DELL Technologies

零信任
开启优化网络安全之路

与经验丰富的技术和安全合作伙伴一起踏上零信任之旅。

许多组织希望提升网络安全成熟度，于是纷纷构建切实可行的路线图，寻找有效的方法来减少受攻击面，检测和响应网络威胁，并实施从网络攻击中快速恢复的方法，所有这些环节都离不开支持零信任的功能。

为应对日益复杂的网络威胁，戴尔利用我们解决方案和合作伙伴的解决方案中内置的安全功能，根据客户的业务目标帮助他们实现零信任。

版权所有 © Dell Inc. 或其子公司。保留所有权利。

什么是零信任?

想象一下，您的网络就像一座城堡。一旦吊桥放下，有人进入，他们就可以在城堡内畅行无阻。将基于边界的防御安全模型更新为更现代化、更安全的零信任框架，时机就是现在。

零信任是一种安全的架构方法，而不是您所购买的产品。零信任在授予任何人或任何对象对资源的访问权限之前，永远不会信任它们，并始终验证合法的业务用途。

这意味着用户和设备在默认情况下不受信任，即使他们已连接到许可的网络，甚至之前已经过验证也不例外。

从不信任，始终验证

安全 IT 生态系统的基础。

零信任框架由美国国家标准与技术研究院 (NIST) 定义，目前已被广泛采用并内置于架构之中。

该框架包括七个彼此关联的支柱，在各个安全领域为 Dell Technologies 提供全面的指导。这些支柱联合起来，形成了一种多面向的集成架构，可实现全面的安全方法，共同保护组织的数据和基础架构安全无虞。

由于集成多样化安全功能以及操作来自多个安全提供商的分散选项比较复杂，因此零信任的采用一直具有挑战性。

NIST

版权所有 © Dell Inc. 或其子公司。保留所有权利。

DELL Technologies

提升零信任成熟度

无论您处于安全旅程的哪个阶段，戴尔的解决方案都能助您一臂之力。

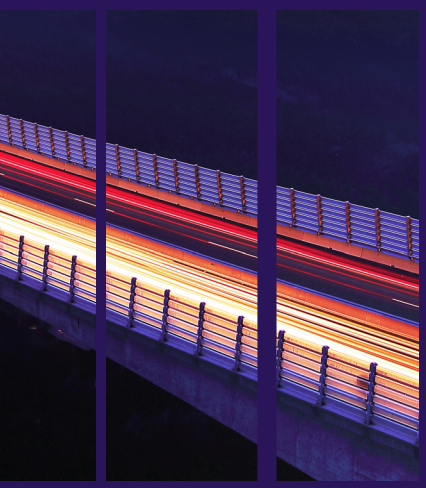
Dell Technologies 将为您的组织带来丰富的选择和灵活性。如果您希望提升网络安全成熟度，我们可以提供具有零信任功能的安全解决方案，来增强您巩固防线、检测和防御恶意网络活动以及从这类活动中恢复运营的能力。

启用零信任原则

提供丰富的选择和灵活性，助力提升网络安全成熟度。

Dell Technologies 可提供安全解决方案和零信任功能，以增强您巩固防线、检测和防御恶意网络活动以及从这类活动中恢复运营的能力。具体如下：

- 内置的保护功能，增强自动化、威胁情报、身份验证和可见性等
- 支持零信任的服务，协助制定路线图、集成关键技术并实施主动管理
- 专业服务、托管服务和安全咨询服务
- 广泛的合作伙伴生态系统



显著简化零信任的采用

利用全面集成的架构全方位实施

零信任是一种安全的架构方法，所以它不是一个单一的产品，需要仔细规划协调各种解决方案。戴尔助您卸下零信任集成的重担。方法如下：

- 戴尔正在构建一种集成的零信任架构

版权所有 © Dell Inc. 或其子公司。保留所有权利。

DELL Technologies

启用零信任原则

以您的特定安全生态系统为基础实行零信任。

戴尔通过支持零信任战略，帮助提升网络安全成熟度，该战略有助于减少受攻击面，增强检测能力并加快从网络威胁中恢复的速度。

图中所示的每个零信任支柱中都包含了面向关键领域的技术、流程和人员，同时需要实施有效的安全和业务策略来保护组织的安全。戴尔安全服务可在以下方面提供帮助：

- 安全成熟度、零信任和风险评估
- 制定战略和路线图
- 关键零信任功能的托管服务

版权所有 © Dell Inc. 或其子公司。保留所有权利。

DELL Technologies

为实现零信任奠定基础

我们提供卓越的嵌入式安全解决方案，助您在通往零信任的道路上占得先机。

Dell Data Protection

Cyber Recovery 数据避风港存储区 | PowerProtect Data Manager | CyberSense Transparent Snapshot | CloudIQ | 系统锁定 | 偏移检测 | 安全的企业密钥管理 | TLS 1.3 | IPv6 | 多因素身份验证 | 单点登录 | 基于角色的访问 | CloudIQ

戴尔 PowerEdge 服务器

软件物料清单 | 安全组件验证 | 硅信任根 | 系统锁定 | 偏移检测 | 安全企业密钥管理 | TLS 1.3 | IPv6 | 多重身份验证 | 单点登录 | 基于角色的访问 | CloudIQ

戴尔存储平台

数据隔离 | 数据不可变性 | 威胁检测 | 访问控制身份验证 | 数据加密 | STIG 强化 | 硬件信任根 | 安全启动 | 数字签名固件 | 基于角色的访问 | 安全快照

戴尔 HCI/CI

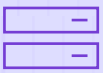
硬件信任根 | 安全启动信任链 | 数字签名更新 | 密钥管理 | 安全日志记录 | 分布式虚拟交换机 | 虚拟机隔离 | 身份验证和授权 | 生态系统连接器 | 持续验证状态 | 软件代码完整性 | 电子兼容性表

戴尔商用 PC

BIOS/固件安全性 | 硬件安全性 | 供应链保障 | 威胁管理软件（EDR、XDR、VDR） | 网络和云数据保护软件

戴尔边缘解决方案

硬件/软件/虚拟机认证 | 安全纳管 | 信任链 | 安全的操作系统/应用程序交付 | 数据权限管理



戴尔网络交换机

SmartFabric | CloudIQ | SD-WAN | VLAN 分段 | 企业 SONiC | 访问控制列表 | RADIUS | TACACS+ | 加密 | 交换机强化 | 微分段 | 虚拟路由和转发

版权所有 © Dell Inc. 或其子公司。保留所有权利。

DELL Technologies

满足不同组织的需求

提升零信任成熟度

零信任定义了一个框架并包含一套用于指导如何实现安全性的原则，并且可以使用各种功能来实现。无论您是全力支持零信任，还是专注于有针对性的改进以遵循零信任原则，戴尔作为经验丰富的安全合作伙伴，都能帮助您推进安全之旅。

化工	信息技术	通信	应急服务
食品和农业	防务	医疗和公共健康	制造
财务	核反应堆	商用	政府
能源	运输	水和废水	DAMS

版权所有 © Dell Inc. 或其子公司。保留所有权利。

DELL Technologies

DELL Technologies

作为一家经验丰富的技术和安全合作伙伴，助力贵组织踏上零信任之旅。

通过实施零信任长期持续不断地提高网络安全性。

戴尔安全服务提供：

针对安全成熟度和总体风险的专业评估。

制定零信任路线图。

持续管理安全活动。

DELL Technologies

Dell.com/SecuritySolutions

请求回电

与安全顾问交谈

请致电 1-800-433-2393

版权所有 © 2023 Dell Inc. 或其子公司。保留所有权利。Dell Technologies、Dell 和其他商标为 Dell Inc. 或其子公司的商标。其他商标可能是其各自所有者的商标。