SURVIVAL

Guide to Security

IBM **Security**

IBM **Security**

面对威胁，你该采取的关键五招

数据泄露所带来的企业成本逐年偏高，每年数据被外泄的消费者数量也越来越多，平均每次数据泄露事件会为企业造成 392 万美金的成本损失；而每笔数据泄露的成本约为 150 美金，企业平均从找出数据泄露的根本原因到将外泄问题获得妥善控制需要花上 279 天！恶意攻击已经成为数据泄露事件的最重要原因，有 51% 的数据泄露都源自于攻击行动，系统故障占了 25%，人为疏失占 24%。

2019 年由于数据泄漏导致的客户流动率为 3.9%
2019 年因数据泄漏而流失的客户比例不到 1% 的组织，其数据泄漏平均总成本为 280 万美元；而客户流动率为 4% 或以上的组织，其数据泄漏平均总成本为 570 万美元，比平均总成本高出 45%
2019 年新发现 Android 木马，不但大量窃取用户个人信息，还会暗中订阅付费服务、制造假点击破坏广告利润分成

2020 年，你也正身处于危险之中.....

- 凭证保护不断被盗取：2019 年违反了 85 亿条记录，使攻击者可以获取更多被盗凭证
- 修补不完的数据安全漏洞：修补漏洞迄今为止，已发现 150,000 个漏洞
- 勒索软件不断更新：勒索软件攻击在 2019 年第四季度年成长率达 67%
- 威胁者投向攻击：媒介营运技术包含物联网，OT 和相连的工业和医疗系统攻击年成长率激增 2,000%
- 利用时下焦点话题钓鱼：黑客利用大众对于新冠肺炎的恐惧心理，制造各式伪装成官方感染数据或卫教信息的恶意文件，发动网络钓鱼攻击

Key Point 1

IBM QRadar

Security Intelligence Platform

以 SIEM 为核心，提供日志管理、网络流量活动监控等功能，内置 IBM X-Force 全球安全威胁情报，也可轻松结合各大 ISAC 情报，并以 AI 为基础提供用户行为分析，让数据安全人员能快速获取必要的可视性，进而协助保护企业自身网络安全与 IT 资产，满足当前数据安全挑战与法规遵循要求。

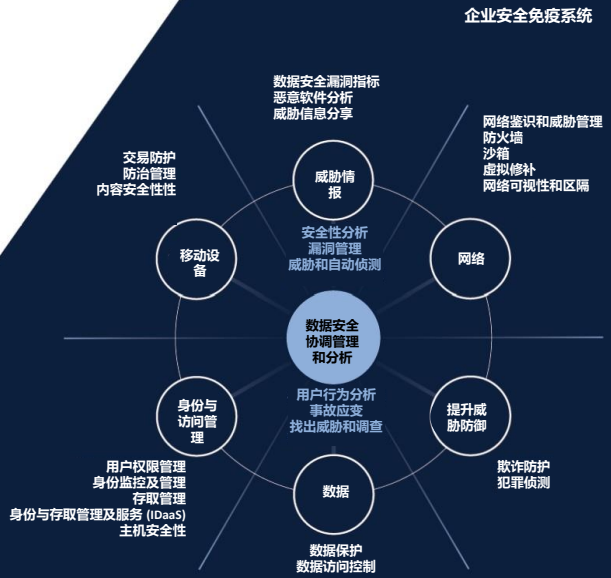
连续十一年荣获 Gartner Magic Quadrant for SIEM 魔力象限领导者殊荣

企业组织每天平均发现 200,000 起数据安全事件，
而网络犯罪被发现之前，平均潜伏期达 191 天，
在这过程中你该做些什么?

“治”不如“防”，在受到攻击后
守住关键数据、流程与客户体验，毫发无伤全身而退
立即打造最新一代信息安全平台“企业安全免疫系统”

IBM QRadar 独特之处

- AI 感知并侦测诈骗、内鬼和高级威胁
- 立即将事件正规化并产生相互关联
- 感知、追踪并链接重大事件和威胁
- 强制执行数据隐私策略
- 从 IBM X-Force 提供专业实时威胁情报
- 搭配 Data Store 授权提供日志无限量储存
- 能在本地或云端环境中部署 QRadar SIEM



持续大量收集

解读安全数据
将 Log 记录文件与网络流量数据标准化与一致化，以供更精准深入的分析。

异常行为监测
归纳资产、用户、服务与网络活动的行为基准，建立常态模型，用以精准监测异常行为。

侦测与分析

人工智能运用
运用 AI 来协助安全分析师调查外在威胁事件。

行为模式分析
实时分析数据安全事件特征，比对已知恶意威胁模式，快速识别与分类数据安全威胁。

历史数据分析
当攻击者采取异常步骤来侵入系统，系统可实时侦测到这些非预期行为并立即预警。

用户行为分析 (UBA)
持续分析个别用户行为，侦测偏差行为，为每个企业内部用户产生各自详细的风险评分，并实时找出被入侵的用户或有恶意的内鬼。

预测分析
运用行为预测模型，提前预测并侦测未来可能发生的异常行为。

用户分组监测
依据相同的使用行为将用户分组，持续监测每个分组中的异常行为，可更快速、更精准地识别识别风险与找到恶意用户。

设备行为侦测
持续监控实体设备，掌握非常规行为、服务与连线，当系统被入侵时可更快察觉并介入。

统计分析
通过统计数据察觉潜伏的威胁，例如有终端设备异常送出大量数据给未授权的云端服务等。

掌握最新数据安全情报
交叉比对事件特征与数据安全威胁情报，例如恶意网域与哈希值 (Hashes) 。当遭受到最新型态攻击时可快速察觉与应变。

实时预警

整合分析结果、串联相关信息，建立从端到端的数据安全事件关联链，判断其严重性，并实时、自动发布警报。

事件调查

运用自然语言处理技术自动建立知识图表，推理事件根源，提供攻击的概观，并且分辨相关的入侵指标。

使用 MITRE ATT&CK 加快回应及可视化各个攻击阶段。

有最大风险的调查优先级清单。

IBM QRadar 智慧安全分析平台 5 大助力

家贼难防，交给 IBM QRadar UBA!

相信每一位数据安全专家都会同意：“人，是数据安全防御最不可控的环节”。 IBM QRadar 用户行为分析 (UBA) 能够实时分析内部人员的使用行为与活动模式，及早发现可疑的异常行为，并判断其风险。QRadar 具备智慧分析能力，协助数据安全管理者将庞大用户数据去芜存菁，发掘异常行为、横向移动、恶意威胁与数据窃取等潜在风险，实时预警与数据安全仪表板。管理者可快速锁定用户进行调查，提早应对防范未然。

IBM QRadar Incident Forensics 数据安全事件鉴定只要短短几分钟

系统遭到攻击，当务之急就是还原过程、鉴定原因、修补问题。鉴识所需时间越长，暴露风险就越大。多数企业需要费时数天才能完成鉴识，早已无法应对瞬息万变的数据安全赛局！IBM QRadar Incident Forensics 可帮助您追踪潜在攻击者的逐步动作，快速进行恶意数据安全事件的深度鉴定调查，鉴识时间由数天缩短为数分钟，并协助您重新修补安全漏洞，避免再次遭受攻击。

让 IBM QRadar Network Insights 大幅减轻看不完的日志恐惧

每天收到爆满的数据安全日志（Log），明知道恶意风险的踪迹就藏在其中，却无法解读！IBM QRarar Network Insights 正如其名：这是个网络威胁的侦测雷达，能够实时分析网络流量与日志数据，将隐藏的威胁摊在阳光下！IBM QRarar Network Insights 可快速执行深度鉴定，将数据安全事件调查时间从数天缩短为数分钟，大幅减少团队调查威胁所需的时间与心力。并协助修补网络安全漏洞，预防灾难再次发生。

IBM QRadar Vulnerability Manager 帮您秒补数据安全漏洞

IT 环境越复杂，来自软硬件的漏洞及其暴露的数据安全弱点就越令人防不胜防。IBM QRadar Vulnerability Manager 可以扫描完整网络环境，自动侦测超过 7 万个已知风险，并结合外部信息随时更新，制定优先应对方案，抢在攻击发生前就阻绝外患。

IBM QRadar Advisor with Watson 用 AI 战胜 AI

人工智能 (AI) 被网络犯罪份子用于攻击行动的案例，在国际上已时有所闻。AI 不仅让网络攻击加速、自动化，更可模仿自然行为，达到更广泛的社交工程与网络钓鱼目的。听起来很可怕？好消息是，您也能用 AI 来战胜 AI！IBM QRadar Advisor with Watson 是 AI 界的数据安全专家，遍读全球无数数据安全报告、新闻、研究，并建立完整“知识图谱” (Knowledge Graph)，能快速分析非结构化数据，并建立安全攻击的关联性，辅助数据安全人员全天候 7×24 预测攻击、实时回应！

IBM QRadar
Security Intelligence Platform

精选案例

Wimbledon 温布尔登网球锦标赛

温布尔登与 IBM Security 合作来保护其数字化活动防止在此著名体育赛事期间遭到数以万计的网络攻击

业务挑战

温网数字体验吸引了一批全新的“数字原生”观众，有助于提升温网品牌价值；然而也面临网络攻击所带来的风险。他们需要找到可信赖的数据安全解决方案，迅速有效地在赛事期间找出并应对近期两亿事件中隐藏的实时威胁。

导入成果

速度提升 60 倍 > Watson AI 与手动分析的安全性威胁侦测结果比较

数量增加 5 倍 > 赛事期间能分析的数据安全事件量

零事故 > 赛事没有发生任何影响官网与其商誉的数据泄露

客户推荐

Alexandra Willis 表示: “虽然我们花了一年时间筹备温网，但我们必须在两周期间呈现完美赛事，尤其是我们要面对数以千万计球迷。” “如果两周赛事期间发生数据安全事故将会重击温网的商誉。温网是英国人民引以为傲的赛事，若不肖份子趁机作乱则不只是影响一场网球赛事而已。”我们必须“固若金汤”。IBM 首席工程师与欧洲区首席技术官 Martin Borrett 表示：“赛事期间我们侦测到近 2 亿起数据安全事件。温网信赖 IBM Security 与我们的云端服务能侦测并阻挡实时威胁。”温网官网受到数个安全性产品的保护，其核心产品系采用 IBM QRadar SIEM 安全情报平台，其能汇集不同基础架构中数千个端点与设备的数据，并分析其关联性以协助安全性团队判断事件的轻重缓急并找出所面对的威胁。


IBM QRadar
Security Intelligence Platform

IBM QRadar
企业安全免疫力检测

立即注册申请

或拨打 400-810-1818 转 2395
立即联络 IBM 业务代表咨询

Key Point 2

IBM X-Force Exchange

实时识别全球恶意威胁情报的云端共享平台，直接与防火墙、入侵防御系统及 SIEM 进行集成，提供潜在风险最佳行动指示，永远领先新兴威胁攻击一步。

IBM X-Force Exchange

全球观测、预警识别、快速扼制让防护一步到位

实时存取丰富的威胁情报数据

IBM X-Force Exchange 提供的开放式平台能增加入侵指标 (IOC) 的环境定义，并结合智能产生的洞察分析。提供实时威胁情报，并且每分钟动态更新一次。软件监控超过 250 亿个网页是否有 Web 威胁，并有超过 96，000 个漏洞分析数据库作为支持。其中提供数百万垃圾邮件和网络钓鱼攻击的深度情报，并监控含有恶意 IP 地址的声誉数据。

共享威胁情报的协作平台

您可以与同行交流，确认研究发现，共享入侵指标的收集内容，帮助彼此做好鉴定调查，或通过私人团队和共享群组，与同侪协作加速威胁环境的分析。

集成式解决方案有助于快速扼止威胁

此解决方案专为第三方集成而设计，拥有 Structured Threat Information Expression (STIX) 和 Trusted Automated Exchange of Indicator Information (TAXII) 的支持，这些都是自动威胁情报分享的既有标准。这能让 IBM Security 产品与 X-Force Exchange 来源的行动情报相集成。应用程序设计界面 (API) 可让您将威胁情报链接到自身的安全产品工具。

简单直觉化的界面，群组共享讨论

一旦产生报告，用户便能增加注解，为其他用户提供额外的洞察和环境定义，或将报告加到群组中。用户也可以提供意见给 X-Force 团队，让他们执行特定报告的分析，进而能更新内容。设定自定义通知和观察名单，让用户收到感兴趣领域的相关建议。

通过观察名单来监控适用指标

只要维护一份待监控的关键字或产品名单，就能研究入侵指标、执行安全调查，然后观察基础架构中目标技术上的漏洞。如果漏洞符合观察名单上的关键字或产品，您就会自动收到通知。若要对这些漏洞采取行动，您可以将漏洞加到群组中，并通过 API 或使用 STIX/TAXII 通讯协定汇入至 SIEM。

将第三方威胁情报授权加到平台

X-Force Exchange 中的 Threat Feed Manager 能从多个来源取出数据，并汇总成一个视图，过程轻松简单。您可以为供应商提供认证，直接在平台上启用第三方威胁情报来源，这样平台就会直接将数据集成至 X-Force Exchange。

从 IBM X-Force 取得最新的行动威胁情报

IBM X-Force 研究团队会通过公开的群组，针对恶意软件活动和新威胁持续增加新的情报。这些群组由 X-Force 安全专家统筹，会在平台上将人工环境定义加到入侵指标中。详细数据包含 TLP 评分、时间范围、目标地区、活动详情，以及深入了解相关参考的链接。当有新信息可用时，用户可以按照集合通知更新。

如何使用 X-Force Exchange，减轻您的数据安全防线负担?

通过了解攻击者的意图，例如无差别攻击或是目标式攻击，分析各项指标
得到具体场景脉络的高阶威胁情报，并立刻建议应对行动，协助企业管理者做出关键决策。

实时搜索最新威胁

X-Force Exchange 监控超过 250 亿个网页是否有 Web 威胁，并有超过 96,000 个漏洞的数据库作为支持。让您能实时搜索追踪最新威胁情报。

全球数据安全专家共享协作

全球用户在 X-Force Exchange 上可通过公开或私密群组共享研究、验证威胁与研议攻击回应计划。

高度集成串接应用

提供 API 让您无缝集成各式安全相关应用，包括支持开放式的标准环境。更容易的将威胁预警直接串接使用。

精选案例

美国城市安全团队有效减少 40% 的时间处理潜在攻击

美国城市安全中心与 IBM X-Force Exchange 合作成功预防数百万个潜在网站攻击，并有效分流威胁攻击

业务挑战

美国城市安全中心团队经常面对微小零星但大量的网站攻击与潜在威胁，与 IBM 携手打造 IT 数字化基础构建，在一个月内，阻止数百万个微小威胁攻击事件。其中，有效分流让极少数的攻击，被判断为需要进一步调查，而这些威胁可能会影响到相关的数据安全团队运作效率。

导入成果

减少 40% 威胁处理时间 > 解决威胁问题，在时间与成本上有效减少 40% 以上的时间成本。

减少 18% 管理时间 > 有效减少人员在安全风险管理上的时间，提高管理控制效率。

人力成本节省 50% > 提高信息安全团队的效率，帮助其节省了 50% 的人力成本。

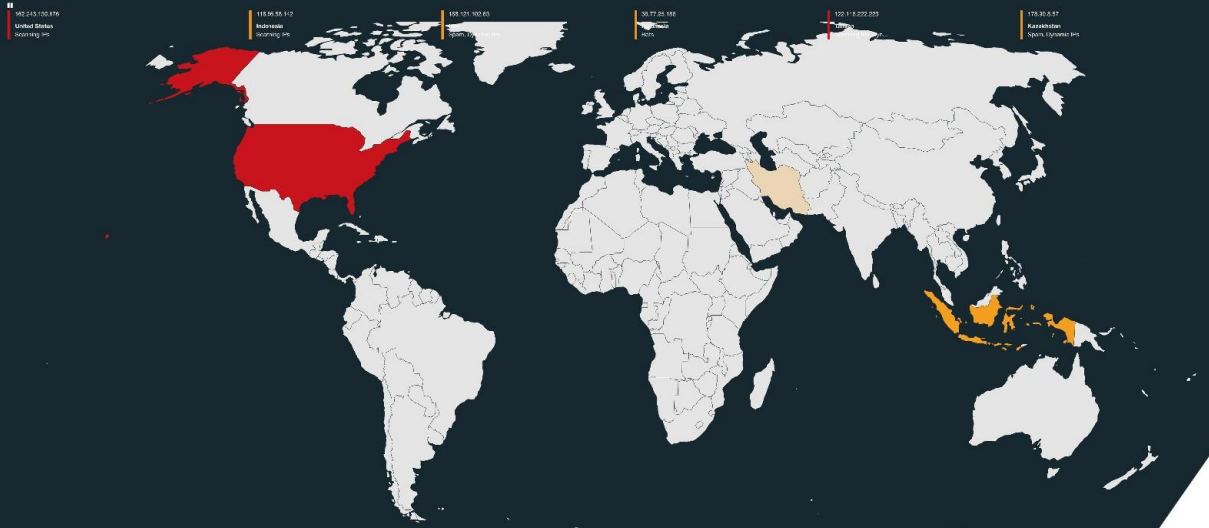
客户推荐

IBM 帮助该市部署了复杂的智慧数据安全解决方案，本解决方案集结成安全信息和事件管理（SIEM），日志管理，异常侦测和设定，及漏洞管理的办法，阻止最严重的安全事件。本解决方案集中并分析对数十个不同系统的监视，已从网络上发生的数百个可疑事件中，分辨出优先处理的数据安全事件。

IBM X-Force Exchange

创建 IBMid 登入

当前威胁活动



过去一小时的恶意 IP 地址

837	0	580	0	164
		响应事件	恶意软件	

IBM X-Force Exchange

立即免费试用

或拨打 400-810-1818 转 2395
立即联络 IBM 业务代表咨询

Key Point 3

IBM Cloud Identity

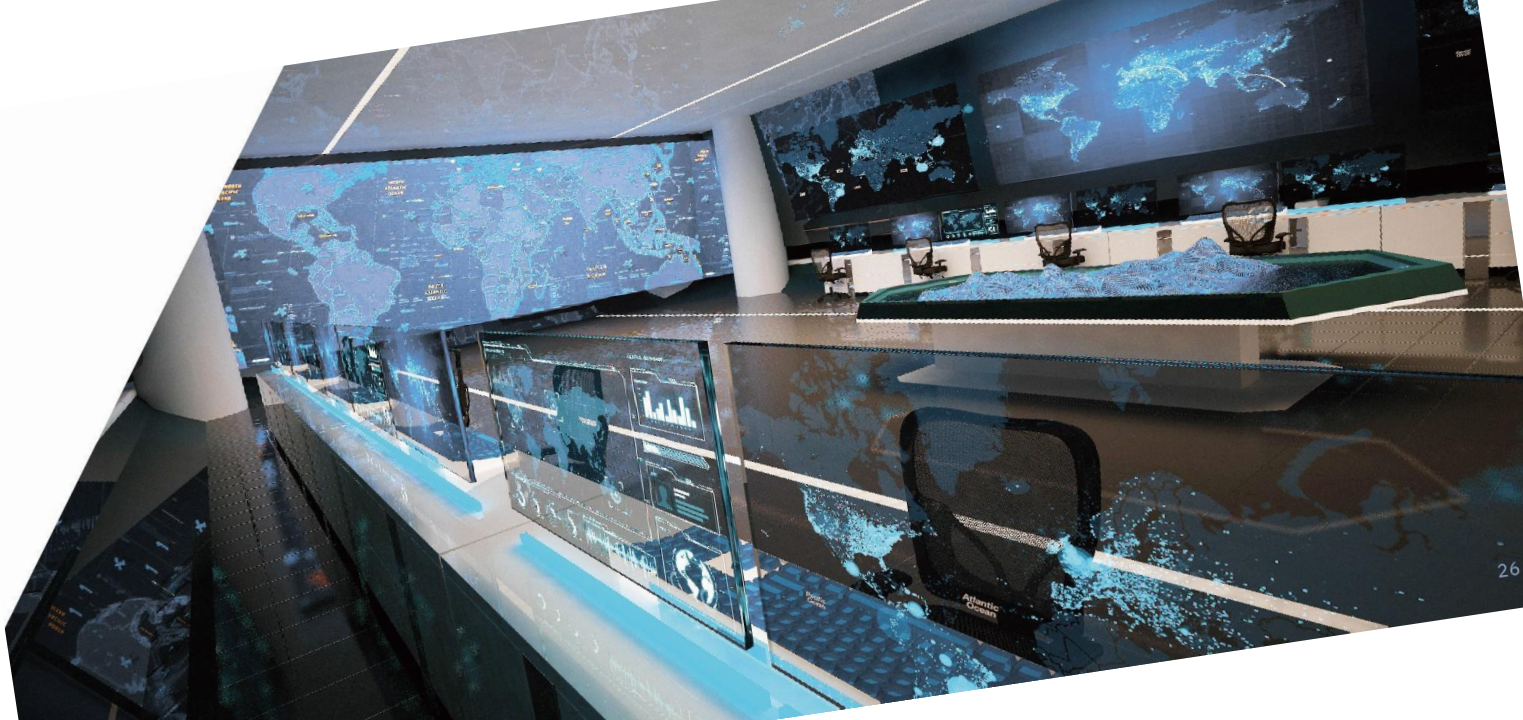
运用云端单点登录（SSO)、多因子认证和身份识别控制来有效保护您的企业内部系统。并提供热门 SaaS 应用程序存取、并预先构建多种模板以协助集成企业内部应用程序。为现今企业远程办公的最佳利器，免去使用 VPN 高授权费用与带宽满载问题！

IBM Cloud Identity 三大措施防护到位

所有设备单点登录 (SSO)
提供统一的应用程序启动程序和 SSO，以便从任何设备都能单点登录任何应用程序。

使用 2FA 登入任何企业系统
使用弹性的 MFA 来保护 Web、云端、行动、VPN 及作业系统。

监测管理云端使用
请求、核准、供应与重新认证用户的应用程序存取。通过风险评分、法规遵循数据及 URL 位置来评估并了解云端应用程序风险。


Atlantic
Ocean

以单点登录方式进行登入

免除输入用户名和密码的麻烦。运用一组登入认证即可登入所有应用程序，让您一键存取浏览器、移动设备及内部部署应用程序。

通过连接器轻松连接 1000 多种应用程序

通过预先构建的连接器或一般模板来加快公司采用新的应用程序。

运用多因子认证来强化安全

利用自定义认证策略来加强安全并符合法令规定。使用 IBM Verify 来注入多种用户认证方法以强化安全。

通过用户自我管理选项来缩减 IT Helpdesk 人力

提供用户自我管理界面，让员工可以请求存取应用程序，并且重设与管理自己的密码。

执行重新认证活动

安排定期的存取检查，以确保持续合规。

利用 IBM MaaS360 Integration 将 SSO 延伸到企业应用程序

将 SSO 无缝延伸到企业移动管理解决方案所涵盖的应用程序。

利用应用程序启动程序轻松寻找应用程序

从集中位置便利地寻找、查看与访问您所有的应用程序。启动程序会集成所有应用程序，包括内部部署和云端中的应用程序。

将 MFA 内嵌至消费者或面对民众的应用程序

提供开发人员各种工具箱，以便他们将最新的认证方法集成至新的应用程序中。

启用用户生命周期管理

简化内部部署和云端应用程序的用户上架、下架和自助式访问要求等策略。

让经理通过授权而有能力控制访问权限

缩减 IT 时间与技能的相依关系。将应用程序所有权的责任授权给事业单位管理者，让他们能够提供员工更快速的应用程序访问。

充分利用您的内部部署 IAM 投资

集成常用的内部部署目录，例如 AD/LDAP。

与 IBM Security Access Manager 无缝集成

单击启动让 IBM SecurityAccess Manager (ISAM) 用户可立即访问 IBM Cloud Identity。

精选案例

美国铁路公司通过改善身份识别管理进而保护企业营运

业务挑战

美国铁路公司通过改进身份识别管理来确保营运正常运作。因原身份识别与控制旧版软件已经到期，公司决定寻求替代解决方案。寻求新导入产品必须不影响任何的现行业务活动下进行更换及切换。

导入成果

减少 30% 时间成本 > 时间与成本同时降低，并且不需要和旧有系统并行运作。

大幅提高安全性 > 通过新系统功能提高安全性，能识别并让正确的用户登入，也阻挡非授权的入侵。

提高管理灵活度 > 能轻松容易地新增用户账号，也能在员工离职后删除该员工的特权账号。

客户推荐

IBM 的新身份识别及管理解决方案帮助美国铁路公司管理企业内部用户权限，以保护其重要资产。新产品导入时，对公司营运影响不大，这对于任何 IT 项目而言都是件非常重要的标准。其将迁移时间和成本减少了 30%，并且无需同时维护两个新旧系统，大大改善用户体验。


IBM Cloud
Identity

IBM Cloud Identity

立即免费试用

或拨打 400-810-1818 转 2395
立即联络 IBM 业务代表咨询

Key Point 4

IBM Security Guardium

为满足企业信息安全、合规、审计等需求，IBM Guardium 在法规遵从、数据可用、数据保留、数据安全四个方面来进行数据保护给予专项治理和加强，并简化安装部署工作，满足企业数据库更完整的监控与实时保护。

您是否面临...

数百个数据库都需要满足监管和合规要求、需要提高大数据项目的数据安全性和合规性，如 Hadoop、NoSQL 等，对安全合规和数据隐私权策略的重视度增加、期望在数据安全和合规策略方面变得更为主动，而非被动应战；希望提升安全解决方案的自动化水平、也需要推动合规性，确保实现真正的安全性。

高效识别安全合规性风险，有效降低风险提高安全质量

满足安全和合规要求的流程效率提升了 20%

使企业组织提升了满足安全和合规要求所需流程的效率。导入后，企业改善了数据库安全、审计协定和报告功能，并实现了自动化，使员工可更高效地处理安全需求。

降低遭主管机关罚款的可能性

导入 Guardium，企业满足了广泛的合规与监管法规要求如：实施 GDPR，并为其提供了有关敏感性数据更深入的可视性。如此一来，企业将遭受主管机关罚款的可能性降低到 2%。

每年在数据泄露复原方面节省了超过 97,900 美元的成本

有助于导入监控和审计、漏洞管理、数据转换、实时安全性原则和智慧化报告，进而识别和防御内外部威胁。投资 Guardium 后的第 3 年，企业发生数据泄露的可能性降低了 45%。

避免了开发和支持内部监控和审计功能所需的人工成本

投资后，企业组织就无需针对如何安全地记录、储存、分析和报告数据库审计存取信息进行开发、测试和部署替代性内部解决方案，进而节省了 960 个工时的企业成本。此外，企业还可以存取由 Guardium 提供的更健全功能。该公司省下了支持内部解决方案所需的 6 个全职员工。

IBM Security Guardium 四大关键要素

满足企业合规报告和审计需求

企业需满足合规和监管方面的需求，包括：HIPA，PCI/DSS，以及欧盟法规 GDPR 等。此外，能够监控经授权用户并阻止未经授权的存取。某家金融服务机构的网络安全管理副总裁介绍说“通过 IBM Guardium，我们能够获得比之前更多的数据洞察力，也能够更深入地了解存取数据的人员行为。”

提高敏感性数据的可视性

提高了对于敏感性数据的可视性，发现、了解数据并进行分类。企业数据每年增长率高达 20%，凸显数据洞察力是确保数据安全的关键。敏感性数据难以洞察，而可帮助发现潜在的问题来源。随着企业承担更多的大数据项目，数据安全威胁倍增，此时更好地了解敏感性数据的所在位置越发重要，能助其在企业数据安全方面做出比以往更明智、更好的决策。

完整保护整个企业环境内的敏感性数据

通过实时保护工具，可以降低员工从事非预期存取的风险，而通过原生的记录功能，就可能会遗漏这些存取。也能够持续监控整个企业环境内的存取，确保数据库、数据仓储、Hadoop、NoSQL 以及文件共享库等各种数据储存系统的安全。此外，它还有助于确保各类数据的安全，无论数据是储存在内部或外部，或储存在大数据环境、私有云或混合云环境中。通过部署集中式解决方案来监控各个平台，带来巨大业务价值。

通过与该领域强大的合作伙伴开展合作，建立可靠环境

与市场领导者的合作提升可靠性，可扩展的解决方案意味着无需延请额外人力，便可支持不同规模的环境；同时，由于其非侵入式的设计，不会对企业数据库或数据仓储的效能产生影响。使得无需延请新的人员，同样规模的原团队也能完成原本的日常工作任务。这代表企业可简化营运，同时提高企业数据安全性原则的质量。

IBM Security
Guardium

精选案例

帮助 Morneau Shepell 全球最大型的员工协助计划保护公司敏感数据

无论您的问题属于何种性质，Guardium 将能保护您所有在安全规范内的数据

业务挑战

Morneau Shepell 全球最大型员工协助计划，需要找到可信赖的数据安全解决方案，因其缺乏对于何种数据存在风险、哪些数据可能导致毁灭性安全威胁的可视性。因此，企业需要保护各种环境内的结构化数据和非结构化数据的安全，并确保做到合规，包括内部环境、外部环境、私有云环境、公有云环境或混合云环境、主机环境或者大数据环境等等。

导入成果

节省 20% 时间 > 在应对安全和合规要求方面能节省 20% 的时间。

降低 45% 数据泄露风险 > 数据泄露可能性降低到最低 45%。

节省 6 名员工人力成本 > 可在未来避免雇佣的员工数量减少到六个以下。

客户推荐

企业组织发现，通过与该领域强大的合作伙伴展开合作，能建立可靠的环境。IBM Guardium 是数据安全与合规性领域值得信赖的市场领导者，受访企业组织表示，通过导入 Guardium 提升了可靠性，使得他们对数据安全充满了信心。此外，可扩展解决方案意味着，无需延请额外的人力，便可支持不同规模的环境；同时，由于其非侵入式的设计，它不会对企业组织数据库或数据仓储的效能产生影响。某家金融服务机构的网络安全管理副总裁也谈到，“我们之前的解决方案不能很好地扩展。现在，通过 Guardium，即便我们新增了一些数据库，但也无须延请新的人员，原同样规模的团队也能完成他们的日常工作任务。”

IBM Security Guardium

加速实现端对端 提高数据防护能力

发现
横跨复杂的数据环境，发现数据并予以分类。

监控
实时监控整个环境的数据存取情形。

管控
管控权限，防堵未经授权的存取。

巩固
巩固数据防护能力，为最敏感的数据设下存取限制。

防护
保护闲置与使用中的数据。

IBM Security Guardium

了解更多

或拨打 400-810-1818 转 2395
立即联络 IBM 业务代表咨询

Key Point 5

IBM Cloud Pak for Security

实现业界首次无需从原始数据来源移动数据而能连接任何友商安全工具、云端和本地部署系统，IBM Cloud Pak for Security 为 IBM 首创开源新技术的数据安全平台，能够搜索并转换来自各种来源的安全数据，汇集企业多云 IT 环境中的关键安全洞察做整合，并在统一的界面下把安全工作流程与自动程序连接起来，让安全部门能够更快速且自动化地对数据安全事件做出回应。

快速回应跨云端网络威胁的开放平台

随着越来越多业务运营移至云端，安全数据往往分散在不同的工具、云端及 IT 环境中。
需要团队花更多时间集成工具与信息，而且还需要维护这些集成，因此保护组织的时间反而变少。
IBM Cloud Pak for Security 协助团队利用开放的安全平台来解决这些问题，串连所有片段的数据安全工具。

专为混合、多云环境设计的安全

Cloud Pak for Security 支持跨任何云端或者本地环境，能轻松地实现“容器化”部署。随着企业不断增加新的云端部署和迁移，Cloud Pak for Security 可以轻松地适应这些新环境并支持不断扩展 – 客户甚至能够将敏感和关键任务工作负载放到云端中，在中心安全平台上持续监视这些负载，并进行控制。

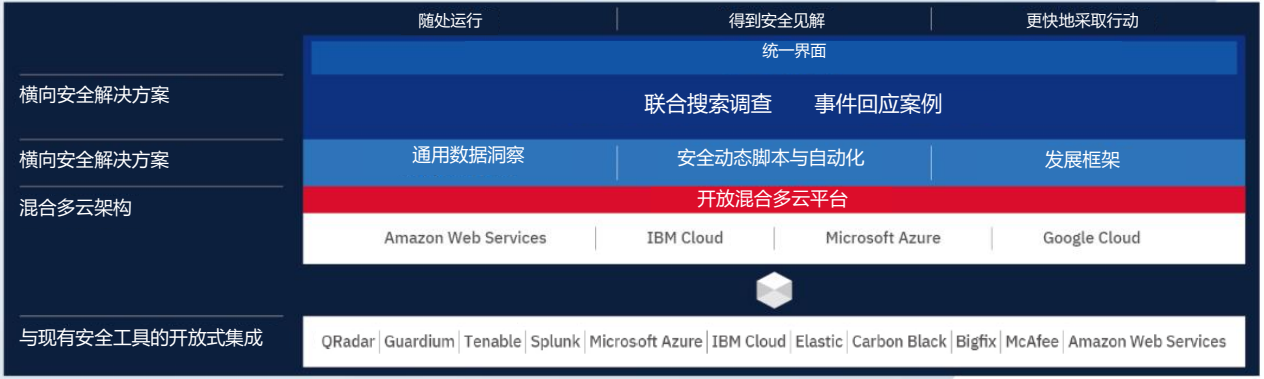
开放弹性的高效部署集成

IBM Cloud Pak for Security 实现业界首次无需从原始材料来源移动数据而能连接任何友商安全工具、云端和本地部署系统。由预先与 Red Hat OpenShift 相集成的储存容器化软件所组成。

统一界面进行洞察威胁及 IOC

此平台通过使用开放式标准来连接您现有的安全工具，以便您搜索混合式多云端环境中的威胁指标。它还会使用统一界面来连接全公司的工作流程。

IBM Cloud Pak for Security 跨云集成 自动化回应



在不移动数据的情况下获得安全洞察

为进行分析而传输数据会带来额外的复杂性。IBM Cloud Pak for Security 能够连接所有数据来源，以发现隐藏的威胁，进而做出更好的基于风险的决策，而无需移动数据。利用 Cloud Pak for Security 的 Data Explorer 应用，安全分析师能够非常顺利地跨任何安全工具或者跨云来搜索威胁。如果没有此功能，安全部门将不得不在每一个单独的环境中手动搜索相同的威胁指标 (例如恶意软件签名或者恶意 IP 地址) 。Cloud Pak for Security 是业界第一款不需要将数据移转至平台即可进行分析以支持此类搜索的工具。

自动的快速回应安全事件

IBM Cloud Pak for Security 在统一的界面下把安全工作流程与自动程序连接起来，如此安全部门能够更快地对安全事件做出回应。该平台支持企业编排数百种常见安全场景的回应，指导用户完成整个过程，用户能够迅速存取适用的安全数据，使用合适的工具。IBM 的安全编排 (Orchestration) 、自动化 (Automation) 和响应 (Response) 功能与 Red Hat Ansible 集成，提供更多的自动化程序 (playbooks) 。通过规范整个企业的安全流程和活动，企业能够更快、更有效地做出回应，同时为自己提供加强监管审查所需的信息。

可在任何地方运行，开放的安全连接

IBM Cloud Pak for Security 可以轻松地安装在任何环境中，无论是本地、私有云还是公有云。它提供的统一界面简化了操作，由预先集成 Red Hat OpenShift 的容器化软件组成 – OpenShift 是业内最完整的企业级 Kubernetes 平台。

IBM Cloud Pak
for Security

IBM Cloud Pak for Security

立即咨询

或拨打 400-810-1818 转 2395
立即联络 IBM 业务代表咨询

IBM X-Force

Cyber Tactical Operations Center

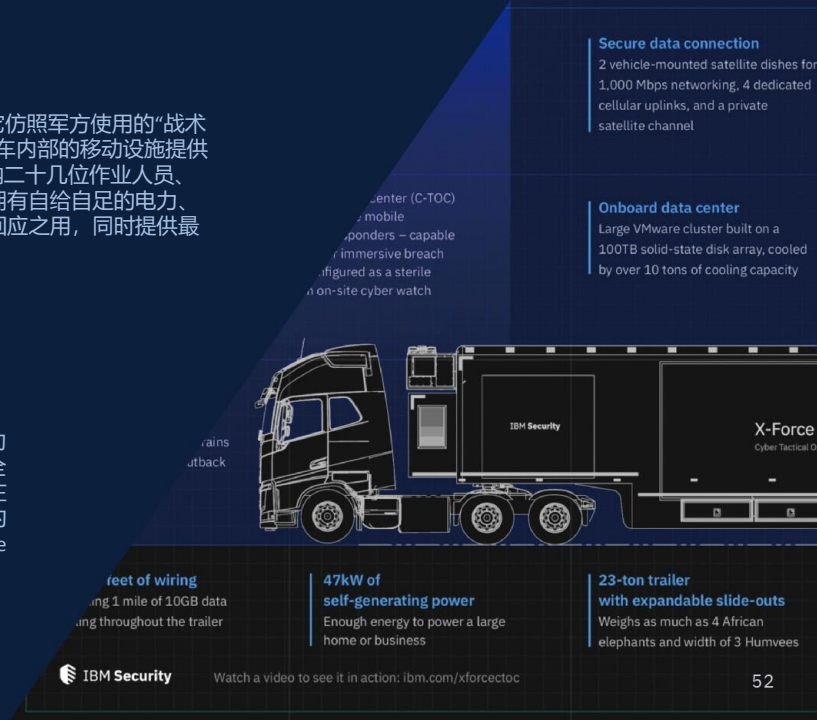
移动数据安全战情中心 **C-TOC**

公司如何为数据安全危害做准备

IBM X-Force C-TOC 是一个可全面运作的移动数据安全战情中心，它仿照军方使用的“战术作业中心”，以及首批应变人员所使用的事件指挥站。这个设在挂车内部的移动设施提供由手势控制的网络安全“观察室”、数据中心与会议室，里面可容纳二十几位作业人员、分析师与事件指挥中心人员。此设施可部署在各种不同环境中，拥有自给自足的电力、卫星及蜂窝通信，可提供无病毒并具复原力的网络，以供调查与回应之用，同时提供最现代的平台以便进行网络安全训练。

为公司的最坏情况做好准备

来自 IBM X-Force Command 的数据安全专家团队与专业黑客能帮助企业训练各种组织的危机应变 – 包括执法部门、情报单位、许多全球各大银行以及各大能源和技术公司。以逼真的沉浸式体验，在模拟和游戏化环境中提供重要的网络安全和领导技能，为组织的最坏情况做好准备。现在就来预约并亲身体验 IBM X-Force Command 的威力吧!




X-Force Command
Cyber Tactical Operations Center
IBM Security
IBM Security
X-Force Co

X-Force Command 专为您量身打造的独特体验

X-Force Command Cycle Range
全球唯一能容纳所有事故现场指挥人员和融合团队的全面实境网络靶场。体验由精英训练小组引导企业负责人员的身历其境模拟。地点在美国马萨诸塞州剑桥市。

移动数据安全战情中心
IBM X-Force Command 网络战术行动中心 (C-TOC) 是一种独一无二的移动网络体验，它可以设定为网络靶场、执行网络调查战情室、或针对特殊安全事件的现场网络监视楼层。目前在欧洲巡回中。

IBM 客户体验中心
与经验老到的事故应变人员、渗透测试人员、设计思考专家和 IBM 高阶主管会面，以构建及磨炼您的网络安全与事故应变策略。

作战从演练危机应用开始
立即了解更多

进一步了解 IBM 解决方案
或拨打 400-810-1818 转 2395
立即联络 IBM 业务代表咨询