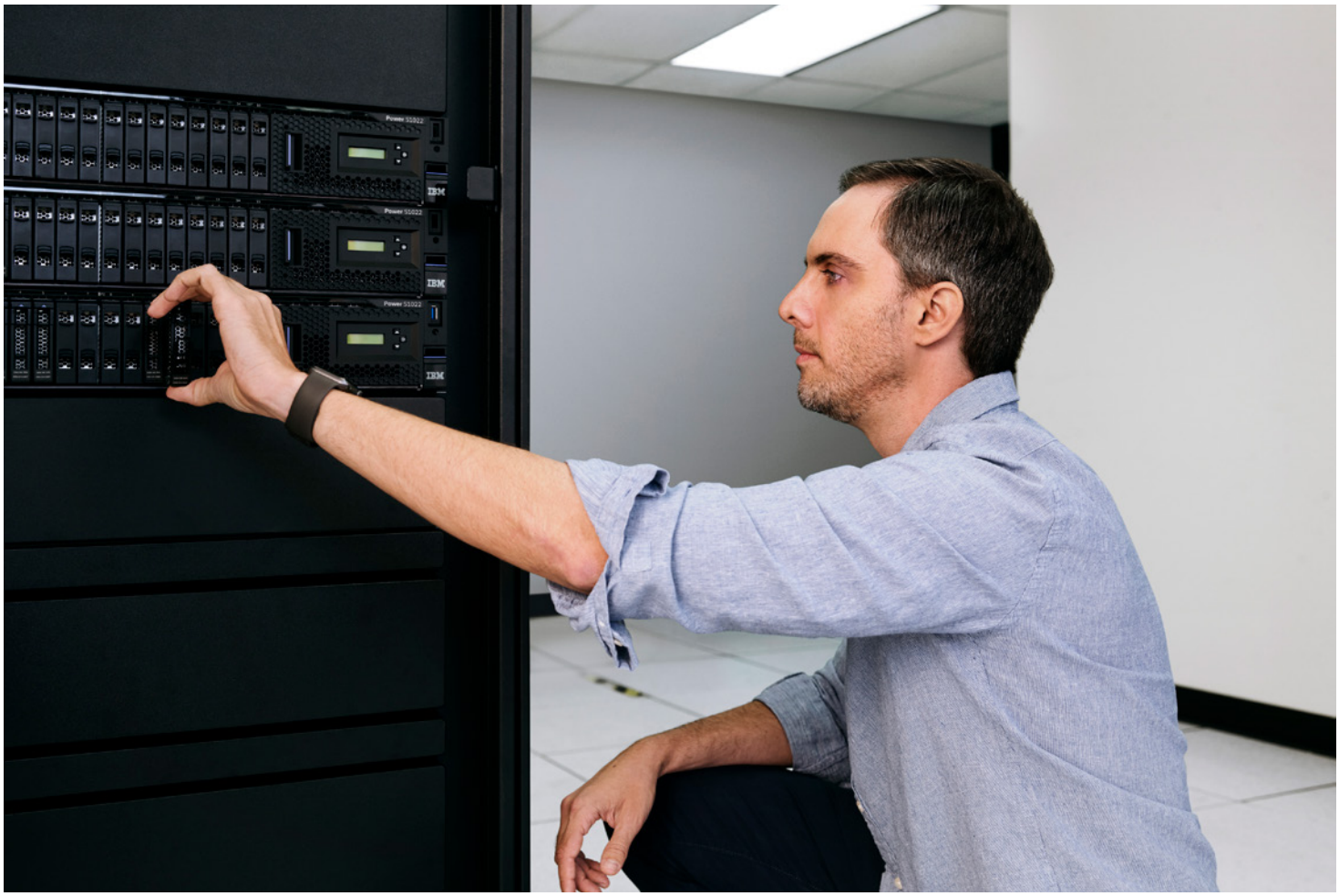
利用 IBM Power 实施多层安全方法

适用于零信任方法的基本基础架构



目录

复杂网络攻击时代下的企业 IT 状态

当今的 IT 格局

自新冠疫情爆发以来，有据可查的破坏性数据泄露事件数量十分惊人。数据泄露的平均成本现在为 424 万美元，比去年报告记录的 386 万美元增加了 10%。这是该行业在过去七年间经历过的最大增幅[1]，这也使得安全保障成为企业和机构必须首先面对的问题。完善安全策略，让企业在这个永不停歇的世界中快速、安全、可靠地发展，是当今许多高管关注的焦点，这也导致安全预算不断增加。然而，支出增加和技术变革也引发了新的复杂问题和风险，让 IT 安全持续面临威胁。专业安全人员最关心的问题之一，就是日益增多的复杂攻击媒介，它们以未曾有过的广度不断暴露出当今企业更多方面的问题。

就在前些年，硬件和固件层面的漏洞可能还并不十分令人担忧；而如今，它们已然成为当今形势下的主要威胁目标。

在许多方面，企业如今须克服的网络安全挑战可依经验归结为两点事实：

- IT 堆栈不断扩大，黑客也在拓宽他们的攻击视野。
- 企业必须赶在未来的威胁迫近之前，以最高级别的安全措施保护其平台，进而保护其混合云基础架构。

424 万美元

数据泄露的平均成本现在为 **424 万美元**，比去年报告的 386 万美元增加了 10%。

当前威胁现状与态势

整体方法

企业依靠其安全系统来防范知识产权、敏感公司信息、客户数据和工作负载隐私等方面在当前和未来可能面临的威胁。

为了防止数据泄露和网络攻击，当务之急是明确专业人员该如何从战略角度处理 IT 安全问题。安全漏洞不仅会导致宕机，而且对任何企业而言，其代价都十分高昂。勒索软件攻击构成最大的威胁，平均而言，每次攻击会给企业造成 462 万美元的损失[1]。IBM® Power® 平台具备出色的完整性，可以通过实施终端检测和响应 (EDR) 以及连续多因子认证 (MFA) 等零信任概念来降低勒索软件带来的风险。

单纯采用业务驱动、合规驱动或经济效益驱动的方法，无法为业务流程提供足够的保护，确保其免受日益增多的 IT 系统风险的影响。孤立片面的方法容易忽视高效集成型安全策略的关键跨学科方面。理想的行动方案应包括规划和评估，以识别与安全相关的关键领域存在的风险。IBM Power 技术和基于 IBM® Power10 处理器的系统为企业的安全策略提供一种全面整体的零信任多层方法，确保企业运营安全且合规。这种多层方法包括：

– 硬件
– 操作系统
– 固件
– IBM® PowerSC 2.0 技术
– 管理程序

采用整体的安全方法有助于企业有效应对影响 安全格局的各种威胁。

黑客越来越精明老练

随着组织不断摆脱传统本地数据中心的配置限制，迁移至混合云或多云环境，网络攻击者则不得不摒弃旧有手段而揣摩新的攻击方式。实施最小权限和加强基于边界的管控措施，会有助于管理数量越来越多的威胁。他们过去所采用的方法不再局限于网络层面，这最终扩大了侵袭的攻击面，增强了攻击能力。

随着数据访问量的增加，安全性变得至关重要

现如今，员工几乎可以在任何地方（跨服务器、混合云环境以及众多移动和边缘设备）存储和访问组织内的数据。服务器和设备间这种密不可分的交叉关系，是数字化转型和现代化持续发展而产生的附带现象。这就很容易创造大量可供利用的攻击媒介。

一再收紧的监管法规政策也会影响风险构成状况

为帮助确保合规而实施的流程也可能会导致增加预期之外的风险隐患。《通用数据保护条例》(GDPR) 只是某种趋势不断发展所催生的产物之一。肩负治理责任的实体开始更加关注组织的数据使用方式。而与此同时，众多组织日常业务运营的复杂程度亦在持续增加。

员工方面随时有出现漏洞的可能

去年，20% 的数据泄露事件源自员工凭证被盗[1]。除了登录信息之外，网络钓鱼诈骗和电子邮件泄露也会让员工在不知不觉中将公司信息置于危险境地。无论企业实施何种安全控制措施，也无论企业处理漏洞的能力如何，员工总会带来一定程度的风险。在网络犯罪猖獗的时代，企业有必要围绕这些常见安全威胁对员工展开培训，并建立相应的上报系统。一个小失误或一次狡猾的恶意攻击，就有可能让企业在保护终端和实现合规方面所做的辛苦工作付诸东流。

与此同时，许多企业都在苦苦寻找并留住称职的网络安全人员，他们发现自己始终处于技能短缺的困境。为了应对这种技能短缺，企业可以实施简化的安全管理措施，实施运营、合规、补丁安装和监控自动化。从端到端安全性中获益，通过额外的终端检测功能，在无需增加资源的情况下加强保护措施。

随着 IT 架构不断演进并适应日渐变化的技术、工作文化及合规潮流，当今网络威胁环境的体量、多样性和发展速度呈现出翻倍式增长。这意味着您的安全策略也必须同步演进并超越网络层面。

零信任安全策略至关重要

整体方法

实施零信任概念有助于组织在通常很复杂的 IT 环境中解决安全问题。各种混合云和多云环境中，IT 专业人员始终在竭力维系可见性和管控力度。零信任有效管理风险的优势在于：改用更全面的策略来约束访问控制，同时不影响性能或用户体验。通过实施各种第三方供应商安全解决方案，可以在堆栈的各个级别上构建安全性。但是，这种方法会加剧业已存在的复杂局面，并将更多漏洞和风险隐患引入企业网络中。最佳措施是采取多层次、零信任的方法。这既可以保护企业的所有数据和系统，也可以最大限度地降低复杂性。因此，IBM® Information Security Framework 有助于在使用整体的业务驱动型安全方法时，确保可采取正确的方式解决各个方面的 IT 安全问题。

IBM Information Security Framework 侧重于：

1. 基础架构——密切分析各类用户、内容和应用，获取洞察成果，防范复杂缜密的攻击。
2. 高级安全与威胁研究——深入了解漏洞和攻击方法，并通过安全防护技术应用相关洞察分析的成果。
3. 人员——采用全面的身份智能系统，管理并扩展企业身份识别，涵盖各种安全领域。
4. 数据——保护企业最受信任资产的隐私和完整性。
5. 应用——降低开发安全度更高的应用程序所需的成本。
6. 安全情报和分析——通过更多的背景环境信息、自动化和集成技术等，全面优化安全功能。
7. 零信任理念——将正确的用户连接至正确的数据并始终予以保护，同时也为企业做好安全防护。

了解有关 IBM Security Framework (PDF, 25.2 MB) 的更多信息，以及如何进一步深入探究。

IBM Power 技术如何保护堆栈

探索 IBM Power

借助 IBM Power 技术，企业可通过在整个堆栈中集成的全面端到端安全性来提高网络弹性并管理风险——从处理器和固件到操作系统和系统管理程序，还有应用和网络资源，然后直至安全系统管理等。

硬件、固件和管理程序

单芯片加速器
IBM Power10 处理器芯片旨在增强侧信道缓解性能，并配备有改进版 CPU 隔离功能，可与服务处理器分开运行。这款 7 纳米处理器的设计可增加计算能力多达 3 倍，从而大幅提高性能[2]。

端到端加密
IBM Power 解决方案的透明内存加密技术旨在实现端到端安全性，满足当今企业面临的严苛安全标准。另外，IBM Power 还可支持加密加速、量子安全加密和全同态加密技术，为防范未来威胁做好准备。与 IBM Power E980 技术相比，在每个内核可达到的“高级加密标准”(AES) 之加密性能上，最新 IBM Power 系统模型的加速加密技术要快出 2.5 倍[3]。无需额外的管理设置，组织就可以从透明的内存加密机制中获益。

EDR 软件
我们必须加强保护客户数据和数字资产，因为不断增长的外部威胁使得终端安全变得愈发重要。通过检测终端存在的任何潜在威胁，企业可以快速采取行动并解决问题，而无需中断业务连续性。集成方法可避免问题复杂化，并保护企业免遭最危险的攻击。

2.5 倍

与 IBM Power E980 技术相比，在每个内核的“高级加密标准”(AES) 之加密性能上，最新 IBM Power 系统模型的加速加密技术要快出 **2.5** 倍[3]。

通过保护所有 API 接口、终端、数据和混合云资源，支持多因子认证和最小权限等原则，可为企业增添了更多的保护层次。

零信任原则
经过不断探索发展，企业开始采用零信任原则来协力管控这些日益增长的威胁。通过保护所有 API 接口、终端、数据和混合云资源来支持多因子认证和最小权限等原则，可为企业带来更多的保护层次。

IBM 零信任框架可顺利实现这一概念。

- **收集洞察成果**——了解用户、数据和资源，制定必要的安全策略来确保执行全面保护机制。
- **保护**——采取快速、一致的方式，验证背景上下文信息并执行策略，做好组织的保护防范。
- **检测和响应**——解决安全违规问题，将业务运营所受影响降至最低。
- **分析和改进**——通过调整策略和实践并做出更明智的决策，不断改善安全状况。

通过实施零信任原则，企业可以安全地开展创新并扩展业务。

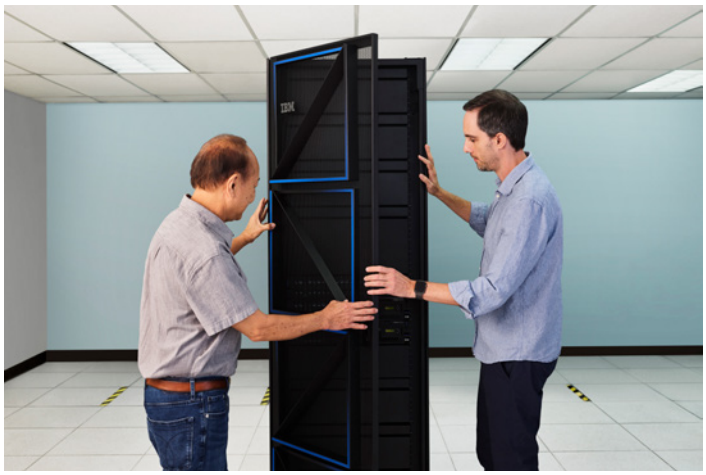
基于 IBM Power10 解决方案的安全启动
安全启动旨在通过数字签名来核查和验证所有固件组件，以起到保护系统完整性的作用。在启动过程中，会以数字方式对 IBM 发布的所有固件进行签名和验证。所有 IBM Power 系统都随附一个可信平台模块，该模块可将服务器上加载的所有固件组件的测量值累积起来，以便对其进行检查和远程验证。

IBM PowerVM 企业管理程序
与主要竞争对手相比，IBM PowerVM® 企业管理程序在安全方面成就卓越，有目共睹，因此，企业可以放心地保护自有虚拟机 (VM) 和云环境。

操作系统

IBM Power 系统为各种操作系统提供领先的安全功能，如 IBM® AIX®、IBM i 和 Linux®。适用于 IBM Power 的 EDR 技术可为 VM 工作负载提供更多的安全性，进而确保为网络中每个终端提供全面的安全保护。对于依赖密码来确保安全的系统，AIX 和 Linux 操作系统使用 IBM PowerSC 多因子认证 (MFA) 技术，这需要对所有用户进行额外级别的认证，防止密码破解类恶意软件带来的攻击。这些功能项因操作系统而异，其部分功能示例如下：

- 在不影响安全性的情况下，分配通常为超级管理员用户保留的管理功能
- 通过单独的密钥库加密文件级别的数据
- 加强对用户可用命令和功能的控制，以及对其可访问对象的控制
- 使用系统值以及用户和对象的对象审计值，在安全审计日志中记录对象的访问情况
- 在整个驱动器上实施加密，先加密一个对象，然后以加密形式写出呈现
- 在为发出请求的用户打开文件之前，先对每个文件进行评估和验证



工作负载、虚拟机和容器

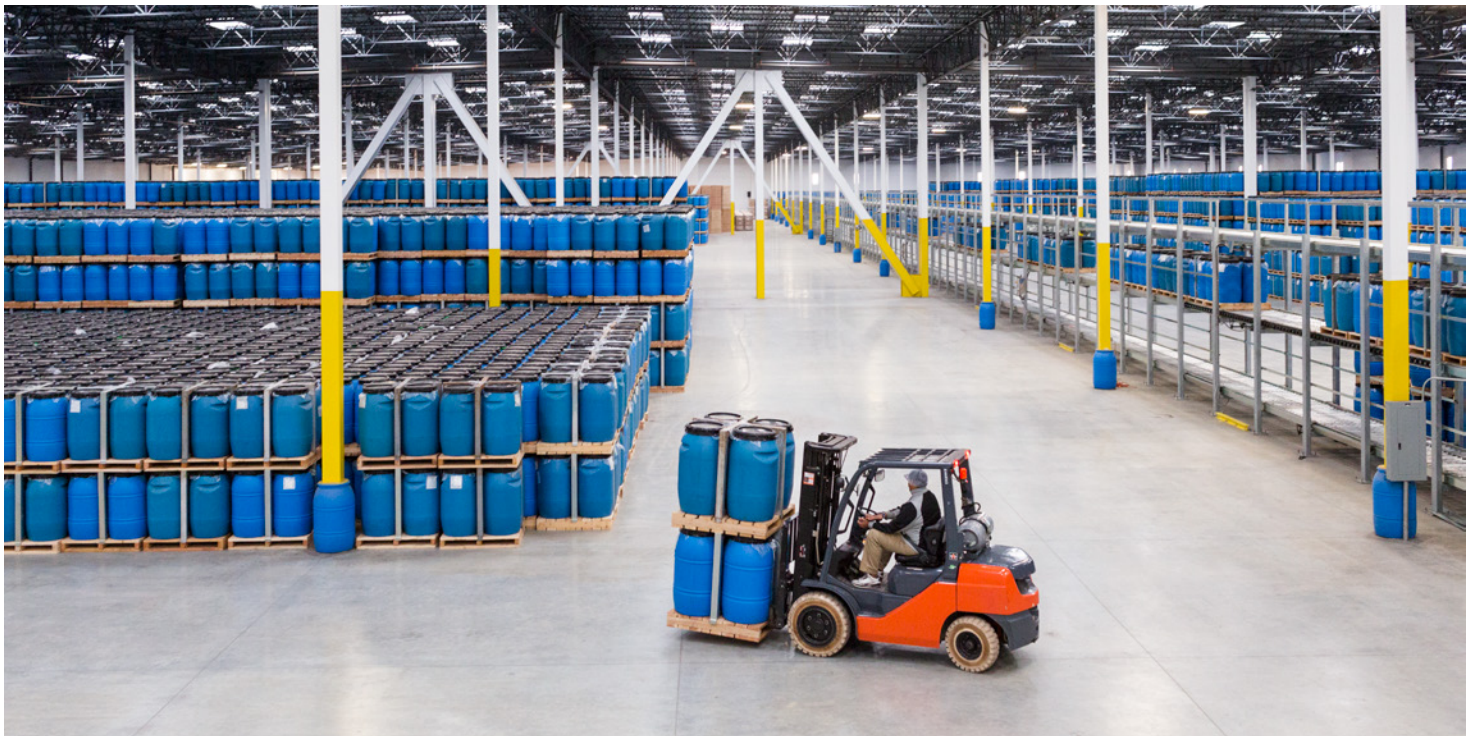
工作负载不再局限于本地数据中心，它们不断迁移至虚拟化混合云和各类多云环境。例如，许多企业正在采用容器跨混合基础架构部署现有应用以及新应用。

这些动态化程度越来越高的环境和工作负载需要同样用途广泛、适应性强的各种安全功能。IBM Power 解决方案可通过以下方式保护工作负载隐私，从而满足各类安全需求：加密算法加速、以及适用于后量子密码和全同态加密 (FHE) 算法的安全密钥存储和 CPU 支持等。

为了满足容器化部署的独特安全要求，IBM 还与 Aqua Security 等独立软件供应商 (ISV) 合作，后者采用了 IBM Power 技术和 Red Hat® OpenShift® Container Platform 等方案，可在容器的整个生命周期内进一步保护容器安全。

IBM Power 服务器旨在通过端到端的内存加密和加速加密性能，保护从本地到云端的各种数据。为云原生工作负载而嵌入的各种策略（包括虚拟机、容器和无服务器功能等）都是为 Red Hat OpenShift 和 IBM Power 客户提供支持而构建，同时还会将企业安全和合规要求相集成，确保应用现代化顺利实施。

动态分区迁移 (LPM)
IBM Power 技术可用于保护动态数据。当您需要从一个系统迁移至另一个系统时，LPM 可通过加密来保护虚拟机。如果您已对本地数据中心或混合云环境或同时对这两者完成了虚拟化部署，那么此功能至关重要。



基于 IBM Power 解决方案的集成安全产品

IBM PowerSC 2.0 技术

IBM® PowerSC 2.0 技术是一种集成型产品组合，可在云和虚拟环境中实现企业安全及合规要求。它位于企业堆栈顶端，同时提供基于 Web 的 UI 界面，用于管理 IBM Power 技术的安全功能，涵盖了从最低级别以上的解决方案中所留驻的各项功能。

凭借其简单易用和自动化功能，IBM PowerSC 2.0 技术可以通过简化合规监控和执行来减少时间、成本和风险。该解决方案可为审计流程提供支持，确保客户能够以更高的效率获取合规认证。它还可通过提高整个堆栈的可视化效果来降低安全风险。

IBM PowerSC 2.0 的标准版本功能

多因子认证 (MFA) 技术
MFA 技术现已集成至 IBM PowerSC 2.0 解决方案中。这简化了 MFA 机制的部署过程，且遵循“从不信任，始终验证”的零信任原则。这种方法支持替代因素，确保用户能够使用基于 RSA SecurID 的认证和证书认证选项登录，包括通用访问卡 (CAC) 和个人身份验证 (PIV) 卡。IBM PowerSC MFA 要求用户提供额外的认证因素来提高系统的保障级别。

IBM PowerSC 2.0 技术可以减少时间、成本和风险

EDR 功能
IBM PowerSC 2.0 解决方案在 IBM Power 工作负载上引入了适用于 Linux 的 EDR，为管理终端安全提供了最新的行业标准功能，包括入侵检测和预防、日志检查和分析、异常检测和事件响应功能等。

合规自动化
IBM Power 系列随附了预先构建的概要文件，可为各种各样的行业标准提供支持。企业可以自定义这些配置文件，并将它们与企业规则融合在一起，而无需接触可扩展标记语言 (XML)。

实时合规性
当有人打开关键安全文件或出现与之相关的交互活动时，进行检测并发出警示。

可信网络连接
当虚拟机未达到规定的补丁级别时发出警示。它还会在修订可用时发出通知。

可信启动
支持检查和远程验证在 AIX 逻辑分区上运行的所有软件项的完整性。

可信防火墙
保护 AIX、IBM i 和 Linux 操作系统之间的内部网络流量，并对其进行路线规划。

可信日志记录
创建集中审计日志，以方便备份、归档和管理。

预先配置的报告和交互式时间线
IBM PowerSC Standard Edition 支持使用五个预先配置的报告进行审计。此外，通过交互式时间线还可以查看虚拟机的使用期限和事件。

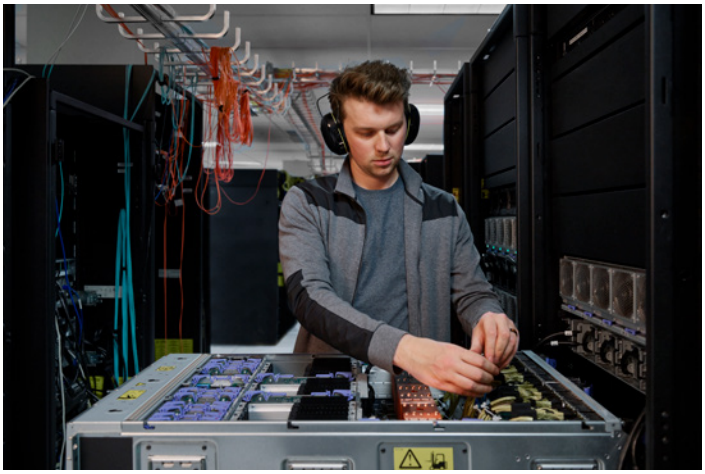
了解如何通过云端和虚拟化环境中的 IBM PowerSC 简化 IT 安全性和合规性的管理工作

最强大的安全方法
就是一种无缝集成的方法

无缝集成

随着网络犯罪分子不断改进其方法，技术演变使得当今企业需要应对更多的新漏洞，当务之急就是要采用一种不会增加组织复杂度的多层次、零信任型安全解决方案。IBM Power 解决方案通过单一供应商紧密集成的深度解决方案，可以保护从边缘到云端直至核心的每一层堆栈。与多家供应商合作会带来各种复杂问题，最终也可能会以多种方式证明其高昂的成本。IBM Power 技术支持处理器级别的端到端加密，且完全不会影响性能。通过集成基础架构，确保堆栈的每一层都纳入管理焦点。

由单一供应商提供安全措施拥有天然的优势，可以简化并加强企业的安全策略。立足于三十年来在安全领域的领导地位，IBM Power 技术与 IBM 内外的各大组织建立了分布广泛的合作伙伴关系，进一步深化和拓宽了其安全专业知识。凭借这些合作伙伴关系，IBM Power 技术可以融入更大的安全专业人员社区，确保可以快速识别问题并从容解决这些问题。在 IBM Security® 和 IBM Research® 各业务部门的支持下，同时还获得了 PowerSC 2.0 产品组合的加持，Power10 服务器能够有力挫败包括内部攻击在内的多种威胁形式，涵括从上到下的所有领域。



安排咨询会议，探索 IBM Power 解决方案的潜力

联系我们 →

注释
1.《2021 年数据泄露成本报告》，IBM Security，2021 年 7 月 (PDF, 3.6 MB)
2. 3 倍的性能是经过对两种服务器产品上的 Integer、Enterprise 和 Floating Point 环境进行投产前工程分析后得出的结论，这两种服务器分别是：配备 2×30 核模块的 POWER10 双插槽服务器，以及配备 2×12 核模块的 POWER9 双插槽服务器产品；两个模块具备相同的能量水平。2 10-20 倍的 AI 推理改进是经过对两种服务器产品上的各种工作负载（Linpack. Resnet-50 FP32、Resnet-50 BFloat16 及 Resnet-50 INT8）进行投产前工程分析后得出的结论，这两种服务器分别是：配备 2×30 核模块的 POWER10 双插槽服务器，以及配备 2×12 核模块的 POWER9 双插槽服务器产品。
3. 根据在 RHEL Linux 8.4 和 OpenSSL 1.1.1g 库上获得的初步测量结果，比较 IBM Power10 E1080（15 核模块）与 IBM POWER9 E980（12 核模块）时，在 GCM 和 XTS 两种模式下，AES-256 每个内核的运行速度大约快 2.5 倍。

国际商业机器（中国）有限公司
了解更多信息，欢迎访问我们的
中文官网：**https://www.ibm.com/cn-zh**

美国出品
2022 年 6 月