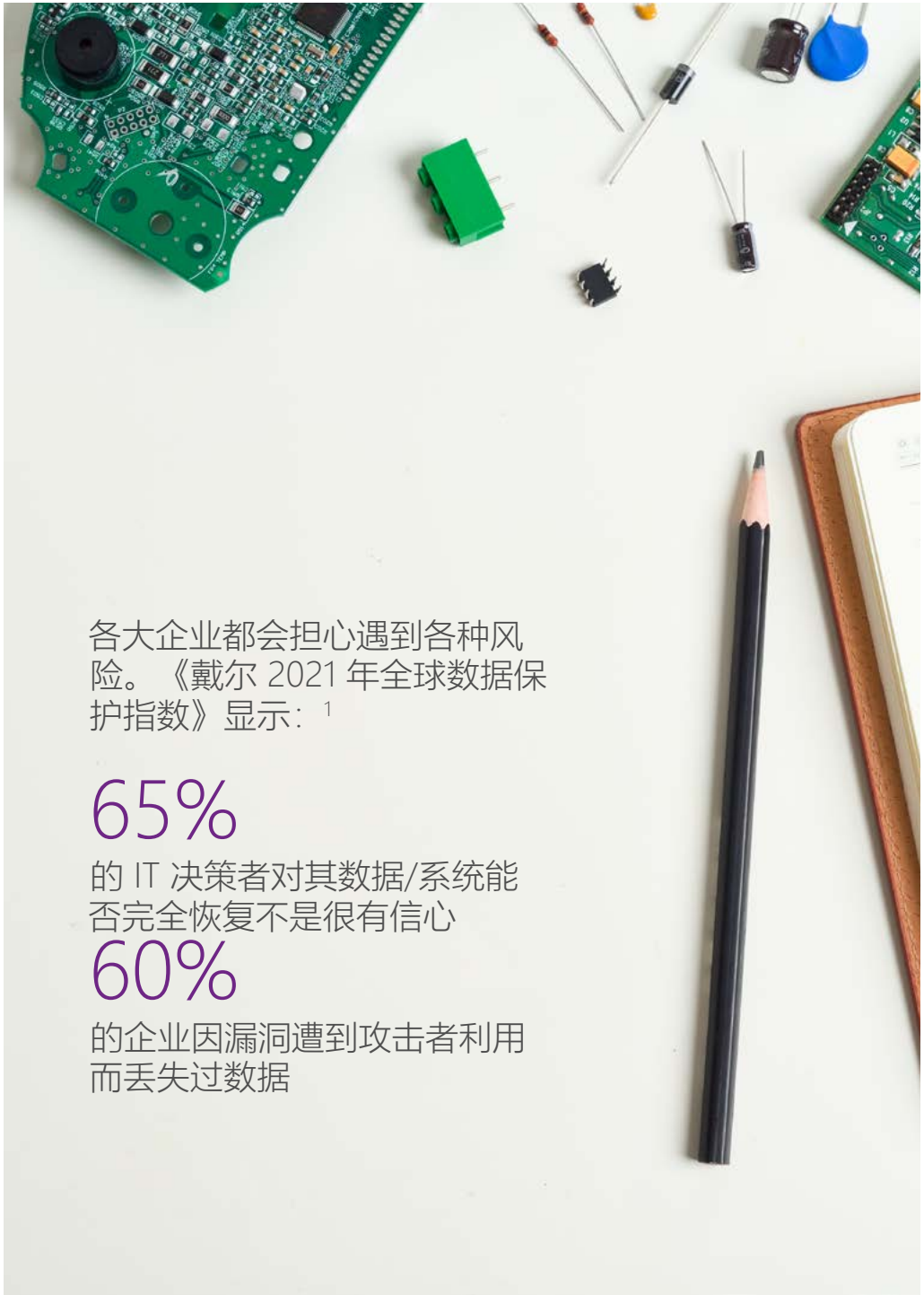
DELL Technologies

利用现代安全方法为企业保驾护航

通过整体安全策略保护您的企业。



各大企业都会担心遇到各种风险。《戴尔 2021 年全球数据保护指数》显示：[1]

65%

的 IT 决策者对其数据/系统能否完全恢复不是很有信心

60%

的企业因漏洞遭到攻击者利用而丢失过数据

快速的数字创新带来了新的安全挑战。

数字化转型正在大幅改变企业的运作方式。虽然这种转变在疫情发生之前便已开始，但随着企业转为远程办公，采用多云环境，在边缘利用数据以及使用 IT 即服务，这一过程得到了加快。

这种快速转型为那些有效利用数据的企业创造了大好良机，**但同时也带来了大量的安全挑战。**随着数字化转型的边界不断扩展，海量生成的数据正在变得更加分散、更加虚拟化，并广泛分布在多云环境中。如果企业缺乏足够的安全保护，**便会不断遭到新的攻击，并暴露更多的安全漏洞。**仅仅是庞大的数据量就带来了不断增长的挑战：**如今，各种规模的企业管理的数据量是五年前的 10 倍**，平均已接近 15 PB。[1]

要应对这些挑战，意味着企业需要确保数据、应用程序和设备安全无虞。这反过来又要求企业采用一种成熟的方法，这种方法需符合以下要求：利用创新技术实现扩展和智能化，针对业务而不是威胁进行统一调整，主动进行恢复规划，并为企业提供全方位保护，而不是采取孤立和片面的防护措施。

网络弹性：
企业能够快速应对攻击并从攻击中恢复，同时尽可能减少损失或避免业务运营中断的能力。

现代安全方法为您保驾护航：戴尔的整体解决方案。

虽然威胁检测和预防仍然是安全防御的第一道防线，但戴尔认为，要有效应对当今的安全挑战，企业需要改变“每个潜在威胁都可以被阻止”这一过时观念。随着大规模网络安全攻击的数量每周（甚至是每日）不断增长，各大企业当前必须随时做好应对攻击的准备，而不是考虑如何避免攻击发生。这种思维方式转变可以提高网络弹性。

戴尔致力于成为值得企业信赖的合作伙伴，进而利用以下优势帮助企业设计和构建安全转型解决方案并管理转型过程：

- 可实现智能化扩展的高级功能
- 针对您的整个 IT 基础架构提供的全方位支持
- 作为全球领先的技术提供商，戴尔在过去数十年间所积累的技术专业知识

戴尔的整体安全解决方案可帮助您的企业转为采用零信任体系结构，并有效应对当今迫在眉睫的威胁。

戴尔现代安全方法的三大要素

为了应对当前和新兴的威胁环境，戴尔奠定了具有以下三大要素的强大安全基础：

1.保护数据和系统

利用一整套高级工具对企业的安全方法进行现代化改造，这套工具与提供商的硬件和流程中的固有功能相辅相成，可针对您的整个 IT 基础架构提供全方位支持。这需要仔细甄选安全合作伙伴，因为几乎没有一家企业能单枪匹马做到这一点。

2.增强网络弹性

企业必须了解其当前的网络弹性级别，以便在面临攻击时保护数据，并为确保业务连续性和可用性做好准备工作。

3.克服安全复杂性

简化并自动执行安全性操作，以通过建立服务合作关系来扩大规模、提供见解并扩展资源。

网络安全领域新提出的另一个重要原则是零信任，也就是说，即使用户和设备已经**属于生态系统的一部分**，默认情况下也不应授予其访问权限。而是需要所有用户和设备接受持续、重复性的验证。零信任体系结构还依赖于强大的数据加密，并根据需要使系统保持隔离以遏制威胁。

要素 1：保护关键数据和系统。

要通过现代安全方法来保护您的企业，您需要重新思考如何保护数据和系统。戴尔可提供固有安全性功能，并针对整个生态系统提供全面支持，从而为企业带来显著的增量价值。

固有安全性

戴尔从以安全性为基准而设计的设备和流程入手。如果硬件、固件和安全控制点中已具有**固有安全性功能**，则表明其在体系结构基础方面处于领先地位。固有安全性功能还可自动执行基本安全要素方面的操作，从而减少甚至消除人为参与和干预的需求。

戴尔通过其平台和内部流程中内置的**固有安全性**功能来提供增量价值。戴尔数十年来在 IT 技术领域表现出色，并且多年来一直在产品设计和流程中推动安全智能创新。客户可利用我们经过强化的设备和流程来获得固有优势。

端点数据保护 — 戴尔可信设备

戴尔可信设备涵盖一系列功能和产品，有助于戴尔成为业界较为安全的商用个人计算机品牌。[2] 戴尔可信设备采用嵌入式技术，可在 BIOS 级别保护设备。只有戴尔会在专用安全芯片上维护受保护的固件映像和用户访问凭据，以防范可能会窃取访问凭据或攻击相应固件的恶意软件。

Dell SafeData 是戴尔可信设备功能堆栈的一部分，可通过以下平台和技术助您保护数据：

Netskope 是一个云交付安全平台，与 Gartner 的安全访问服务边缘 (SASE) 框架相一致，该框架包含面向现代企业的网络和数据安全控制功能，此外还包含零信任网络访问 (ZTNA) 功能。

Absolute Persistence® 技术嵌入在戴尔笔记本电脑和台式机的固件中。这项技术可在网络内外的设备和数据以及自我修复应用程序（如 VMware Carbon Black 和 Netskope）之间提供连续的防篡改连接。该连接通过基于云的 Absolute 控制台进行管理。

戴尔 Managed Detection and Response：端点安全性产品组合 Dell Technologies Managed Detection and Response 由 Secureworks® Taegis™ XDR 提供支持，这是一种完全托管的**全天候端到端服务，可监视、检测、调查和响应整个 IT 环境中的威胁。**

最后是 **APEX Backup Services**，这是一个基于软件即服务 (SaaS) 的数据保护平台，可为在本地和云环境中运行的 SaaS 应用程序、端点设备和工作负载提供安全、可扩展且经济高效的备份、保留、合规性和恢复服务。

戴尔的安全供应链计划符合（且在某些方面已经超过）美国政府推广的最佳实践和标准，而且我们还在不断改进。

在整个 IT 基础架构中扩展安全性

服务器

我们的戴尔 PowerEdge 服务器在设计和构建时采用了网络弹性体系结构，用于在服务器生命周期的每个阶段内置安全保护机制。其中的关键组件包括：

硬件信任根。这是戴尔在硬件生产过程中嵌入到产品芯片中的加密密钥，可确保 BIOS 无法被篡改。

签名固件、偏移检测和 BIOS 恢复。用于提供内置的数据和系统保护功能、可靠的检测和监视功能，以及在出现问题时进行快速恢复的解决方案。客户购买 PowerEdge 后，不仅能获得一台服务器，还可获得产品本身固有的全面的安全功能集。

存储

戴尔存储设备中的操作系统代码经过强化，可确保所有敏感数据都安全无虞。

这些平台具有各种功能，**例如多因素身份验证、基于角色的访问控制以及静态/动态数据加密等。**

对于**密钥管理，**我们提供 CloudLink 等内部解决方案，以及与客户现有密钥管理服务集成的选项，还允许客户灵活使用本地密钥管理商店。

安全开发生命周期和供应链安全

固有安全性不仅限于我们的产品中内置的技术功能。此外，戴尔还会管理旨在确保客户所接触的产品具有高级别安全性的内部流程。

戴尔安全开发生命周期定义了硬件和软件开发的安全控制措施，并由内部团队管理。该团队通过与多个行业标准机构进行协作，以确保执行最佳实践。戴尔供应商还与戴尔就一系列要求达成了一致，以确保整个采购周期的安全性。

戴尔供应链安全性可确保我们的产品在安全性、完整性、质量和抗风险能力方面始终保持一致。戴尔针对供应链风险的各个方面实施了多项先进计划，这些计划包括实施威胁知情产品设计，为成千上万开发人员提供安全开发实践培训，保障我们工厂的安全，推出物流安全计划，提供交付后的支持和服务等。

整体安全性功能

作为从核心到边缘再到云端的 IT 提供商，戴尔在安全性方面具有整体优势，并且可以提供面向整个 IT 领域的解决方案，**这是一种只有少数供应商才有资格提供的集成式解决方案。**

戴尔的安全愿景是，安全解决方案应具备整体性、智能性和可扩展性，涵盖整个企业，并符合一致的目标和策略应用情况。我们的安全解决方案涵盖基础架构、云环境（公有云、私有云和多云）、应用程序（包括任务关键型传统应用程序）以及全新的云原生应用程序和设备。

戴尔固有安全性解决方案的强大之处总结如下：有了这些内置功能，您就不再需要采用带有不同协议和控制台的第三方安全产品，这些产品都需要用户针对相关系统进行学习和管理。

要素 2：增强网络弹性。

通过现代安全方法加强网络保护的另一大关键要素是增强网络弹性。无论您的网络安全保护措施有多么完善，都不可能阻止每一个潜在威胁。各大企业必须假设他们将在某个时间点遭受得逞的网络攻击。

不过，他们不应为此蒙受巨大损失。要做到这一点，关键是要**准备好**尽快恢复数据，并尽可能减少攻击对业务运营造成的影响。针对网络攻击做好准备意味着：企业能够降低网络攻击对财务状况造成的影响，减少因运营中断给客户带来的不良体验，**最重要的是，在您知道企业可以快速完成灾难恢复后，便可对此高枕无忧。**

网络弹性不单是一项技术，还是一种成果，它通过结合规划、控制和集成技术来实现，这些技术可管理整个生态系统中的检测、保护、响应和恢复等功能。

戴尔可提供全面的技术解决方案和服务，旨在帮助各种规模的企业增强网络弹性，并帮助客户制定相关策略，以便在网络攻击中断其运营**之前**还原数据和恢复正常运营。

“借助 PowerProtect Cyber Recovery 解决方案，我们将能够还原数据并恢复正常运营，并且不会让勒索软件攻击者得逞。”

戴尔客户 Moreno Valley Unified School District 技术、创新与评估部门执行总监 Glen Alegre

戴尔网络保护解决方案的整体产品组合

网络恢复和弹性解决方案

APEX Cyber Recovery Services
一种完全托管的解决方案，可隔离关键数据，进而防范网络攻击和勒索病毒的入侵。该解决方案通过让戴尔对日常网络恢复存储区的运营进行托管，以及协助进行恢复活动，从而简化企业的恢复操作流程并加快遭受网络攻击后的恢复速度。

PowerProtect Cyber Recovery
一种获得 Sheltered Harbor 认可的网络弹性解决方案，可借助物理隔离的安全数据存储区，对数据进行隔离，并确保数据不可变，从而通过恢复已知良好的数据，使企业在遭受勒索病毒或网络攻击后能够恢复正常运营。

CyberSense
一种增量分析工具，可与 PowerProtect Cyber Recovery 配合使用，其可通过扫描安全存储区中的备份映像，获悉勒索病毒攻击的迹象，并在发现可疑活动时生成警报。

由 Superna 提供支持的 PowerScale Cyber Protection
针对驻留在 PowerScale 和 Isilon 平台上的非结构化文件数据发起的勒索病毒攻击，进行实时审核、主动检测和自动数据恢复。

网络恢复咨询和托管业务弹性服务

业务影响分析
通过我们特有的方法评估和验证业务弹性计划成熟度以及停机时间造成的影响。

网络恢复解决方案和服务
通过集成了人员、流程和业界卓越技术的策略来实现网络恢复，以在企业遭受网络攻击后恢复其业务流程。

事件响应和恢复
如果企业遭到入侵，网络恢复专家团队将提供自定义解决方案。

要素 3：克服网络安全复杂性。

与采用单一供应商的企业相比，采用多个数据保护供应商的企业每年的预计数据丢失成本是前者的 4 倍。[3] 复杂性是确保网络安全的一大挑战，因此使用现代安全方法加强网络防护的最后一步是克服网络安全复杂性。

由于安全运营团队要管理端点、服务器、网络、存储和云的安全解决方案，因此可能会导致效率不断降低，风险和成本迅速增加，从而致使防护级别或技术生产力受到影响。通常情况下，两者均会受到影响。

没错，如今我们仍然依赖先进的工具来提供网络防护，但也有越来越多的人认识到，在采用新技术时，**我们只是在安全工具上层层加码**。这样一来，维护这些工具的复杂性会很快超出管理能力，并会增加风险。

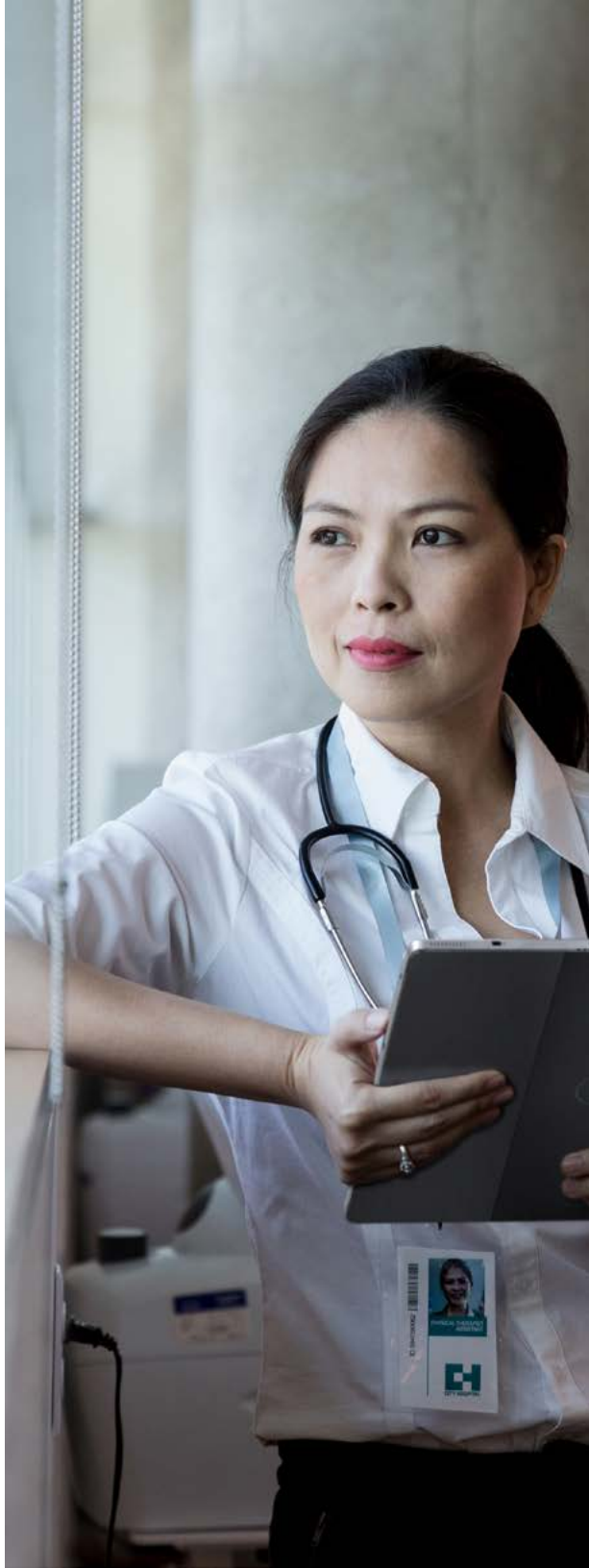
企业需要更好的方式来进行扩展。戴尔的方法具有以下优势：

产品具有固有安全性
这有助于将用户的一些基本安全需求分流到设备上，从而带来根本上的优势。

自动化、智能化和整合
戴尔可为您提供整合工具和供应商的特有优势，尤其是考虑到我们与 VMware 等企业建立了密切的合作伙伴关系，这种优势就更为明显了。

智能创新
戴尔将人工智能 (AI) 和机器学习 (ML) 融入到了我们的安全工具中。例如，Cloud IQ 是面向智能基础架构的 AIOps 解决方案。CloudIQ 集成了主动监视、自动化通知和建议、ML 以及预测性分析等功能，可降低戴尔基础架构系统面临的风险。

充当您值得信赖的顾问与合作伙伴
转为采用戴尔提供的专业安全服务是一种行之有效的方法，可对受限资源进行扩展，并降低复杂性。您还可以联系戴尔的认证安全专家团队，他们会采用基于 AI 的全新功能来增强您的安全态势，并助您从容应对迫在眉睫的威胁。



增强企业的安全态势。

随着企业不断扩展安全功能，并变得更加成熟和更具有网络弹性，克服复杂性对于企业持续取得成功而言至关重要。戴尔是您值得信赖的合作伙伴，可助您顺利实施现代安全解决方案。我们通过提供专业知识和端到端工具，助您取得以下三大核心成果：

保护数据和系统
选择戴尔作为您值得信赖的安全合作伙伴，凭借我们庞大的规模和丰富的资源，获得针对整个企业的 IT 环境所提供的高级工具和固有功能。

增强网络弹性
规划、准备和实施成熟的网络弹性计划，进而保护关键数据和应用程序，并减轻网络攻击造成的影响。

降低安全复杂性
采用自动化功能、整合安全工具并充分利用戴尔安全专家实现智能扩展。

戴尔会全心全意帮助我们的客户实现业务突破。借助我们的现代安全解决方案，企业可获得安全且富有网络弹性的环境，从而能够专注于发挥其核心竞争力、实现业务突破并推动人类进步。

DELL Technologies

关于 Dell Technologies

Dell Technologies 帮助组织和个人打造数字未来，实现工作、生活和娱乐方式的转变。我公司为客户提供业界较为全面，而且具有创新意义的技术和服务产品组合，让他们为数据时代做好准备。

更多详情，请访问 www.dell.com/securitysolutions

资料来源

1《戴尔全球数据保护指数》，2021 年。

2 基于 2017 年 8 月的戴尔内部分析。

3 戴尔委托 ESG 所撰写的技术评论《Analyzing the Economic and Operational BenePts of the Dell EMC Data Protection Portfolio》，文中评估了 Dell EMC 数据保护产品组合的经济价值，2020 年 9 月。实际结果可能有所不同。

版权所有© 2022 Dell Inc.保留所有权利。