远离网络威胁，打造安全体验

人物表

英文名	中文名	性别	身份
ROBB BOYD	罗伯波伊德	M	嘉宾，思科公司技术达人，解答专家
JIMMY AY PURSER	吉米雷皮尔瑟	M	嘉宾，思科公司技术达人，解答专家
JENNIFER GEISLER	詹妮弗-盖斯勒	F	嘉宾，思科网络系统市场高级管理人员
TOM GILLIS	汤姆-吉利斯	M	嘉宾，思科安全专家
MARK GUNTRIP	马克-冈特瑞普	M	嘉宾，思科产品经理
DARREL LEWIS	戴劳-刘易斯	M	嘉宾，思科工程师
SHA YU	于莎	F	嘉宾主持人

JENNIFER GEISLER：真是令人恼火。

ROBB BOYD：怎么了？

JENNIFER GEISLER：我正在做节目调查，主要是关于僵尸网络的，我在研究几样东西，然后我的竞价不见了，它竟然消失了。

ROBB BOYD：竞价？竞什么价？

JENNIFER GEISLER：是这样的，我想买一个僵尸程序，然后我意识到我要的

是一个僵尸网络，我可以租用僵尸网络一段时间，我觉得肯定不错。

ROBB BOYD：噢，那你要僵尸网络干什么？

JENNIFER GEISLER：是这样，我觉得如果我们使用几千个僵尸程序来收看节目的话，我们可以使收视率加倍，增加观众数量。

ROBB BOYD：你真这么想？似乎是个好主意，不过……这事儿不该做。

JENNIFER GEISLER：好吧，你的意思是继续吧，让我输掉竞价，开始录制节目？

ROBB BOYD：你已经输了，不是吗？

JENNIFER GEISLER：好吧，随它去吧。好了，史蒂夫，我们开机吧。

ROBB BOYD：古语有云：亲不敬，熟生蔑。自以为熟悉也会产生同样的不良影响，它诱使我们产生一种自以为是的满足感，使我们看不清现实。多年以来，网络战争即将到来的可怕警告不绝于耳。很多人认为这种预言是无稽之谈，而另一些人则把它当作学术问题或军事问题看待。但很多人都没意识到，网络战争已经到来，战斗已经打响了。战争的前线，就是你的公司资产，知识产权，研究，图表，敏感的专有数据，机密的客户信息以及职员信息，战争此刻就在进行。现在恶意软件只是罪犯用于实施攻击的众多工具中的一种。认为今天的网络安全挑战，就是处理恶意软件问题，则完全忽视了大局。它是一个非法运行的，复杂的电子商务网络，其目的是收集知识资产和公司资产，它本质上并不是简单的恶意软件问题，而是大规模的网络间谍攻击。在所有的国家，每一个人正深受其害。这是 ScanSafe 公司发表《2009 年全球安全威胁年度报告》的开场白。你可以在我们的节目附录里找到报告全文，我强烈建议你去看看。但我们下一个小时的目标是

消除你可能持有错误观念 ,由恶意软件或任何一种破坏造成的网络安全问题并非暂时的故障。我们来看一下节目要点 。无边界安全：其真正含义所在？副总裁兼总经理汤姆吉利斯将为我们解释。他和詹妮弗盖斯勒将会一起详细阐述。由思科出版社出版的他的新书《无边界网络安全》,这是本优秀读物。什么是僵尸程序？你对这种威胁有多了解？你知道如何去解剖一个僵尸程序？为什么要解剖？因为它不但是监控我们正在对付的日益复杂的病毒的最好方法之一 ,它在分辨这些活跃病毒的共同特征时也同样出色，再看看云安全：你的云放在个人 HYPE CYCLE 曲线的什么位置？要弄清楚的是，云安全的重点是保护它为你提供的服务而不是云。因为不管你如何定义它 ,有很多证据都表明…你知道吗？有很多功能都蕴含着丰富的道理，SaaS 为一种交付模式，ScanSafe 在这方面已取得了了不起的成就。协议监督：好的网络设计永远不会过时，随着异地服务的增加，让我们的网络畅通的压力也增加了。达瑞尔-刘易斯是互联网工程任务组 LISP 工作小组的联合主席，该小组负责定位器/标识符分离协议，现在你对这个概念可能不熟悉，但它很快将为我们带来有利的变化。让我们拭目以待。我喜欢精彩的网络安全节目，敬请观赏。

JENNIFER GEISLER：你好，汤姆，谢谢你的参与。

TOM GILLIS：谢谢你，詹妮弗。

JENNIFER GEISLER：你的书很引人入胜，书名是《无边界网络安全》

TOM GILLIS：是的。

JENNIFER GEISLER：我得说我通常不读思科出版社出版的书，但是当你说“无边界网络”的时候，这引起了我的注意，我在想“他说的正是我熟悉的领域”。但我

邀请你到本节目的原因是，你提到了无边界网络安全，我想知道，你写这本书的动机是什么？

TOM GILLIS：我发现我对客户一遍一遍地重复着同样的话，当他们问我“天啊，无边界网络，这听起来很棒，但是网络安全问题呢？”所以我觉得客户需要明白，安全问题是无边界网络的核心，它是我们的愿景和灵感的重要部分，如果我们检视一下是什么在推动着无边界网络，我们将发现是安全，网络安全在今后五年将产生巨大变化。这就是我写这本书的动机。

JENNIFER GEISLER :我不敢想象没有安全可言的无边界网络或任何一种网络。。首先，我们的观众可是信息技术的高智商群体。你想让他们从这本书得到什么信息？他们能从中学到什么？

TOM GILLIS：我们大部分的观众目前在进行安全维护时，都是采用基于与物理基础设施联系极为紧密的方案。但是在大多数企业中，iPhone，Google Android，iPad 各种不同的电脑设备的出现，还有云计算，平台服务，虚拟基础设施服务以及各种储存数据的服务，这两方面的趋势共同催生了一种需求，那就是一系列与物理基础设施联系不是如此紧密的全新安全措施。

ENNIFER GEISLER：好的。如果我继续把眼光放在网络边界安全和终端设备安全上，这种趋势会影响到我吗？

TOM GILLIS：问得好，目前，大部分客户主要在两个地方进行网络安全维护，一是在终端使用传统的反病毒软件，二是在所谓 DMZ,或隔离区的边界，而该边界在世界范围内可能有两个、三个或四个物理地点。我们的确需要更具动态和可用性的安全技术，所以，无边界网络安全架构，我们不是要在两个、三个或四个

地点进行安全维护，而是在世界各地的数十个、数百个甚至数千个地点。而此时的终端，不只是运行大量程序的胖客户端，想象一下你能在 iPhone 上运行传统的反病毒软件吗。

JENNIFER GEISLER：不。

TOM GILLIS：听起来很可怕，是吗？

JENNIFER GEISLER：你无法做到。

TOM GILLIS：它的运行会不正常，所以你需要非常小的轻量级代理程序来连接你的终端和网络中的一个扫描点。

JENNIFER GEISLER：是的。如果我从信息技术的角度去想“我的网络里正在发生这样的事情。”

TOM GILLIS：我应该要怎么做？

JENNIFER GEISLER：没错，这些事情正在发生，汤姆，你现在说的这种安全架构对我来说太遥远，目前我对它无能为力。我要等思科生产出最终产品。

TOM GILLIS：是的。

JENNIFER GEISLER：是这样吗？

TOM GILLIS：我觉得这肯定是一趟旅程，今后五年将会发生巨大的变化。好消息是，我觉得这趟旅程的很多方面都是由思科发起的，我们有很多方案，我认为是遥遥领先于市场的。一个很好的例子，就是我们对 ScanSafe 的收购，ScanSafe 使我们能够为网络流量提供一致的策略执行，不管是在思科目前提供的设备上还是在云中，而且我们能够在先前谈到的世界范围内的成百上千个地点提供它。

JENNIFER GEISLER：非常好。

TOM GILLIS：ScanSafe 是我们加快实现这个目标，并把它转变为客户能够使用的方案的最关键因素，目前我们在支持数千位客户使用这种方案。

JENNIFER GEISLER：好的，这么说来我不用担心，因为这一切正在发生，这一趋势正在发展，我作为一名 IT 人，我必须要开始面对它，我不能依靠传统的安全方法。这件事我今天就可以开始做，这样我才能跟上这些疯狂的趋势。

TOM GILLIS：这是一种思考方式。如果我是从事 IT 行业的，我有着严格的安全策略，而我却发现职员们带着新的智能手机和智能设备接入公司网络。思科也有这样的事，对吗？

JENNIFER GEISLER：司空见惯。

TOM GILLIS：公司有其支持使用的设备，大家也有自己使用的设备，而这两种设备并不总是一样的。

JENNIFER GEISLER：没错。

TOM GILLIS：到处都有这样的现象。而作为产品供应商的思科及其竞争对手要能为客户提供解决这个问题的工具。这就是无边界网络安全架构的核心——为你提供在任何设备上随时随地建立策略执行点的工具，允许你的用户使用智能手机和网络型新应用程序。只要我们能安全地使用，它就是一款优秀的、有价值的、有效率的工具，那就是我们真正要做的事。

JENNIFER GEISLER：从 IT 的角度来看，也就是“使用”与“不使用”的问题。

TOM GILLIS：这是一个很有趣的现象，你不妨想想，在公司野餐活动上，为什么没有人愿意坐在 IT 部门的人的旁边。那是因为他会经常说“不行”，这很扫兴的，对吗？所以，现在你不用说“不行”，你可以说“可以”。

JENNIFER GEISLER：好的。

TOM GILLIS：因为最终用户不但可以使用这些新技术，而且使用过程还很安全可靠，我也可以执行我的政策。还有一种思考方式，那就是，你的公司政策可能很简单，比如，“这是我的客户数据信息”

JENNIFER GEISLER：对。

TOM GILLIS： “我只想让销售人员得到它们”。

JENNIFER GEISLER：很有道理。

TOM GILLIS：这虽然只有两句话，但是它能转变为一万条防火墙规则；所以当你用物理基础设施应用这些东西的时候，它就会变得无比复杂。

JENNIFER GEISLER：没错。

TOM GILLIS：但是有了无边界网络安全架构，我们可以依据你是谁，用的是什么程序以及你要得到什么资料来建立和执行策略。所以它不受设备和物理基础设施的约束，它简化了 IT 人员的工作，并使他们从经常说“不”的拒绝者转变为说“行”的业务推动者。

JENNIFER GEISLER：太棒了，这是 IT 人员梦寐以求的。最后，我有一个问题。我听说了你的一些传闻，我只是想弄清楚。

TOM GILLIS：那可能只是传闻，我希望…我不知道人们都在说些什么。

JENNIFER GEISLER：我要让你难堪了，也许它并不是你所想象的那样坏，因为我会挑选那些比较小打小闹的传闻。

TOM GILLIS：是什么？

JENNIFER GEISLER：据说你开的是电动汽车？

TOM GILLIS：一台电动汽车，这是真的，不用汽油，它叫特斯拉，所以…

JENNIFER GEISLER：特斯拉？

TOM GILLIS：是的，我认为它是地球上最酷的汽车。

JENNIFER GEISLER：我听说它们的速度很快。

TOM GILLIS：是的，没错。但只有一个方法弄清楚它能跑多快。

JENNIFER GEISLER：坐着它兜风？

TOM GILLIS：是的。

JENNIFER GEISLER：既然你现在乐于说“可以”，我们现在应该去兜风吗？

TOM GILLIS：让我们把“不行”转变为“可以”，我们去兜风吧。

JENNIFER GEISLER：好吧，我们走，谢谢。

TOM GILLIS：好的，谢谢你。

JENNIFER GEISLER：我们去兜风。

TOM GILLIS：走吧。

VOICEOVER：仅限直播节目，观众可以向在线专家提出问题。只需输入问题，点击提交，然后定期点击刷新就行了。

ROBB BOYD：僵尸程序解剖，这让我想起了高中时解剖青蛙的情景，青蛙被钉在桌子上，四肢张开然后我们开始解剖它。

JIMMY RAY PURSER：然后害怕得头发都竖了起来。

ROBB BOYD：现在想起来还是害怕，不过你的发型很好看，但是…那么， 僵尸程序解剖，僵尸法医鉴定，考虑到观众关心的问题，我首先想到的就是：如果我觉得这台电脑被感染了，我应该怎么办？它是网络上的一个用户，我可以对它

进行物理访问，我能否简单地把病毒清理了，然后永无休止地杀毒和重装电脑？我觉得这场战争我永远不会胜出。

JIMMY RAY PURSER：你知道吗，伙计，这就像在沙滩上挖洞，我是说，你挖出的沙子越多，就会有越多的沙子掉回去，是吗？这是一场无休止的战争，所以，不要错过任何能让你了解僵尸程序如何运行的机会，要对它进行解剖。如果我们发现网络中出现了被感染的电脑，而且它能够让我们在沙盒中运行它，或者这是我们故意让它感染的电脑，我们就要认真分析这些僵尸程序并弄清楚是什么使它们运行，是什么使它们起作用，为什么它们那么厉害，以及为什么如此难以阻止它们传播？ 为什么阻止病毒攻击和拒绝服务攻击是小菜一碟？也许不是小菜一碟，但是比阻止僵尸程序攻击较为简单，僵尸程序会让人产生恐惧，伙计。

ROBB BOYD：没错。这当中大有学问，我们已经说过了。比方说，我这台电脑被感染了，你说我要进行处理，我第一步要做些什么？

JIMMY RAY PURSER：其一，在我们开始之前，我要提及一个加拿大人，罗恩鲍斯，他运行着一个叫 scullsecurity.org 的网站。他在上面有一个博客。而且他写了一篇很好的指导文章，如果你是解剖僵尸程序的新手，那就登录他的网站 scullsecurity.org。遵照上面的僵尸程序解剖步骤，他把僵尸程序解剖分成了四部分。他是一位优秀的程序员，他在上面发布了很有用的信息，你可以浏览这些信息并自学。所以这真的非常了不起，他的网页上甚至有僵尸程序供你下载，所以…

ROBB BOYD：下载僵尸程序。

JIMMY RAY PURSER：没错，所以这很棒，你可以练习…

ROBB BOYD：用它去做我们待会要讲到的事，可以吗？

JIMMY RAY PURSER：都是一样的东西，伙计。所以这真的非常有趣。

ROBB BOYD：给我们演示一下我们要了解什么。

JIMMY RAY PURSER：我们要进入网络并假设它被感染了，明白吗？我们让电脑在沙盒环境下运行，我们就可以开始对它进行解剖，我们要了解是什么让这台电脑感染了？僵尸程序的特别之处是它能与主控机进行交流，对吧？命令与控制组成了僵尸程序。这就是为什么它们如此难以发现，因为它们很安静，除非收到了指令，如果你发出了指令，它们就会大显身手。所以，我要找到哪个是运行的监听器，虽然僵尸程序都很隐蔽，但它肯定会有一个监听器，我们必须要把它找到。我们来看看所有这些连接，看看这个 TCP 连接，它的端口有四个 7，它是第一个值得怀疑的。

ROBB BOYD：它跟其他数值完全不同，对吗？

JIMMY RAY PURSER：是的，我甚至可以在 Google 上搜索到端口号，你会发现它未必是分配的数字。任何超过 1024 的数字都值得怀疑，因为它不常见。所以我看到它就会觉得，“奇怪了，都是 7，这可不常用。”

ROBB BOYD：很多僵尸程序并非那么容易就能找到。

JIMMY RAY PURSER：是的，没错。

ROBB BOYD：但是这仍然很关键，是吗？因为至少我们可以先易后难嘛，，对吗？

JIMMY RAY PURSER：是的，没错，你说得对。这个僵尸程序很明显，它无处遁形。

ROBB BOYD：低级的僵尸程序。

JIMMY RAY PURSER：但是它能方便我们开始进行一些分析，开始解剖僵尸程序的时候，我们必须查看两样不同的东西。我们要查看它的运行时间以及它现在在干什么，然后我们将程序代码逐条分解，弄清楚它的运行原理。僵尸程序虽然很小，但是你仍然要面对大概一千行左右的代码。它是连续的，明白吗？所以，所以我们要逐条将其分解。 好了，我们在这里尽可能演示多一点和它好好玩玩。现在，我们的第一步是分析运行时间。我们要弄清楚是什么在监听 777 端口。通常来说，我们首先要做的，是到微软网站上下载 Windows 调试工具，网站上有大量这样的工具，有 32 位的，也有 64 位的。我喜欢 404 版，它比新版的要旧一点，但是它的功能似乎更好，这只是我个人的意见，有些人喜欢新版的，但是，伙计，我还是使用 404 版的，它还没让我失望过，至少在做这个演示之前，我们来看看吧。

ROBB BOYD：选择调试代码要像选择雪茄一样挑剔。

JIMMY RAY PURSER：那是真的。首先我们要做的是连接到那个进程，这是一个 RUNTIME 进程，我们要现场进行分析，所以我们要查看这台电脑上正在运行的一切进程。对于可执行文件我们可以不假思索地忽视它，虽然不是绝对，但大部分时候，可执行的文件不会受感染，因为它们很难附着，它们的运行是选择性的，通常，如果我向上面附着了一些东西，它就会出现诊断错误，也不再能启动执行。所以大多数人…或者说大多数编写僵尸程序的人不会把僵尸程序附加在可执行文件上，他们大多数会把僵尸程序附加在 Rundll 程序，它也是一种可执行程序。但是我要找的是 Rundll 库，里面有我所有的 Dll 文件，而 Rundll32 则

是很大的一个程序。

ROBB BOYD：关键点。

JIMMY RAY PURSER：它非常庞大，所以那就是我的目标。我们把它打开，我要做的第一件事，就是查看那个系统里有什么。我可以看到那是一个看起来很有趣的 DLL 文件。这个文件名我认不出来，通常来说我要找的文件其文件名会有数字，或者是一个伪装的系统文件。里面可能有很多东西。它看起来很可疑是因为我不知道它是什么。我一般都清楚自己的系统以及系统上运行着什么。

ROBB BOYD：多数优秀的管理员都知道他们的系统上运行着什么，虽然不是面面俱到，但是…

JIMMY RAY PURSER：不，不，但是，如果你发现了可疑的东西，但是你仍然不确定，是吧？所以我要测试它，弄清楚它是什么。

ROBB BOYD：我们下一步要干什么？

JIMMY RAY PURSER：我们加载这个程序并运行它，不，不保存，好了，出来了一大串数据，一连串的代码，这让人看起来有点头晕。这些是我分配的所有程序，它们被附加到 Rundll32 进程上，不，这些是我载入模块的时候出现的子进程，毫无疑问它们都是 Dll 文件。大部分的僵尸程序在某种程度上都是 DLL 文件，因为它们要安静地运行，它们的运行极为高效，我要找的…就是这个，Windows system32。我想“它在我们 system32 驱动文件里运行”但是，同样，它也值得怀疑。我想做的就是输进一个断点，我知道它在监听 777 端口，是吗？我们在这里看到了。这有一个正在运行的监听器，我要附加并激活那个僵尸程序，但实际上它对电脑没影响，我要让它觉得电脑要和它交流，所以我要输入一个断点。

ROBB BOYD　　It's like a pause button at a certain point?　　像是在某点上的暂停按钮吗？

JIMMY RAY PURSER：十分贴切，我们把它们称为断点，所以我要输入断点接收，断点…

ROBB BOYD：这让我想起一部不错的电影，《惊爆点》，

JIMMY RAY PURSER：确实是部不错的电影啊，？我希望他们会出续集。

ROBB BOYD：很超前。

JIMMY RAY PURSER：没错，千真万确。言归正传，我现在已经把断点附上去了，同样，它也会产生很多文件，看起来都像是奇怪的错误，不用担心，一切都很正常。我在查看断点列表以确保断点附加上去了，好的，很好，看看这里，它已经附加到 Windows system32，我得说这一点非常重要。这就是我们附加到这个僵尸程序上的，我的断点列表会显示出来，好的，这是断点集合，这是它的存放地点，现在我们继续运行这个程序。输入“G”，运行调试器，现在你在下面可以看到“调试器正在运行”，现在我让它运行了，系统觉得一切都很好。我们继续下一步，把我们熟悉的 Telnet 附加上去。清屏，输入 Telnet，local host，把它附加在那个端口号上。现在…看看这个，我们受到了攻击，把它们附加上去后，系统立刻就受到了攻击，这让我知道我找到了那个僵尸程序，我预料到那个 DLL 文件就是僵尸程序，所以我把断点输了进去，再把 Telnet 附加上去，僵尸程序会对附加在上面的任何东西作出反应。那就是僵尸程序的致命弱点，因为它们要交流，特别是在 TCP 上，它要启动 TCP 程序，任何东西附加在它上面，它都会回应。

ROBB BOYD：这是信息交流流程的基本部分。

JIMMY RAY PURSER :没错 ,这些规则不会改变 ,是吧？这就助了我一臂之力，所以当我找到…如果那里没有受到攻击，我会想“继续搜索吧”。也许我要寻找这里面的另一个断点。

ROBB BOYD：从我们所看到的来说，这个僵尸程序没有独特的活动，除了和我们连接上了，是吗？

JIMMY RAY PURSER：现在我们和它连接上了，我们知道系统受到了攻击，看看这里，"断点 0 攻击"，我知道我找到了控制那个僵尸程序的 DLL 文件，这非常棒 。下一步我要弄清楚它在内存的哪部分运行，输入“K”，输入“K”后，堆栈将会显示出来，它会告诉我它在内存的哪部分运行。通常来说，不管是哪种僵尸程序解剖，我的下一步都是把这些数字写下来，因为当我进行静态解剖时，我要用它们作参考。这一步的分解，也是僵尸程序解剖的关键之处。

ROBB BOYD：这样做的目标就是让你得到可以用来进行交叉对比的信息。

JIMMY RAY PURSER：没错，我发现…我知道系统里有一个僵尸程序，我也知道那个僵尸程序在 7777 端口监听 ,现在我要找到这个僵尸程序所处的 DLL 文件，现在我已经知道了，然后我可以分解这个文件，我把它打开，附加到可执行文件上，这里有个小文件夹，选择“所有文件”，点击这个 DLL 文件，它恰好就是桌面上那个文件。

ROBB BOYD：这不是很方便吗？

JIMMY RAY PURSER：连续点击“下一步”，所有的东西都会上载上来，看，可以了。我们加载了所有东西准备进行解剖 ,现在我们来看看这个僵尸程序是什么，

它是由什么组成的，我们可以拉到下面。我知道我们的时间不多了，我在这里只想演示几样东西。一件非常重要的事情，就是看清楚我在哪里创建第一个互斥。互斥所在的地点就是我启动这个程序和监听器的地方，所以我们可开始解码这个僵尸程序并弄清它的行为，看看这个。这是一个很有趣的名字："liuhong -061220"

ROBB BOYD：那是一个签名吗？

JIMMY RAY PURSER：通常来说那是编程人员留下的信息，很多编写僵尸程序的人会把一些东西写到上面，比如"思科技术达人"秀"最棒"

ROBB BOYD：他们总是很自负。

JIMMY RAY PURSER：总是。他们总会以某种方式写上签名。

ROBB BOYD：你没有发现写着那句话的僵尸程序，是吗？

JIMMY RAY PURSER：发现过一次。

ROBB BOYD：是詹妮弗编的吗？

JIMMY RAY PURSER：我编的。

ROBB BOYD：好的。

JIMMY RAY PURSER：但是詹妮弗花了很多钱来让我编写它，但是你可以看看这些偏移量，稍微弄清楚它们来自哪里，"Liuhong"听起来像是一个中国人编写的僵尸程序，是吗？或者可能是有人想让它看起来像个中国人编写的僵尸程序。

ROBB BOYD：好啦，我们没有僵尸偏见，所以…

JIMMY RAY PURSER：谁知道呢？谁知道？谁都说不准。

JIMMY RAY PURSER：但是关键的一点，就是查看这里的参考代码，现在我就可以开始逐步地，逐条地分析和解剖这个僵尸程序，因为我清楚地知道我确实找

到它了。对任何一种僵尸程序解剖最困难的事情就是把它找到，一旦我找到了它以及调用它的 DLL 文件，我就可以进入里面，把它分解开来，解决它，控制它，和它玩玩，并彻底地了解它，你会发现不用十分钟就完成解剖，根本不用多少时间。

ROBB BOYD：利用免费工具吗？我是说，多如牛毛…

JIMMY RAY PURSER：免费工具，分文不用，分毫不损。

ROBB BOYD：不错，绝了，真是好东西。这就是僵尸程序的解剖，节目附录的网页链接里还有更多信息。

JIMMY RAY PURSER：我们肯定会把更多东西放到节目附录里面。

ROBB BOYD：因为这是一个说不完的话题。

JIMMY RAY PURSER：说不完，千真万确，它是煅炼技能的好方法，这点是肯定的。

ROBB BOYD：我知道，非常好的东西，谢谢。

JIMMY RAY PURSER：马克-冈特瑞普，欢迎来到思科技术达人“秀”，伙计。

MARK GUNTRIP：你好，吉米-雷，很高兴能来到这里

JIMMY RAY PURSER：马克，你要和我们谈谈 ScanSafe 方案，是吗？

MARK GUNTRIP：没错。

JIMMY RAY PURSER：我有一些问题，显然，我不知道我是否真的相信，所以我希望你能来这里说服我，让我觉得这是个好主意。因为我已经有一个方案在做你们做的事，但是我们边说边探讨，我们来看看你有什么东西。

MARK GUNTRIP：好的，希望这个环节结束时能让你相信，好吗？

JIMMY RAY PURSER：我们不妨一试。

MARK GUNTRIP：好，这就是 ScanSafe 的业务概述，我觉得在这里有几件关键的事情：没错，我们提供的是网页过滤方案，我们提供的是云中的网页安全解决方案。如果你把预置型解决方案与我们在“云”中所做的事情相比较。觉得找到目标用户的关键就是弄清楚什么是用户基础。所以，不管你是在总部的办公大楼里，还是在环游世界，还是在用黑莓冲浪，你都能得到一致的安全策略，一致的安全方案，不管你是谁以及你如何连接互联网互联网。

JIMMY RAY PURSER：好吧，伙计，但是我正在使用 IronPort，我不知道这个和 IronPort 有什么区别。

MARK GUNTRIP：这是一个很好的问题，从思科的角度来看，这在很大程度上都是选择问题，有很多客户，很多公司喜欢他们的预置型解决方案。你可以从思科买到它。但也有很多公司都想得到云安全服务，就像分析师们所说的，它是增长速度最快的安全部署选择。

JIMMY RAY PURSER：没错，云安全很热门。

MARK GUNTRIP：现在你也可以从思科得到它。

JIMMY RAY PURSER：好，好，好，我同意你所说的。

MARK GUNTRIP：当我们开始把它们结合的时候我们会把这两样东西合二为一。

JIMMY RAY PURSER：好的，我明白，不错，不错。

MARK GUNTRIP：在这里我只说几样关键的东西。嗯…用户粒度，我们会配合你们的认证服务，这是意料之中的事。

JIMMY RAY PURSER：是的，我明白你的意思。

MARK GUNTRIP：你可以继续用你的策略，没错。对于这个策略，网址过滤很久之前就存在了。所以，我们的服务内容领域远不止于此。我们看看动态网页分类，这些网页我们以前可能没见过，可能它们的存在了为时很短很短，我们要查看网页上的内容，弄清楚那是什么类型的网站，然后我们就可能应用策略。

JIMMY RAY PURSER：你们怎么做？

MARK GUNTRIP：我们…

JIMMY RAY PURSER：你有介绍怎么动手的幻灯片吗？

MARK GUNTRIP：我们会说到那一点。

JIMMY RAY PURSER：好，好，好

MARK GUNTRIP：我们会说到那一点，别催我。

JIMMY RAY PURSER：好吧，伙计。这是什么态度？

MARK GUNTRIP：我们再看看融入搜索引擎方面，很多人通过搜索引擎访问网页内容。如果你看看搜索引擎结果页面，不管是谷歌、雅虎还是必应，在每条搜索结果旁边都有一个图标，上面标明这条结果是符合政策，还是违背政策，它是否有恶意内容？所以在你点击那个链接之前先已经先行一步， 在病毒攻击你的网络前就把问题解决了。

JIMMY RAY PURSER：这些图标指示清晰吗？普通的用户能否分辨网页的好坏？

MARK GUNTRIP：无比清晰，复选标记，红色大 X，一只甲虫的图片。

JIMMY RAY PURSER：那确实是很简单。

MARK GUNTRIP：不错。

JIMMY RAY PURSER：好的，好的，我明白你说的话。

MARK GUNTRIP：大老粗都看得懂。我们再看看安全问题，这个问题我很想详细阐述，我们要如何处理零日攻击威胁，还是从反病毒软件谈起把。但是我要省略这部分，稍后再作更为详细的解说。

JIMMY RAY PURSER：好的，听起来不错。

MARK GUNTRIP：就像你设想的那样，所有这些管理都是通过网页方式实现的。我们在“云”中，但是你不会失去任何控制，你通过网络浏览器做你想做的事。它控制的是“云”而不是你身旁的主机。

JIMMY RAY PURSER：好的，非常好。

MARK GUNTRIP：然后我们看看报表，我们花了很多时间与精力来开发它，同样，我想详细地阐述它，但不是现在。

JIMMY RAY PURSER：好的。

MARK GUNTRIP：我想卖个关子，明白吗？

JIMMY RAY PURSER：我明白，伙计，明白。

MARK GUNTRIP：我们接下来看看全球基础设施。简单来说，我们在世界各地有许多数据中心，至于质量，我们建造的时侯就既重视了数量也考虑了质量。我觉得关键的一点就是，当你面对一个基础设施，你会想的是：它是否牢固？它是否可靠？我可以信任它吗？

27:17

JIMMY RAY PURSER：当真？

MARK GUNTRIP：它能保证公司网站链接的安全吗？如果网站链接出现故障，就会造成你的经济损失，这个基础设施的正常运行时间长达七年。

JIMMY RAY PURSER：确实是很了不起，伙计，对于任何数据中心来说，它真的…不错…不错。

MARK GUNTRIP：我们在里面有大量的后备信息，简直让你难以置信。

JIMMY RAY PURSER：那可是七年时间，伙计，很长的…好的，继续，那真是好东西。

MARK GUNTRIP：好。

JIMMY RAY PURSER：好极了，我们说到了精彩部分。

MARK GUNTRIP：没错，这就是我想向你展示的。

JIMMY RAY PURSER：好的。

MARK GUNTRIP :这是 ScanSafe 名符其实的安全架构 ,我们用它来保护用户，它补充了反病毒软件的功能，这是一个流程图，我会给你说明。

JIMMY RAY PURSER：开始吧。

MARK GUNTRIP：好的。这是网页，用户想要得到里面的信息，而这边则是想得到信息的用户。

JIMMY RAY PURSER：好的。

MARK GUNTRIP：对于这个网页，我们不会去查看它的网站，也不会去查看它的网页，我们查看网页上的每一条内容。

JIMMY RAY PURSER：每一个元素。比如…

MARK GUNTRIP：每一个元素。

JIMMY RAY PURSER： Flash ，PDF

MARK GUNTRIP：没错，还有 HTML，图像，网页上所有的东西。

JIMMY RAY PURSER：Java 语言？

MARK GUNTRIP：脚本，是的，所有东西。如果你查看 PDF 文档的话，你一定可以查看在里面运行的脚本。

JIMMY RAY PURSER：没错，伙计，那是真的。

MARK GUNTRIP：所以我们把每一个网页分解成各个不同的组件，把它完全分解。

JIMMY RAY PURSER：好。

MARK GUNTRIP：一旦我们得到这些组件之后，不管有多少种组件，我们都会把所有信息传送到我们称之为爆发性威胁检测中心的地方。爆发性威胁检测中心现在大概有 26 种不同的扫描码，扫描码是高度集中的网页内容分析引擎，而且不同扫描码分析不同内容。

JIMMY RAY PURSER：真的吗？好吧。

MARK GUNTRIP：所以我们有 Java 语言扫描码，有 Windows 可执行文件扫描码，Flash 文件扫描码，PDF 文档扫描码，它们各自分析特定的一种内容，各司其职。

JIMMY RAY PURSER：它们可以分析…好的，明白。

MARK GUNTRIP：它们唯一的任务就是分析那种内容，我们之所以能在云中做这些事情有几个原因，因为如果用传统部署方案去做这些事较为困难。第一个原因是我们有大量的数据。

JIMMY RAY PURSER：没错。

MARK GUNTRIP：我们每年都会接收到数十亿个网页请求，不，是每一天，每天数十亿个网页请求，我们在 2009 年收到了大概一万亿个网页请求。

JIMMY RAY PURSER：真的吗？

MARK GUNTRIP：而且我们每天都接收大量不同的数据，大概来说，我们每天接收五千万个各不相同的 Flash 文件。

JIMMY RAY PURSER：不可能，各不相同的？

MARK GUNTRIP：各不相同的 Flash 文件。

JIMMY RAY PURSER：天啊，厉害。

MARK GUNTRIP：每天接收超过两亿份不同的 PDF 文档，所以我们有一个很大的数据集来让我们建立起这些扫描码来分析这些数据。

JIMMY RAY PURSER：不可思议，好吧。

MARK GUNTRIP：我们用几种不同的方法进行分析，第一种是通过检查有没有异常情况，这个文件看起来正常吗？所以我们就有了这个文件异常情况扫描码。它唯一的任务就是查看这些文件并分析它是否正常，它有没有问题。

JIMMY RAY PURSER：所有这些文件，抱歉手指碰到屏幕了，但是这些 Java 文件和 PDF 文件最终都汇集到这里吗？

MARK GUNTRIP：它的工作是查看那些看似安全的文件，查看 GIF 文件，以及查看那些很多系统都不会进行分析的各类文件。也许它会分析到一个 GIF 动画文件，既然是 GIF 动画文件，那它有多少帧呢？如果只有一帧，这就有问题了。

JIMMY RAY PURSER：对于 GIF 动画文件 ？

MARK GUNTRIP：没错。所以它会查看这些文件并分析：它看起来正常吗？分析就基于我所拥有的知识以及对内容的了解，分辨这个 GIF 文件是否正常。

JIMMY RAY PURSER：好。

MARK GUNTRIP :很简单 ,但是如果你没有这么广泛的查看能力 ,你就做不到。

JIMMY RAY PURSER：合情合理，我明白这一点，因为我也是一个程序员，所以我知道这些东西里面都有程序设计模板 ,规则以及开发工具箱 ,这让你能够使它们相互转变，我明白你所说的，这说得通，这可能比那个更为详尽，好的，我听明白了，很不错。

MARK GUNTRIP：不错。下一步，分析完毕之后，就是开始把它分解，我们不妨做更详细的分析。

JIMMY RAY PURSER：没错，这就是难办之处。

MARK GUNTRIP：然后弄清楚：这个文件的设计合理吗？它是好，还是不好？看看这个 Windows 可执行文件，我可以把它连起来，以它举例。那么，我们要再次提到查看能力 ,如果我们要分析 Windows 可执行文件 ,那就查看它的内容，如果它只有三部分或更少，那么它有七成的几率是恶意文件。

JIMMY RAY PURSER：好的。

MARK GUNTRIP：同样，你可以很快地完成它。

JIMMY RAY PURSER：好，好。

MARK GUNTRIP：所以，我们查看…

JIMMY RAY PURSER：我明白，伙计。

MARK GUNTRIP：我们查看它并分析：它看起来有问题吗？然后我们再查看它

的内容并分析：它的内容有问题吗？但是我们第三要查看的是该文件的行为。特别是当你开始查看脚本的时候，即 Java 脚本，甚至是 Flash 和 PDF 文件内部的脚本，查看它们的行为元素，弄清它们想干什么。

JIMMY RAY PURSER：好的。

MARK GUNTRIP :我们有一个浏览器 ,它模拟最终用户的浏览器 ,上面有 cookie 程序及其他一切东西，它处在我们的数据中心，用于运行这些脚本，让它觉得自己达到了最终目标。它会迷惑脚本，让它做想要做的事。

JIMMY RAY PURSER：就像处在一个沙盒里。

MARK GUNTRIP：没错。

JIMMY RAY PURSER :好的。我们还剩下大概一分钟 ,我们正在分析这些文件，分析完毕后，我们又该怎么办呢？

MARK GUNTRIP：分析完毕后，所有东西都传送到 Meta 扫描仪，它考虑所有这些意见之后，再确定文件里是否含有恶意内容。那就是反病毒软件跟我们的处理方法的最大不同之处，我们的世界里不只有黑白两种颜色，我们有 26 种不同的意见。

JIMMY RAY PURSER：所有这些分析数据发挥了重大作用。

MARK GUNTRIP：我们考虑所有意见后才会说“这条内容是好还是坏？”我们努力覆盖其中的灰色地带。

JIMMY RAY PURSER：这真的非常棒。好的，马克…

MARK GUNTRIP：而且它是双向的。

JIMMY RAY PURSER：它是双向的吗？

MARK GUNTRIP：通过对恶意软件反向查找，我们可以阻止这条信息。

JIMMY RAY PURSER：那就是说你知道某台电脑是否感染了。

MARK GUNTRIP：是的。

JIMMY RAY PURSER :马克 ,你知道吗？这真是非常棒的方案 ,伙计 ,我得说，你说服了我，这确实是很棒的方案，我非常欣赏。如果你们想得到 ScanSafe 的更多信息，你可以登录…？

MARK GUNTRIP：你可以登录 scansafe.com，也可以登录 cisco.com，找到网页上的云安全一栏，上面讲的都是这些。

JIMMY RAY PURSER：马克，谢谢你，伙计，真的非常感谢你来到思科技术达人“秀”。

JIMMY RAY PURSER：马克-冈特瑞普，欢迎回到思科技术达人“秀”。

MARK GUNTRIP：谢谢你，吉米-雷，很高兴再次来到这里。

JIMMY RAY PURSER：马克，我们…你想谈谈 ScanSafe 的 WIRe，老实说，伙计，我讨厌网管，我讨厌它的方方面面。但“云”的糟糕之处在于，它是“云”，能见度有限，所以虽然我的网管可能很差，但在“云”里它可能更糟糕。但是你认为 WIRe 不会出现这种情况？

MARK GUNTRIP：那就是我们开发 WIRe 的全部原因，WIRe 代表网页智能报表。但我们开发它的目标就是：如果你想把网络加入“云”中，你不必承受低能见度的痛苦。事实上，我们能增强你习以为常的传统方案。

34:06

JIMMY RAY PURSER：这可是一项难题，伙计，你得证明给我看，老弟。

MARK GUNTRIP：好的，好的。我们看到的一切都是实时的，对吧？这是一个实时系统，它跨过互联网传送，高在“云”端。

JIMMY RAY PURSER：没有预录的动画演示或者什么戏法之类？好的。

MARK GUNTRIP：没有，没有那样的东西。

JIMMY RAY PURSER：好的，好的。

MARK GUNTRIP：我会很快地演示一遍。

JIMMY RAY PURSER：好吧，我们看看。

MARK GUNTRIP：首先，这是一个标准的报表生成软件包，是吗？你可以保存自定义报表 ,实际上可以保存无限的自定义报表。然后在下面 ,我们有预录报表，预定义报表，我点击其中一项。处在“云”中的巨大好处就是，特别是当你查看预先定义报表的时候，我们可以把它添加到随时需要的报表上。不用更新，这套软件服务不需要那样的东西。

JIMMY RAY PURSER：这一切都在托管模式下运行吗？我不用在我的电脑上运行任何软件？

MARK GUNTRIP：这只是你的浏览器，我们用的是火狐浏览器。

JIMMY RAY PURSER：火狐浏览器？好啊，很棒。

MARK GUNTRIP：所以我们把存储器，数据库及一切你要购买和维护的东西都放到了“云”里，事实上，WIRe 的整个基础设施就是一个固态存储设备。

JIMMY RAY PURSER：真的吗？

MARK GUNTRIP：它是前端硬件 I/O 端口的，它的建造…

JIMMY RAY PURSER：了不起。

MARK GUNTRIP：基本上像是建造一个有数百万用户的跨国公司的报表基础设施，建造如此强大的基础设施，人们就不会坐在那里翘首以待了，对吧？

JIMMY RAY PURSER：是的，我知道。

MARK GUNTRIP：你会坐着等待报表，但你不会坐着等待网络服务。所以，如果我们通过浏览器提供这些报表，你的动作最好还是快一点。

JIMMY RAY PURSER：没错，基于网络的东西，通常都会有些慢，就算是本地网络也是如此，但这个…你是从远程数据中心得到这些东西的？

MARK GUNTRIP：对。

JIMMY RAY PURSER：好吧，没问题，没问题。

MARK GUNTRIP：没错，没错。这是一份很普通的报表，它是前面 24 小时的整体概览报表，同样…

JIMMY RAY PURSER：它只是总体报表，说明你的网络上发生了什么。

MARK GUNTRIP：对，没错。你想要漂亮的图表吗？我们有漂亮的图表，我们可以拆分这个饼状图，总之，应有尽有。

JIMMY RAY PURSER：真的很棒。

MARK GUNTRIP：是的，你甚至可以旋转它，我不想让你太兴奋，所以我不会那样做。

JIMMY RAY PURSER：如果你那样做的话，有些经理就会经常问你要更多的图表，伙计。

MARK GUNTRIP :我们得到了这份靓丽、高级的报表 ,我们再看看上面的标签，这就是我们开始进行信息分析的地方。所以，你可以查看前面 24 小时的，甚至

是前面 12 个月的，如果你想看的话，你可以查看前面 12 个月的记录分析一下发生了什么事。

JIMMY RAY PURSER：可以保存那么多记录吗？天啊，太多了。

MARK GUNTRIP：你可以选择每隔五分钟看一次。

JIMMY RAY PURSER：真的吗？

MARK GUNTRIP：这里所有的记录基本上…我之所以称它为实时，是因为它是两分钟前的记录。

JIMMY RAY PURSER：我要问一下，我能看到的最快最新的记录是什么时候的？两分钟前，伙计，这真是…

MARK GUNTRIP：如果你在 11 点 02 分点这个按钮，你可以看到全球用户在 11 点钟时的一切记录。

JIMMY RAY PURSER：全球用户？

MARK GUNTRIP：全球用户。

JIMMY RAY PURSER：厉害。

MARK GUNTRIP：你现在在圣何西，有些人可能在新加坡，悉尼，不管哪里，你在两分钟内都可以看到他们的使用记录。

JIMMY RAY PURSER：听着，有一点事情让我觉得“云”里的网管不合情理，“比如说，因为，我数据都在那儿。为什么我没有好的管理程序来发掘这些极为有用的信息呢？所以…了不起。

MARK GUNTRIP：你要的就是这个。

JIMMY RAY PURSER：很棒，我得说。我现在知道为什么…我是说，一定要花

很多钱来建立数据中心，固态存储驱动器及大量其他设备。

MARK GUNTRIP：这是一项很大的投资，这是为所有 ScanSafe 客户提供的标准服务，网页过滤，网页安全，这些都是标准服务。

JIMMY RAY PURSER：好的，不错。

MARK GUNTRIP：我们来看看这些标签，但是在看之前，我要快速添加一个过滤器，点击它就可以了，好了，“类别等于…”这个类别。它里面有着很大的带宽。

JIMMY RAY PURSER：是的，没错。

MARK GUNTRIP：我们再点击“时间分析”, 这是查看相同数据的另一种方法，进行这一步时，你可以看到过滤器也跟着运行，这种设计便于使用。我们查看 24 小时内的报表时，可以知道发生了什么记录，但是你不知道那是什么时候发生的，下一步是弄清楚“这件事是什么时候发生的。”带宽出现了一个很大的峰值，我们查看一下就可以轻易得出结论：好的，这大概是在下午 3 点时发生的。

JIMMY RAY PURSER：好。

MARK GUNTRIP :这是在工作日发生的，我不能置之不理。对于这个时间分析，我们的客户喜欢的另一项用处就是查看趋势。

JIMMY RAY PURSER：当然，当然。

MARK GUNTRIP：什么东西随着时间变化了？是吧？例如你指定火狐浏览器为唯一允许的浏览器，你可以查看之前和之后的用户代理字符串，它有没有产生影响？分析有哪些流氓浏览器，通过深入发掘找到那些用户，然后把问题解决。

JIMMY RAY PURSER：这点非常重要，伙计，有些安全警报是由某些禁止在网

络上使用的浏览器引起的。因为它们有很多漏洞，我们没办法修理它们，能缩小范围确实不错，因为它们是其他网站攻击的目标，所以这非常好。

MARK GUNTRIP：没错，没错，你可以解决掉网络上的这个危险。

JIMMY RAY PURSER：很好，很好，很好。

MARK GUNTRIP：嗯，我们看过了概况，趋势，时间分析，弄清楚了这是什么时候发生的，下一步就是深入解剖。

JIMMY RAY PURSER：这是精彩部分，伙计。

MARK GUNTRIP：是的，到目前为止我没向你展示的，是我们存储在这里面的数据量，让我看看。这是信息的另一方面，我们不但用各种方法分析它， 我们也储存了大量的数据，把滚动条拉下来，我们要看看…一些你意料之中的东西，包括你的类别，你的分组，你的用户，我们还要看看…你的…你的流入及流出文件扩展名，你的路径，你的查询字符串，这些都被储存下来了。所有 HTTP 标头信息。

JIMMY RAY PURSER：天啊，不可能。

MARK GUNTRIP：你的中介主机，响应以及请求内容类型。

JIMMY RAY PURSER：这非常美妙，因为有些人实际上…我是说，如果有人在浏览色情网站，你就能知道，他们是在主动浏览色情内容还是被拉进去的。

MARK GUNTRIP：没错，你可以看看查询。

JIMMY RAY PURSER：真的很棒。

MARK GUNTRIP：他们是在 Google 上主动搜索，还是他们上 CNN 网站的时候无辜地被拉进去了，同样，那也是信息的一部分。你不但会知道员工上过哪些网

站，你也会知道他们上那些网站的途径和原因。

JIMMY RAY PURSER：没错，当然了，这非常重要。

MARK GUNTRIP：对。我们再往下拉，你可以看到完整的网页地址，详细的用户代理字符串，现在这里面大概有 87 条不同的属性，每一条对我们的客户都有充分的适应性。你可以对其中一条作出报表，你也可以过滤任何一条，所以你基本上可以做你想做的事。

JIMMY RAY PURSER：我的天啊，好的，这确实是很了不起，我很喜欢，这是非常好的功能，伙计。

MARK GUNTRIP：看看这个，同样，我们努力让它变得简单，这里的所有东西用鼠标拖放就行，如果你想建一份报表，你可以建立它。

JIMMY RAY PURSER：好的，但是稍等一下，如果我删除了这些东西，它们不会永久删除的吧？我是说，它们是持久会话的，对吗？

MARK GUNTRIP：对。

JIMMY RAY PURSER：如果我退出了，再次登录它们也还在那里。

MARK GUNTRIP：是的，是的。如果你无意中删除了它们，你可以添加回去。

JIMMY RAY PURSER：好的，好的。

MARK GUNTRIP：这不是大问题，无关紧要。你可以建立任何东西，同样，我们也努力让它变得简单，这不是什么惊天动地的东西，因为要建立这份报表，但至少我们要让它简单点。

JIMMY RAY PURSER：你说得对，但是你不用请一个数据库管理员来处理它，你不用让人来做。因为我曾经试过无数个夜晚坐在那里，建立水晶报表和学习结

构化查询语言 ,诸如此类 ,我觉得…天啊 ,我可不是数据库管理员 ,我可以黑它，但是我不知道如何去使用它，你知道我的意思吗？

MARK GUNTRIP：说得对。

JIMMY RAY PURSER：所以…很好，不错。

MARK GUNTRIP：所以我们把它设计得很简单，这里所有的东西…我们是在用浏览器看这些东西 ,你可以把它导出 ,制成 PDF 或者电子表格 ,不管什么格式。如果你想下载它，把它交给另一个人，你完全可以那样做。

JIMMY RAY PURSER：这真是太棒了，伙计。

MARK GUNTRIP：几秒钟之内就返回了七千行，我们可以返回多达一百万行，读取一百万行，这可是大量的数据。

JIMMY RAY PURSER：没错，确实如此。

MARK GUNTRIP：它也跟我们在这里列出的一样，相同的格式，什么都一样。

JIMMY RAY PURSER：这真是…听着，你知道，这就是工具，对吧？我喜欢这种工作和处理方式，因为我有大量的数据，但是这同时也引起一个数据超载的问题。我有这么多数据，我甚至不知道从哪里着手，是吗？因为实在是太多了，是吧？就像一盘碗豆，明白吗？我是说，数据太多了，很难从中找到要找的东西，但是我喜欢我们的功能，看看这个吧。

MARK GUNTRIP :那是我们到目前为止的全部处理方法 ,包括概况 ,时间分析，深入解剖，当然除非迫不得已，没人会去分析一百万行数据的。

JIMMY RAY PURSER：当然不会，我不想那样做，那是自讨苦吃。

MARK GUNTRIP：没错。这一切都在“云”中，所有东西，它为 ScanSafe 所有，现在则是思科的，它得到恰当的管理和维护。所以你再也不用担心“我的数据库会崩溃吗？”也不用担心全球性数据库联合的困难。所有东西都在那里，你可以实时查看全球信息。你会看到报表几秒钟就会返回，而不需要一整夜，你不用点击按钮后第二天早上才看到报表出现在屏幕上。

JIMMY RAY PURSER：马克，本环节还有一分钟就要结束了，在这一分钟里，你还有什么简单轻松的功能向我们展示？

MARK GUNTRIP：还有一样我要展示的功能是…同样，这个功能也符合我们简单的宗旨

JIMMY RAY PURSER：是的，简单就是好。

MARK GUNTRIP：如果你要定期生成报表，例如每天一次，每周一次，每月一次，随便你选，假如你每周要预约 20 个报表，这 20 个报表不会发给 20 个人，最有可能的是发给两个小组，所以我们就有合成报表这个功能。所以当你预约报表时

JIMMY RAY PURSER：哈哈哈

MARK GUNTRIP：你不用预约八个时间，八份不同的报表。

JIMMY RAY PURSER：太好了。

MARK GUNTRIP：把它们分成小组。

JIMMY RAY PURSER：这真是太棒了。你知道吗，伙计？我不擅长编制报表这种事情，虽然它是小菜一碟，但如果它占用了我所有的工作时间，我将会很生气。但是…你让它变得有点太简单了，不是太简单，你让它变得对我来说很简单，非

常好。

MARK GUNTRIP：没错。你可以得到你想要的东西，但是你不用费尽千辛万苦才能得到它。

JIMMY RAY PURSER：非常棒。

MARK GUNTRIP：所以你可以决定，我想添加什么报表？所有用户报表，所有预先定义报表都在里面要，添加它，它就会被添加到列表中，我甚至可以把它上下移动。你想把它放到顶部吗？那就放到顶部。

JIMMY RAY PURSER：马克，非常感谢，伙计，这真是太棒了，我很喜欢，伙计，ScanSafe 网络信息报表，这真是非常的好，伙计，恭喜你们，我非常佩服，伙计，非常感谢

MARK GUNTRIP：谢谢，很高兴能来这里。

JIMMY RAY PURSER：我们一定要让你再来这里。

ONSCREEN TEXT： LISP——定位器/标识符分离协议。

JIMMY RAY PURSER：达瑞尔-刘易斯，谢谢你来到思科技术达人“秀”。

DARREL LEWIS：很高兴来到这里，很高兴。

JIMMY RAY PURSER：伙计，我们让你来这里谈 LISP，对于 LISP 是什么，人们有点不清楚，有些人觉得它太复杂了，它到底是什么？

DARREL LEWIS：LISP 是由思科设计的一种协议。

JIMMY RAY PURSER：噢，等等，协议，由思科设计，听起来像是私有协议。

DARREL LEWIS：LISP 的美妙之处，我想也是它的最强大之处，就是，它是一

个开放协议，思科对它没有知识产权。思科的整个开发对外完全公开，我们邀请竞争对手，邀请其他用户一起出力，它是基于 IEIF，即互联网工程工作小组的开放标准开发的。

JIMMY RAY PURSER：真的吗？这真是太好了。那么它解决什么问题？

DARREL LEWIS：LISP 用于解决路由的可扩展性问题，或说解决日益增长的互联网路由表的问题。

JIMMY RAY PURSER :让我们看看这个幻灯片 ,我想你已经准备了那张幻灯片。

DARREL LEWIS：好，…这个…

JIMMY RAY PURSER：继续。

DARREL LEWIS :这个幻灯片是要解释存在着什么问题以及问题的根源是什么，这是互联网路由表，它正在增长，朝右上方，不断增大。我们要做的，是当越来越多的站点按多宿主设计的时候避免给站点增加越来越多的路由 ,是吧？我们觉得多宿主对于一个网站来说很有吸引力。我们想让它…思科，一家网络公司，想让人们长期使用网络。我们觉得让他们这样做的同时不增加对路由表的压力很重要。

JIMMY RAY PURSER：我有两个问题要问你，我们不是用 BGP 协议解决了这个问题吗？

DARREL LEWIS：是的，目前站点利用 BGP 得到多宿主，大的网站比如 cisco.com ,或者 Facebook 或者任何一个大公司。LISP 能够提供多宿主的好处，包括故障切换，容量规划和流量工程，我们要向小型市场提供所有这些好处，他们部署起来更简易 ,而且他们不需要有 BGP 协议配置方面的高深知识就能部署。

JIMMY RAY PURSER：我得说，伙计，如果你试过设置 BGP 协议配置的话，那真的很痛苦。

DARREL LEWIS：没错。

JIMMY RAY PURSER：那么，现在问第二个问题，因为你刚好提及了它，网站多宿主服务的用户真的从大企业逐渐转向中型客户和小型客户吗？因为我们现在都要依靠互联网，我们从上面得到了很多生意。

DARREL LEWIS：是的。

JIMMY RAY PURSER：现在网站多宿主服务真的能提供给大部分的企业了吗？

DARREL LEWIS：是的，我觉得网站多宿主能吸引企业的原因有几个，首先，他们能得到更大的容量，我们想看到…人们从互联网上得到更多的东西。视频，Web 2.0，互联网上的很多东西，这增加了互联网的流量。另一个原因是，因为互联网对小企业很重要，他们要随时在线，他们希望在服务提供商链接崩溃的时候网站仍然可以使用，他们希望业务不致中断。

JIMMY RAY PURSER：当然了，伙计。

DARREL LEWIS：每天都是如此。

JIMMY RAY PURSER：所以我们发现了问题，解决方案是什么？因为我们好像仍然…我们好像仍然需要一个巨大、轰鸣的路由器和巨大的一张路由表。问题就在这里，LISP 如何去解决这个问题呢？

DARREL LEWIS：好的。LISP 所要做的就是把人们不断注入互联网的路由挑出，然后清除它们。但是如果在互联网上没有相应的路由，网站怎么能找到目的地呢？这就是最大的问题。

JIMMY RAY PURSER：是的。

DARREL LEWIS：LISP 有一个映射和封装功能，所以我们要做的就是把这些表不用路由表，而使用映射系统。然后我们有这些网站，这边的这些网站请求这个网站的位置并找到映射，然后映射结果将会返回原来的网站上。

JIMMY RAY PURSER：如果我们反复请求这些网站，我们会添加额外的访问延迟吗？

DARREL LEWIS：当一个网站与另一个网站只有第一次进行交流时才会使加入一点点延迟，第一次以后，两个网站间的交流，不管一天进行多少次，它的速度都与现在一样。

JIMMY RAY PURSER：我们再回过头来看一看，因为我们先前谈过这个问题，我们谈到的其中一件事就是，路由表规模已经增长到多大了。

DARREL LEWIS：是的。

JIMMY RAY PURSER：我在想，“天啊，它现在已经很大了”，你做的这些解释我以前从没有把它们联系在一起，而且不仅如此，而且你还不得不把路由表放在放在好几个位置呢。

DARREL LEWIS：是的，路由表不但存在于路由器软件里面，它还会被推到路由器的转发信息库（FIB），即路由器的实际硬件。所以，随着运行速度越来越快，我们向客户提供这些也越来越昂贵了。因此，互联网总体来说就变得更昂贵。

JIMMY RAY PURSER：没错，这是真的。

DARREL LEWIS：所以通过降低互联网运营费用，我们也使客户得到了更便宜的互联网接入服务。

JIMMY RAY PURSER：这真的是很棒，我们几乎真正实现了…非常少见的双赢局面，客户与供应商都是赢家。

DARREL LEWIS：正是如此，我们的目标就是鼓励客户部署，让他们得到更易使用，更简单的多宿主网站，让供应商得到更便宜，更易操作的处理器。

JIMMY RAY PURSER：好的，我们继续，这非常棒。

DARREL LEWIS：好的，我们再谈谈数据包的整个通信过程。

JIMMY RAY PURSER：我喜欢讨论这个。

DARREL LEWIS：好的。这里是通信的源，这就是在 LISP 站点上的一台电脑，这台电脑就是我们现在用的电脑，LISP 不改变主机，也不改变网站。它们有着与今天一样的 QOS，一样的安全系统，它们使用一样的防火墙和交换机。LISP 改变的是这些边缘路由器，这些 ISR 或 ASR 路由器，它们在网站的边缘运行。这个作为例子的网站指向域名系统里的目的 ,然后它发送一个数据包到网络的边缘，就像今天的网站一样。在这个网络的边缘，这个 LISP 路由器上有目的的映射，这个映射由这些出口隧道路由器控制。在这个例子中，他们把优先权设为 50-50，所以他们想让这两条链接都被网站所使用。

JIMMY RAY PURSER：负载平衡吗？

DARREL LEWIS：没错。

JIMMY RAY PURSER：不是负载平衡，而是共享。

DARREL LEWIS：负载均衡，是的。

JIMMY RAY PURSER：负载均衡，谢谢，很好。

DARREL LEWIS：所以，当这个…当 S2 把这个数据包封装时，它不会改动原

来的数据包，它会添加一个新的外部标头。这个新的外部标头有这个目的网站位置的目的标识，而这个路径定位器会把这个数据包发送到指定的路由器接口。这就保证了…数据包被发送到正确的地方，然后数据包会被解封装，没错，由 S 发送出的原来那个数据包现在到达了 D。

JIMMY RAY PURSER：这非常棒，那么…这更像是…我们现在谈的是协议，但它听起来更像是 OVERLAY 模型。

DARREL LEWIS：是的，它被加到上面。LISP 的美妙之处是，一个网站可以使用 LISP 也可以和其他 LISP 网站交流，或者与非 LISP 网站交流，它可以自己做决定。所以它被添加到上面，这会发生几件有趣的事，现在我独立于我的供应商，但关键的是，我在这里可以使用 IPv6，那里也可以使用，这里也可以，而这个内核仍然是 IPv4。

JIMMY RAY PURSER：这太棒了。

DARREL LEWIS：是的，确实是很棒，所以 LISP 可以使用 IPV4 和 IPV6，它不区分协议，我们希望互联网能得到发展，不管是使用 IPV4 的互联网还是使用 IPV6。事实上，我们想帮助网站在它们之间迁移，并让使用 IPV4 和 IPV6 协议的网站彼此交流。

JIMMY RAY PURSER：那么…我要问你一个问题，因为你从 LISP 起步时就参与其中了。我会直率地提出这个问题，它是为 IPV4 而设计然后再用于 IPV6 吗？

DARREL LEWIS：不是。从第一天起 LISP 就支持 IPV6，不论是协议规范还是我们的实施。

JIMMY RAY PURSER：真的吗？

DARREL LEWIS :是的。目前互联网上有使用 IPV4 和 IPV6 的网站在使用 LISP。不是开玩笑吧？那真是太棒了，伙计，我知道我们几乎还没谈到重点，但我真的很想知道…因为我觉得它是一项很好的技术，真的。而且我觉得我们应该开始从这个角度看待网络设计。如果我想了解关于它的更多信息或者深入了解它的精要部分，我最好登录哪些网站？

DARREL LEWIS：我觉得刚开始时最好的网站可能是 cisco.com/go/lisp，但是如果你要了解更多关于协议规范的问题和 LISP 社区，不只是了解思科，而是整个 LISP 社区，你可以登录 lisp4.net 或者 lisp6.net，如果你使用 IPv6 的话。

JIMMY RAY PURSER：很棒，非常棒。好的，我记得你告诉过我你在上面有一个 Facebook 网页，是吗？

DARREL LEWIS：我们确实是有一个 Facebook

JIMMY RAY PURSER：伙计，你们真是太时髦了。

DARREL LEWIS :我们确实有一个关于 LISP 的 Facebook 小组 ,但更重要的是，Facebook 是我们最早的测试网站之一。

JIMMY RAY PURSER：真的吗？

DARREL LEWIS :是的 ,所以你可以越过 LISP 进入 Facebook ,你不用运行 LISP，你只需登录 www.lisp4.facebook.com。

JIMMY RAY PURSER：真的太棒了，伙计，我肯定会上去看看。达瑞尔，这是非常好的东西，伙计，谢谢你来这里向我们解释这些，希望你能再次来到节目向我们提供更多资讯，因为这真是太棒了。

DARREL LEWIS：好的，乐意之极。

JIMMY RAY PURSER：谢谢你，伙计，非常感谢。

DARREL LEWIS：保重。

VOICEOVER　仅限直播节目，观众可以向在线专家提出问题。只需输入问题，点击提交，然后定期点击刷新就行了。

ROBB BOYD：每次我们上来谈到这些无边界网络安全话题时，我仍然…恕我直言…我总是觉得无边界网络安全是个矛盾说法。同时，我阅读到的资讯和我接触的客户让我觉得很多东西都已经发生了，无边界网络一词已经流行了。思科已经围绕着这个词研究一年了。你觉得客户对它有什么看法和反应呢？博客圈有让你们感到头疼的问题吗？情况到底怎样？

JENNIFER GEISLER :也没什么，我觉得他们的认识是“天啊，这已经是现实了”，因为我们觉得…我们会说“我们不能进入无边界网络世界 ”，但是我们已经进入了。我们随时随地都连接着无边界网络，而且我们想安全地进行连接，所以无边界网络安全已经成为现实，我们现在正面对这个现实。值得回味的是，思科真的经常谈论它，因为我们知道我们能帮助解决他们的问题。

ROBB BOYD：你们所做的是…正如我经常说的市场营销先于产品开发。

JENNIFER GEISLER：确实。

ROBB BOYD：或者说公共产品开发，当然，产品开发有可能早在告诉公众之前就开始了，但我现在发现技术已经紧贴着趋势了。看到技术赶上趋势时，你会说“好吧，它现在用这种方式提供了，他们使用这些先进技术让它变得简单了。”因为我觉得网络安全…人们总是说他们想要安全，只要安全不妨碍他们就行了。

JENNIFER GEISLER：没错。

ROBB BOYD： “我不想提它，我不想让它阻碍我，但是我坚决支持网络安全”，是吗？要等到出了事，大家才会注意到这个问题。所以你录了一个关于僵尸程序的节目。

JENNIFER GEISLER：是的，我觉得那很重要，因为他想要说明的在其他几个环节里也得到了说明：它并非我们所想象中的那样难。我们有一些很好的内置工具来减少这个过程中的臆测，所以你能实际地部署网络安全，而且…我要过渡到你的 BOT，很不错的僵尸程序。

JIMMY RAY PURSER：谢谢你，伙计。

JENNIFER GEISLER：不用客气。

JIMMY RAY PURSER：谢谢，它们是我亲自编写的。

ROBB BOYD：你只是涉及了冰山一角，是吧？

JIMMY RAY PURSER：伙计，只有…千分之一，只说到了沧海一粟，我只是想告诉大家怎样才能发现一个僵尸程序，如何去消除电脑上出现的假警报，并且研究一些基本的僵尸程序解剖。光是僵尸程序解剖就能录制一集节目，但可能仍然只是触及它的皮毛。希望这可以抛砖引玉，，让大家学点好东西。

ROBB BOYD :你觉得这样现实吗？让今天的客户花这样的时间去学那种程度的知识，也许只学初级程度的，因为他们觉得你所说的东西对他们要做的事很有价值，但他们都很忙，我们都很忙，对吧？而这种东西…你觉得人们…

JENNIFER GEISLER：我觉得…我觉得痛苦是刺激人去行动的好方法，如果我们感觉到了痛苦…

ROBB BOYD：先苦后甜？

JENNIFER GEISLER：是的，没错，所以我们说…很多时候我觉得我们应该对痛苦作出回应，打断痛苦的循环，燃起解决痛苦的热情，马上努力做好准备。

JIMMY RAY PURSER：关键是要知道从哪里开始，我的意思是，人们常说“我需要什么工具才能开始？它要花我多少钱？有没有好的参考网站？”一旦这片基础打好了，想做的人自然会做，不想做的人还是不会做。

ROBB BOYD：我很喜欢 ScanSafe 的马克-冈特瑞普，口音很逗，是吧？至少我们南方… 他是威尔士人，我说“天啊，我不知道你是什么士人，与我何干，伙计。”

ROBB BOYD：那地方离德州不远，你跟他录了两节很精彩的片段，很有意思。

JIMMY RAY PURSER：是的。

ROBB BOYD：我觉得它很有意思，云安全，那听起来像是另一个矛盾说法，他不是在保护“云”，说明白了，

ROBB BOYD：而是把安全当作服务来提供，或者把软件当作服务，这儿的意思是，呃，安全就是服务，客户会留意这些东西吗？我是说，这样做现实吗？我觉得它们有着本质的区别，因为我想要那些看得到能管理的安全维护设施。

JENNIFER GEISLER：我觉得“云”真的已经起步了。

JIMMY RAY PURSER：我也有同感。

JENNIFER GEISLER： 云”的运转能带来很大的价值，再说一次，现实是，如果我们要有一个安全的“云”，必须要有安全维护，否则我们不能把东西放到“云”里，是吗？

JIMMY RAY PURSER：是的，不幸的是，好像只有那些大公司才会雇佣全职的

安全维护人员，要知道，维护安全，人人有责啊。大一点的公司有网络安全维护小组来管理那些安全维护设施。有了“云”P7，我可以是一个小公司，而把软件当作服务提供，我所有的职员都带着它们出门，伙计，你知道我的意思吗？

ROBB BOYD：是看看他们的客户单，他们有很大的客户在使用这种解决方案。

JIMMY RAY PURSER：确实是。

ROBB BOYD：当我开始研究它时，因为我以前根本不理会 ScanSafe，老实说，当我们刚开始得到它们时…

JIMMY RAY PURSER：我也是。

ROBB BOYD：因为它没有…

JENNIFER GEISLER：但是你喜欢安全维护，而你却不理会它。

JIMMY RAY PURSER：那时我只是觉得它不是一个好主意，我在想“我们有 IronPort，我们到底还要这个干嘛？”

ROBB BOYD：我很高兴你当时向他问起了这个问题。但是我也看到的规模这个问题，你谈到了当你想到网络安全时，你就会想“我要保护所有的远程办公室和世界各地的数据”。然后我觉得…在通常情况下，你要部署很多安全维护设施，然后对它们进行管理，然后还要监控这些多变的东西。然后他们说到…它与 IronPort 相似的地方是，越多人使用，信息就越多，因为它被所有人分享了。

JIMMY RAY PURSER：是的。

ROBB BOYD：所有人都得到了更好的结果，但是用户的适应能力以及短时间内经历这样的部署…这只是另一种想法，它目前好像很成功。从你的顾问角度来看，你也觉得是这样吗？

JIMMY RAY PURSER：是的。

ROBB BOYD：好吧。

JIMMY RAY PURSER：绝对是的。

ROBB BOYD :你说达瑞尔刘易斯谈了…LISP ,很抱歉 ,为什么 LISP 那么难说？

ROBB BOYD：好的，它是定位器/标识符分离协议的缩写？

JIMMY RAY PURSER：是的，是的，实际上是一个天文爱好者朋友让我对它产生兴趣并研究它的，他在思科工作，叫肯-杜拉索。他说“伙计，你听说过 LISP 吗？”我说“没有，没听过。”然后我们开始研究它 ,“这真是太棒了，伙计，我们要把它带上节目，我喜欢这项技术。”我问过了身边的人，没有人听说过它，你在互联网上也找不到多少信息。所以我想“我们一定要把它带上节目，这是网络安全的变革。”

JENNIFER GEISLER：他把它带上了我的节目。

ROBB BOYD：是的。

JIMMY RAY PURSER :没错 ,你说得对。我想让最好的东西在最好的节目播出。

JENNIFER GEISLER：没错，没错，我喜欢你的思维方式。

ROBB BOYD :这是典型的情况 ,吉米-雷发掘了人们尚未意识到的东西 ,他说“伙计们，我们要帮助他们。”所以现在多了十个人知道了那个协议，收看节目的十个人，但是他又说“我们要怎样销售这件东西？”詹妮弗则有资本和团队来营销用于无边界网络的东西，我们在改变世界，亲爱的。

JENNIFER GEISLER：购买 LISP 吧。

ROBB BOYD：他们可能很快就会来敲你的门，来分享你的预算，但是…

JENNIFER GEISLER：没问题啊。

JIMMY RAY PURSER：我们把你的电话号码告诉了他们。

JENNIFER GEISLER：空集与非空集的交集仍然是空集。

ROBB BOYD：但是要谢谢汤姆吉利斯。

JENNIFER GEISLER：是的，他…

ROBB BOYD：要谢谢汤姆吉利斯，他写了一本书。

JENNIFER GEISLER：他确实是很棒，是的。

ROBB BOYD：无边界网络安全，这书名起得真合适。

JENNIFER GEISLER：是的，完全正确。我觉得他提出了一个很有力的观点，那就是：它已经出现在各个地方，它已经成为了现实，我们也可以在这方面有所作为。我不想太多地引用他书里的文字，但他确实谈到了这点，但是我建议人们去读一读这本并不厚的好书。

ROBB BOYD：好主意。

JIMMY RAY PURSER：它是一本好书。

ROBB BOYD：好极了。好了，伙计们，非常感谢，很精彩的节目。

JENNIFER GEISLER：谢谢你们。

ROBB BOYD：伙计们，非常感谢收看今天的节目，希望你们会喜欢。我们想听听你的意见，欢迎大家踊跃反馈。填写反馈问卷，告诉我们你喜欢什么，不喜欢什么，想更多了解哪些内容，再点击查看控制台上的相关链接内容。你还能在思科技术达人“秀”官方网站，以及我们的播客，Facebook, Twitter 等了解更多信息，包括我们的博客。这就是今天的节目。代表思科技术达人“秀”全体同仁，非常感

谢你的收看，下次再见。

JIMMY RAY PURSER：我们要去兜风，稍后再把车开走。

TOM GILLIS：你下车吧，让金发女孩上来。

JIMMY RAY PURSER：好吧，我就知道。