可信赖的数据中心和存储基础架构

DELL Technologies

intel

可信赖的数据中心存储基础架构

成长型企业面临着与大型企业类似的诸多数据中心存储基础架构挑战，但不同之处在于成长型企业缺乏相同的资源来化解这些挑战。在竞争日益激烈的形势下，这些成长型企业需要持续进行创新，但容量、停机时间、数据失窃和不合规等问题都成为了他们的拖累。他们必须确保宝贵的数据和 IT 资产随时可用、耐用、可扩展且受到保护。面对这些充满挑战性的市场动态，成长型企业如何才能取得成功？

成功的成长型企业明确致力于优先使用可信赖的数据中心基础架构，包括存储基础架构。图 1 说明了可信赖的数据中心技术与改善的运营成果以及最终企业取得成功之间的关系。

可信赖的数据中心最佳实践和技术与企业成功之间的关系。

数据中心安全和可信赖的优秀做法可以通过以下方面衡量：

- 更频繁地更新基础架构
- 企业上下致力于安全的基础架构技术
- 成功实施安全的基础架构技术

数据中心安全和可信，有助于获得更好的技术结果，比如：

- 中断次数更少
- 更快恢复服务和数据
- 减少数据丢失、安全事件数量
- 能够更好地满足法规遵从性要求

最终，技术和安全性能可实现更大的业务成功，包括：

- 缩短产品上市时间
- 提高客户满意度
- 增加市场份额
- 加快收入增长

来源：Enterprise Strategy Group

运营可信赖的数据中心的三个主要方面包括：

1.定期更新和淘汰数据中心基础架构

2.致力于部署可信赖的技术

3.实施这些技术

可信赖的数据中心存储技术包括诸如加密、嵌入式固件安全功能等现代数据安全功能，以及备份频率和复制等数据保护实践。

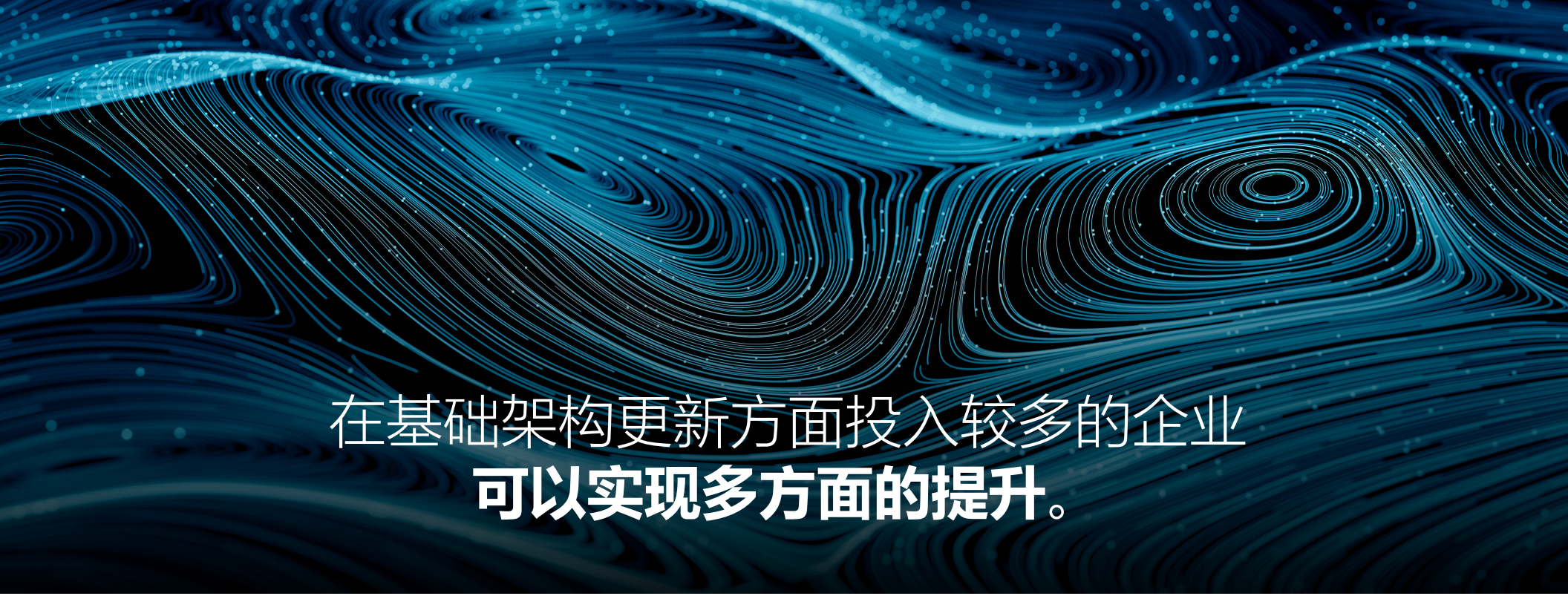
降低威胁数据的风险

成长型企业需要优先提高其 IT 环境（包括存储基础架构）的安全性和可靠性。通过尽可能减少存储中断（如安全漏洞或数据丢失）对业务造成的负面影响，成长型企业不仅可提升市场竞争力，而且可取得成功。

存储服务对企业运营至关重要，这些服务出现任何中断都可能会产生不利影响。

- 相对于竞争对手而言，网络安全风险可能会对企业造成损害
- 中断可能会打乱客户服务
- 数据丢失会影响工作效率，不合规的情况通常会导致直接的财务损失

作为安全策略的一部分，应包括制定更新和淘汰基础架构的计划。新基础架构通常包含旧解决方案可能缺乏的许多安全和数据保护功能。简言之，在基础架构更新方面投入较多的企业可以实现多方面的提升。



在基础架构更新方面投入较多的企业**可以实现多方面的提升。**

除了更新基础架构之外，成功的企业还致力于采用其他几种存储基础架构最佳实践，例如：

- **加密敏感数据以防止其失窃或损坏**
- **投资基础架构解决方案，并在其固件中内置卓越的安全功能**
- **将敏感数据复制到辅助存储系统，以尽可能延长正常运行时间并提高可恢复性。**

成功企业的运营环境往往更可靠、抗风险能力更强且难以入侵。整体来说，他们所遇到的导致数据丢失或损害的安全事件数量更少、不遵从内部治理或监管要求的不合规情况更少，发生的中断次数也更少，而且能够更快地从中断中恢复。相应地，这些企业所具有的超强技术实力使他们能够在市场中战胜竞争对手，提高客户满意度，实现市场份额和收入的双增长。

另一个会导致 IT 和业务风险的因素为是否致力于满足合规性要求，这是出色企业关注的焦点。法规遵从性要求（包括内部要求和监管要求）可能非常严格。对于资源受限的成长型企业而言，拥有一种能够高效确保满足合规性要求的方法至关重要。同时，所采用的方法必须行之有效，因为许多成长型企业没有条件承受与不合规相关的经济处罚。

确保存储基础架构的可用性

存储可用性中断可能由多种原因造成。自然灾难的冲击可能导致某个地点离线，人为错误可能会导致服务中断，而系统（无论服务器、存储或网络组件）可能会发生故障。对于那些运行较新基础架构并在高安全性和高可靠性技术解决方案方面进行较大投资的 IT 组织，则卓有成效。

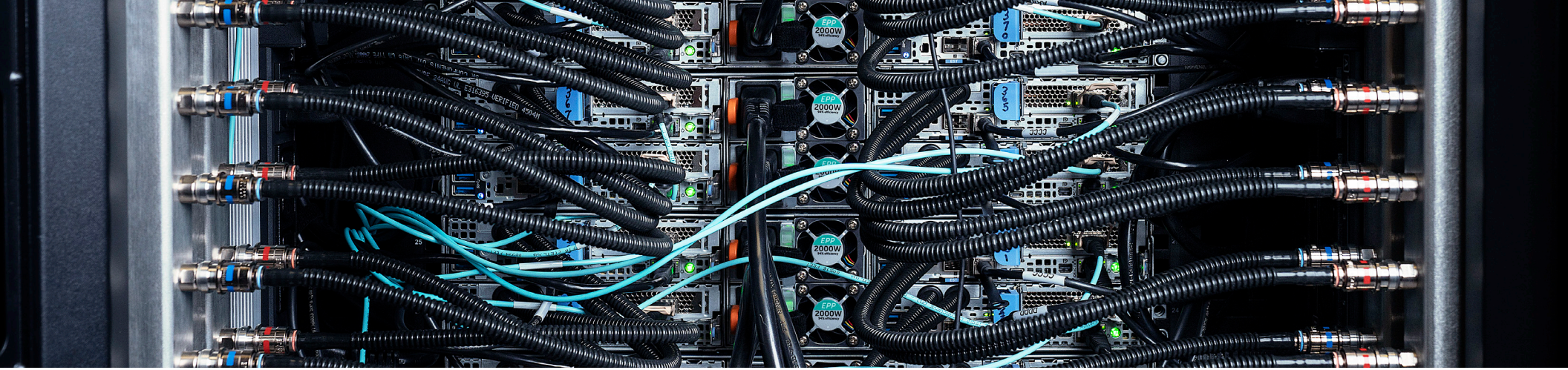
存储基础架构的可用性对于日常运营以及持续开发和提供新业务服务至关重要。存储中断会对依赖这些服务的客户和其他人员产生立竿见影的影响。对开发团队的影响则不太明显。软件开发实践在很大程度上已从单一的瀑布式方法转向了敏捷、持续的开发和交付模型。存储服务的丢失可能会导致开发工作停止，造成开发工作中断的风险，并且需要大量的恢复时间。

企业需要**一如既往地确保客户数据安全。**

通过可信赖的数据中心存储，提高业务敏捷性

专注于可信赖的数据中心技术（包括存储服务）的企业发现，他们在创新、交付新产品和满足客户期望方面具有更好的优势。随着消费者和其他企业利用持续可用的数字服务，这些期望变得越来越明显。随着对持续访问业务服务的需求不断增加，同时提供高度可用和高度可扩展的应用程序的压力也随之增加。那些能够运行这些类型的应用程序的企业可更具竞争力和发展优势。

高可用性和可扩展性本身不足以满足当今数字服务的需求。企业需要一如既往地确保客户数据安全。数据泄露非常普遍，虽然使用者可能期望出现一些安全漏洞，但这些攻击会导致财务和声誉损失。成长型企业可以利用可信赖的数据中心存储基础架构来抵御数据泄露、勒索软件的风险并防范其他破坏性的网络安全威胁。



企业应致力于更好地遵守本文概述的最佳实践：

经常更新服务器和存储基础架构，并使用具有更出色的安全性和数据保护功能的解决方案。

优先选择具有“内置”安全功能的服务器解决方案。虽然较新的服务器本身往往比较旧的服务器更安全，但有几个特定的安全功能需要重点关注：

- 能够检查所有系统更新是否均经过加密验证
- 自动锁定配置设置
- 执行完整系统擦除

通过投入有效实施最佳实践所需的财务和人员资源来确保这些最佳实践的实施。

任何组织都不能忽视安全威胁，否则可能会产生重大不利影响。可信赖的数据中心存储基础架构模型的最佳实践概述了企业级组织为有效满足存储、安全性、合规性和运营要求而使用的相同最佳实践。

详细了解 Dell Technologies 如何能够帮助您提升可信数据中心成熟度。

DELL Technologies

intel