SupportAssist for Business PCs：安全性概览

我们总结了与 SupportAssist 安全性相关的五大关键问题并予以解答。

SupportAssist 可帮助您识别整个 PC 机群的硬件和软件问题，自动获得戴尔技术支持。SupportAssist 可解决系统性能和稳定性问题，减少安全威胁，监视和检测硬件故障，并自动发起与戴尔技术支持的接洽流程。

此外，SupportAssist 会主动从您的 PC 收集遥测数据，并根据您的服务计划提供 PC 利用率和修正见解。

目录

I：引言

笔记本电脑出现故障可能会造成中断，让人烦躁。这些问题会严重影响员工的生产力，而且这往往出现在情况十分糟糕的时候。因此，企业首席信息官越来越关注其 PC 机群的质量和正常运行时间。

许多首席信息官已采用先进的前沿技术，利用从数据科学中获得的见解来处理数十亿个数据点，帮助 IT 管理员提高效率。来自终端用户系统的系统状态信息会发送给公司的 IT 部门，或者是硬件或软件供应商，以便快速解决问题或防止问题出现。采用 SupportAssist 连接技术的 Dell ProSupport Plus 可通过 TechDirect 门户提供整个 PC 机群的单一视图，在硬盘出现故障时发出警报。

虽然需要此技术来确保正常运行和效率，但 CIO 有时会对其收集的信息及其处理方式存有疑问。

以下问题非常关键：

- SupportAssist 收集哪些数据？
- 将数据传输回公司的 IT 部门或计算机供应商时，如何保护这些数据？
- 到达目的地后，数据是否以私密且安全的方式存储？
- 戴尔如何遵守 GDPR 和其他标准？

本文评估了这些问题以及其他相关问题，以此来评估由数据科学提供支持的技术。本文简要概述了 SupportAssist（作为 ProSupport Suite for PCs 的一部分）如何提供全面的支持服务，从而能够在问题发生之前预测和解决这些问题。此外，本文还详细介绍了 Dell Technologies Services 如何在处理、传输和存储数据时保护敏感数据。

II：SupportAssist 简介

SupportAssist 是戴尔的智能连接技术[1]，使组织能够获得针对其整个 PC 机群的自动化技术支持。它可以监视终端用户设备，主动检测硬件和软件问题，并提供关于系统使用情况的见解。

当检测到问题时，SupportAssist 会根据服务计划，自动向技术支持部门创建支持案例。问题类型将会决定警报是发起技术支持请求还是触发自动部件派送。SupportAssist 可收集硬件和软件数据，供技术支持人员进行故障处理和解决问题。

Dell ProSupport Suite for PCs
通过单一解决方案提供全面的支持功能，无需叠加服务。[2] 了解详情。

重要功能

- 全机群主动式和预测式检测，提高问题解决速度
- 在单一屏幕中快速分析运行状况、应用程序体验和安全性评分
- 戴尔编写的脚本库，用于自动执行任务和修复整个机群中的问题
- 自动创建和部署戴尔 BIOS、驱动程序、固件和应用程序的自定义更新目录
- 在 TechDirect 中灵活地定制您的视图和控制面板

可用功能因购买的 PC 支持计划而异。

- 借助 ProSupport Plus，终端用户可使用整套 SupportAssist 功能，包括预测式问题检测和故障预防。

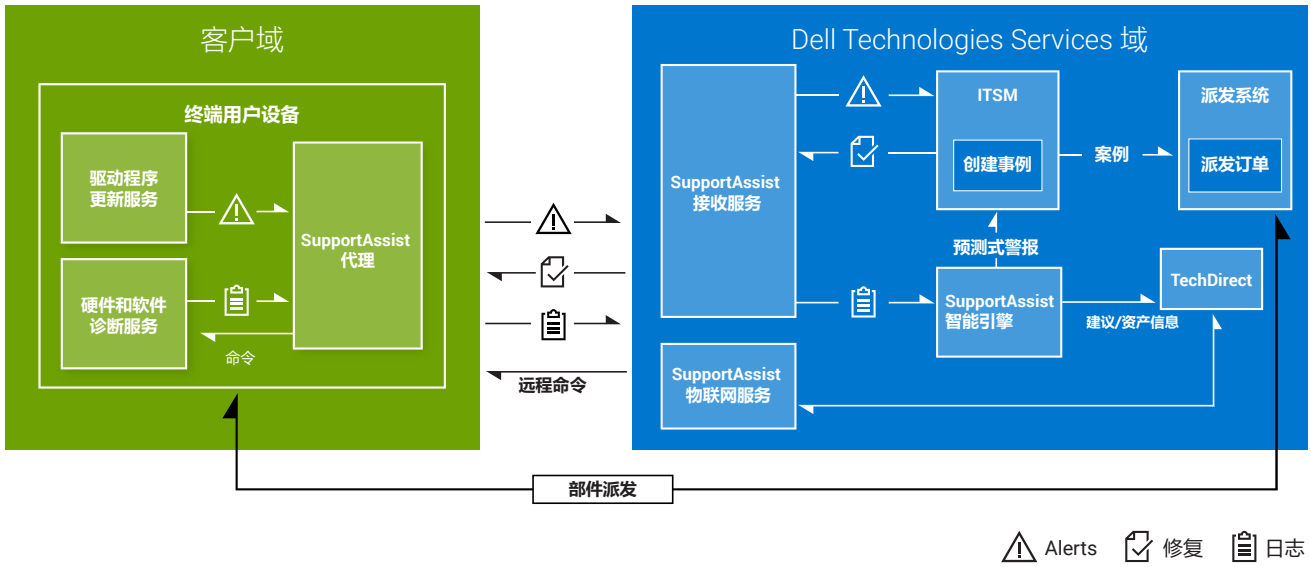
有关特性和功能的完整列表，请查看管理员指南。

III.SupportAssist 体系结构

SupportAssist 由一系列服务组成，可持续监视系统，并按计划对设备进行运行状况检查。此信息将传回 Dell Technologies 服务器，以便分析数据并提供建议。

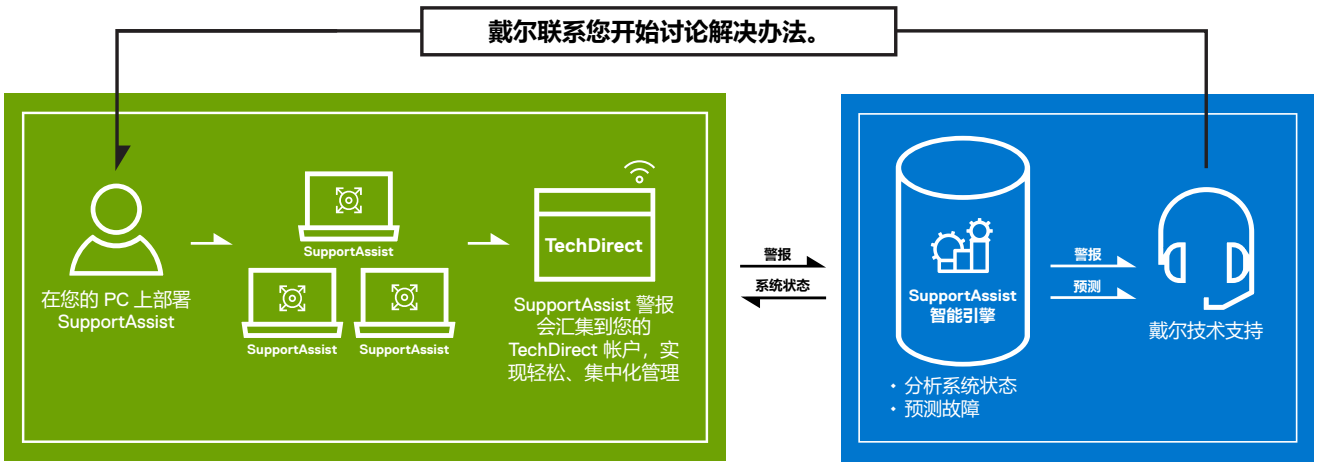
有关 SupportAssist 部署和修正所需的网络、端点、端口、防火墙或网关要求的完整列表，请查看我们的部署指南。我们的修正脚本由戴尔开发，在执行前会经过测试、签名以及确认。

SupportAssist 体系结构



使用 TechDirect 集中管理 SupportAssist

SupportAssist 警报会汇集到组织的 TechDirect 账户，实现轻松、集中化管理。拥有 ProSupport 或 ProSupport Plus 服务计划的组织还可以选择将警报自动转发给 Dell Technologies Services。



使用 TechDirect 集中管理 SupportAssist（续）：

SupportAssist Insights 作为实用的分析组件，可以收集系统利用率数据，并且该数据可以在 TechDirect 中查看。其中包括 CPU 利用率、可用硬盘空间、最大电池容量、电池运行时间以及更多有用的信息。TechDirect 可以显示所有系统、特定设备组中的系统或单个系统的此类信息。这样一来，客户能够发现性能问题，并做出更好的业务决策（例如，是否升级或更换硬件）。

IV.SupportAssist 安全性

组织的 CIO 或 CSO 可能对 SupportAssist 收集的数据类型以及如何管理这些数据存有疑问。本节将回答这些问题，展示 SupportAssist 如何仅收集解决客户问题所需的数据，然后以极高的安全意识处理这些数据。

SupportAssist 收集哪些数据?

SupportAssist 可自动收集故障处理所需的数据，并将其安全地发送给技术支持人员。我们可以利用这些数据提供自适应、智能且加速的支持体验。

服务编号用于识别正在使用的特定终端用户设备，是仅有的从设备收集的公司相关信息。当 SupportAssist 确定应主动发运部件时，戴尔会使用安全存储（配合加密、保留策略等措施）在 Dell Technologies 服务器上的现有联系信息。

作为日常系统监视的一部分，我们将收集并且每 24 小时发送以下系统信息：

- **模式版本：**用于日常系统监视的模式版本
- **代理版本：**部署在系统上的 SupportAssist 版本
- **服务编号：**系统的唯一标识符
- **系统型号：**系统型号名称
- **注册信息：**SupportAssist 的注册状态
- **操作系统版本：**设备上运行的操作系统版本
- **SP 版本：**操作系统的服务包
- **UTC 日期：**向 Dell Technologies Services 发送日常系统监视信息的日期和时间
- **BIOS 版本：**系统上安装的 BIOS 版本
- **状态：**依赖于严重程度的警报状态，例如警告
- **描述：**有关系统故障的信息，例如，CPU 使用率高
- **硬盘可用空间：**系统硬盘中的可用空间
- **内存利用率：**已使用的系统内存容量
- **CPU 利用率：**已使用的 CPU 容量
- **本地日期：**系统的日期和时间
- **最后启动日期：**系统上次重新启动的日期和时间
- **Windows 更新运行日期：**上次在系统上更新 Windows 的日期和时间
- **24 小时内蓝屏数：**过去 24 小时内出现的蓝屏次数
- **警报信息：**警报的唯一标识符

有关从活动系统收集的系统监视数据的更多信息，请单击此处访问 Dell.com 页面。

所有信息均通过安全渠道传输。

如何保护修正脚本?

在上传到修正平台之前，所有戴尔编写的修正脚本都使用戴尔证书进行签名，并经过广泛的测试和验证，以确保这些脚本按预期执行，而不会产生意外结果。这是在执行之前验证脚本真实性的基础。例如，如果脚本在端点上遭到修改或替换，则证书签名验证将失败，并且 SupportAssist 将阻止脚本执行。这可以防止执行未经授权或可能有害的代码。戴尔以外的任何人都无法修改这些脚本，从而确保其完整性。建议在更广泛地部署之前，在指定的一组 PC 上测试脚本。

自定义工作流脚本遵循不同的流程。当客户上传自己的脚本时，修正系统同时接受未签名的脚本和使用客户证书签名的脚本。这些脚本在传输到 PC 以及在静态存储时会保持完整性。建议在更广泛地部署自定义脚本之前，先在特定的一组 PC 上对其进行测试。

TechDirect 连接和管理功能支持创建站点和组，使客户能够在测试计算机上验证戴尔编写的脚本和自定义脚本。修正控制台中的所有信息都在 TechDirect 的租户边界内受到严密保护，只有经租户管理员授予适当角色的用户，才能访问这些信息。此外，结果也可以导出为 CSV 文件以供进一步分析。

SupportAssist 如何安全地存储和传输数据?

从 SupportAssist 发送到 Dell Technologies Services 的数据通过 256 位加密技术进行加密，并使用传输层安全性 (TLS) 协议安全地传输。

安装包期间，每台计算机上会在运行时生成一个加密密钥。加密密钥和盐一起用于加密安装的信息。行业标准算法用于加密静态数据。

在密码学中，盐是随机数据，用作单向函数的输入来对数据（密码或密码短语）进行"哈希处理"。盐的主要功能是防御字典攻击或其散列等效攻击（一种预先计算的彩虹表攻击）。

所有加密密钥均使用安全随机数生成器生成。传输中的数据使用基于超文本传输安全协议 (HTTPS) 的 TLS 保护。所有加密算法均为行业标准，静态数据都经过加密。

在机外通信中，使用 HTTPS 传输用户提供的反馈、诊断遥测事件，并在 Dell.com 或 Microsoft Azure IoT Hub 上查询 API 以获取还原过程中使用的系统信息。采用安全的 MQTT 作为发布-订阅方法。

在将内容传输或下载至终端用户设备时，标准 HTTPS 用于保护客户端和后端基础架构之间的通信。HTTPS 或安全 MQTT 用于保护遥测数据的传输、与 Dell.com 或 Microsoft Azure IoT Hub 的后端 API 的通信，以及从 Dell.com 检索的内容的下载。

所有网络组件都位于防火墙后面，由网络安全团队管理。网络流量受到严格控制。所有入站流量都通过特定端口传输，并且仅发送到相应的目标网络地址。SupportAssist 利用网络带宽处理需要连接到 Dell Technologies Services 基础架构的各种事件。使用的带宽可能因 SupportAssist 监视的目标系统数量而异。请参阅"从连接的 PC 收集的信息"文档，以了解有关平均数据使用量的详细信息。

SupportAssist 如何处理数据?

SupportAssist 利用收集到的数据为客户提供自动化、主动式和预测式支持。如果系统出现问题，SupportAssist 将生成警报，以便技术支持工程师进行故障处理。

SupportAssist 还使用收集到的数据来预测组件何时会出现故障，它使用的是人工智能软件，该软件基于从现场数千万台戴尔系统收集到的数据。这种预测式警报可用于在部件出现故障之前派送部件，从而实现出色的系统正常运行时间和数据保护。

最后，SupportAssist 使用这些数据来检测和删除用户系统中的病毒和恶意软件，以优化操作系统性能，并提供有关 BIOS、驱动程序和固件更新的建议。

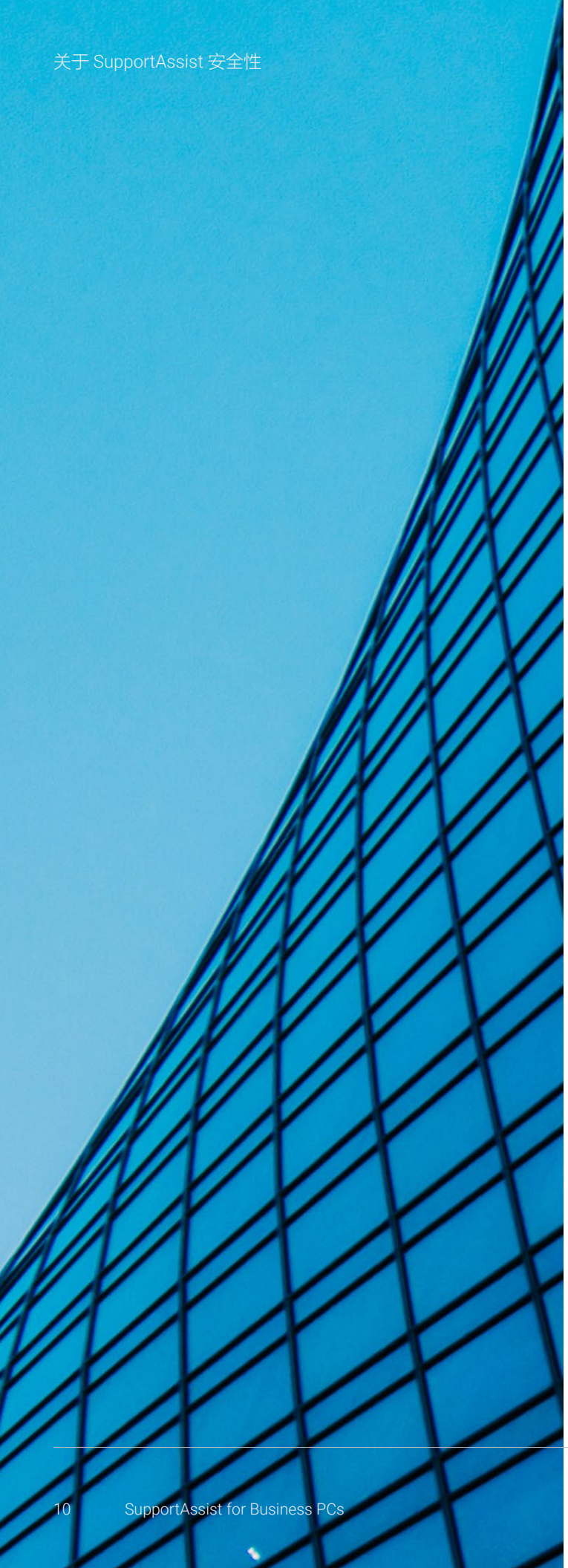
系统应用程序使用情况通过 Insights 组件提供有关系统使用情况的见解。

物理安全性

Dell Technologies Services 将 SupportAssist 数据（包括应用程序、系统、网络和安全组件）保管在位于美国的数据中心，以保持高级别的可用性和安全性。SupportAssist 数据受到多种措施的保护。

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。

物理及逻辑安全措施保证存储数据的安全。



逻辑安全性

SupportAssist 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，该工具根据戴尔数字 (IT) 准则进行审核和评估。

- **审计：**维护受监视设备日志，仅供 Dell Technologies Services 基础架构和/或应用程序访问。这些日志记录了所有登录或访问操作系统或 SupportAssist Web 服务器控制台的行为。

根据安全性方面的最佳实践，使用互联网安全中心 (CIS) 建议的控制措施来强化 IT 管理的内部版本。

最后，SupportAssist 生态系统在其数据中心内采用本地高可用性，并在另一个数据中心内使用相同的基础架构。唯一的例外是具有内在高可用性的技术，例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。关系数据库、简单存储服务和数据仓库都经过加密，并使用最低权限。所有关系数据库均不向公众开放。使用 HTTPS 保护数据仓库。

Dell Technologies 有哪些安全实践和策略?

开发

我们的内部安全开发生命周期标准 (SDL) 是 Dell Technologies 产品组织的基础参照，为安全产品和应用开发提供了重要基准。戴尔根据 ISO/IEC 27034 和基于 NIST 安全软件开发框架 (SSDF) 的标准定义了 SDL 控制目录。这些工具帮助戴尔团队为客户打造安全的产品，并防止戴尔开发/支持的软件和硬件中出现安全漏洞和弱点。工程团队在开发新特性和功能时必须采用这些控制措施。这些控制措施包括分析活动以及侧重于关键风险领域的规范性主动措施。

分析活动（包括威胁建模、静态代码分析、扫描和安全测试）是不可或缺的组成部分，旨在在整个开发生命周期中识别和缓解安全缺陷。此外，SDL 还包括规范性控制措施，以帮助确保开发团队主动解决特定安全问题，包括开放式 Web 应用程序安全项目 (OWASP) 前 10 名和 SANS 前 25 名等行业标准中列出的问题。

SupportAssist for Business PCs 与这一强大的 SDL 框架保持一致，采用戴尔 SDL 成熟度模型来实施符合行业标准的安全控制。DevSecOps 计划通过在持续集成和持续部署 (CI/CD) 环境中自动执行 SDL 控制并实施安全策略，保护戴尔的现代软件开发和部署流程。这些 CI/CD 工具可自动执行构建、测试和部署流程，确保代码更改作为开发工作流程的一部分得到持续集成和测试。

SDL 工程师执行 SDL 安全评估，以识别软件中的安全问题和漏洞，并向开发团队提供修正这些安全发现的建议。这种保障使我们能够了解我们安全实践的成熟度以及我们软件和硬件的安全态势。

此评估包括：

- 使用渗透测试进行漏洞评估。
- 由 SecureWorks 等知名供应商进行第三方安全测试。
- 评估验证、授权和身份管理解决方案。
- 使用业界卓越的软件组成分析工具彻底扫描所有第三方库和组件。
- 传达有关特定安全增强功能的戴尔安全公告。
- 与我们的全球安全组织合作，对数据进行严格分类，将隐私和安全工作结合起来，以保护电子数据的安全。
- 使应用程序接受安全审计和治理程序。

GDPR

戴尔已实施相应措施，旨在确保我们拥有必要的流程和程序来履行 GDPR 规定的义务。戴尔会跟踪全球隐私法律的发展动态，并确保遵守相关隐私法规规定的适用义务。如果戴尔作为数据处理方，则会根据共同商定的表格或标准数据处理协议表格对数据进行处理。有关更多信息，请访问以下链接：

- 戴尔关于 GDPR 信息安全的公司声明和控制措施摘要
- 戴尔针对 GDPR 合规性的承诺
- 戴尔有关 Dell Technologies 客户的合规性常见问题解答

安全流程和经过验证的行业实践保障 SupportAssist 的安全性。

安全验证测试

定期对 SupportAssist 应用程序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、开放式 Web 应用程序安全项目 (OWASP) 交叉检查以及第三方库。

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。

变更管理

Dell Technologies 变更管理流程遵循公司变更管理委员会规定的 ITIL Foundation 最佳实践。所有变更都通过变更请求工单进行管理。访问该系统以启动变更的人员都需要接受 ITIL 培训，并熟悉 SDL。应用于后端基础架构的所有更新和升级均受版本控制，以便进行适当的跟踪和追溯。团队采用自动构建流程来应用新的构建或撤销已部署的构建或热修复。

在 Dell.com/support 上发布的每个版本都包含有关引入的变更和已知限制的信息。

所有新功能和变更全部由我们的产品管理团队进行梳理，并通过记录计划和变更管理流程确定优先级。

身份验证

SupportAssist 使用 Dell MyAccount 向 Dell Technologies Services 基础架构、应用随机对称密钥、JWT 和操作系统登录组进行身份验证，以实现即开即用的身份验证。

为数据库管理团队和运行支持团队等可访问 SupportAssist 组件的小组分配不同的职责和访问权限。生产环境的所有更新都要经过一个明确定义的变更控制流程的审核，该流程体现了相互制衡原则。

注重安全的社区

戴尔提供基于角色的安全培训课程，让新员工和现有员工了解特定工作的最佳安全实践以及如何使用相关资源。Dell Technologies 致力于在整个社区打造安全意识文化。此外，开发者社区是戴尔 Security Champion 计划的一部分，该计划的目的是在软件开发实践中培养安全左移思维。

事件报告

Dell Technologies 要求所有人通过电子邮件地址 security@dell.com 及时向我们的计算机安全事件响应小组 (CSIRT) 报告各种可疑活动、网络安全问题或威胁。

漏洞响应

Dell Technologies 致力于更大限度地降低与产品、应用程序和云服务中的安全漏洞相关的风险。为了及时实施漏洞响应实践，戴尔遵守 Dell Technologies 漏洞响应标准 (VRT) 中概述的准则。戴尔积极参与各种社区工作，包括事件响应和安全团队论坛 (FIRST) 和卓越代码软件保障论坛 (SAFECode)。戴尔的流程和程序符合 FIRST PSIRT 服务框架以及 ISO/IEC 29147:2018 和 ISO/IEC 30111:2019 等其他标准。

Dell Technologies 力求在商业上合理的时间内修复产品、应用程序和云服务中的漏洞。确切的时间线可能因具体漏洞及其影响而异，例如漏洞修正工作/影响的复杂性。产品安全事件响应团队 (PSIRT) 负责协调报告给我们的所有产品漏洞的响应和披露事宜。所有 Dell Technologies 产品漏洞披露信息均在戴尔安全公告、通知和资源页面在线获取。有关戴尔漏洞响应实践的更多详细信息，请参阅戴尔漏洞响应政策。

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、发展和共享方面与其他优秀供应商协作，进一步加强安全开发事业。行业协作示例包括：

- Dell Technologies 是卓越代码软件保障论坛 (SAFECode) 的联合创始人，目前担任董事会主席。其他董事会成员包括来自 Microsoft、Adobe、SAP、英特尔、西门子、CA 和 Symantec 的代表。SAFECode 成员共享和发布软件保障实践和培训。

定义产品安全最佳实践和加强安全开发事业领域的行业佼佼者。

行业联盟（续）

- Dell Technologies 一直活跃于事件响应和安全团队论坛 (FIRST)。FIRST 是事件和漏洞响应领域的优秀组织，受到广泛认可。
- 戴尔积极参与开放群组可信技术论坛 (OTTF)。OTTF 牵头制定了全球供应链诚信计划和框架。
- 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。

行业安全标准

- 戴尔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）
- 事件响应和安全团队论坛 (FIRST)
- 开放群组 (The Open Group)
- 卓越代码软件保障论坛 (SAFECode)
- 存储网络行业联盟 (SNIA)

Dell Technologies 已通过 ISO 9001 认证。戴尔会对其所有的开发和制造中心进行定期季度审计和合规性审查。

V. 结语

SupportAssist 连接技术提供智能自动化和修正功能，可帮助组织的戴尔台式机和笔记本电脑机群实现更长的正常运行时间。 Dell Technologies Services 专注于安全流程、安全数据传输和安全数据存储，能够为这项尖端技术提供出色的安全性。

有关问题和更多信息，请访问 **Dell.com/SupportAssist**

[1] 有关支持的系统和要求，请参阅我们的用户指南（供个人使用的 SupportAssist for Home PCs 版本）或管理员指南（适用于 PC 机群管理的 SupportAssist for Business PCs 版本），并单击“支持的 PC”。主动式和预测式功能取决于您的有效服务计划和 Dell Technologies 业务规则。有关 ProSupport Suite for PCs 的功能，请查看我们的管理员指南，然后单击“连接和管理功能与戴尔服务计划”。有关适用于 PC 的 Dell Care Suite、Premium Support Suite 或 Alienware Care Suite 的功能，请查看用户指南，然后单击“SupportAssist 功能与戴尔服务计划”。

[2] 基于戴尔在 2023 年 12 月进行的分析。