TREND MICRO 趋势科技

可信赖的网络安全专家

Guess?® --让混合式威胁看得到，管得了

趋势科技威胁发现设备（Threat Discovery Appliance）使得Guess？改进了安全性并且显着减少了符合合规工作所需时间

“威胁发现方案正是我们所需要的——该方案如此简单，几乎可以即插即用。”

——Guess?，Inc．IT部网络经理Scott Forrest

执行综述

客户名称：Guess?, Inc

行业：服装／零售

地点：加州洛杉矶（总部）

员工数量：10,800

挑战：

- 以前的安全解决方案均未能有效地检测并拦截混合式威胁（间谍软件、灰色软件、恶意软件）。
- 客户端软件和签名文件的大小不断增加，使得从广域网中将之清除出去变得越来越困难。
- 对IT部门而言，升级工作变得越来越复杂而耗时。

解决方案：

- 威胁发现设备可以识别混合式威胁并实现快速补救。
- 趋势科技的端点、讯息和防火墙解决方案提升了安全性。

业务成果：

- IT部门对整体安全性和用户行为获得了高度的可视性。
- 自动威胁感染监测／警报极大地简化了合规工作（每天仅需10-15分钟即可查看并解决系统的相关警报，而在以前则每周都需要花费4天的时间来完成该项工作）。
- 提高了对网络感染的可视性，从而能够更好地调整安全流程。

挑战

Guess?, Inc的IT团队在安全上花费了大量时间。公司以前的安全解决方案无法捕捉更新的混合式威胁，因此使得管理工作变得越来越难、越来越耗时，特征码文件不断加大，占用了公司网络更多的带宽，而升级工作也常常需要在几乎所有的客户端和服务器上彻底地重装系统方可解决问题。

“一直以来我都在考虑更换我们以前的安全解决方案，但是我们一直没有真正地对此进行过积极考察”，Guess的IT部网络经理Scott Forrest说道，“在一次‘午餐学习会’上，趋势科技谈到了新型混合式威胁和最新的针对性技术解决方案。我对他们提到的趋势科技威胁发现设备的安全评估非常感兴趣。我认为这是确定我们的问题范围并提高整体安全性的适用方法”。

解决方案

威胁管理服务包括发现、清除和生命周期管理服务。在两周的时间内，Guess实施了威胁发现系统的试用评估并于随后在网络中部署了相关设备—威胁发现设备（Threat Discovery Appliance）。该设备允许IT人员识别并分析公司范围内的威胁安全问题，包括未被检测的感染、危险的恶意代码行为和做法、潜在恶件进入位置以及其它可能造成漏洞的情况。

“我的整个团队每天都会对报告进行多次审查”，Forrest说道。“趋势科技威胁发现设备准确地向我们显示出我们的安全解决方案存在的缺陷。在20-30分钟内，我们只需进行极少的一次性工作，即可使该方案接通并开始运行。对我们的工程师而言，该方案非常直观，我们可以从总体上看到节点和网络中正在发生的事情。此前我们从未获得过这样的可视性，该服务让我们得以深入了解总体的威胁安全环境。我还没有看到市场上有哪种产品能与趋势科技威胁发现设备一样——它绝对是独一无二的方案。”

有了对网络和员工行为的了解，IT部门就能够清除网络中的恶件和间谍软件。对网关安全也添加了新的规则，而对防火墙规则也根据威胁发现服务报告进行了相应调整。

IT部门也依据TDA结果部署了趋势科技企业安全解决方案，其中包括：

- 终端安全（趋势科技防毒墙网络版OfficeScan客户端—服务器套件）
- 讯息安全（趋势科技ScanMail for Microsoft Exchange）
- 防火墙功能（趋势科技入侵防御防火墙）
- 安全管理和监测（趋势科技控制管理器）

趋势科技云安全2.0(Smart Protection Network)将为这些紧密集成的内容安全产品提供支持，它们将共同针对各种新兴威胁提供保护，同时使Guess的IT团队显着降低安全管理的成本和复杂性。

结果

除了帮助Guess的IT部门定制了一个更加有效的新型解决方案之外，威胁发现设备带来的益处还包括一个提供自动威胁监测的新增安全层。过去，两名工程师每周都需要用两天的时间来遵守《萨班斯奥克斯法案》（SOX）和支付卡行业（PCI）的相关规定。对日志文件需要进行手动审查，而对问题的解决过程也非常耗时。

“威胁发现设备为我们带来了对安全问题的自动记录和自动通知——这样就节省了大量时间”，Forrest表示。“我们不再需要花费几天的时间来审查日志，每天只需用10分钟或15分钟的时间就能满足SOX和PCI的相关规定。如果没有提醒，则我们就无需花费时间——这样就为我们节省了大量时间。”

更快速地发现威胁将大大减少响应时间，有助于更好地保护公司资产。高可视性使得IT部门对保护公司和满足安全目标充满了信心。

威胁发现服务为IT部门提供了一个向管理层展示一个内容简洁的安全画面的绝佳机会。“我和我们的首席运营官以及首席信息官见面以评估威胁发现服务的成果”，Forrest解释说。“执行综述报告非常完美，很适合非IT经理和高管。形式简短明了，让他们知道正在进行的事情，可以很好地了解架构的基本风险级别。毕竟，IT不是我们公司的核心业务——我们关注的是服装制作。通过不太复杂的产品而给我们带来最多的信息——这对双方而言都是最好的结果。威胁发现服务方案正是我们所需要的——该方案如此简单，几乎可以即插即用。”

部署环境：

- 5个地点（美国、北美、香港）
- 3,000台计算机和服务器
- OfficeScan客户端-服务器套件第10版（OSCE 10）
- ScanMail for Microsoft Exchange，第5版（适用于Exchange Release 8）
- 入侵防御防火墙第1.2版
- 控制管理器企业版第5版

> “我还没有看到市场上有哪种产品能与趋势科技威胁发现设备比肩——它绝对是独一无二的方案。”
>
> ——Guess?，Inc．IT部网络经理Scott Forrest

公司简介：

Guess?, Inc设计、销售、经销并特许经营各种现代服饰、工装、手袋、手表、鞋类和其它相关消费产品。截止2009年8月1日，该公司在美国经营431家零售店铺，并在北美以外的其它地区经营723家零售店铺，其中有106家为自有店铺。该公司还通过全球各地的著名百货商店和专卖店经销产品。

- 趋势科技企业安全
  http://us.trendmicro.com/us/home/enterprise/
- 趋势科技智能保护网络
  http://www.smartprotectionnetwork.com
- 威胁管理服务
  http://us.trendmicro.com/us/solutions/enterprise/security-solutions/threat-management/key-components/
- OfficeScan客户端-服务器套件
  http://us.trendmicro.com/us/products/enterprise/officescan-client-server-edition/index.html
- ScanMail for Exchange
  http://us.trendmicro.com/us/products/enterprise/scanmail-for-microsoft-exchange/index.html
- 控制管理器
  http://us.trendmicro.com/us/products/enterprise/control-manager/