安全连接网关

我们的技术将数据保护和威胁防护集成到安全、自动化的支持体验中

高达

60%

接受 Forrester 调查的 IT 领导者表示利用连接技术可降低风险[1]

它还可针对特定 Dell EMC 硬件作为直接连接版本部署，以及用作适用于 PowerEdge 服务器的 OpenManage Enterprise 中的服务插件。Dell Technologies Services 致力于根据市场、法规和客户见解实施安全功能，帮助我们的产品满足客户的安全目标与法规遵从性要求。

目录

1: 引言:

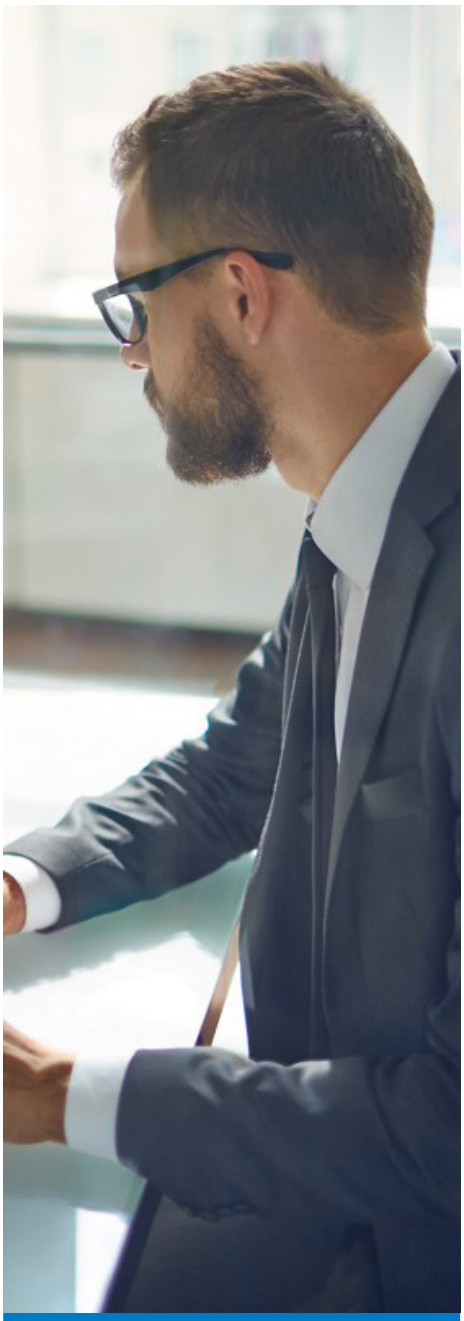
在当今的超数字化世界中，成功的创新领导者纷纷转向 IT 服务提供商开展合作，以便将 IT 支持服务外包。根据 Dell Technologies Services 委托 Forrester Consulting 开展的一项研究[1]，59% 的 IT 领导者表示，通过与合适的 IT 服务提供商合作，他们能够将 IT 员工的精力从日常运营转移到创新和战略计划上。

作为出色的 IT 服务提供商，Dell Technologies Services 致力于确保其 IT 支持服务和技术不会招致潜在的安全威胁。每一天，我们都竭尽所能，更大限度降低客户环境中部署的 Dell EMC 产品的风险。本文探讨了如何将安全性构建到安全连接网关的设计、实施和运行之中，确保为复杂数据中心基础架构提供安全的自动化 IT 支持体验。

通过利用超过 25 年的开创性 IT 支持技术，安全连接网关安全体系结构旨在阻止威胁入侵和保护数据完整性。虽然我们的技术持续监控客户设备以发现问题，并启动加速解决问题，但是：

- 我们只使用来自活动系统的遥测和事件数据。
- 我们加密系统状态数据，然后通过使用传输层安全性 (TLS) 协议的 HTTPS 在互联网中传输。
- 我们的授权技术支持工程师使用多因素身份验证进行远程访问，解决连接系统上的问题。
- 我们使用业界卓越的安全实践，在我们自己的地点处理、存储并使用遥测和事件数据。

此外，我们还与多家优秀供应商（如 Secureworks）合作，严格审查在整个安全连接网关体系结构和流程中集成的安全措施，确保您获得可靠的私有安全体验。



网络攻击和数据欺诈或失窃是首席执行官担忧的十大问题中的几个[2]

2: 安全连接网关介绍

Dell Technologies 的安全连接技术可消除您在问题预防中的疑虑，让您有更多时间专注于更重要的项目。虚拟设备版和应用程序版是您的环境与 Dell Technologies Services 之间的安全双向连接工具，非常适合在一个位置监控整个数据中心内的 Dell EMC 设备，涵盖数据存储、服务器、网络产品、CI/HCI 和数据保护。

您还可以灵活地针对特定 Dell EMC 产品将我们的技术作为直接连接版本部署，以及用作适用于 PowerEdge 服务器的 OpenManage Enterprise 中的服务插件。请访问 Dell.com/Support 以核实特定 Dell EMC 硬件和软件支持的连接选项。

数据是安全连接网关的命脉。我们会利用来自客户环境中的系统状态数据，同时将其与来自现场和技术支持团队以及组件制造商的多年事件及工程数据相关联。

查看安全连接网关的可报告项目和适用于 OpenManage Enterprise 的服务插件，详细了解收集的系统状态信息。

借助复杂先进的 AI 模型（包括机器学习），我们的连接技术可以发现并应用模式，第一次就能够准确检测出需要采取行动的相应问题。它可以发现硬件和软件问题，创建案例，并向我们发起联系请求，以开始解决问题，避免其造成巨大的代价。在通过安全连接网关连接时，它可以预测服务器硬盘和背板上的故障。根据问题类型，警报还可能启动自动化部件派发。

此外，该技术还可实现安全的双向通信，以便经授权的技术支持代理远程访问托管设备进行故障处理和解决问题。

连接安全性

定期对安全连接网关及其支持基础架构进行**第三方安全评估**。

应用程序评估包括数据传输和 API 安全性、静态和动态源代码分析、公共漏洞和暴露 (CVE) 和开放式 Web 应用程序安全项目 (OWASP) 交叉检查以及第三方库和产品。

基础架构评估包括内部和外部网络设备、服务器和服务提供商。

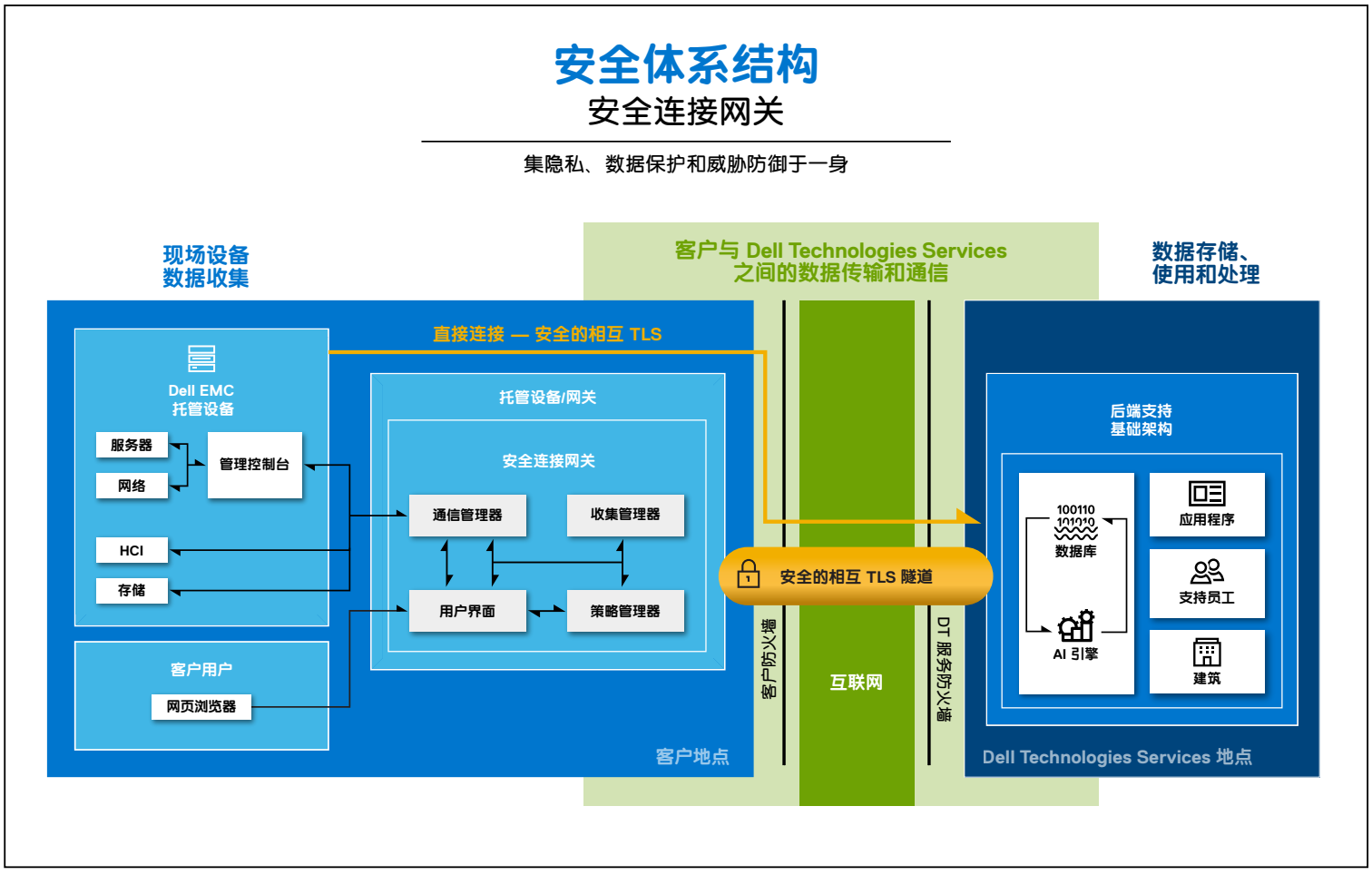
3: 安全体系结构概述

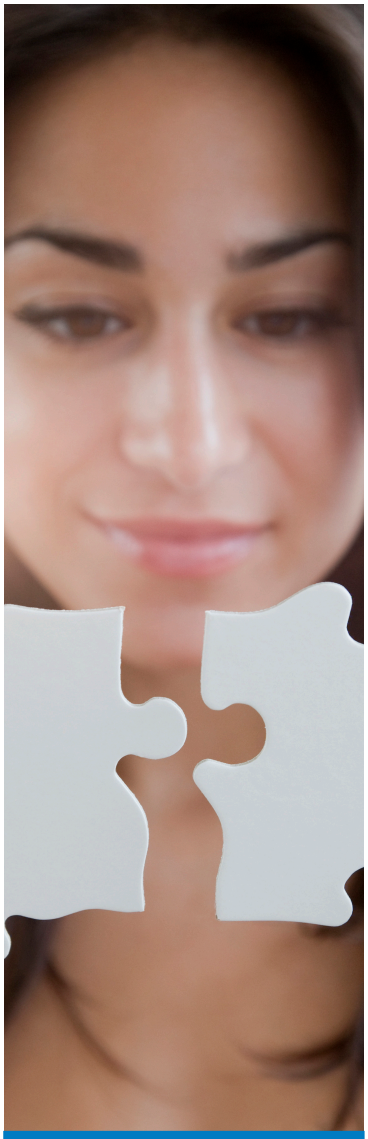
Dell Technologies Services 致力于使用我们的自动化、主动式和预测式连接技术，更大限度降低安全威胁风险。我们的安全体系结构按照严格的行业标准构建，在产品开发和部署的每一步都遵循可衡量、可重复的安全实践。请参阅第 4 节，了解更多信息。

下面的图 A 概括介绍了安全连接网关安全体系结构。在接下来的部分中，我们将分析我们的技术如何仅从 Dell EMC 托管设备收集诊断和修复问题所需的系统数据，然后在确保以下流程更为安全和私密的情况下处理这些数据：

- 现场设备数据收集
- 数据传输和通信
- 在 Dell Technologies Services 存储、使用和处理数据

图 A:





客户通过安全连接网关中策略管理器的审核功能，可以进一步提升现场数据收集的安全性。

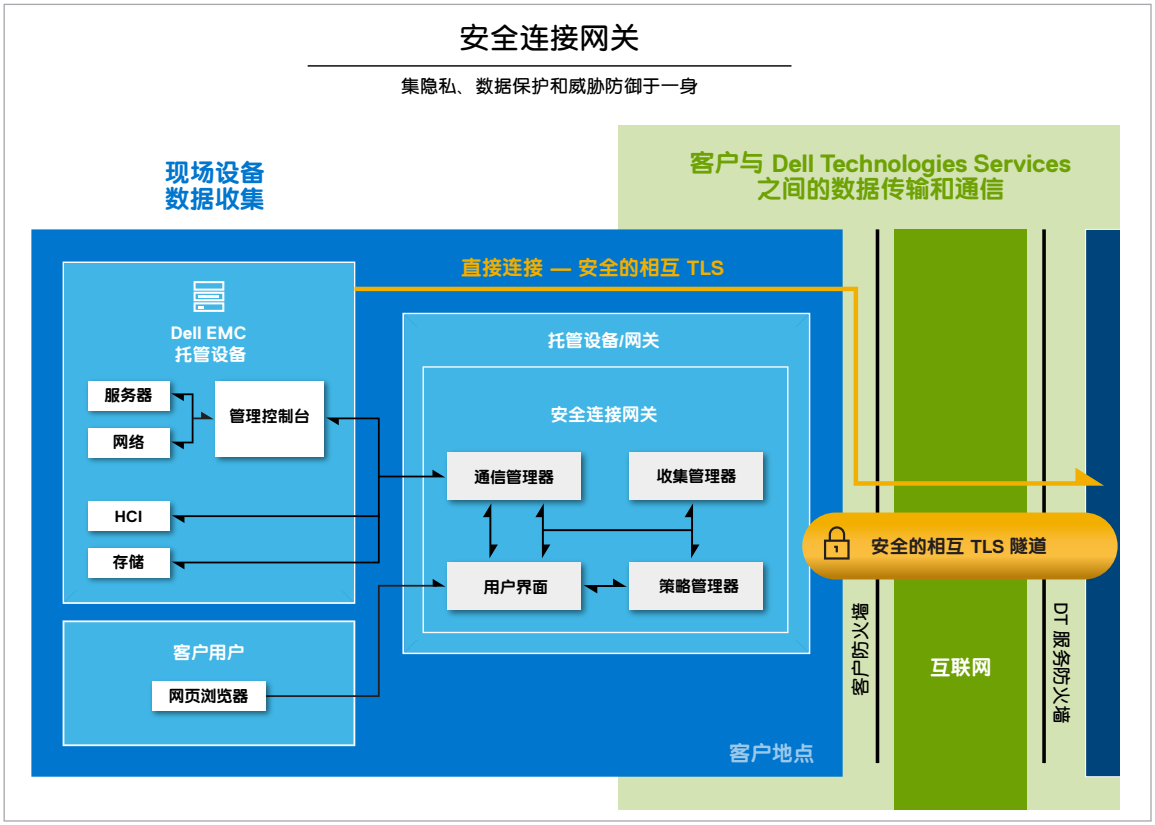
4: 安全连接网关的安全方案详情

4-1: 安全的现场数据收集

尽量减少防火墙接入点

安全连接网关可聚合 Dell EMC 设备间的通信，并在客户的防火墙中充当单一入口和出口点，供所有基于 IP 的远程服务活动使用。请参见图 B。通过尽量减少用于远程 IT 支持技术的防火墙接入点，Dell Technologies 可减少公司防火墙面临的安全风险。

图 B: （摘选自图 A — 安全体系结构）：



作为现场网关，安全连接网关以虚拟形式部署在客户提供的虚拟机管理程序中。每个网关服务器分别充当一个代理，负责传输进出托管设备的信息。在发生临时本地网络故障时，安全连接网关还可以使 Connect Home 事件排成队列。这些网关服务器有自己基于底层操作系统的 Web 用户界面。

对于某些客户，直连版本适合具有多种 Dell EMC 硬件产品的异构部署。此解决方案通过客户的防火墙充当单一的安全通信点。它集成到产品的操作环境中，因此，不需要单独的服务器来提供入站远程支持和 Call Home 功能。

尽量减少防火墙接入点（续）

对于使用 OpenManage Enterprise 系统管理控制台的 PowerEdge 数据中心客户，嵌入式服务插件是一个替代实施选项。OpenManage Enterprise 虚拟设备中的此连接插件在客户提供的虚拟机管理程序上运行。它充当托管服务器和机箱设备的服务自动化层，并提供与 Dell Technologies Services 后端的单一、安全的直接连接。

充当安全通信代理

安全连接网关在托管设备、策略管理器和 Dell Technologies Services 后端支持基础架构之间起到通信代理的作用。部署它的网关服务器是 HTTPS 处理程序。该网关利用不同的通信方法，包括设备发现、事件管理、遥测数据收集和遥测数据管理。消息类型包括：

- 设备状态心跳轮询
- 数据文件传输 (Connect Home)
- 许可使用情况数据传输
- 用户验证请求
- 设备管理同步

所有消息都使用多种协议进行安全保护。在接下来的一节中，我们将深入了解构建到安全连接网关数据通信和传输中的其他安全功能，包括使用支持端到端传输层安全性 (TLS) 通道和行业标准加密的 HTTPS 协议。

客户控制授权要求和访问权限

如果安全连接网关在客户的数据中心监控设备，客户可以选择使用策略管理器来控制远程访问连接、诊断脚本执行以及其他相关活动的授权要求。客户可以为员工以及通过远程连接诊断和修复问题的技术支持工程师设置访问权限。

以下策略管理器功能可确保授权和权限管理的安全性：

- 安全连接网关会定期轮询策略管理器的权限更改，并在本地高速缓存权限。就策略管理器而言：
  - 在上次轮询周期之后，规则集高速缓存将随配置更新而自动更新。
  - 它被配置为通过商定的特定端口，以 HTTPS 侦听程序的形式接收消息。
- 当安全连接网关收到远程访问请求或任何其他操作时，将执行从策略管理器高速缓存接收的策略。
  - 权限可以随基于设备类型或同一设备类型中的特定型号的策略，按层次进行分配。
  - 客户可以通过策略管理器的 Web 用户界面接受或拒绝所请求的操作。他们还可以创建筛选器，对授权和操作设置进一步限制。

日志记录和审核追踪

通过安全连接网关中的策略管理器审核功能，客户可以进一步提升现场数据收集的安全性。策略管理器会记录所有远程服务事件和连接、诊断脚本执行，以及支持文件传输操作。然后，策略管理器将它们作为纯文本审核日志文件存储在其数据库中。它会跟踪对自身（策略管理器）的访问、策略更改，以及所有授权或拒绝访问活动。

客户可以掌握所有这些信息，原因是：

- 审核需通过策略管理器 Web 用户界面查看，且无法编辑。
- 还可以将审核日志配置为流式传输到他们环境中的系统日志服务器。

安全连接网关

支持的 TLS 1.2 密码套件：

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

设备控制安全选项

由于客户并不总是启用策略管理器进行授权和权限管理，因此安全连接网关通过设备控制选项提供相关的安全功能。

客户可以：

- 根据设备类型、管理员组、组织或业务部门、设备的物理位置或他们选择的任何其他标准来创建自定义组
- 按照这些设备组定义特定的权限和访问权限

所有设备管理操作（包括技术支持工程师的远程活动）都将被记录，而且必须由技术支持代理在后端批准。

通过这种方式，客户可以完全控制和了解通过安全连接网关管理的设备。

双因素身份验证和数字证书管理

验证是实现安全的现场数据收集的重要一环。安全连接网关使用数字证书作为其在客户网关服务器上部署的身份证明。该证书将网关服务器的身份与一个密钥对绑定，后者用于加密和验证与后端的通信。Dell Technologies Services 的证书颁发机构 (CA) 是安全连接网关密钥基础架构的中央存储库。

数字证书管理用于通过我们的私有证书颁发机构自动登记数字证书。这可以：

- 实现对每个证书请求的程序化生成和验证。
- 确保仅在网关服务器上颁发和安装证书。不能在其他计算机上复制和使用证书。

安全连接网关使用在我们的后端支持基础架构上部署的数字证书进行连接和验证。技术支持代理使用双因素身份验证连接客户环境中的安全连接网关。

4-2: 安全的数据传输和通信

安全通信隧道

客户与 Dell Technologies Services 后端支持基础架构之间的所有通信都由安全连接网关从客户站点向外发起。它采用基于互联网的行业标准传输层安全性 (TLS) 256 位加密，以及 Dell Technologies Services 签署的数字证书验证，创建安全的端到端通信通道。后者在上一节安全的现场数据收集中进行了详细介绍。

因此，安全连接网关连接具有以下特性：

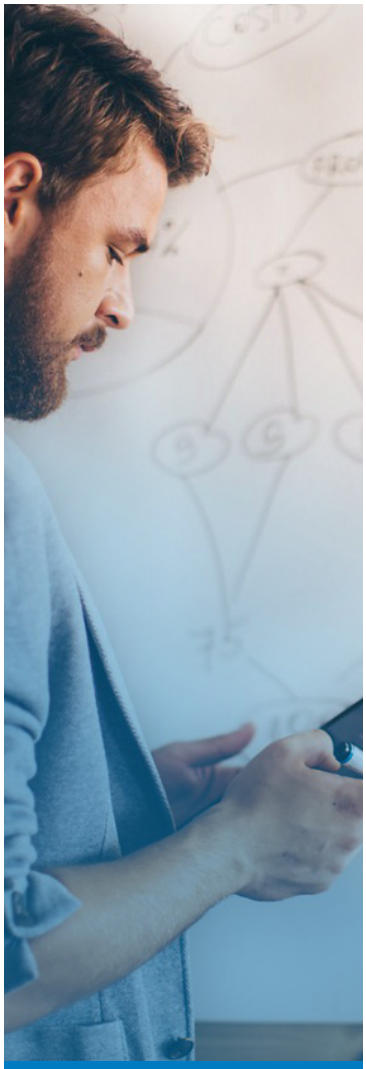
- **可靠的数据传输：**传输的每一条消息都使用消息验证码进行消息完整性检查，防止在传输过程中存在漏检的数据丢失或更改。
- **基于 TLS 的私有、安全会话：**采用行业标准算法的对称加密可为每次连接生成唯一的密钥。在协商过程中，不能修改通信而不被检测到。
- **经过验证的参与方：**由于该连接是安全的，因此它可以识别通信参与方，并使用公钥加密对其进行验证。此方法可防止电子欺骗和中间人 (MITM) 攻击。

使用安全 TLS 隧道的通信

网关服务器使用 TLS 通道来确保为以下功能提供安全的环境：心跳轮询、远程通知和远程访问。在本节中，根据图 C，我们将详细了解这些核心通信流程和协议如何确保我们的技术提供自动化、主动式和预测式体验。

心跳轮询

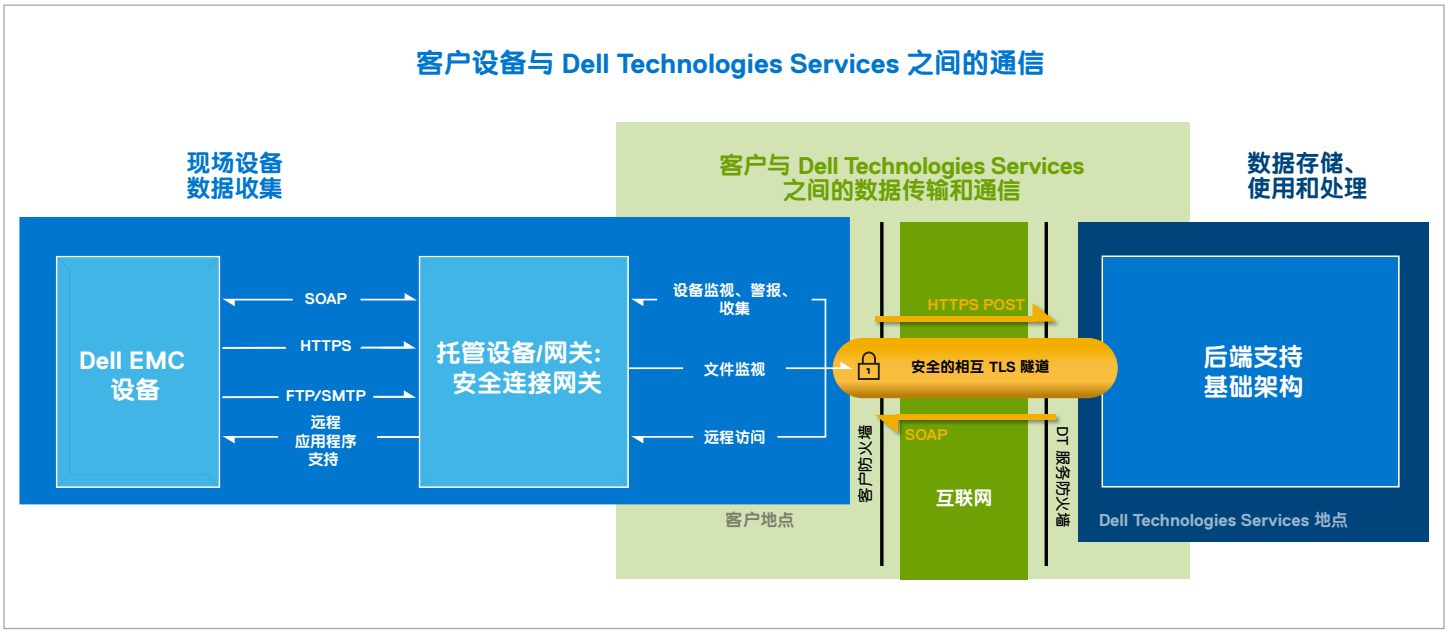
客户系统必须建立连接才能从安全连接网关体验中受益。心跳轮询用于检查设备的连接状态，定期向后端传送所收集的遥测数据。这些数据还可识别部署有安全连接网关的网关服务器。



业界卓越的验证保护连接免遭电子欺骗和中间人攻击

使用安全 TLS 隧道的通信（续）

图 C：安全体系结构



远程通知或 Connect Home 功能

安全连接网关为设备向后端发送事件文件充当安全的管道。这其中包括错误、警报、警告情况、运行状况报告、配置数据和脚本执行状态。

- 生成警报时，将生成一个事件文件并将其发送到网关。
- 安全连接网关通过 HTTPS 侦听程序服务接收该文件。
- 对于使用 FTP 和/或 SMTP 侦听程序来提供安全连接网关服务的旧式产品，文件将进行加密传输。
- 网关会压缩文件并通过 TLS 通道将其发送到后端，然后从侦听程序目录中删除该文件。
- 文件将在后端解压缩以进行分析。
- 安全连接网关还可以通过加密通信通道将文件发送到后端。此外，安全连接网关可以配置为使用故障切换通道，即 FTPS 或客户电子邮件服务器。

通过从活动系统的各个组件收集系统监控数据，Dell Technologies Services 能够提供自适应、智能化、加速的支持体验。系统 ID 是识别要处理的特定系统所需要的，也是从设备收集的与公司相关的唯一信息。当我们确定应主动发送部件时，我们将使用事先在 Dell Technologies 服务器上安全存储的现有联系信息。

有关从活动系统收集的系统监控数据的完整列表（包括在常规 24 小时周期之外收集的数据），请参阅安全连接网关的可报告项目文档和适用于 OpenManage Enterprise 的服务插件。

远程访问

我们的技术支持团队还可以远程访问客户站点的设备，以便对问题进行故障处理或执行设备特定的操作。异步消息传递可确保远程访问会话由安全连接网关从客户站点发起。接下来，安全的远程访问会话将按照如下所述建立：

- 在 Dell Technologies Services 后端进行会话验证后，技术支持代理请求设备访问权限，包括服务请求编号（如果可用）以及其他设备或用户标识符。
- 远程访问请求在后端进行排队，直到网关将设备的心跳消息发送到后端以获取访问权限。
- 作为回应，后端服务器会发送响应，其中包括请求信息、后端服务器地址和用于连接网关的唯一会话 ID。
- 安全连接网关使用其本地存储库确定设备的本地 IP 地址。然后，它会从策略管理器检查高速缓存的策略，以审查连接权限。
- 如果允许，安全连接网关会与后端服务器建立单独的持久 TLS 连接。TLS 连接始终由网关发起。后端服务器不能发起到网关服务器的入站连接。这可确保不受外部攻击的影响。

安全连接网关和后端服务器之间通过通道进行通信，直到通信终止或在不活动一段时间后超时。

网络安全性

所有网络监视组件全部位于防火墙后，由我们的网络安全团队进行管理。网络流量受到严格控制。所有入站流量全部通过特定端口传输，并且仅发送到相应的目标网络地址。

4-3: 安全的数据存储、使用和处理

存储和使用安全

物理安全

Dell Technologies Services 将大多数安全连接网关数据（包括应用程序、系统、网络和安全组件）托管在位于美国的数据中心中，旨在保持高水平的可用性和安全性。这些数据通过使用各种措施（包括物理安全）受到保护。安全特性包括但不限于：

- 内部安全警卫
- 摄像头
- 虚假入口
- 车辆封锁
- 特殊的停车场设计
- 防弹玻璃和墙壁
- 使用无标志的建筑物

仅限已获授权的人员出入基础架构所在的数据中心。通过智能卡控制出入。

逻辑安全

安全连接网关生成的数据依据戴尔隐私政策进行存储。

仅限通过内部工具对 Dell Technologies Services 基础架构（服务器、负载均衡器、网络共享等）进行逻辑访问，同时根据 IT 准则审核和评估这些工具：

逻辑安全（续）

- **服务器和数据库安全性：**服务器和操作系统组件驻留在经过安全审查的标准映像上。定期审查供应用程序使用的安全更新，包括 Microsoft 和其他软件供应商发布的更新。在发布关键安全更新时，首先在非生产映像上进行测试，并及时应用到活动服务器以避免风险。
- **审核：**维护监控设备日志，仅允许经过授权的 Dell Technologies Services 基础架构和应用程序访问。这些日志会记录所有试图登录或访问操作系统或安全连接网关 Web 服务器控制台的操作。

利用推荐的互联网安全中心 (CIS) 控制安全最佳实践来强化 IT 管理的内部版本。此外，还在所有服务器和网络设备上实施行业标准安全准则。

最后，安全连接网关生态系统在其数据中心及单独数据中心中的相同基础架构内同时采用本地高可用性。唯一的例外是具有内在高可用性的技术，如大数据群集和私有云。对于数据分析，Dell Technologies Services 利用我们完全控制和管理的云环境，包括私有云、混合云和公有云。

验证

安全连接网关使用戴尔 MyAccount 向 Dell Technologies Services 进行身份验证，并使用操作系统登录组进行机上验证。

对于拥有安全连接网关组件访问权限的组（如数据库管理团队和运营支持团队），将分配单独的职责和访问权限。生产环境的所有更新都经由明确的变更控制流程进行，该流程具有严格的审核和制衡机制。

处理安全性

注重安全的社区

我们提供基于角色的多层次安全培训课程，以针对特定工作的安全最佳实践以及如何使用相关资源对新员工和现有员工进行培训。Dell Technologies 努力在其整个社区中营造安全意识文化。此外，我们的开发人员社区是戴尔 Security Champion 计划的一部分，该计划的目的是在我们的软件开发实践中培养安全左移思维。

开发

我们的内部**安全开发生命周期标准 (SDL)** 是 Dell Technologies 产品部门的共同参照，旨在以市场期望和行业实践为基准，评估产品和应用程序的安全开发活动。它定义了产品团队在开发新特性和新功能时应采用的安全控制措施。SDL 同时包含与主要风险方面相关的分析活动，以及规范性主动控制措施。分析活动（如威胁建模、静态代码分析、扫描和安全测试）旨在发现和解决整个开发生命周期中的安全缺陷。规范性控制措施旨在确保开发团队能够通过防御性编码来防止特定的常见安全问题，包括在开放式 Web 应用安全项目 (OWASP) Top 10 或 SANS Top 25 中发现的安全问题。安全连接网关

我们利用可重复、安全的产品和应用程序开发流程

开发（续）

采用了戴尔 SDL 成熟度框架，以实施符合行业标准的安全控制措施。

安全连接网关代码是使用敏捷开发方法开发的。代码通过行业标准自动化软件持续进行集成。代码版本通过安全组权限进行检入和控制。

每个软件版本都依据我们的安全策略接受安全评估，包括：

- 使用渗透测试进行漏洞评估
- 由多家优秀供应商（如 Secureworks）进行第三方安全性测试
- 评估验证、授权和身份管理解决方案
- 使用业界先进的软件构成分析解决方案扫描所有第三方库和组件。此外，还传达针对特定安全改进的戴尔安全公告。
- 我们的全球安全组织进行数据分类。此过程将隐私和安全性结合在一起，确保电子数据得到保护。

应用程序还会接受安全审核和治理。

变更管理

根据我们公司变更管理委员会的要求，Dell Technologies 变更管理流程遵循 ITIL 基金会的最佳实践。所有变更全部通过变更请求票证进行管理。访问我们的系统以发起变更的人员需要接受 ITIL 培训，并熟悉 SDL。应用于后端基础架构的所有更新和升级都接受版本控制，确保正确跟踪和追溯。团队采用自动化内部版本流程来应用新的内部版本，或撤销已部署的内部版本或热修复。

在客户地点安装的应用程序可以根据客户的偏好进行升级。提交到 Dell.com/support 的每个版本都包含与引入的变更相关的信息及已知的限制。

所有新功能和变更全部由我们的产品管理团队准备，同时使用记录计划变更流程确定优先级，由变更控制委员会进行审核和批准。

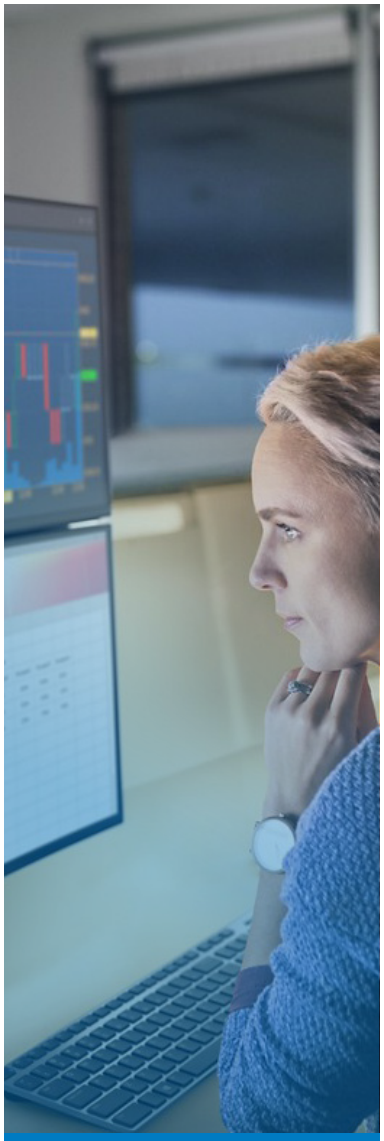
供应链风险管理

在计划、采购、生产、配送、退货生命周期的每个阶段，Dell Technologies 均遵循业内卓越的最佳实践。我们采取全面的方法来保护供应链，包括推动国际 SCRM 标准和最佳做法，以便在全球市场上保持可信 ICT 供应商的地位。

有关我们供应链保障实践的更多信息，请参阅此处。

事件报告

Dell Technologies 内任何观察到可疑活动或怀疑存在网络安全问题或威胁的人员都必须立即向我们的计算机安全事件响应小组 (CSIRT) 报告该事件。这包括安全流程中可能影响我们的环境或导致系统和/或数据泄露的弱点或漏洞。然后，CSIRT 会对该事件展开全面调查，报告事件的人员会提供 CSIRT 开展调查所需的所有资料和详细信息。CSIRT 团队使用 CSIRT 事件响应计划，其中详细说明了响应和解决戴尔内部和非面向客户的网络安全事件的正式流程。这些事件可能对戴尔资产、计算机网络或数据处理设备以及戴尔及其适用子公司、员工、服务提供商、合作伙伴或客户信息构成潜在威胁。



产品安全最佳实践相关行业协作

漏洞响应

Dell Technologies 致力于帮助客户更大限度降低与我们产品中的安全漏洞相关的风险，为客户提供及时的信息、指导和缓解措施，应对漏洞造成的威胁。我们的产品安全事件响应团队 (PSIRT) 负责协调响应和披露报告给我们的所有产品漏洞。所有 Dell Technologies 产品漏洞披露均可在线获取。

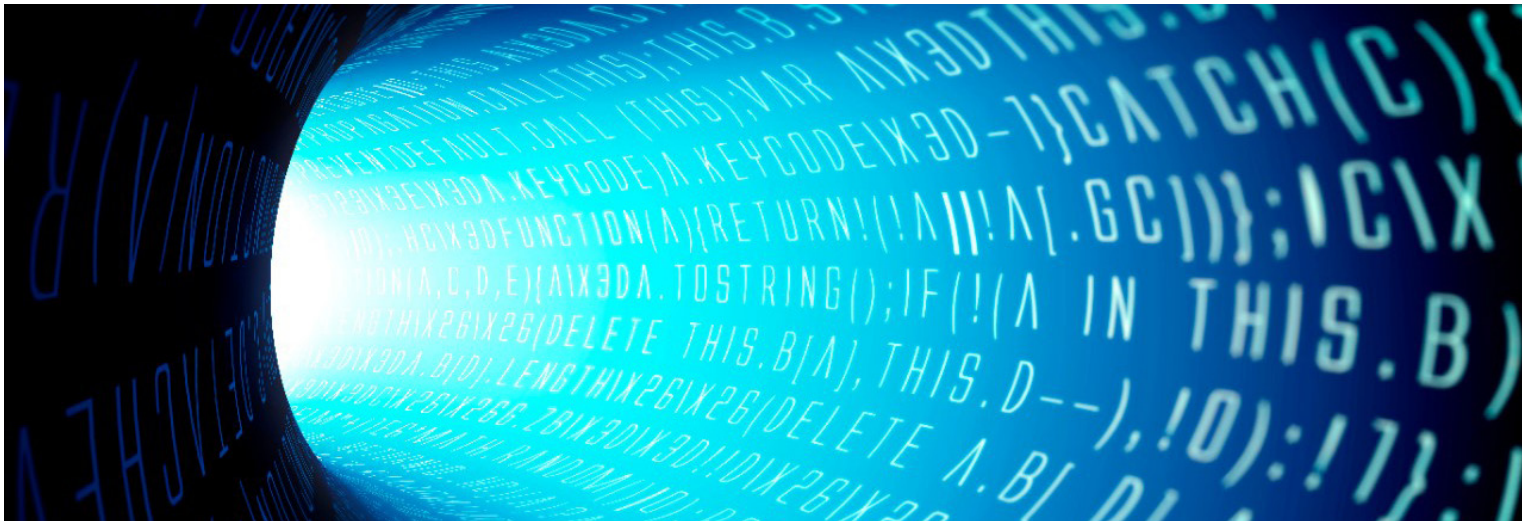
详细了解我们的漏洞响应政策

行业联盟

Dell Technologies 参加了多个全行业性的团体，以便在产品安全最佳实践的定义、演变和共享方面与其他领军供应商协作，进一步加强安全开发事业。行业协作示例包括：

- 戴尔通过其 EMC 实体联合创立了卓越代码软件保障论坛（The Software Assurance Forum for Excellence in Code，SAFECode），目前正担任其董事会主席。其他董事会成员包括来自 Microsoft、Adobe、SAP、英特尔、Siemens、CA 和 Symantec 的代表。SAFECode 成员相互之间共享和发布软件保障实践和培训。
- Dell Technologies 是事件响应和安全小组论坛（The Forum for Incident Response and Security Teams，FIRST）的活跃成员。FIRST 是事件和漏洞响应领域的主要组织和全球公认领导者。
- 我们积极参与开放群组可信技术论坛（The Open Group Trusted Technology Forum，OTTF）。OTTF 领导着全球供应链完整性计划和框架的开发工作。
- 早在 2008 年，戴尔便是受到内建安全性成熟度模型（Building Security In Maturity Model，BSIMM）项目评估的最初 9 家公司之一，并且一直参与该项目。一名 Dell Technologies 代表在 BSIMM 顾问委员会中任职。
- 戴尔员工是 IEEE 安全设计中心的创始成员，此中心是根据 IEEE 网络安全计划发起的，旨在帮助软件架构师了解并解决普遍存在的安全设计缺陷。

请访问我们的安全和信任中心，获取资源和解决方案，以帮助您找到企业安全问题的答案。



行业安全标准

我们的员工积极参与标准机构和行业联盟，专注于制定安全标准以及定义行业范围的安全实践，包括：

- 云安全联盟（Cloud Security Alliance，CSA）
- 分布式管理任务组（Distributed Management Task Force，DMTF）
- 事件响应和安全小组论坛 (FIRST)
- 信息技术标准国际委员会（International Committee for Information Technology Standards，INCITS）
- 国际标准化组织（International Organization for Standardization，ISO）
- 互联网工程任务组（Internet Engineering Task Force，IETF）
- 开放群组 (The Open Group)
- 结构化信息标准促进组织（Organization for the Advancement of Structured Information Standards，OASIS）
- 卓越代码软件保障论坛 (SAFECode)
- 存储网络行业联盟 (SNIA)

ISO 9001 认证

Dell Technologies 已经过 ISO 9001 认证。公司定期对其所有开发和制造中心进行季度审核和合规性审查。

5：结语

我们的连接技术通过自动化、主动式和预测式警报提供毫不费力的 IT 支持体验，尽可能确保关键数据中心基础架构的正常运行。选择与 Dell Technologies Services 合作，客户可以放心，我们承诺在其遥测数据的收集、通信、传输、使用和存储方面提供可靠的私有安全体验。

有关问题和更多信息，请访问 DellTechnologies.com/SecureConnectGateway

1 来源：Forrester Consulting 于 2021 年 4 月代表 Dell Technologies 进行的委托研究，《The Role Of IT Services Providers Expands To Strategic Collaboration》

2 来源：《World Economic Forum Global Risks Report 2021》。http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf