中大型企业产业解决方案

产业解决方案总览

大型企业结合 IT 与企业目标，以提升效率和竞争优势。但是这些创新技术的价值，会因全球网路安全风险和复杂性的增加而遭受危害。

趋势科技 EPS 企业安全防护策略提供具有集中管理安全防护架构的产业解决方案，能够整合整个大型企业的邮件、Web、端点及网路安全防护功能，让组织获得更大的投资报酬率。

金融业

银行与保险机构目前积极投资于可提升通路客户管理、后端办公室转型及加强大型企业风险管理的技术上。

愈来愈多针对金融服务的网际网路安全威胁，在许多情况下，这些安全威胁来自攻击线上客户入口、自动柜员机与自助服务技术。安全威胁破坏企业、泄漏私密的客户资料、窃取金融资产与破坏客户信任的恶意程式与诈骗活动。

金融服务机构的趋势科技安全整合多层次产品与服务，提供已知或未知安全威胁的智慧型防护。此完整的安全架构以 Trend Micro™ EPS 企业安全防护策略为基础，防护多重安全威胁。此紧密整合之集中式管理平台促使产品间紧密合作，共同防护每个网路端点，包含客户入口与 ATM。

深入了解趋势科技的金融服务安全架构。

窃取私密金融资料 降低客户信任度 PC 系统与网路效能速度变慢 增加服务台	散播病毒 提供网路钓鱼与网路诈骗入侵的机会 浪费员工的宝贵时间	破坏业务与停止交易 需要耗费时间与金钱才能复原 损坏客户	窃取使用者姓名、密码与金融资产 提升复原客户损失的成本 增加诈骗	泄漏私密与金融资料 导致罚金、罚款与制裁 提供不当内容入侵

成本	• 邮件传递速度变慢	帐号资料 • 危害客户服务 • 提供骇客入侵的机会	责任 • 强制支付规定的罚金	的机会 • 增加法律责任

End-to-end Trend Micro Security Framework

间谍程式防护安全功能可封锁间谍程式进入，并阻挡由间谍程式所收集的资料传出。	垃圾邮件防护可阻挡垃圾邮件消耗网路资源以及员工浪费的宝贵时间。	防毒功能可防护每个网路进入点，从闸道与网路到电子邮件与档案伺服器、桌上型电脑和行动装置。	网路钓鱼防护功能可阻挡窃取身份识别，并防护使用者名称、密码与私密金融资料的安全。	网路内容与网站过滤器可让公司管理员工使用网际网路，并封锁恶意或非工作所需的网站。

医疗业

医院与医疗保险机构目前积极投资于能创造出更具成本效益环境的技术上，以协助他们处理病患需求、管理法规异动及提供服务。

医疗机构受到来自于网际网路威胁的风险范围很广泛，大到瘫痪攸关人命的生命支持系统，小到侵害资料安全进而危害病人的隐私权。像间谍程式这种渗透性威胁会干扰 IT 人员从事核心企业营运工作，导致成本上升，生产力下降。

趋势科技针对医疗机构设计的安全架构结合了多层次的产品与服务，可提供智慧型全面防护以对抗已知和未知的安全威胁。这项以趋势科技™ 大型企业防护策略为基础的安全架构包含创新的解决方案，可以监控医疗资讯系统与网路，以即时且精准地侦测出未知的安全威胁。趋势科技紧密整合且集中管理的安全技术，可以毫无漏洞地跨产品协同作业，保护每一个网路端点。

深入了解趋势科技为医疗服务供应者提供的安全架构。

• 桌上型电脑与笔记型电脑受损 • 系统与频宽速度减缓 • 丧失生产力 • 智慧财产遭窃	• 病毒扩散机制 • 生产力降低 • 邮件系统耗损增加	• 企业营运中断 • 修复成本高 • 丧失智慧财产资料 • 组织恢复能力降低	• 易受网路诈骗 • 丧失隐私权 • 身分资讯遭窃 • 须对使用者损失负受信责任	• 遗失利害关系人资料与学生私人记录 • 联邦管理机关制定的罚则 • 传送不适当的电子邮件与不当使用网际网路进行合法暗示

制造业

制造业目前积极投资于能够保护重要资讯和保障供应链管理系统的安全的技术上，以确保能维持生产力并顺利完成订单。

网际网路安全威胁为制造业机构带来严重的风险，无时无刻不在挑战关键 ERP 系统与供应链网路能否继续执行。恶意程式与诈骗诡计有愈来愈多是针对智慧财产、金融资料，以及客户与员工的私密资讯而来。病毒、网路蠕虫、机器人程式或间谍程式会渗透网路、中断生产并导致盈亏结算的损失。

趋势科技针对制造业机构的安全架构结合多层次的产品与服务，为已知与未知的安全威胁提供智慧型防护。此完整的安全架构是以 EPS 企业安全防护策略为基础，在包含客户与合作伙伴入口在内的每个网路进入点防止恶意程式的攻击。此单一且集中式管理的安全平台可促使产品间紧密合作，以取得更佳的整体防护。

深入了解趋势科技针对制造业机构的安全架构。

›窃取私密资料 ›失去合作伙伴与客户之间的信任 ›网路效能速度变慢 ›失去生产力 ›技术支援成本增加	›病毒与诈骗扩散机制 ›员工与合作伙伴的生产力降低 ›邮件系统的损耗增加	›生产与供应链流受到破坏 ›智慧财产的损失 ›复原成本增加 ›客户信任度降低 ›骇客相关的攻击	›诈骗容易度与可信任度增加 ›用于弥补客户与合作伙伴之损失的成本垫高 ›违反法规遵循会处以罚金	›损失智慧相关资料 ›联邦管理员课征的罚金、罚款与奖惩附加条款 ›误引法据

公共部门

政府机关与公教机构目前积极投资于能够协助他们降低成本、保护私密资料并促进跨机构合作的技术上。

公共部门机构网际网路安全威胁风险的涵盖范围，可从私人政府资讯与智慧财产权的损失，到联邦管理员课征的罚金、罚款与制裁。生产力减少与公共评等降级也会转移公共管理目标与专案的重心。

趋势科技的公共部门安全架构结合多层次的产品与服务，针对已知与未知安全威胁提供智慧型的完整防护。此安全架构以 Trend Micro™ EPS 企业安全防护策略为基础，内含创新的解决方案可监控资讯系统与公共管理网路，以即时准确地侦测未知的安全威胁。趋势科技紧密整合且集中式的管理安全功能，可促使产品间紧密合作，共同防护每个网路端点。

深入了解趋势科技的公共部门安全解决方案。

›损害桌上型电脑与笔记型电脑 ›系统与频宽速度变慢 ›失去生产力 ›窃取智慧财产	›病毒扩散机制 ›降低生产力 ›邮件系统的损耗增加	›破坏业务运作 ›补救的高成本 ›遗失智慧资产资料 ›降低组织的恢复力	›易受诈骗 ›失去隐私 ›身份识别遭窃 ›使用者损失的信托责任	›遗失私密资料与私密的学生记录 ›联邦管理员课征的罚款 ›不当电子邮件与使用网际网路的合法性