ORACLE

核心数据，固若金汤

Oracle 数据库如何防范网络勒索软件

Jim Kong
Oracle Sehub Security and Manageability

内容

1. 什么是勒索软件
2. 勒索软件的问题有多大
3. 勒索软件如何传播
4. 如果受到攻击，该怎么办
5. 如何保护自己免受勒索软件攻击

什么是勒索软件?

美国网络安全和基础设施安全局 (CISA)

什么是勒索软件?

勒索软件是一种恶意攻击，攻击者加密或窃取组织的敏感数据并要求支付赎金，以恢复使用或不公开敏感数据。

请确保您的企业名称不会在明天的热搜中出现！！

- **参考:** https://www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf

勒索软件的问题有多大?

近期的勒索软件攻击

5月 2021

- Colonial Pipeline 运营 5,500 英里的管道（德克萨斯到新泽西）
- 每天运输 1 亿加仑燃料
- 关闭了整个燃料输送管道 - 影响美国东海岸的汽油和天然气输送
- 支付75个比特币或440 万美元
- 黑客收到赎金后，发送了一个软件，但整个恢复过程很慢

3月 2021

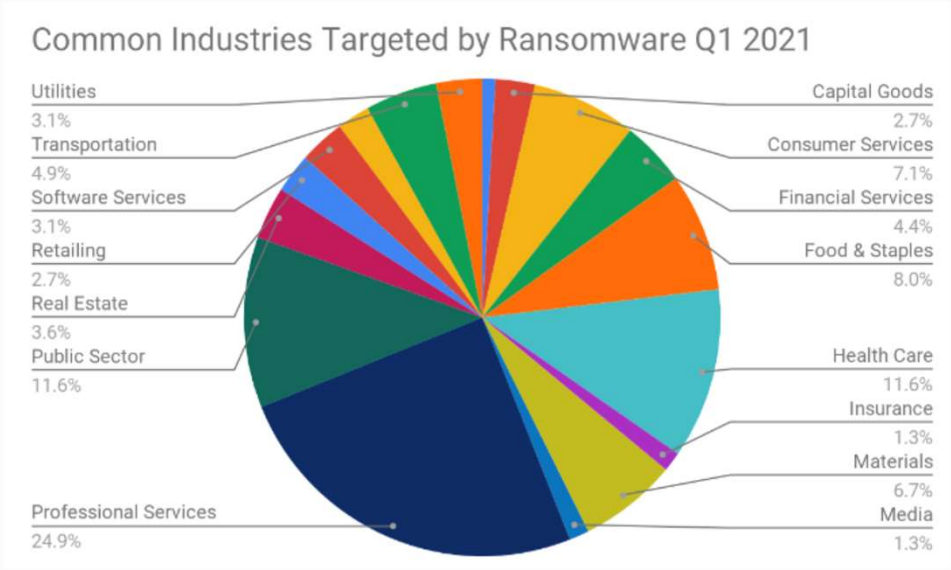
- 黑客利用 Exchange 零日漏洞，安装了 web shell 恶意软件，即使服务器更新补丁，仍无法阻止攻击者完全访问受影响的服务器。
- 对文件进行加密， 并获取了获取电子邮件帐户的访问权限
- 在美国超过 250,000台服务器，30,000 家组织受到影响

12月 2020

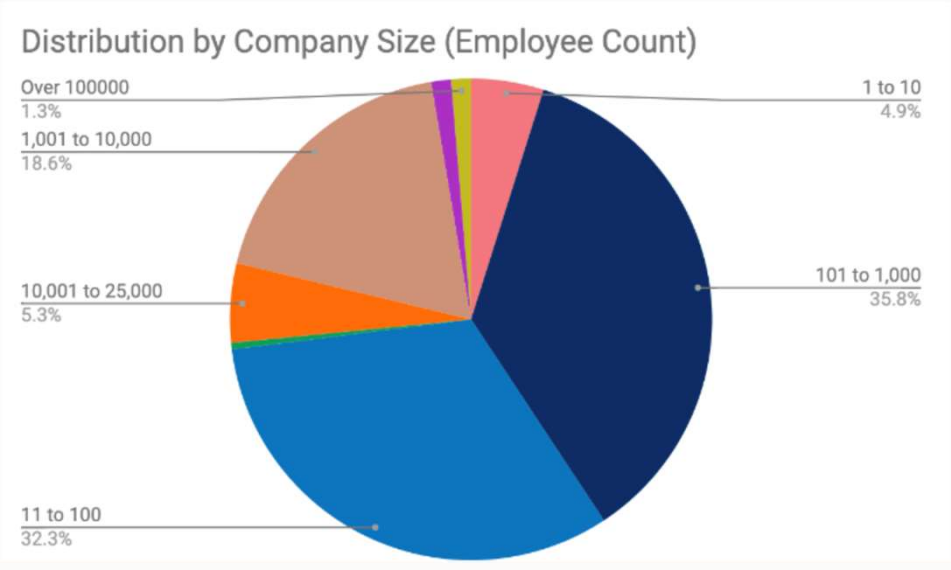
- SolarWinds生产销售网络和系统监测类的软件, Orion是一款功能强大的网络性能监控程序
- Orion源码进行篡改添加了后门代码(运行传输文件、执行文件、分析系统)
- 美国有超过 18,000 个组织受到影响（几个政府机构）
- 微软、VMWare 和思科受到影响
- 影响客户对供应商产品的信心

没有任何行业和企业规模可以免受勒索软件攻击

截止至2021Q1受过勒索软件攻击的行业



按企业规模划分



Source: Coveware

不是是否而是何时你会受到攻击的问题

截止2021年9月根据ENISA排名前 9 的安全威胁

1. **勒索软件**
2. 恶意软件
3. 加密劫持
4. 电子邮件相关威胁
5. **对数据的威胁；** （如数据泄漏）
6. 对可用性和完整性的威胁
7. 虚假信息——错误信息
8. **非恶意威胁；** （主要基于人为错误和系统配置错误）
9. 供应链攻击

Source: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

网络安全保险

2021 年的损失超过了 2018 年、2019 年和 2020 年的总和——整个行业的保费都在上涨，保险公司开始限制保险范围

最低保费增幅为90%，对于IT系统复杂/敏感数据量大的公司，增幅将接近200%

一些保险公司（例如：AXA）正在完全退出勒索软件保险市场——不仅仅是因为损失，还因为勒索软件付款可能为恐怖活动提供资金，而保险勒索软件付款似乎正在导致赎金需求规模的螺旋式增长

保险覆盖的要求越来越严格：

- 静态和动态加密
- 多重身份验证

2020 年赎金支付总额增加了 341%，达到 4.12 亿美元

基于区块链分析这代表了一个下限——实际数字几乎肯定更高
https://blog.chainalysis.com/reports/ransomware-update-may-2021

勒索软件是如何传播的?

勒索软件攻击媒介

- 开放远程桌面协议 (RDP)
- 网络钓鱼
- 常见服务的模糊 URL
- 未打补丁的系统
- 被盗帐户

90% 的攻击来自用户、系统或数据库漏洞

勒索软件攻击剖析

勒索软件攻击很少有针对性

经常使用“恶意软件即服务”和现有的僵尸网络

高度自动化的大量攻击

- 为了创造收入
- 事务性的，类似商业的

勒索软件攻击分解

尝试攻击：
电子邮件、

准备工作：黑客团队开始恶意活动，建立指挥控制中心

最后阶段：
加密或渗透，要求支付赎金-比特币

Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
Amazon.com
Email ID:

数据泄露：从受感染系统中抓取数据并复制到外部命令和控制系统

取本地、域和网络
，包括用于备份的

侦察：搜索其他系统和网络上的易受攻击位置

你好！

您的存储空间已受损。
您的文件归我们所有。

目前，您的所有文件和文件夹都是安全的。它们已被转移到我们的安全服务器并加密。如果您想找回您的文件或不想让他们泄露，请发送 0.04 比特币到这个比特币钱包：
1DHtv7TPk1VoGchJJs21dzKfLxRtTTFNGf

您必须在 2020 年 6 月 3 日之前付款，否则您的文件将从我们的服务器中自动删除、泄露或出售。
您的唯一 ID 是：148.71.84.153
请将您的 ID 和付款确认通过电子邮件发送至：
cloud@mail2pay.com
付款确认后，您将收到有关如何下载所有文件的说明。

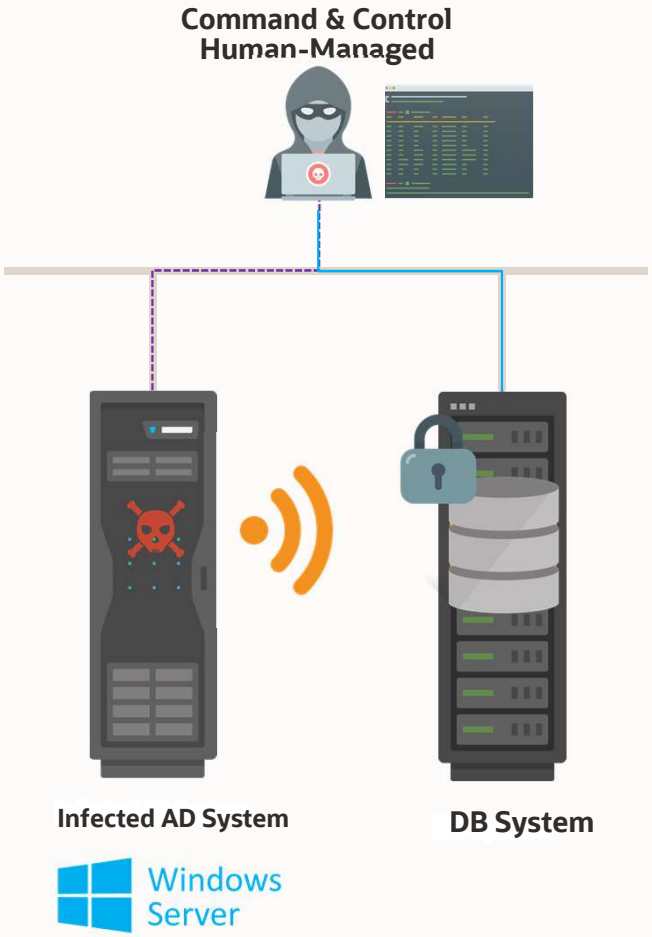
如何获得比特币：
购买比特币的最简单方法是 LocalBitcoins 网站。
https://localbitcoins.com/buy_bitcoins
！！！注意力！！！
即使您的所有文件都是备份并且您有它们的副本，也不要忽略此消息。
考虑到我们收集的大量敏感和私人信息，如果不付款，我们保留泄露或出售您所有数据的权利。

谢谢您的合作。
云安全

横向移动:

损坏，删除数据库文件

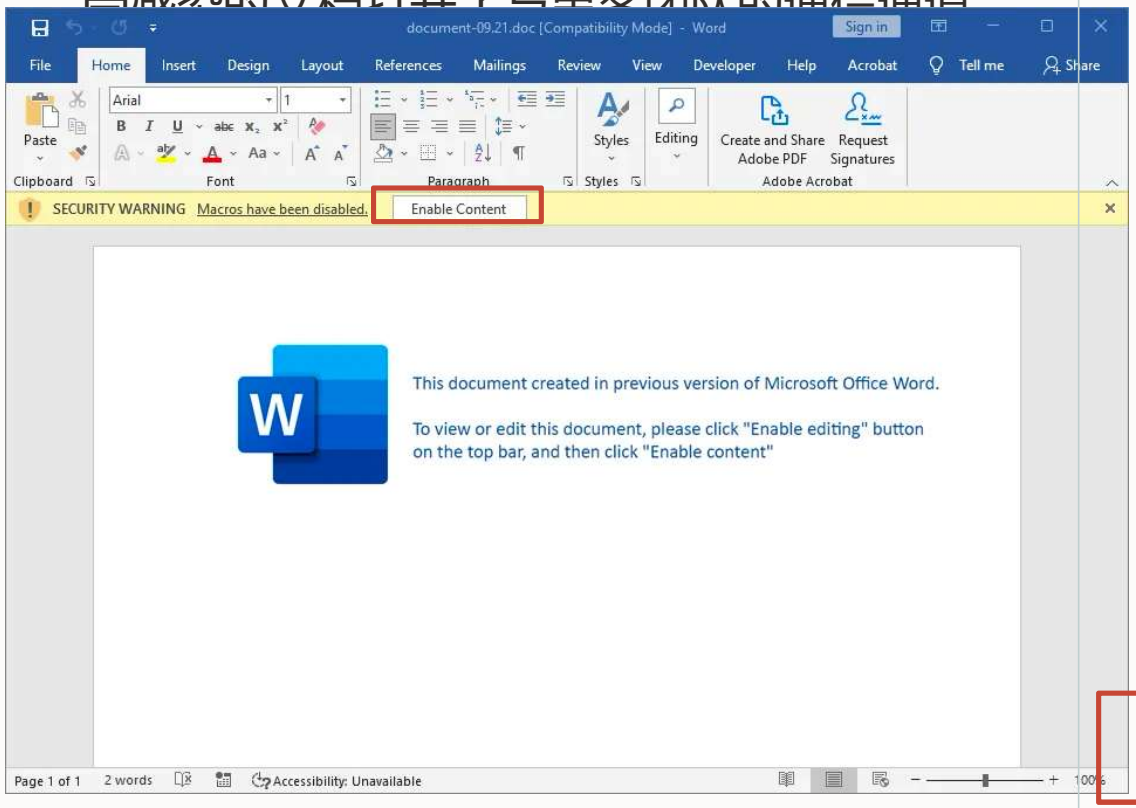
1. 恶意程序入侵，部署“搜索”程序
2. 在网络上侦察和搜索数据库监听器
3. 一旦找到，打开一个带有命令和控制服务器的端口，该端口由黑客团队管理
4. 攻击者尝试暴力破解用户/密码组合并获得对数据库的管理员访问权限，以便：
   - 删除部分或全部数据库表
   - 更改数据库记录
5. 最后尝试加密数据库文件



横向移动:

向任意存储中植入恶意负载

受感染的文档打开了与黑客团队的通信通道



横向移动:

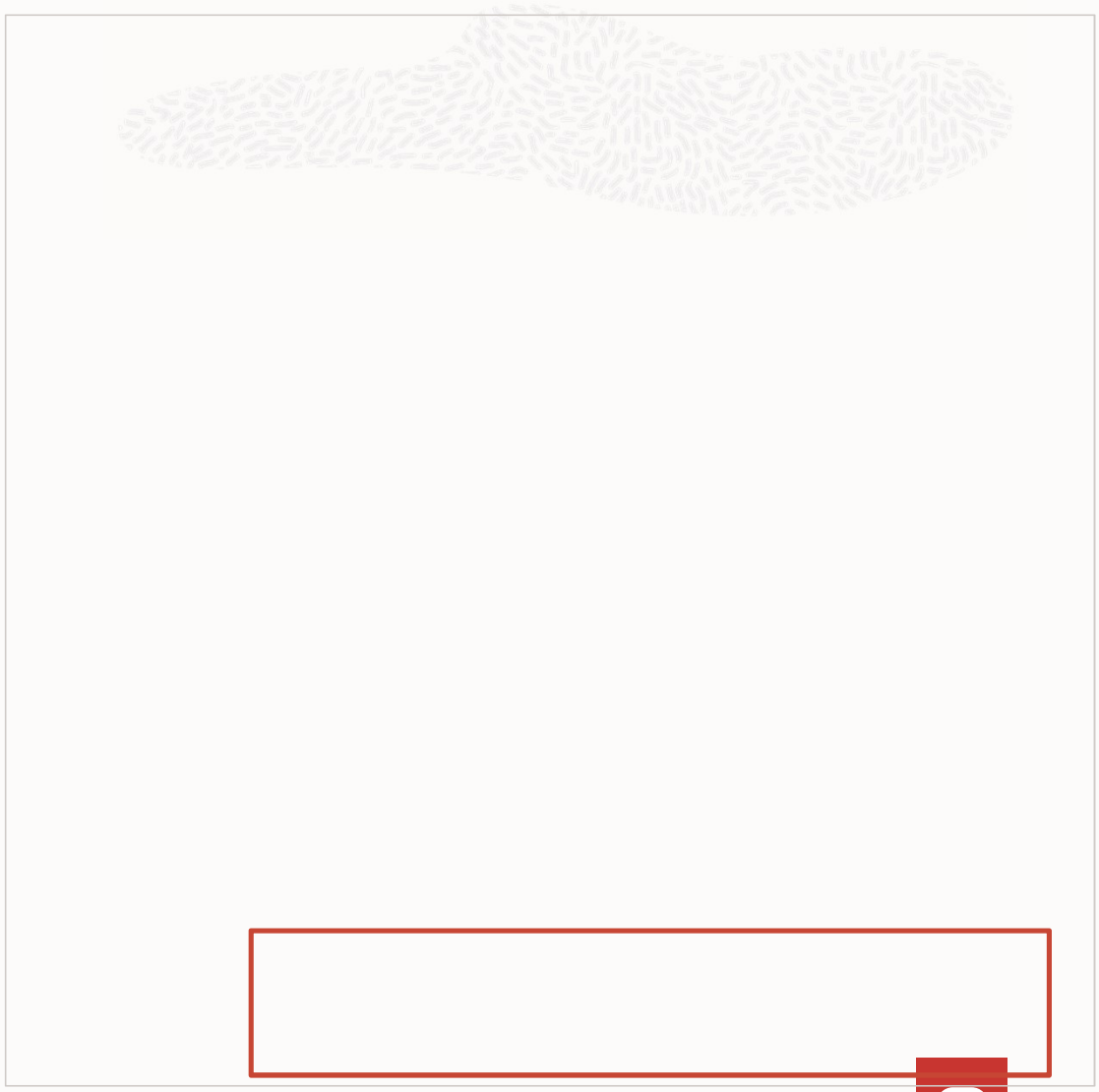
感染备份设备

黑客团队将搜索备份可见挂载点，例如 CIFS 甚至 DDBOOST

并会使用后门进入备份设备

或者，将等待被篡改的文件被备份

攻击的最后阶段是删除任何备份数据



如果我受到攻击，我该怎么办？

典型结果

支付赎金

- 可能获取解密密钥并取回您的数据
- 执法部门或许能够追回部分赎金

不支付赎金

- 从备份重建您的系统

我该如何保护自己?

Gartner®

“检测、保护、恢复:
现代备份应用程序如何保护您免受勒索软件的侵害”

2021报告

1. 避免使用网络共享协议 — 在实现备份数据存储时避免使用简单的网络共享协议，例如 CIFS 或 NFS

2. 确保为帐户配置了运行所需的最低权限。

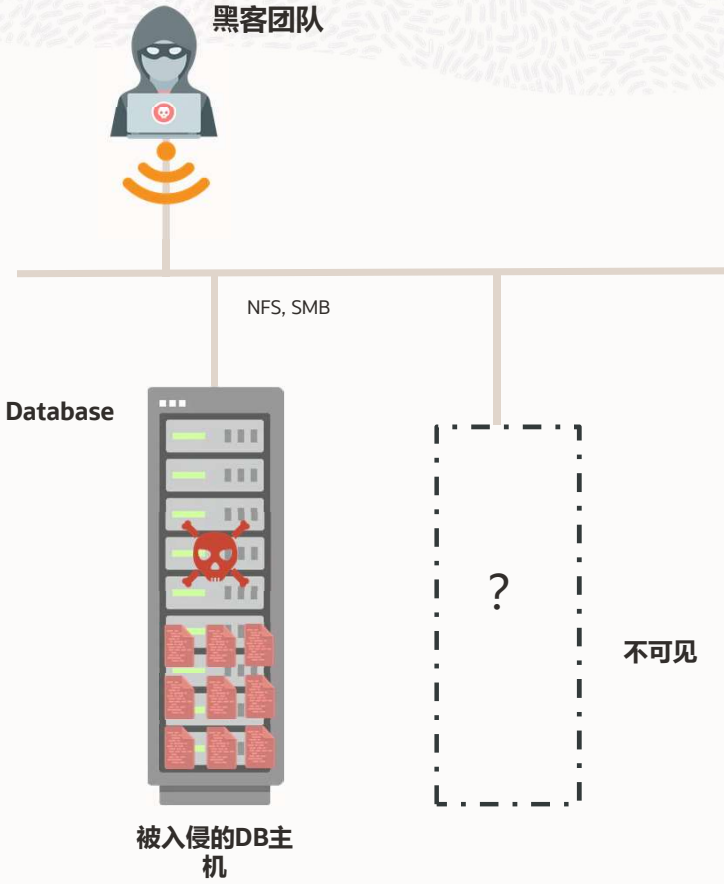
3. 将物理备份存储集成到同时运行备份软件的设备（或设备集群）中。 这隐藏了备份数据存储，因此只能通过破坏备份系统的管理控制台或获得对底层操作系统的根级别访问权限来对其进行攻击。

勒索软件并不神奇

为了达到勒索的目标，它需要利用：

1. 可见的挂载点和文件
2. 可见的操作系统命令
3. 可见的操作系统用户凭证

勒索软件不会轻易影响看不见的东西

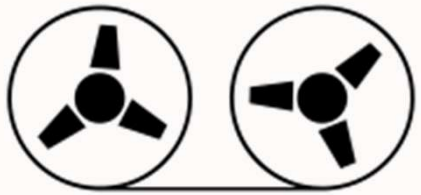


针对数据库破坏的推荐防御方案

不可变更的离线备份

好

离线备份到类似磁带的存储设备上

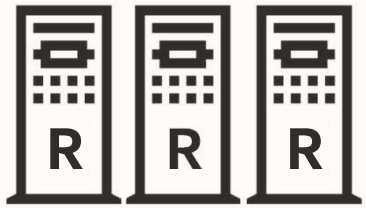


较好

Oracle数据库云备份服务

最好

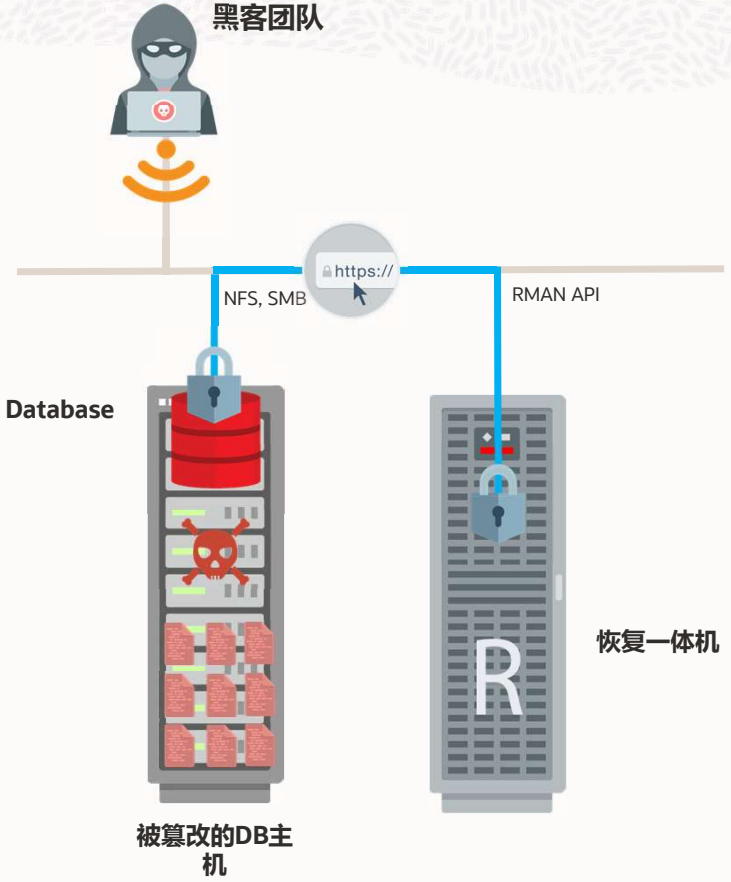
零数据丢失一体机



恢复一体机不使用任何可见的挂载点，也不使用原始文件。

数据库通过备份模块管理的隐藏通道访问恢复一体机，而该通道是建立在专有 RMAN API 之上。

DB和恢复一体机之间的通信也可以加密，防止任何入侵

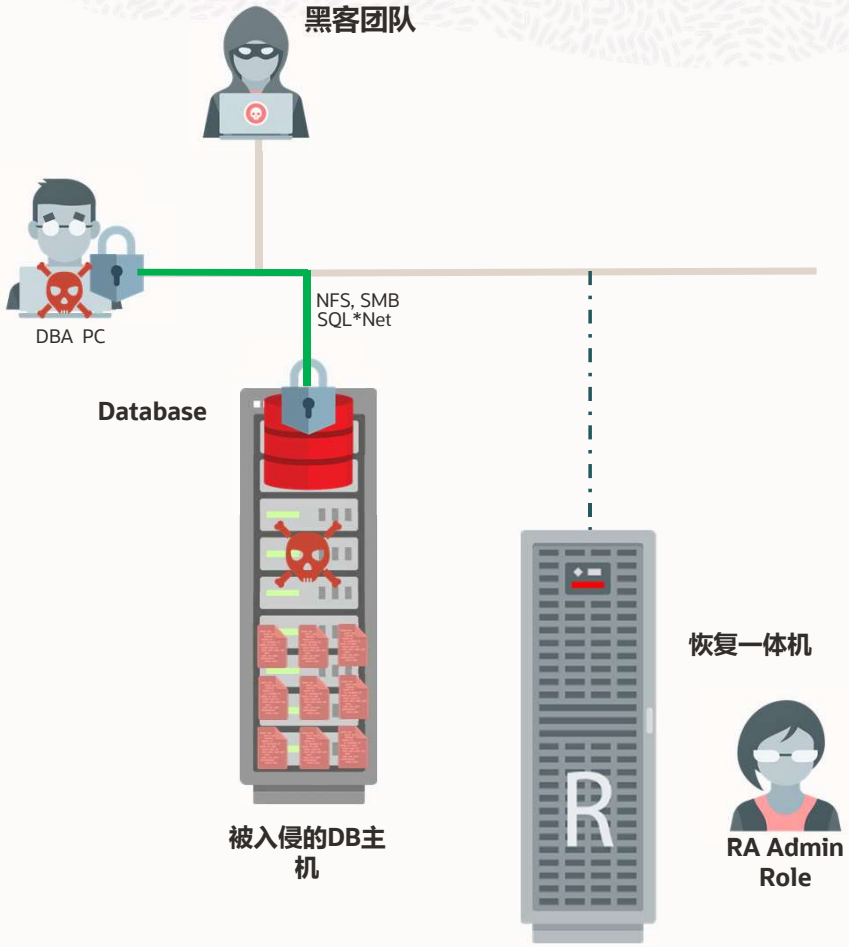


恢复一体机不使用可见的管理员凭据来完成工作。

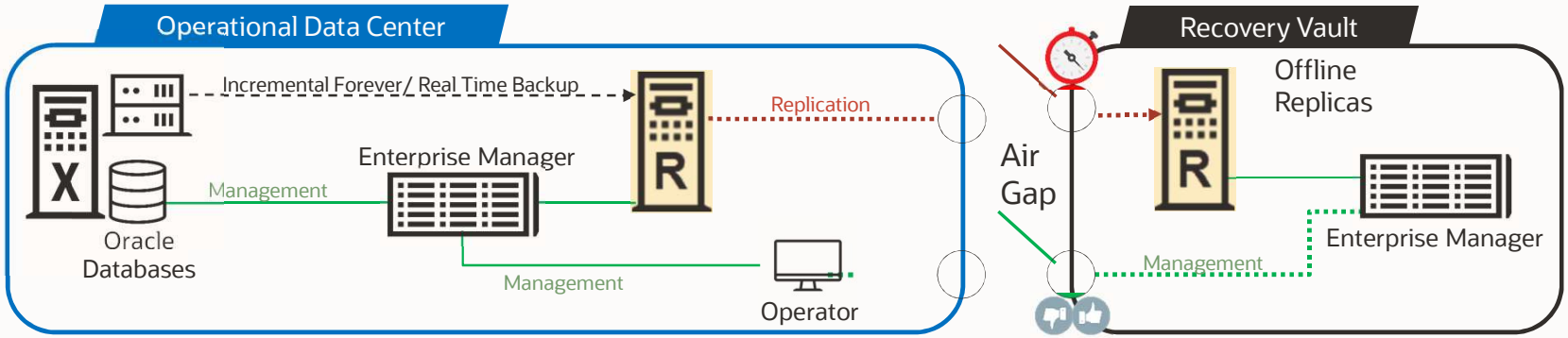
如果黑客入侵易受攻击的 PC 客户端并破解 DBA 凭证，这不会影响恢复。

DBA 无权从恢复一体机中删除备份卷。

恢复一体机专用管理员角色存储在隔离的地方



不可变备份

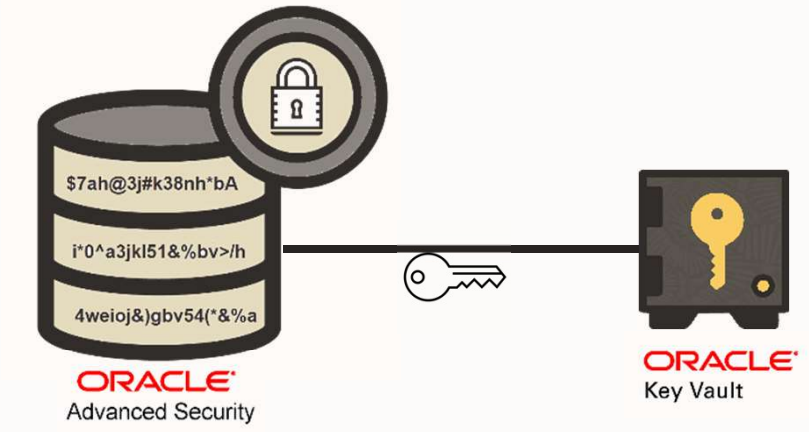


恢复一体机恢复窗口合规性 -

- 设置备份的最短保留时间——可以增加，但不能减少
- DBA、RA 管理员或任何其他 RA 用户不能更改或删除窗口内的备份
- 数据中心内部的网络隔离（即由“air-gap”隔开）的技术组件,会定期与所有关键生产数据进行快速同步,其他时间保持断开。

针对数据库泄露和勒索的推荐防御措施

- 透明数据加密（Oracle 高级安全的一部分）
- 用于密钥存储和分发的 Oracle 秘钥保险库



还有什么?

以下方面也可以缓解风险:

- 数据库保险库 - 帮助将数据与特权帐户、受损的应用程序服务帐户隔离开来 - 这可以防止勒索软件通过数据库渠道传播
- 数据安全/数据库安全评估工具——帮助识别可能被攻击者用来访问数据库的配置错误
- 审计保险库和数据库防火墙 – 检测访问异常并发出警报（例如：攻击者连接或尝试连接到数据库）。 如果数据库被用作攻击的传输向量，可能会捕获正在进行的攻击（很少见，但理论上可能）

恢复一体机的关键优势

- 自动恢复验证: 数据库恢复保证
- 实时事务保护: 保护到最后一个事务
- 职责分离: 限制跨 Oracle 恢复一体机架构的访问
- 网络隔离（air gap）保险库备份 : 保险库同步可防止任何入侵
- 弹性平台 : 无单点故障的高可用架构

在 Oracle 数据库上还可以做的

已知的软件漏洞是常见的载体

- 考虑使用自治数据库，其中补丁在发布后会非常快速地自动应用
- 缩短补丁周期以在发布后立即应用补丁

大多数攻击针对 Windows 平台

- 考虑在 Solaris、Linux 或其他 Unix 变体上运行您的数据库

勒索软件可能不会传播到其他数据中心

- 考虑在另一个位置/网络中有一个 Data Guard 备用库

大多数攻击都会加密文件系统

- 考虑使用 Oracle ASM 进行存储。 由于 ASM 是原始文件系统，因此恶意软件很难定位。

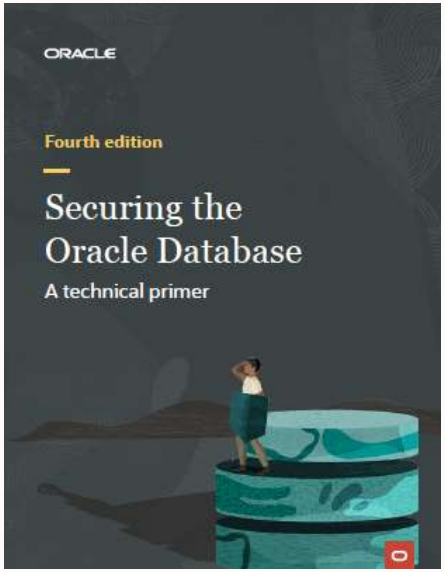
我怎样才能了解更多?

保护 Oracle 数据库

第四版

Oracle 数据库安全团队

URL: https://oracle.com/securingthedatabase



数据库安全办公时间

直接连线Oracle数据库安全产品经理

每个月的第二个星期三，美国中部时间 09:00 和 18:00（相同时段）

URL: http://bit.ly/asktomdbsec

或者搜索

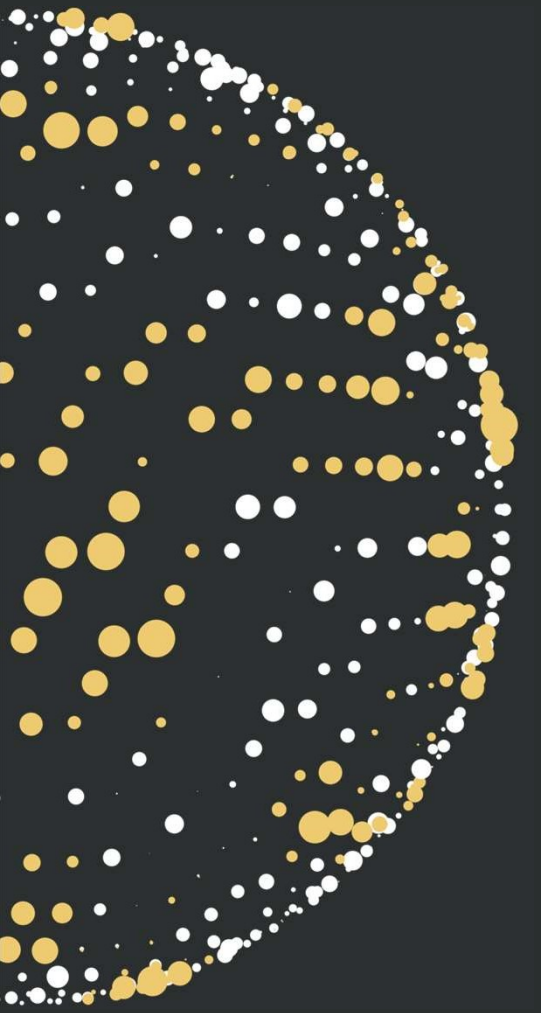
AskTom 数据库安全办公时间

数据库安全 LiveLabs

- 亲身体验 Oracle 的数据库安全特性、选项和产品
- 始终可用并定期更新
- 无需特殊技术技能（网络、系统或 DBA）
- 无需在笔记本电脑上安装任何东西即可更新技能：您所需要的只是互联网连接！
- 以 3 种不同的方式在几分钟内轻松部署即用型数据库安全环境：
  - 在您自己的 OCI 账户中
  - 在您的免费试用账户中
  - 通过预订免费的 Livelabs 账户
- 公共数据库安全 Livelabs URL：

  搜索 “security”

  https://bit.ly/golivelabsdbsec (**go live labs dbsec**)



Thank You