



这份信息图表总结了Gemalto支付数据安全状态(The State of Payment Data Security)全球研究的重要调查结果, 在该研究中Gemalto于全球范围内调查了全3,700多名IT与IT安全从业人员, 了解公司如何保护支付数据并评估新的移动支付方法的日益广泛应用所带来的安全风险。

重要调查结果



多数公司都曾遇到过涉及支付数据的数据破坏问题

54% 的受访者都表示所在公司曾遇到过涉及支付数据的数据破坏问题, 在过去两年中平均会遇到四次这类问题



并不是所有公司都知道支付数据所在的位置

55% 的公司并不知道其支付数据的存储位置

支付数据有很多面临安全威胁的薄弱点



42% 表示薄弱点出现在数据存储时

33% 表示薄弱点出现在公司和金融机构或支付处理器之间传输时

25% 表示薄弱点出现在销售网点数据时

支付数据安全并不一直都是最优先考虑的问题



54% 的公司并未将支付数据安全列为五大安全优先性之首

31% 的公司表示它们会分配足够资源来保护支付数据

支付方法的趋势



在未来两年内移动支付会增加一倍

> 目前所有支付活动中**9%**都采用移动支付方式

> 在未来两年内, 所有支付活动中**18%**都会采用移动支付方式



有一半公司都计划采用移动支付方式

今天, **14%**的公司都接受移动支付, 如苹果支付(Apple Pay)、三星支付(Samsung Pay)或其他非接触式支付方式, **51%**的公司计划在未来接受移动支付方式。



并不是所有公司都对自身保护下一代支付方法的能力充满信心

54%的公司并不相信或不能确定其现有安全协议是否能够支持这些平台。

支付数据安全趋势

保护支付数据所使用的顶级安全技术

93%
防火墙

92%
杀毒/反恶意软件

75%
入侵检测与预防(IDS/IPS)

46%
数据加密

40%
多因素认证

31%
SIEM

5%
其它

41%
私有网络连接性

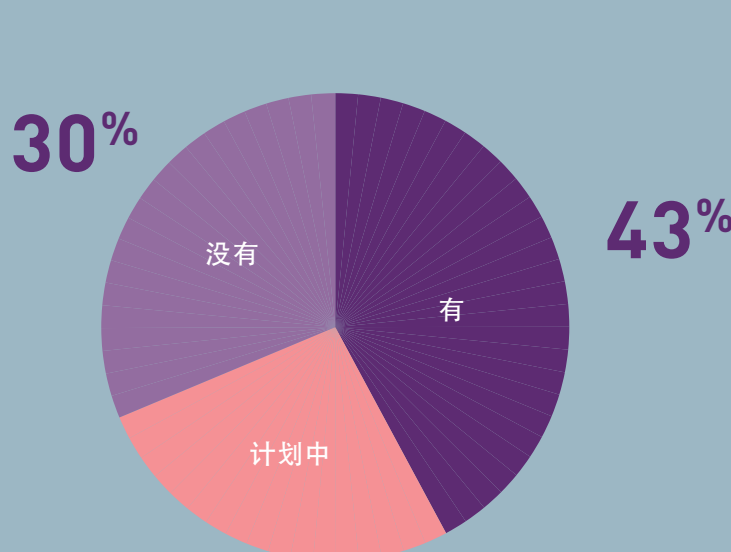
37%
威胁监控

31%
数据丢失预防

注意: %表示使用这些安全技术保护支付数据的受访者百分比。

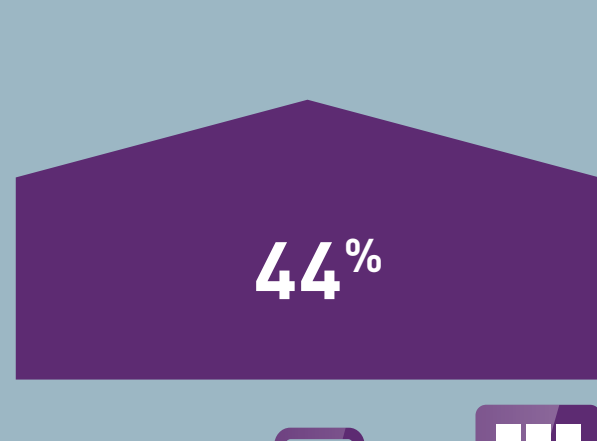
保护支付数据所使用的顶级安全技术

只有**43%**的公司销售点采用加密或令牌化处理。**27%**的公司计划实施此类保护方案, **30%**的公司并未使用该方案。

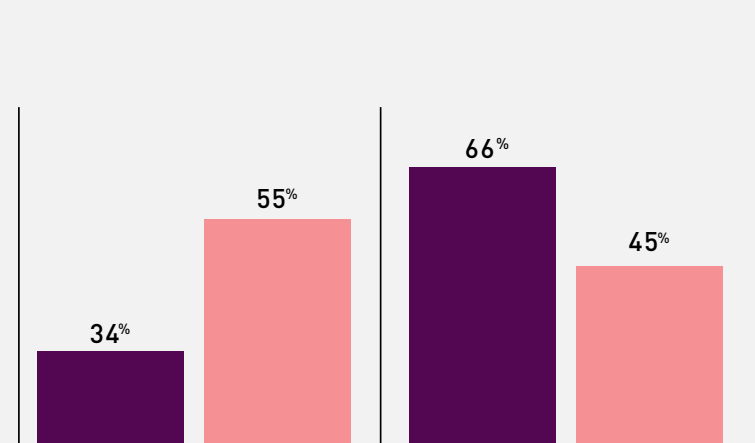


支付数据端对端加密

44%的公司使用端对端加密方式在支付数据从POS机终端转移出来并发送到金融机构时对其进行保护。



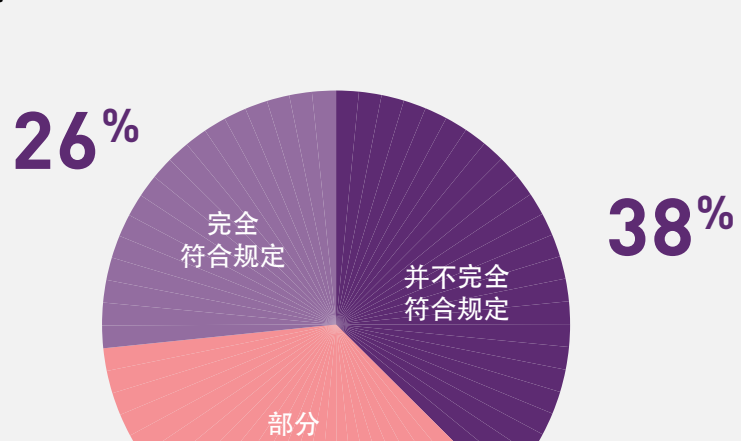
多因素认证主要用于内部员工, 很少用于第三方或供应商



PCI DSS并不足以确保支付数据的安全性与完整性

> 只有**17%**的公司表示必需符合PCI DSS规定要求

> 实际上, 有**74%**的公司并不是完全符合或只是部分符合PCI DSS规定要求



支付数据安全的所有权并未集中起来

谈到谁是确保支付数据得到安全保护的最大责任人时, 我们所调查的IT专业人员回答如下:

