行Backup Exec进程（在Backup Exec 21中引入）

付钱还是不付钱

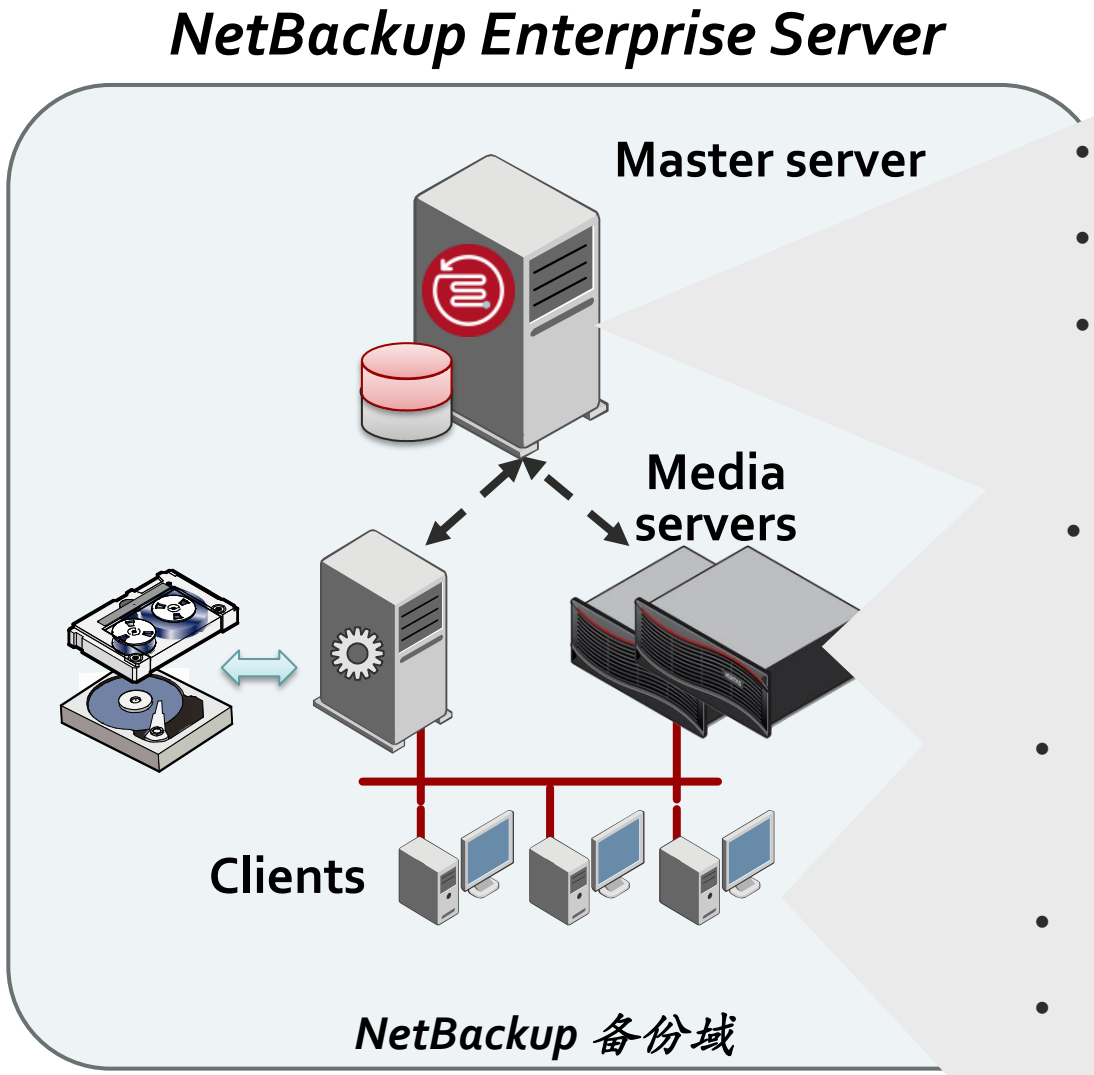


企业级可扩展架构

86,400 任务/天

无限制介质服务器数量

无限制客户端数量



- 支持Linux、UNIX平台
- 安全、稳定、无病毒侵入风险
- 硬件配置要求低，无需SSD等昂贵设备
- 多台Media Server间备份作业负载均衡和故障切换
- SAN-Client技术，减少业务主机资源占用
- 业务与备份设备隔离
- 提高系统稳定性、可扩展性和易管理性

Lenovo NetApp

NetBackup平台可靠性

可靠的安全加固

•采用Linux系统

•STIG安全加固

•NIST安全指导

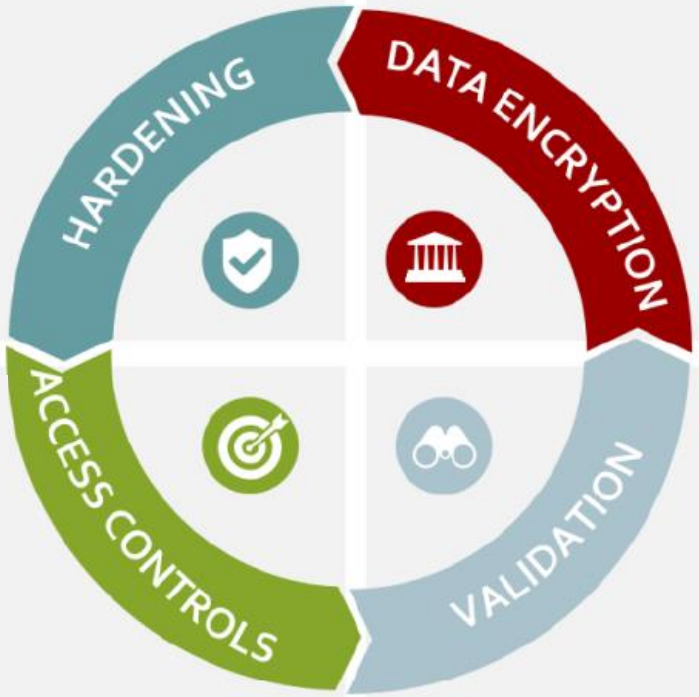
•内置SDCS

安全的用户管理

•RBAC用户管理

•使用非常规不可交互用户管理

NBU



MSDP加密

•AES 256-bit加密

•符合FIPS 140-2 标准

漏洞检测

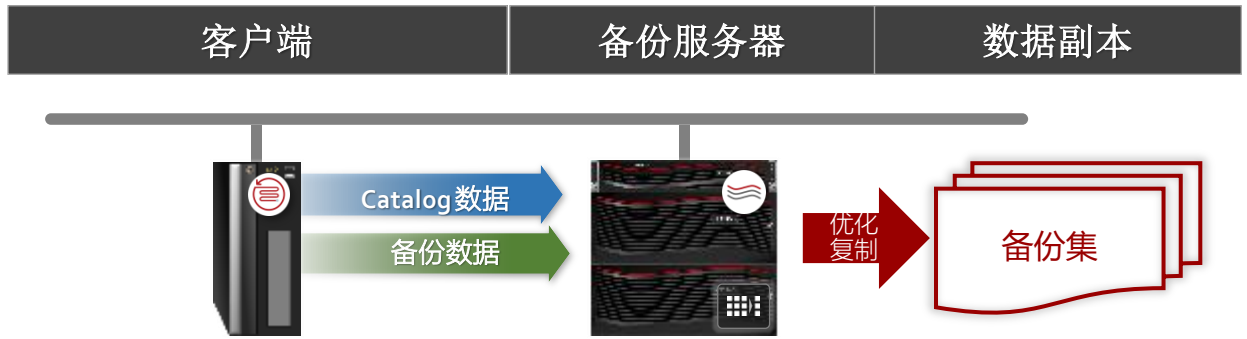
FindBug, PMD , Coverity代码分析

•运行时态漏洞扫描Nessus, Qualsys, Trustwave , OpenSCAP

•第三方工具入侵检测

Lenovo NetApp

数据保护黄金法则 3-2-1



- 三个数据副本以上
- 2种介质选择
- 通过NBU SLPs 进行数据副本生命周期管理

Veritas 数据洞察

查找，汇总组织中的所有数据并为其分配相对价值：

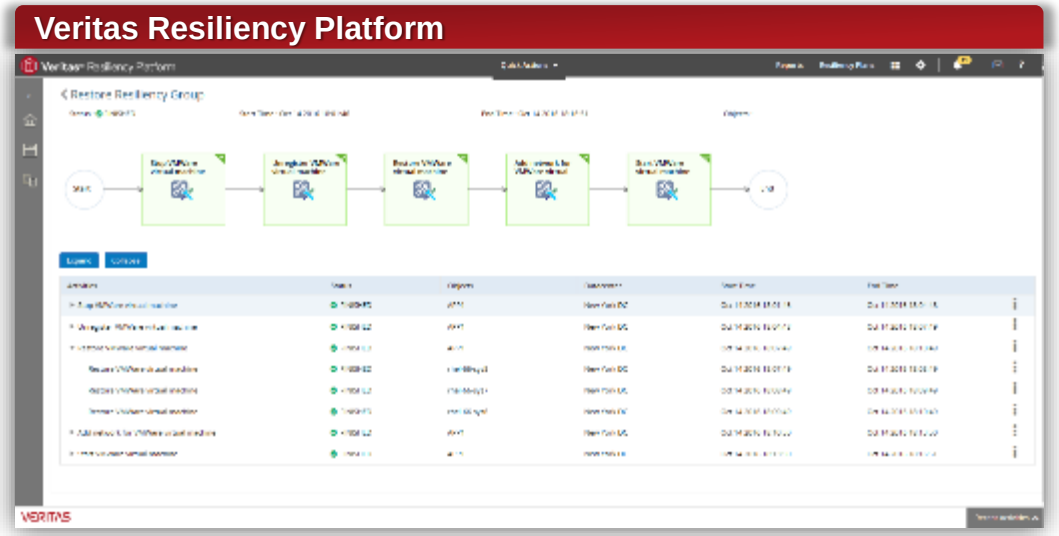
- 扫描识别并删除勒索软件
- 确保合规
- 优化存储空间
- 做出明智的数据决策

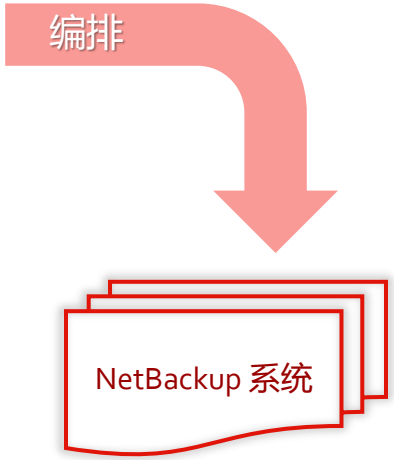
数据洞察分析

可预测的灾难恢复（NetBackup & VRP）

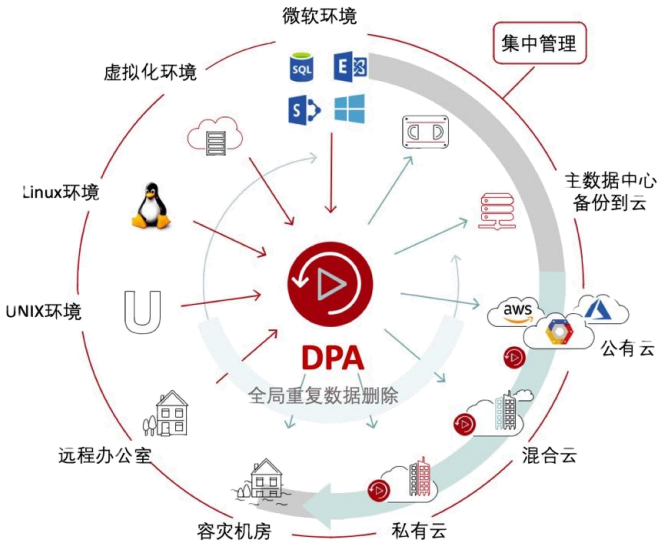
Veritas Resiliency Platform

- 一键编排复杂的恢复流程
- 零中断演练可确保随时进行灾难恢复
- 一款统一解决方案即可满足您的各种服务级别目标





联想与Veritas的整套解决方案



DPA备份一体机

应用保护

TS系列磁带产品

离线保护

- 备份系统
- 长期归档数据

服务器端

（应用系统、数据库、虚拟化等）

CIFS/NFS

*.*locked
*.*kraken
*.*crypto
*.*cry
*.exx

黑名单

.pdf
.xls
.doc
.jpg
.giv

白名单

Pattern:
SMB…
SMB…
SMB…
SMB…

深度学习

Crypto Spike

文件保护

- 黑白名单拦截勒索病毒
- 深度学习防范可疑用户（疑似感染病毒用户）
- 基于用户或文件类型快速恢复单个/多个文件

客户端

（终端客户，Windows/Linux）

ECX

快速应用保护

- 基于Ontap快照快速恢复应用 Oracle, Vmware, SQL

保护/物理链接

链接

通过联想凌拓解决方案

防止勒索病毒和文件恢复白皮书

v1.0

Lenovo NetApp

让我们帮您打造您的数据安全

Lenovo NetApp

谢谢！

智慧数据构建智能世界