技术资料

DriveTrust™ 技术：概述

简介

随着数字信息日趋重要，对这类信息的保护意识也越来越强烈。希捷利用 DriveTrust™ 技术开创新的安全存储时代。

虽然可以使用防火墙、防病毒软件和智能卡在网络和本地存储级别管理数据安全，但仍然存在数据被盗或丢失的风险。硬盘中存储着敏感数据，所以是计算流程中的关键组件。

DriveTrust 技术使硬盘本身实现安全功能，提供可信赖存储的基础。

什么是 DriveTrust 技术？

DriveTrust 技术利用硬盘的封闭计算环境，是基于硬件的安全功能的硬盘级平台。虽然操作系统专门设计用来支持各种应用程序，但硬盘是运行专用代码（固件）管理硬盘功能的封闭存储环境。硬盘是实现数据安全功能的理想位置，因为其内部操作与计算系统的其他组件相隔离。

DriveTrust 平台不仅仅能够保护磁盘上存储的数据。该平台还在主机与硬盘之间建立对所发送数据的信任，并使硬盘能够对应用程序进行验证、分配安全存储分区、处理数字签名并提供多种其他安全功能。

DriveTrust 技术为开发人员和 IT 管理员提供了多种工具，使他们能够轻松、高效地保护计算环境。DriveTrust 资源就像一个包含多种基于硬件的安全功能、可保护数字信息的工具箱。

DriveTrust 技术：概述

DriveTrust 技术的元素

DriveTrust 技术包含四个元素，如图 1 所示。

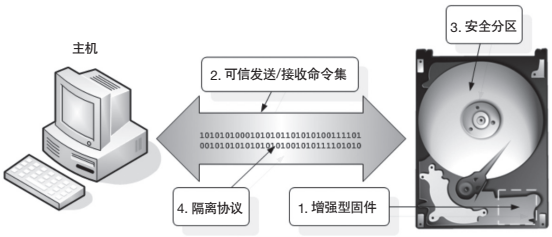

图 1：DriveTrust 框架包括增强型固件和硬件、可信发送/接收命令集、硬盘上的安全分区以及隔离协议。

1. 增强型固件和硬件

固件是在硬盘的内部计算机中运行的软件；通常，固件用于管理极为复杂的硬盘功能，如移动读取/写入磁头、跟踪磁盘上的坏扇区以及存储数据位置的位图。DriveTrust 技术添加优化硬盘存储资源的其他安全代码，扩展了硬盘的功能。DriveTrust 技术相当于在硬盘中实现加密服务提供程序，它提供加密、散列、安全存储、解密、数字签名和随机数字生成功能。

2. 可信发送/接收命令集

可信存储需要安全的通信基础架构。DriveTrust 通信通过可信发送/接收（出/入）命令集发送，该命令集用于协调定义 ATA 和 SCSI 接口的标准组织。ATA 和 SCSI 接口协议中包括安全消息传递的内容，以支持包括 DriveTrust 技术在内的安全技术支持。

3. 安全分区

200GB 的硬盘保留约 200MB 不可寻址空间，用于内部系统内存。DriveTrust 技术使用此空间创建安全分区，该分区在逻辑上和物理上均与硬盘存储的其余部分相独立，使用有效的条件访问控制，是存储加密密钥的最佳位置。

如果硬盘采用 DriveTrust 技术，则只有提供正确凭证的应用程序能够访问上述安全分区，并在其中存储应用程序代码、其他内容或数据。ISV 可利用该功能构建具有其他功能的应用程序，如增强的身份验证、时间戳、对比日志记录或事务数据。

4. 隔离协议

软件应用程序、基本输入/输出系统和其他程序均可通过严格控制的通信渠道与应用 DriveTrust 技术的硬盘互操作。ISV 和其他开发商可以编写应用程序，并通过隔离协议将它们分配给硬盘中的安全分区。如果应用程序尝试访问这些安全分区，则必须向硬盘的管理员功能提供根据管理协议分配的凭证。管理员功能对应用程序进行验证，激活相应的安全分区，从而允许该应用程序通过可信发送/接收命令集与安全分区交互。

DriveTrust 技术的应用

通过在数字数据存储位置提供安全保护，DriveTrust 技术已成为安全 IT 环境的坚实基础。在大多数组织内，都可以应用 DriveTrust 功能来解决数据安全性问题。这些应用包括：

- **全磁盘加密。**强大数据验证和加密功能的组合，可针对被盗或丢失保护数据。该解决方案能够对出入硬盘的所有数据进行加密和解密。DriveTrust 不同于其他数据加密应用程序，它的加密密钥受密码保护，永远也不会使用明文或任何可读格式存储在硬盘上。
- **用于改变硬盘用途或在硬盘生命周期终结进行处理的安全清除功能。**政府机关和大型公司往往支出数百万美元，以确保无法从报废或改变用途的硬盘中恢复敏感数据。只需更改 DriveTrust 硬盘上的加密密钥，就能快速、安全地使存储的所有数据变得不可读且不可用。用户可在几秒钟内完成上述操作，不会像标准磁盘清除方法一样耗时且容易出现人为错误。

DriveTrust 技术：概述

- **保护生物技术验证数据的基于硬件的安全功能。**生物技术验证是一项最先进的技术，用于确认用户身份，但如果生物技术凭证本身面临危险，会出现什么问题？DriveTrust 技术支持软件应用程序将生物技术数据存储在硬盘的隐藏分区，即安全分区中，可保证最高级别的安全性。

- **在存储局域网、网络附加存储和独立磁盘冗余阵列等多硬盘环境中，可对应用 DriveTrust 技术的硬盘进行集中验证和凭证检查。**可信赖计算集团正在制定开放标准，以允许企业在其网络或基于阵列的存储基础架构中实现策略驱动的验证机制，为存储系统中应用 DriveTrust 技术的硬盘提供安全的管理基础架构。DriveTrust 技术提供的基层保护可补充实施的其他安全措施，提高存储架构的安全性。

- **企业可通过硬盘配对和加密管理支持 USB 连接的移动硬盘。**支持 USB 连接的移动硬盘会带来极高 IT 安全风险，因为只需数分钟即可复制和盗取存储的大量信息。IT 部门可使用 DriveTrust 硬盘配对功能，保证各部门的计算机只能使用已批准的移动硬盘。

DriveTrust 技术的目标用户？

DriveTrust 技术为个人和企业提供安全基础，来保护敏感数据并实现其他应用程序功能。独立软件供应商 (ISV) 和计算机制造商可使用希捷提供的 DriveTrust 软件开发套件集成或利用安全功能。

希捷供应两个应用 DriveTrust 技术的产品线：用于数字录像机的 DB35 系列™ 硬盘，以及用于笔记本电脑的第一代应用全磁盘加密功能的 Momentus® 5400 FDE 硬盘。3.5 英寸 DB35 系列硬盘使用 DriveTrust 技术将硬盘与机顶盒设备配对，以保护硬盘中存储的内容。DriveTrust 技术使 DB35 系列硬盘能够使用安全存储在隐藏分区上，并使用密码保护的凭证，从而在启动时应用双重挑战–响应验证过程。

2.5 英寸 Momentus 5400 FDE.2 硬盘可自动对所有数据加密，所以，用户必须提供正确加密密钥才能访问数据。该硬盘使用专用芯片，可高效地加密和解密硬盘上存储的所有数据，而且不会对性能产生任何不良影响。DriveTrust 使用由密码派生的格式，提供强大验证功能并在安全分区中存储加密密钥。

领导硬盘行业应用开放标准

可信赖计算集团是一个非营利行业组织，其宗旨是开发、制定和推广有关硬件支持的可信赖计算和安全技术的开放标准。希捷以及加入可信赖计算集团 (TCG) 的其他行业领导者，其中包括AMD、Hewlett-Packard、IBM、Intel、Microsoft 和 Sun Microsystems 合作开发先进技术，以确保计算环境中各个组件按照预期方式工作。这些可信组件也称为“信任源”，可用于验证其他组件并控制对系统的访问。

希捷向可信赖计算集团提供 DriveTrust 技术，作为制定开放性标准以提高存储设备可靠性和安全性的框架。之后成立了 Storage Work Group，该组织的成员包括所有领先硬盘制造商以及闪存设备、存储管理和存储集成供应商。希捷是 Storage Work Group 的主要领导，目前正在积极推动标准化工作。

Storage Work Group 正在制定核心存储规范，以支持使用可保护数据并与可信赖系统互操作的安全存储解决方案。其主要目标是帮助用户保护数据、密码和加密密钥等信息资产，以免受到攻击或丢失。应用 DriveTrust 技术的硬盘已成为可信赖计算流程中的信任源，用于验证和保护硬盘上存储的数据。

DriveTrust 技术：概述

另外，Storage Work Group 与高级技术配件 (ATA) 和小型计算机系统接口 (SCSI) 标准组织进行合作，在 ATA 和 SCSI 可信发送/接收协议中结合安全有效载荷。核心存储规范中定义了有效载荷命令集，并确保使用 ATA 和 SCSI 接口的所有存储设备，即采用 USB 连接的闪存设备、磁带驱动器和硬盘能够识别可信发送/接收命令。

核心存储规范目前正在准备出版，今后，应用 DriveTrust 技术的产品都将符合此开放规范。

希捷：基于硬盘的安全功能领域领导者

DriveTrust 技术提供将硬盘转变为可信计算源所必需的工具。DriveTrust 技术提供的安全功能完全对用户透明，并且不会增加常用计算资源的负担。

希捷将继续开发基于硬盘的安全功能，并向 ISV 和技术供应商提供该项技术，努力为企业用户和家庭用户提高整体计算环境的安全性。

有关如何使用 DriveTrust 技术以及该技术如何解决符合性问题的更多信息，请参阅 DriveTrust 技术一般概述白皮书和 DriveTrust 技术符合性白皮书。

有关可信赖计算集团的更多信息，包括 TCG 的 Storage Working Group 的其他成果，请访问相关网站：www.trustedcomputinggroup.org。

希捷亚太区市场行销
北京 +86-10-82861316/17/18
上海 +86-21-61416222
深圳 +86-755-25834570
香港 +852-23689918
新加坡 +65-64887498
日本 +81-3-54622901
韩国 +82-2-5627201
台湾 +886-2-25451305
澳大利亚 +61-2-87482700
新西兰 +61-2-87482700