存储产品选择技巧：如何制定有效的网络弹性战略

01

全球企业当前面临的威胁

02

网络安全和风险管理

03

NIST 框架：IBM 网络弹性生命周期的基础

04

存储基础架构的作用

05

存储架构解决方案

06

实现最优的安全平衡

全球企业当前面临的威胁

无论是由于人为失误、系统故障还是恶意犯罪行为导致的数据泄露，都是当今企业面临的最严重且成本最高昂的威胁。Ponemon Institute 最近的一项调研发现，在过去的 12 个月中，全球数据泄露的平均成本高达 386 万美元。[1] 受数据泄露影响的组织也面临着正常业务运营中断、宝贵数据丢失、业内声誉受损等风险。

此外还有相应的人道代价。在世界经济论坛（WEF）发布的《 2019 年全球风险报告》中，将网络攻击列为人类福祉所面临的最大风险之一。在 WEF 的调研中，有 82% 的受访者预计他们由于网络攻击而遭受数据被盗或金钱损失的风险将会增加，而 80% 的受访者表示运营和基础设施受到破坏的风险也会因网络攻击而增加。[2]

IT 组织需要一种系统化的安全方法来应对普遍存在的威胁带来的新挑战。

如今，IT 组织需要一种系统化的安全方法来应对普遍存在的安全威胁带来的新挑战。领先的企业已开始采用创新型的存储技术，例如受保护复制功能。他们还利用现有的高效物理气隙方法来阻止威胁并实现其业务目标。此类方法的关键在于成功的风险管理。

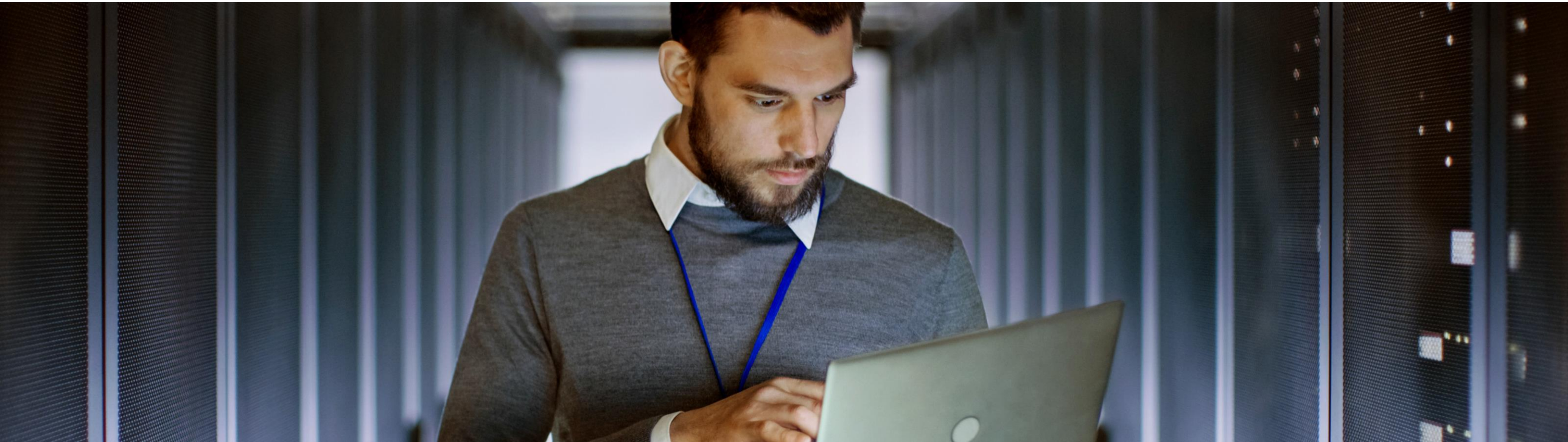
网络安全和风险管理

目前，市场上已经有很多方法致力于帮助企业避免业务中断、最大程度地降低成本。Ponemon Institute 建议采用以下四种战略来降低数据泄露成本：[1]

- 组建事件响应团队
- 使用广泛加密
- 采用业务连续性管理
- 提升员工培训力度

为了实现和维持强大的网络安全战略，企业需要采用程序化方法，了解拥有哪些数据和系统资产及其价值所在，以及这些资产面临着哪些风险。通过采用风险管理原则来描述组织当前和期望的安全状态，企业便可考虑一系列可能的实施层。一个强大的框架对于评估和实施网络弹性战略而言至关重要。

一个强大的框架对于评估和实施网络弹性战略而言至关重要。



NIST 框架：IBM 网络弹性生命周期的基础

2018 年，美国国家标准技术研究院 (NIST) 发布了《关键基础架构网络安全改善框架》。该框架包含三个部分：框架核心、框架实施层和框架配置文件。[3]

“框架核心”部分给出了一系列网络安全功能。每个组织（如果尚未采取的话）都可以采取这些必要且可实现的步骤：

- **识别**：帮助企业了解危及系统、人员、资产、数据和功能的网络安全威胁和风险。
- **保护**：确保通过适当的保障措施交付关键服务。
- **检测**：识别发生的网络安全事件。
- **响应**：针对网络安全事件采取措施。
- **恢复**：复原因网络安全事件而受损的所有功能或服务。

结合使用这些功能，可以更好地了解组织的网络安全风险管理。有了更清晰的了解，组织便可采用适当的存储解决方案。

结合使用这些功能，可以更好地了解组织的网络安全风险管理。

存储基础架构的作用

长期以来，存储一直在企业运营中扮演着“数据管理员”的角色。除了在数据未被存储到主存储器时提供容器来存储数据之外，该系统存储层还一直提供保护功能，帮助企业从异常事件中恢复过来。随着时间的推移，这些功能集也有所增加：

- **备份：**从 20 世纪 60 年代起，存储就能支持应用用户在独立的媒介中保存数据版本，避免被意外的删除、损坏或主设备故障所影响。
- **高可用性：**从 20 年前起，存储就一直提供适当的设计方式，以构建多路径访问、多服务器访问并在机房内复制在线数据副本。
- **灾难恢复：**从 20 世纪 90 年代末起，存储就一直提供适当的设计方式，用以远程构建复制的活动数据副本，保护企业免受停电或自然灾难的影响。
- **快速在线数据恢复：**自 21 世纪 10 年代起，存储开始提供数据副本快照，以便在数据意外删除或损坏的情况下快速恢复数据。

在每种情况下，存储系统、管理软件和运营流程都引入了新功能，来解决特定的风险案例。

从一般的存储功能转变为与网络弹性相关的特定功能，有四种主要功能可跨块存储、文件存储、对象存储、磁带存储、软件定义存储和云存储进行交付：

- **隔离性**是指快照或备份数据与网络其余部分的分离程度。通过使用受保护的副本、云对象存储或物理气隙，可以实现逻辑隔离。
- **不可变**或防篡改存储可防止任何外部或内部攻击者更改或删除数据。
- **性能**是网络弹性框架中的一项重要功能。您的组织从网络攻击中恢复的速度如何？尽管磁带在备份数据的隔离性和不变性方面表现出色，但恢复可能需要花费数个小时。
- **易于复用**或易于访问备份数据，对于测试恢复过程、验证备份以及将数据复原到沙盒环境中，进而在勒索软件事件发生时找到有效的恢复点而言非常重要。

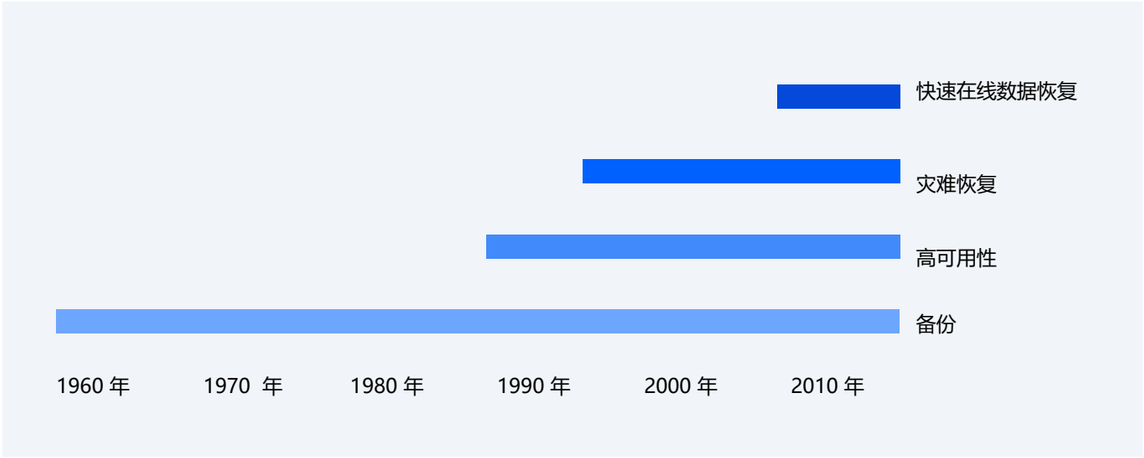


图 1：存储保护功能随着时间的推移的发展

由网络攻击造成的逻辑数据损坏 (LDC) 威胁 - 特别是勒索软件或磁盘擦除器攻击 - 提出了一系列新的安全保护考虑事项。为了提供所需的弹性级别，解决方案提供商可以借用一些已经存在的存储工具来实现备份和灾难恢复。但是，还需要新的存储功能来应对新的威胁。

您需要采用一种结合了存储功能和运营流程的机制，保存最新的数据恢复副本，即使面临复杂的恶意软件攻击。一旦检测出攻击并启动了响应，您可以使用这些保存的副本，重启应用，恢复正常的服务。

IBM® Safeguarded Copy 借助不可变时间点生产数据副本和双重控制安全性来防止因用户失误、恶意破坏、恶意软件或勒索软件攻击而导致数据被删或被改。

IBM Redpaper™ *DS8000® Safeguarded Copy* 确定了创建保留副本所需的三个新功能：

- **粒度**：企业必须能够创建多个保护副本，在损坏事件发生时将数据丢失降至最低。
- **隔离**：保护副本必须与活动的生产数据隔离开来，避免受攻击的主机系统损坏保护副本。（这种方式又称作“气隙”。）
- **不变性**：必须保护数据副本不被未经授权的操作所影响。[4]

在“支持网络弹性框架的五种关键技术 (Five Key Technologies for Enabling a Cyber-Resilience Framework)”报告中，IDC 添加了两个新的考量因素：“自动化和编排”及“监管报告和保证”。[3] 这两个因素并不仅仅适用于 LDC 攻击弹性，也非常适于列入最佳实践列表。

存储架构解决方案

一款成功的存储解决方案可提供一系列广泛的功能，让您能够实现弹性的 IT 运营，应对 LDC 攻击或意外中断。综合型的解决方案能够整合存储功能、网络配置、管理控制和物理安全功能。

下面让我们来了解一下当前可用的一些关键网络弹性解决方案和技术，包括快照、基于 WORM（一次写入，多次读取）媒介的受保护备份、磁带气隙保护和云对象存储等。

基于快照的传统备份和恢复

在满足传统备份要求方面，快照已成为性能最佳、成本效益最高的方法之一。空间高效的只读数据副本可提供经济高效的恢复点，用于快速复原以前的数据版本。利用快照从意外删除或损坏中恢复过来已经得到了广泛普及。

受保护快照

保护快照的最佳方法是什么？其中一种方法是将存储卷从生产系统复制到同类型的次级存储系统。然后，您可以利用周期快照作为次级阵列上的恢复副本。软件应该提供自动化的复制和快照功能。非生产存储系统不能直接连接任意应用服务器，唯一一个活动的存储数据连接应该是备份副本传入的端口。

在发生 LDC 恶意软件攻击或者测试恢复行动时，您应该将非生产系统上存储的数据副本当作恢复副本源使用，这些副本可以回传至生产存储系统。通过使用非生产存储系统，您可以在生产副本和受保护副本之间提供一个逻辑气隙。系统之间的物理隔离与实施设计有关；距离更近，即使是在同一个数据中心里，您就能获得更高的性能和更低的网络成本；远程设施中也可以使用非生产存储解决方案进行灾难恢复。

利用 WORM 媒介，保护备份

功能齐全的备份和存档软件系统可以将数据的完整副本移至托管存储空间，并通过存储更改的数据来维护备份版本。WORM 媒介非常适合用于保护恢复副本。盒式磁带可标记为 WORM，并用于写入恢复副本，避免被磁带机覆写。一旦被标记为 WORM 盒带，应用或管理服务器中的任何恶意软件都不能毁坏备份副本。

与空间高效的快照不同，写入磁带的完整副本需要耗费一定的时间才能完成数据移动。复原的速度也比快照慢得多。您需要根据企业的具体需求自定义设计方式，但是您最好是采用全面防护，利用备份将数据保存在离线媒介中，增强基于快照的恢复功能。

强大的磁带气隙保护

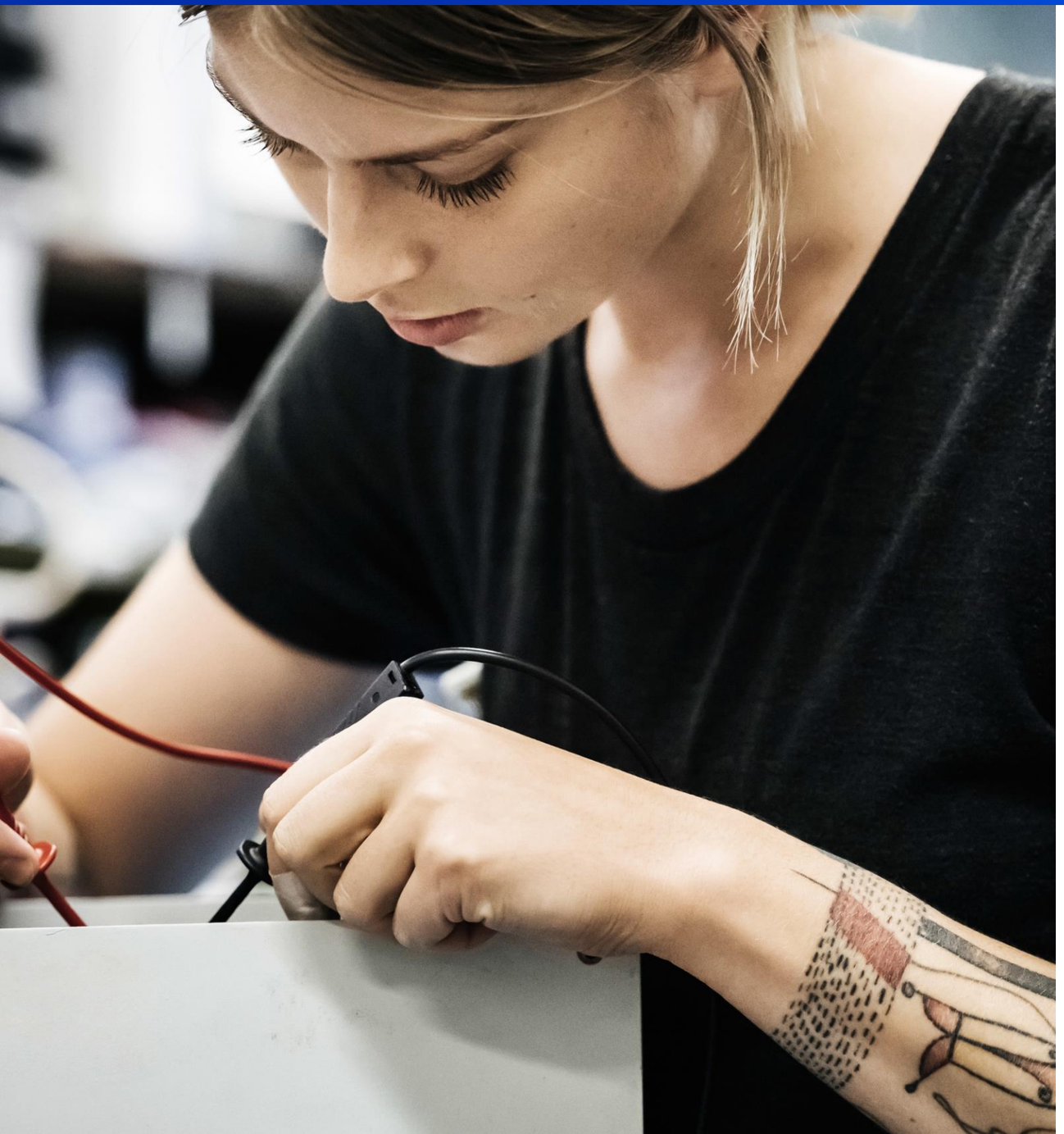
“气隙”一词指的是系统或网络的物理或虚拟隔离，以避免因恶意软件被感染、系统故障或人工失误而导致数据受到广泛损坏。气隙的基本理念是定期让次级存储系统上线，融合最新的变更，然后再让次级存储系统下线。借助使用快照功能来创建副本的方法，您可以快速挂载这些副本，恢复受损的应用。

不过，对复制数据的完全保护也确实存在一些局限性。您可以使用磁带库，实施最全面的保护方法，即不允许任何网络或软件访问受保护的副本。磁带“离线设计”的特性提供了一个真正的物理气隙和最安全的保护机制之一，用于抵御网络犯罪。

如需详细了解如何利用磁带保护数据，包括使用气隙技术、WORM 和其他安全功能，请参阅“IBM 磁带解决方案可提供强大的现代数据保护功能”解决方案简述。

借助云对象存储保护数据

云对象存储是一种持久、安全且经济高效的数据归档与保护方式。通过定义相关策略，您可以灵活地指定默认、最短和最长保留期限。在将数据馈入到云端时，您可以对单一对象或多个对象应用这些保留期限和其他合法保留功能。这意味着在保留期到期及所有合法保留功能被移除之前，对象均不会被删除。



实现最优的安全平衡

拒绝访问数据或销毁数据的网络攻击已经不再四处横行。实际上，它们正在变得越来越复杂。因此，在组织所用技术与数据保护理念之间实现适当的平衡，对于构建有效的安全战略而言至关重要。从成功的攻击中恢复所需的措施也将是良好安全态势的重要组成部分之一。

在这两种情况下，许多具有关键安全功能的存储解决方案在保护组织的系统免受一系列危害性威胁方面发挥着主要作用。但是，如果对当前的威胁形势以及您需要保护的信息了解得不够深入，实现平衡就会变得非常困难。

现代企业可以利用 NIST 框架和风险管理原则等方法来帮助构建全面的存储战略。快照、磁带气隙保护和云对象存储等技术可用于构建和实施网络弹性解决方案，以帮助组织在面临日益严峻的威胁时确保安全。

不要让您的组织在面对攻击时措手不及。有关如何制定经协调的网络弹性战略的更多信息，敬请访问 https://www.ibm.com/it-infrastructure/ storage/mainframe。

资源

1. “2018 Cost of a Data Breach Study: Global Overview”.Ponemon Institute. 2018 年 7 月.
2. “Global Risks Report 2019, 14th Edition”.World Economic Forum（瑞士日内瓦）. 2019 年.
3. Phil Goodwin 和 Sean Pike. “Five key technologies for enabling a cyber resilience framework”.IDC. 2018 年 7 月.
4. Bert Dufrasne、Francesco Anderloni、Roger Eriksson 和 Lisa Martinez. “IBM FlashSystem A9000 and A9000R Business Continuity Solutions, A draft IBM Redpaper publication”.IBM Corp. 2018 年 11 月.