

# 安全运营中心过载的自动化和协调解决方案。

市场研究表明：  
先自动化，然后协调。



安全运营中心 (SOC) 平均使用 **25-30** 款工具。\*



**60%** 的安全运营专家表示人工处理能力有限。\*



**83%** 的市场现在正在实现自动化，还有 **13%** 计划或希望实现自动化。\*



**27%** 计划购买工具来实现自动化并协调运营事务。\*

## IDC 对自动化的证实

通过 McAfee 集成威胁防御解决方案，IDC 证实有 **50-100%** 的操作实现了自动化。



**25** 个威胁分类步骤



**3** 个威胁保护平台：  
终端、Web 和网络安全



**3** 个安全分析引擎



**9** 种不同的威胁情报检查

## 实现了自动化的威胁功能包括：

通过动态终端防范零日恶意软件

防范“随看随下”下载勒索软件

通过应用程序控制防范服务器恶意软件

威胁追踪

通过 IPS 防范恶意软件



## IDC 证实了三步威胁追踪流程的自动化：

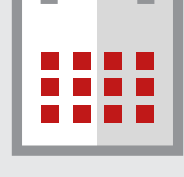
步骤 1: 系统自动提交文件进行验证

步骤 2: 证明有恶意后，系统应用预先确定的策略

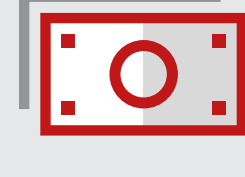
步骤 3: 管理员对攻击进行补救



## McAfee 解决方案实现投资回报 (ROI) 的速度更快。



4 年投资回报率为 **208%**



投资回收期为 **20** 个月

示例：全美百大公司 FDIC 银行

## McAfee 解决方案可提高生产率。

**1-2** 个管理平台窗格  
监控环境

**77%** 每年减少的事件数量

**90%** 提高的事件解决速度

**98%** 减少的停产时间

## McAfee 解决方案的真实效益。

**302 万美元** 四年平均 (每年) 效益

**500-1000 万美元** 解决方案支持的额外客户效益 (每年)

售价 (美元)。

利用 McAfee 的集成威胁防御解决方案，通过自动化和协调简化威胁管理。

下载免费安全报告，网址：  
[mcafee.com/orchestrate](http://mcafee.com/orchestrate)。