

保护机密信息的再访问

简介

研究目的

ESG调查了308位IT和信息安全专业人士，他们来自于北美和西欧的各大型企业(员工人数不少于1000人)，负责或熟悉各自企业保护机密信息安全的当前策略、步骤和技术。

调查旨在回答下列问题：

问题定义和范围

- 安全专家认为企业有多少数据是机密的？
- 用户知道他们有多少份机密数据的副本吗？它们存放在何处？
- 最大的痛点是什么？

市场动态和采购计划

- 什么推动了对机密数据安全解决方案的需求？在什么样的时间范围内？
- 用户会首先着手解决机密数据保护的哪一块？
- 鉴于全球经济正在衰退，用户如何制定机密数据保护开支的预算？

策略、流程和步骤

- 具体来说，哪些机密数据安全策略和步骤是最重要的？
- 这样的话，它们该如何界定、监测和执行？
- 这些策略、流程和步骤的有效性如何？
- 需要做怎样的变化？

技术部署和采购计划

- 目前在使用哪些工具？
- 未来12个月内又将部署哪些工具？
- 用户会部署加密技术吗？如果是的话，部署在哪里？
- 加密技术的部署本质上是策略性的还是战略性的？它们会不会有变化？
- 用户如何管理加密密钥？这个做得是否足够？会不会有变化？

调查的参与者涉及各行各业，包括制造业、金融服务业、通讯和媒体、医疗保健、零售业、政府和专业服务。如需详细资料，请参阅本报告中的“研究方法”和“受访者资料统计”章节。

目录

目录.....	1
插图目录.....	2
表格目录.....	3
内容概述.....	4
研究概况.....	4
报告结论.....	4
简介.....	6
研究目的.....	6
确定机密数据.....	7
保护机密数据安全的驱动因素.....	9
保密开支将保持稳定.....	10
哪里机密数据有风险.....	11
机密数据的安全是企业努力的方向.....	14
机密数据的安全措施.....	15
机密数据的安全策略和步骤.....	17
数据加密技术日益普及.....	20
大型企业如何决定哪些数据需要加密，如何加密.....	20
加密技术部署.....	22
网络加密技术也有所增加.....	23
了解和预测潜在的加密问题.....	25
制定加密策略.....	26
密钥管理：需求和挑战.....	29
密钥管理执行趋势.....	31
迈向统一的密钥管理服务.....	32
密钥管理业务.....	35
对 IT 专业人士的研究启示.....	39
机密数据的安全风险模型.....	39
加密和密钥管理方面的建议.....	42
对技术厂商的研究启示.....	43
研究方法.....	45
受访者资料统计.....	46
受访企业（按地区划分）.....	46
受访企业（按员工人数划分）.....	46
受访企业（按角色划分）.....	47
受访企业（按行业划分）.....	47
受访企业（按年收入划分）.....	48

版权所有©2009。Enterprise Strategy Group, Inc. 保留所有权利。

所有商标和公司名称是其各自公司的财产。本出版物中包含的信息是由 Enterprise Strategy Group (ESG) 认为可靠的来源提供的，但 ESG 不保证其可靠性。本出版物可能包含 ESG 的观点，这些观点随着时间的推移可能会有所改变。本出版物的版权归 ESG 所有。未经 ESG 的明确许可，不得对本出版物的整体或部分以硬拷贝方式、电子方式或其他方式进行复制或将其分发给无权接收它的人，否则都将违反美国版权法并将引起民事损害诉讼，乃至刑事诉讼。