

保护、检测、恢复

借助 HPE ProLiant DL325 Gen10 和 HPE ProLiant DL385 Gen10 服务器实现安全虚拟化

跻身全球最安全的行业标准服务器产品组合之列¹

19 亿

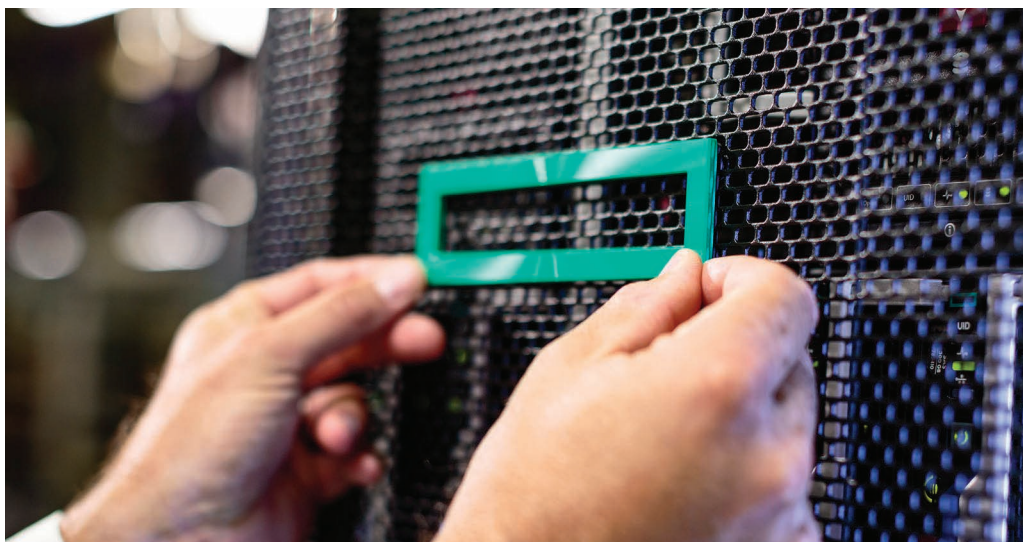
6 个月内的数据泄露记录²

15 倍

勒索软件攻击增加的倍数³

6 万亿美元

到 2021 年，网络犯罪预计会造成
的损失⁴



您的数据是否受到妥善保护？

虚拟化仍是混合环境中有效提高敏捷性和效率的主要手段。2016 年，26% 的工作负载已实现虚拟化，但诸多企业领导者并不想止步于此，而是希望把虚拟化工作负载的比例提高到 80% 以上⁵，首当其冲的便是服务器的虚拟化。⁶ 实际上根据分析师的预测，2020 年，41% 的新服务器都会以虚拟化方式交付，而 2015 年这一比例仅为 33%。⁷ 这就很自然地解释了一个事实：企业借助服务器虚拟化节约了近 20% 的成本。⁸

随着数据中心虚拟化程度的提高，服务器理应成为企业的强力护盾，运用前沿的创新技术，有效预防、检测安全攻击并恢复攻击造成的损坏。正因为如此，我们

开发了独有的安全技术，可为企业提供全新的安全基础，有效保护企业的数据和业务。

HPE ProLiant DL325 Gen10 和 HPE ProLiant DL385 Gen10 服务器专为虚拟化而构建，具有强大的安全功能，可帮助保护企业的硬件、固件和网络，抵御未经授权的访问和未经批准的使用。慧与还提供一系列嵌入式和可选的软件和固件，可供企业按需选择，构建出适用于企业网络和数据中心的远程访问和控制最佳组合。

采用 AMD EPYC™ 处理器的 HPE ProLiant DL325 Gen10 和 HPE ProLiant DL385 Gen10 服务器支持诸多高级安全功能，企业可以运用这些功能为虚拟化创建出安全性出众的服务器解决方案。

¹ 基于外部企业于 2017 年 5 月对多家制造商的多种服务器产品进行的网络安全渗透测试。

² CNBC, "The number of devastating cyberattacks is surging—and it's likely to get much worse" (破坏性网络攻击数量正在激增并积极有可能进一步恶化)，2017 年 9 月。

^{3, 4} Forbes, "Hewlett Packard Enterprise Releases iLO Amplifier Pack With Server System Restore" (慧与发布支持服务器系统还原技术的 iLO Amplifier Pack)，2018 年 2 月。

^{5, 6} IDC, "2016 年虚拟化基础设施与软件的市场趋势：市场调研报告"，2016 年 12 月。

⁷ TechTarget, "2017 年 IT 工作重点"，2017 年 2 月。

⁸ 适用于 HPE iLO Advanced Premium Security Edition 许可证。

FIPS 140-2 一级验证

支持 HPE iLO 5 的 HPE ProLiant DL325 Gen10 和 HPE ProLiant DL385 Gen10 服务器采用智能微处理器、安全存储和专用网络接口，可以在符合 FIPS 140-2 一级要求的模式下运行。

有关慧与安全功能的详细信息，请参见

- [HPE 安全计算生命周期白皮书](#)
- [HPE Gen10 安全参考指南](#)
- [解密服务器信任根 — Moor Insights & Strategy 白皮书](#)

⁹ 慧与内部测试，2017 年 2 月

我们的解决方案合作伙伴



立即分享

获取更新

保护

HPE 硅信任根技术

慧与是唯一一家提供硅信任根的供应商，能够把基本固件锚定到自定义 HPE iLO 5 芯片上。这项技术可创建无法更改的“指纹”，用于验证固件代码是否有效以及是否有损坏，这样服务器就不会使用受损固件启动。

安全启动

安全启动是在 BIOS 中实现的一项行业标准安全功能。安全启动可确保，在启动过程中启动的任何驱动程序和操作系统启动加载程序都有数字签名，而且都会根据 BIOS 中安全存储的一组可信证书进行验证。启用安全启动后，只有经过验证的驱动程序和操作系统启动加载程序才会执行。

AMD 安全处理器

在 AMD EPYC 片上系统上嵌入专用 AMD 安全处理器。此处理器可以管理安全启动，实现固件级别的 HPE 硅信任根连接并在启动过程中验证 HPE BIOS。AMD 安全内存加密 (SME) 支持内联加密和解密，可以安全地生成及管理密钥，对性能的影响微乎其微。AMD 安全加密虚拟化允许使用高性能加密引擎对虚拟机 (VM) 内存内容进行透明加密，此外，该加密引擎可以使用多个密钥进行编程，供系统中不同的 VM 使用。

安全的供应链

慧与仔细审查组件供应商并从贸易协定法案 (TAA) 指定的国 (地区) 采购组件，以此降低威胁供应链安全的风险，如假冒伪劣材料、恶意软件和其他不可靠组件。不仅如此，慧与还通过内部开发 BIOS、管理固件和 iLO 5 芯片，进一步减少安全问题和威胁。安全服务器选件 (如机箱入侵检测套件) 可以进一步降低遭到篡改的风险，即使服务器断电后也能提供强力保护。

检测

运行时固件验证

服务器运行时保护由慧与专属技术提供支持，可以对服务器的重要固件执行日常检查。如果发现关键固件中被插入了损坏代码或恶意软件，则系统会创建 HPE iLO 审核日志警报来通知管理人员固件出现损坏。此功能的实现倚赖 HPE 特有的硅信任根技术。

恢复

自动恢复重要固件

虽然固件漏洞鲜有发生，但如果出现，有了 ProLiant Gen10 服务器增强的内置安全功能为系统提供保护，便能安全且自动地把固件恢复到前一个已知的良好状态。⁹

大规模还原服务器

特有的 **HPE 服务器** 系统还原功能利用 **HPE iLO Amplifier Pack** 软件，单击一次即可安全还原众多服务器，数量多达 10,000 台。如果遭受勒索软件攻击或出现其他漏洞，您可以自动或手动把服务器的重要固件、固件配置设置、操作系统和主机环境恢复到可以运行的状态。

慧与创新

HPE ProLiant DL325 Gen10 和 HPE ProLiant DL385 Gen10 服务器以及 AMD EPYC 处理器融合了慧与在安全防护和性能方面的前沿创新技术。iLO 5 的高级功能支持安全启动、日常固件扫描和自动还原到上次已知的良好配置。

立即了解详情

立即采取行动，让服务器免遭网络犯罪分子的攻击。请与慧与或授权的渠道合作伙伴代表联系，了解更多信息。

有关详细信息，请访问

hpe.com/servers/dl385

hpe.com/servers/dl325