DELL Technologies

Microsoft

白皮书

利用 Windows Server 2022 和新一代 Dell EMC™ PowerEdge™ 服务器的组合功能获得高级安全保护

通过更安全的硬件、固件和操作系统环境来加强对业务关键型工作负载的保护

根据 Cybersecurity Ventures 的统计，2021 年全球网络犯罪造成的总损失预计为 6 万亿美元，到 2025 年将增长到 10.5 万亿美元。[1] 在六年内，仅勒索软件攻击就增长了 61 倍，其造成的损失在 2021 年达到 200 亿美元；目前，每 11 秒就会发生一次勒索软件攻击。[1] IDC 在 2021 年开展的一项调查发现，全球有超过三分之一的受访组织在过去 12 个月内遭受过勒索软件攻击或入侵（而且不止一次）。[2] 虽然 IBM 估计目前一次数据泄露造成的损失约为 424 万美元，[3] 但泄露事件造成的真正损失可能要高得多：在一些实例中，美国医院因遭受勒索软件攻击而不得不将急救患者转到其他医院，并拒绝接收救护车送来的患者。[4]

对组织而言，固件攻击可能是尤为有害的一种威胁。原因在于，以固件为目标的攻击可在操作系统 (OS) 启动之前植入恶意软件，而此时在操作系统上运行的基于软件的安全机制甚至还没有启动。然而，尽管此类攻击在过去五年间增加了五倍，但只有不到一半的组织为其系统采取了抵御固件攻击的强化措施。[5] 归根结底，工作负载的安全性取决于其运行所在的整个堆栈的安全性。

在恶意软件威胁的频率、种类及其造成的损失呈指数级增长的情况下，为了满足安全需求，现代安全机制必须采用多层形式。这是因为恶意软件可能会在硬件和固件层面侵害系统，也可能会在启动过程中侵害系统，而针对这些环境，纯软件定义的安全机制无能为力。为了应对这一漏洞，现代服务器安全机制不能采用仅侧重一个方面的策略。它必须内置于整个基础架构堆栈中。新一代 Dell EMC™ PowerEdge™ 服务器和 Windows Server 2022 的组合能为管理员简化协调硬件、固件和操作系统的重要任务，以充分保护业务关键型工作负载。

Windows Server 2022 安全核心服务器与新一代 PowerEdge 服务器结合使用的优势

安全核心服务器是 Windows Server 2022 中的一项新功能，它利用硬件、固件和操作系统功能来防御当下和未来的威胁。通过在新一代 PowerEdge 服务器硬件上运行 Windows Server 2022 安全核心服务器软件，可以为像贵组织这样的企业提供三大显著优势：

- 高级保护
- 预防性防护
- 简化的安全性

高级保护

根据 Microsoft 威胁情报数据，安全核心 PC 提供的防感染保护能力是普通 PC 的两倍多；Microsoft 如今正通过 Windows Server 2022 安全核心服务器将相同的技术引入服务器领域。[5] 安全核心服务器提供的保护旨在为服务器上的关键工作负载和数据打造安全平台。具体而言，安全核心服务器利用处理器对于动态可信度量根 (DRTM) 技术的支持，将固件置入基于硬件的沙盒中。这种隔离有助于限制数百万行拥有极高权限的固件代码中的漏洞所造成的影响。

基于虚拟化的安全性 (VBS) 与 Windows Server 2022 中的固件隔离相辅相成，将操作系统的关键部分（如内核）与系统其余部分隔离开来。这有助于确保服务器始终致力于运行关键工作负载，此外也有助于保护相关应用程序和数据免遭攻击和泄露。

为了进一步强化 PowerEdge 服务器固件的安全性，使其能够更好地抵御攻击，Dell Technologies 还会帮助保护 PowerEdge 服务器供应链，确保服务器从工厂运输到客户现场的过程中不会被篡改（下文的通过 Dell Technologies 供应链完整性提供额外安全保障中给出了更详细的说明）。

预防性防护

安全核心功能有助于主动防护和中断攻击者可能用来入侵您的系统的多个路径。VBS 中受虚拟机管理程序保护的代码完整性 (HVCI) 功能可将代码完整性 (CI) 决策功能与 Windows 操作系统的其余部分隔离开来，这有助于确保内核内存仅在通过 CI 验证之后才会得到执行。VBS 还支持使用 Windows Defender Credential Guard，后者将用户凭据与密码存储在操作系统无法直接访问的虚拟容器中。

安全核心服务器标配可信平台模块 2.0 (TPM 2.0)，为敏感密钥和数据（例如在启动过程中加载的组件测量值）提供受保护的存储区域。它可验证启动期间运行的固件是否已由预期作者有效签名且未经篡改，这种能力有助于提高安全性。此硬件信任根还提升了 BitLocker 驱动器加密等功能提供的保护力度，该功能使用 TPM 2.0，有助于创建可整合到零信任安全策略中的基于认证的工作流。这些防护措施相互结合，让您的 IT 和 SecOps 团队能够更好地在需要其关注的诸多安全领域中合理分配时间。

新一代 PowerEdge 服务器支持符合行业标准的统一可扩展固件接口 (UEFI) 安全启动。UEFI 安全启动功能会检查在操作系统运行之前加载的 UEFI 驱动程序和其他代码的加密签名，从而确保固件未被恶意软件篡改。此外，PowerEdge 服务器支持 TPM 2.0，可提高固件和操作系统的安全性。

简化的安全性

在您采用安全核心 PowerEdge 服务器后，Dell Technologies 即可为您提供一组符合安全核心承诺的硬件、固件和驱动程序。Microsoft 与 Dell Technologies 密切合作，以简化 PowerEdge 服务器的安全支持功能。

通过 Windows Admin Center 中的新功能，管理员能够轻松配置 Windows Server 2022 安全核心服务器的操作系统安全功能。借助全新 Windows Admin Center 安全功能，管理员只需单击一个按钮就能启用高级安全性。Windows Admin Center 会显示 Windows Server 2022 安全核心服务器所有必要安全功能的状态，还让管理员能够按需在一处开启各种功能。

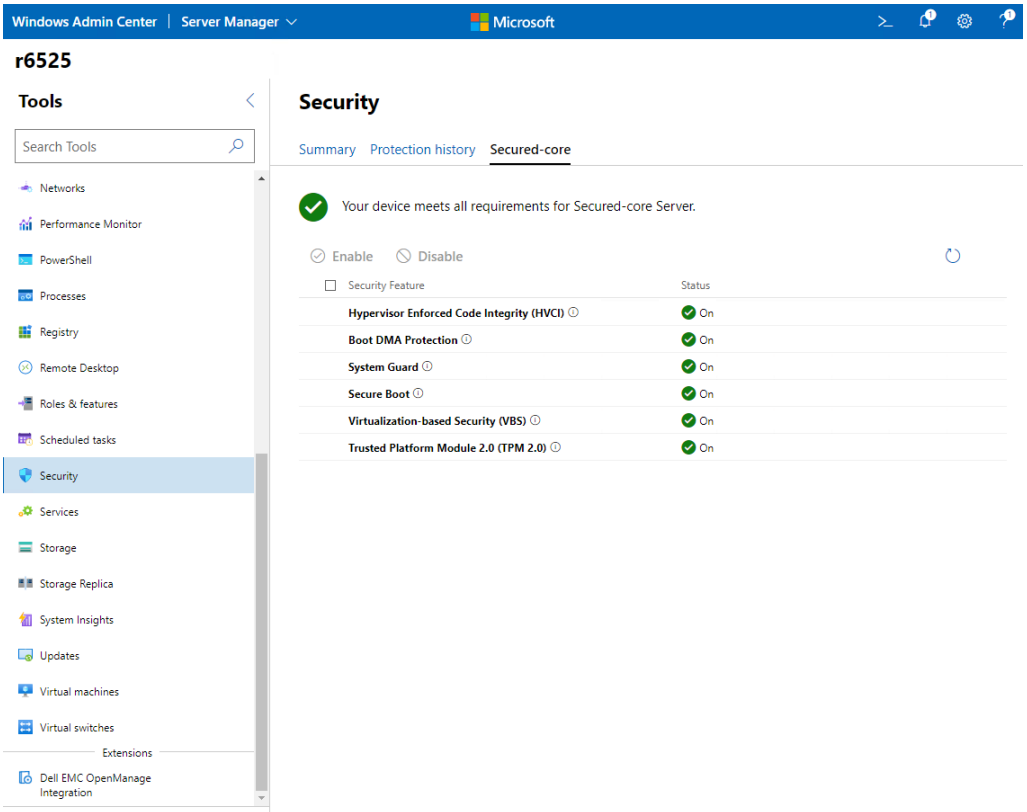


图 1. Windows Admin Center 中的安全核心确认屏幕截图

Dell EMC™ OpenManage™ Integration with Windows Admin Center 是 Windows Admin Center 的扩展程序，可进一步简化安全核心服务器的管理。该 Windows Admin Center 扩展程序可通过远程管理 PowerEdge 服务器，简化 IT 管理员的安全工作（以及其他工作）。在 Windows Server 2022 安全核心服务器环境中，OpenManage Integration with Windows Admin Center 扩展程序使您能够通过 Windows Admin Center 查看 PowerEdge 服务器的资源清册，并提供 PowerEdge 服务器组件的运行状况、硬件和固件资源清册信息的统一视图。

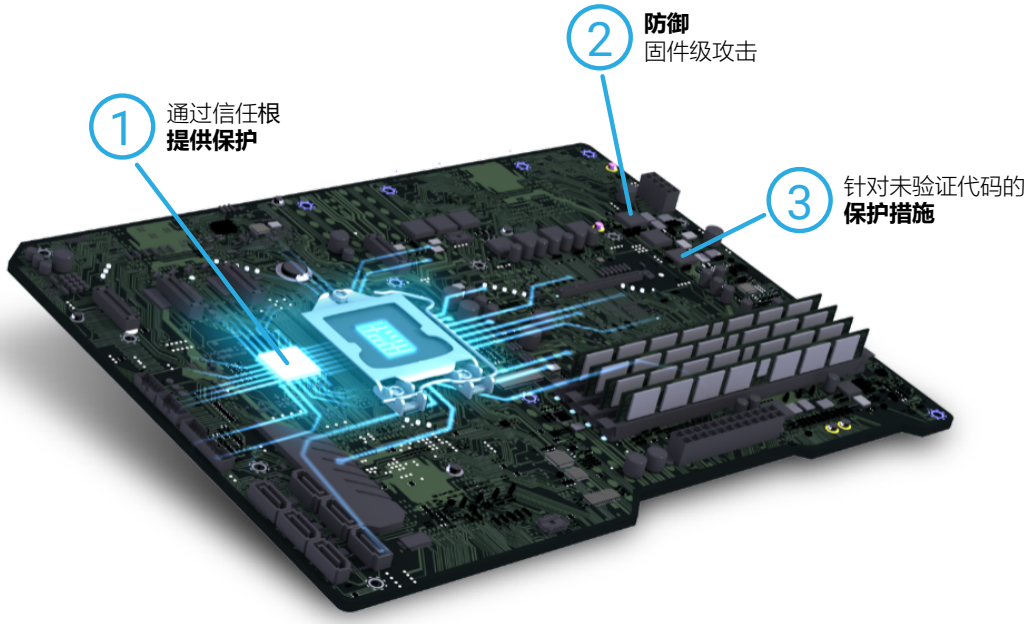
面向 Windows Server 2022 安全核心服务器的 PowerEdge 服务器支持

由于安全核心服务器的防护具有多层性质，因此硬件 OEM 的支持至关重要。PowerEdge 服务器经过 Dell Technologies 的测试和认证，可确保硬件和固件满足 Windows Server 2022 安全功能的要求。此外，PowerEdge 服务器中的硬件和固件均已经过配置，可有效支持 Windows Server 2022 安全核心服务器。表 1 详述了 PowerEdge 服务器中的硬件如何支持 Windows Server 2022 的各项功能。

表 1. Windows Server 2022 安全功能与新一代 Dell EMC™ PowerEdge™ 服务器中的关键支持功能的对应关系

	Windows Server 2022	新一代 Dell EMC™ PowerEdge™ 服务器
高级保护	安全核心系统将固件置于基于硬件的沙盒中，这有助于限制基于固件的漏洞产生的影响。 VBS 将操作系统的关键部分与高级恶意软件隔离开来。	Dell Technologies 助您保护 PowerEdge 服务器的供应链，以确保从工厂运送到客户现场的途中，服务器未遭到入侵或其固件未遭到篡改。
预防性防护	HVCI 和 Windows Defender Credential Guard 等 VBS 功能可全方位防范漏洞，并更好地保护凭据等敏感资产。 TPM 2.0 提供用作安全基础的硬件信任根。	PowerEdge 服务器支持行业标准 UEFI 安全启动，可检查在操作系统运行之前加载的 UEFI 驱动程序和其他代码的加密签名。 PowerEdge 服务器支持 TPM 2.0。
简化的安全性	通过 Windows Admin Center，您可以轻松配置安全核心服务器。	Microsoft 与 Dell Technologies 携手合作，以简化 PowerEdge 服务器的安全支持功能。Windows Admin Center 与 Dell EMC™ OpenManage™ 的集成进一步简化了安全核心服务器的管理。

高级多层安全性剖析



1 通过信任根提供保护

通过 Dell Technologies 等卓越 OEM 制造商以及英特尔和 AMD 等芯片供应商的携手合作，安全核心服务器结合了行业标准硬件信任根，以及内置于当今现代 CPU 中的安全功能。

安全核心服务器使用 TPM 2.0 和采用 DRTM 技术的现代 CPU，实现更安全的服务器启动，并大幅减少固件漏洞。

2 防御固件级攻击

安全核心服务器使用现代 CPU 中基于硬件的安全机制，确保系统在启动后进入可信任状态，从而防止高级恶意软件篡改系统，并抵御固件级攻击。

System Guard Secure Launch 使用 CPU 验证设备，从而提高启动安全性，助您防范高级固件攻击。

3 针对未验证代码的保护措施

在可信计算基础中运行的代码可确保运行完整性，不会发生泄露或遭遇攻击。

在 HVCI 的支持下，安全核心服务器仅启动由已知和经批准的机构签名的可执行文件。虚拟机管理程序设置并强制执行相关权限，以防止恶意软件尝试修改内存并使其可执行。

新一代 PowerEdge 服务器支持 Windows Server 2022 中的安全连接功能

新一代 PowerEdge 服务器支持 Server Message Block (SMB) AES-256 加密，以满足注重安全性的工作负载的要求。通过这种支持，运行 Windows Server 2022 的 PowerEdge 服务器可以为工作负载数据提供端到端加密，从而实现额外的安全防护。Windows Server 2022 中用于 SMB 的 256 位 AES 加密也足够可靠，如果使用强度足够高的密码，甚至可以抵御量子计算机的暴力破解式攻击。

PowerEdge 服务器和 Windows Server 2022 通过 AES-256 加密进一步将端到端 SMB 加密从单个服务器扩展到群集的内部通信，以保护东西向 SMB 数据流量。这些额外的 SMB 加密控制可进一步强化对工作负载的保护，并封堵攻击途径。

最后，Windows Server 2022 充分利用第三代英特尔® 至强® 可扩展处理器中包含的英特尔® Advanced Encryption Standard New Instructions（英特尔® AES-NI），以及 AMD EPYC™ Zen 3 处理器中包含的 256 位矢量化 AES 加密 (vAES256)。这些高级处理器的指令集可提高 PowerEdge 服务器中 AES-256 加密的性能。凭借这些先进的安全技术，Dell Technologies 和 Microsoft 可确保您的业务关键型工作负载兼顾可靠的安全性与迅捷的响应速度。

通过 Dell Technologies 供应链完整性提供额外安全保障

Dell Technologies 供应链完整性可在制造和运输过程中保护硬件和固件组件免受损害。在硬件完整性方面，Dell Technologies 致力于确保在将产品运送给客户之前，产品本身不会遭到篡改，也不会嵌入假冒组件。Dell Technologies 采取的控制措施涵盖了供应商选择、采购、生产流程和治理，直至审核和测试。生产过程中的材料检验有助于识别出标识有误、偏离正常性能参数或包含错误电子标识符的部件。

在软件完整性方面，Dell Technologies 力求确保在将产品运送给客户之前，固件或设备驱动程序中不会插入恶意软件，并会防止出现编码漏洞。Dell Technologies 的全球制造基地均已通过 ISO 9001 认证。严格遵守这些流程和控制措施有助于更大限度地降低假冒组件嵌入 Dell Technologies™ 产品的风险，以及减少恶意软件插入固件或设备驱动程序的风险。此外，Dell Technologies 还将这些举措纳入软件开发生命周期 (SDLC) 的实施流程之中。

Dell Technologies 还致力于确保制造设施和运输链的物理安全。Dell Technologies 要求某些生产 Dell Technologies 产品的工厂满足指定的货运资产保护协会 (TAPA) 设施安全要求，包括在重点区域使用闭路监控摄像头，安装门禁系统，以及在出入口不间断地安排人员值守。作为业界卓越的物流计划的一部分，Dell Technologies 还制定了保护措施，以防止产品在运输过程中遭到盗窃和篡改。最后，通过面向 PowerEdge 服务器的 Dell Technologies Secured Component Verification (SCV)，Dell Technologies 客户能够验证其收到的 PowerEdge 服务器是否与工厂生产的产品相匹配。

通过 Windows Server 2022 和新一代 Dell EMC PowerEdge 服务器打下更好的安全基础，从而保护您的重要工作负载

工作负载的安全性由其运行所在的基础环境决定。未来，恶意软件和数据泄露威胁只会继续增长，恶意攻击者会不断探索能够绕过基于软件的传统安全措施的攻击途径，而这种做法将进一步加剧上述威胁。固件攻击专门在启动过程中针对服务器发起攻击，而在此时，基于软件的安全机制尚未开始保护系统。现代服务器保护措施需要的是涵盖硬件、固件和操作系统的多方面安全机制。

如今，升级到 Windows Server 2022 比以往要更有意义。Windows Server 2022 中的安全核心服务器功能可帮助组织应对固件和操作系统威胁。配合 Dell Technologies 的硬件和软件完整性保护，运行 Windows Server 2022 的新一代 Dell EMC PowerEdge 服务器可以为涵盖硬件、固件和操作系统的整个堆栈提供现代安全性。Windows Server 2022 以及新一代 PowerEdge 服务器支持的安全连接功能将这种安全性从单个服务器扩展到数据中心内的整个群集。此外，对 Windows Server 2012 的支持将于 2023 年 10 月结束，因此，是时候着手制定升级计划了。[6]

要详细了解 Windows Server 2022 和新一代 Dell EMC PowerEdge 服务器如何助您保护关键工作负载和数据，请访问 www.delltechnologies.com/en-us/solutions/microsoft-oem/。

[1] Cybersecurity Ventures，《Cybercrime To Cost The World $10.5 Trillion Annually By 2025》，2020 年 11 月。https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/。
[2] IDC，《IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach》，2021 年 8 月。
[3] IBM，《How much does a data breach cost?》2021 年。www.ibm.com/security/data-breach。
[4] Dan Goodin，《Hospitals hamstrung by ransomware are turning away patients》，*Ars Technica*。2021 年 8 月。https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/。
[5] Microsoft，《New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats》，2021 年 3 月。www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/。
[6] 截至本文撰写之时。有关 Windows Server 2012 支持结束的最新信息，请访问 Windows Server 2012 生命周期页面：https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012。

DELL Technologies

Microsoft

通过 Windows Server 2022 实现现代化。
云就绪型操作系统，通过混合功能提升本地投资的价值。