零售安全：在节省资金和金钱的同时保护客户数据

概述

零售 IT 环境面临着前所未有的技术变革。商店提出更多要求，而客户在使用店内服务时希望兼具性能和安全性。零售组织还要应对有组织的、资金雄厚的黑客，他们会利用网络和销售点 (POS) 系统中的任何弱点。许多攻击导致的不良后果就是盗取信用卡和其他客户数据。

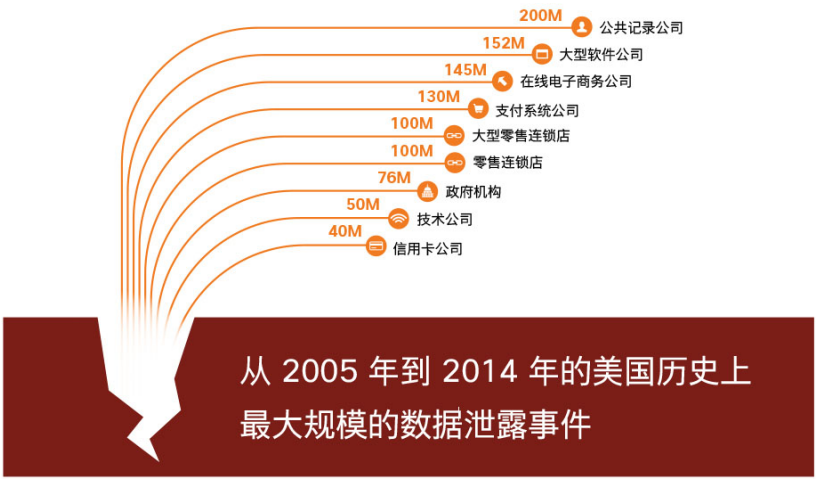
此白皮书总结零售网络所面临的挑战，并介绍提供有效、最新和可靠保护的 Cisco® 安全解决方案：思科云 Web 安全 (CWS)。

零售 IT 环境面临的威胁日益增多

给店内网络带来所需的性能和安全功能并非易事。从对店内互联网访问的简单控制，到支付卡行业数据安全标准 (PCI DSS) 的复杂合规性要求，零售组织必须积极思考如何控制网络流量。有效的安全解决方案必须提供网络控制，与此同时还能适应不断加快的店内网络变化速度。最重要的是，它必须适应威胁环境不断增加的复杂性。

不管行业和安全专业人员如何努力，零售 IT 环境中的重大攻击和漏洞率仍在不断提高。受害者有财富 10 强零售商，也有全球性的特许经营餐厅（图 1）。攻击者一直都是针对支付系统。这些漏洞使企业品牌和客户信心受损，有时导致总计高达数亿美元的缓解与恢复工作。

图 1. 美国历史上最大规模的数据泄露事件（基于攻击成本）



来源：Bloomberg、Privacy Rights Clearinghouse、Breach Level Index

店内访客 Wi-Fi 和交互式移动购物体验导致新服务量增加，例如购物应用和店内网络访问。虽然这些店内服务可以实现显著的客户价值，但也增加商店网络的复杂性并给现有的 IT 资源带来更多压力。在线服务扩大攻击面，使企业更多地暴露给搜索并利用网络漏洞的人。因此，对零售商而言，投资于保护店内和总部的客户数据非常重要。

物联网 (IoT) 是零售商必须管理的另一 IT 趋势。IoT 代表通过嵌入式技术连接到互联网的物理对象网络，同时与内部网络和外部环境进行交互。例如，根据从店内商品收集的上下文客户信息，零售商可以将有关产品的相关实时信息推送到感兴趣的消费者的设备中。

其他的 IoT 业务应用有：通过使用 RF 标签或为供应链中的供应商提供到内部系统和数据的访问来实时跟踪入站库存，从而加快业务运营。IoT 中范围广泛的设备将增加店内关键技术的数量。许多情况下，安全性并不会内置到这些设备中，可能仅在事后添加。

考虑到整个零售业中苛刻的利润率，组织面临着残酷现实：既要应对不断变化的威胁环境，同时还要为客户提供创新的、个性化的购物体验。升级 POS 系统或投资安全技术以便控制数据丢失的风险越来越有必要。为了应对日益严重的威胁环境，零售业不再袖手旁观。最近，有多个组织联合起来，共同制定“零售网络情报共享中心 (R-CISC)”计划。

零售业的薄弱点

根据 2013 年威瑞森数据泄露调查报告，2013 年，在遭受攻击最多的行业中，零售组织和餐厅位居第二。即使客户继续在数据已泄露的零售店内购物，Retail News Insider 在 2014 年的一份报告中仍建议他们可以开始使用现金而不是信用卡，而这会导致客户减少支出。

根据 Interactions Consumer Experience Marketing 在 2014 年的一份报告，有证据显示攻击者在以零售组织为目标时没有创造力。该集团发现：“与其他行业相比，攻击者在攻击零售组织时利用相对较少的方法来获取数据。” 在零售攻击中，97% 的攻击涉及支付系统篡改。

在检测安全漏洞方面，零售组织面临着巨大挑战。通常，在第三方（通常是执法机关或欺诈检测）找到异常活动指标之前，恶意软件会一直存在于零售 IT 环境中。根据 Verizon Enterprise Solutions 在 2014 年《彭博商业周刊》文章中引用的一项为期三年的研究，公司通过他们自己的监控发现漏洞的时间平均仅占 31%。对于零售商来说，这个数字是 5%。

表 1 显示了在 2014 年报道的四个最大漏洞示例，以及恶意软件在发现之前驻留在 IT 环境中多久。

表 1. 2014 年的最大网络漏洞的特征

角度	时间长度	攻击方法	故障点
美国酒品店	17 个月	“低调且缓慢的恶意软件”	技术
美国和加拿大的工艺品连锁店	8 至 9 个月	被修改的 POS 系统	流程
美国和加拿大的家居连锁店	半年期计划	用来避开检测和攻击注册的自定义恶意软件	未得到重视的安全性；不用的产品功能
在线零售交易	季度期计划	遭到黑客攻击的数据库	人员和技术

来源：Sophos、Bank Information Security、Krebs on Security、Bloomberg News、Private WiFi.com 和 Huffington Post

不断增长的 IT 能力和功能需求

零售业的 IT 网络环境越来越复杂， 而对它们的管理也日益复杂。在 IT 行业，人才短缺越来越严重，使得应对这些店内互联网连接环境时的难度加大。为了应对短缺问题，尤其是在网络安全方面，IT 部门将零售 IT 环境的管理和运营集中化。

其中一个最为棘手的问题是店内网络中存在的复杂性，店内网络最初用于将销售点 (POS) 终端连接到后端服务器和企业 WAN。这些店内网络以前用于处理很少的流量，现在服务于其他多种应用，其中包括营销、员工到内部网和互联网的访问、IoT 使用案例、警报和视频监控系统以及访客 Wi-Fi。

不断会有更具吸引力的技术为零售商上线，为客户提供无可比拟的价值并使它们成为零售商的必备技术以部署在商店内。同时，这些解决方案将会消耗更多带宽并需要更多的数据处理。更为复杂的问题是很难预测因机构而异的带宽需求。这些需求不仅取决于每家商店的规模，还取决于所使用的不同技术。

最初，大多数的店内网络的安全模式专门用来保护内部网络流量。如今，商店支持家庭网络之外的通信，这包括与业务合作伙伴、供应商和互联网的连接。

为了提供足够的安全性，要求组织在店内网络中部署新的预防性和检测控制，这可以提供更复杂的设备和用户的网络级分离、高级网络使用控制以及可接受的使用策略实施。考虑到零售业遇到的恶意软件和攻击类型，不言而喻，连接到零售网络的所有设备都处在恶劣环境下。

威胁环境是如何定义的？ 首先，攻击者对准最省力的途径，即在环境中找到立足点。这通常包括 POS 终端的中心。遗憾的是，许多领先的 POS 系统配备了商品硬件、操作系统和软件组件，但攻击者使用简单攻击即能轻松入侵。即使 POS 供应商对系统适当地修补，但修补无数台设备的运营成本非常高昂，通常需要手动更新。

POS 系统到公共互联网的传统连接会引发风险。此类设置使远程操作成为可能，其中 POS 后端系统位于不同的设施内，并且可以提供远程支持。但是，运营团队必须在简化设备管理和降低网络型攻击的风险之间做出选择。这不是合理或必要的权衡。

传统的 Web 安全网关需要在总部安装集中化的网关。每个商店或分支机构将所有流量转发到中心聚合点进行检查，然后这些流量流向互联网。考虑到店内流量（包括入站和出站）不断增加，此方法会占用大量有限的带宽。合规性也是必须考虑的一个重要因素，因为零售 IT 属于 PCI DSS 的范围。为遵守法规并通过年度评估，组织需要实施主动网络控制来保护连接，并帮助确保处理持卡人数据的系统的持续安全性。

总之，店内网络通常具备一个作用：将 POS 系统连接到企业 WAN。这些解决方案通常部署在组织的安全边界内。零售组织中涉及 POS 系统的最新安全漏洞表明，此网络架构不再适合构建或运行店内网络。

IT 环境中常见的差距

由于零售商面临解决安全问题的关键时间压力，零售企业通常认为单点解决方案可以保护重要资产。但是，一个聚合的安全模式提供的不仅仅是单点解决方案，还必须实施足够的网络安全控制来解决如今的问题并满足以后的需求。

部署到商店的直接互联网连接就证明了单点解决方案与全面的安全解决方案之间的差距。部署直接互联网连接时，即已添加新的防火墙来保护商店网络。防火墙部署在以下两种模式之一。

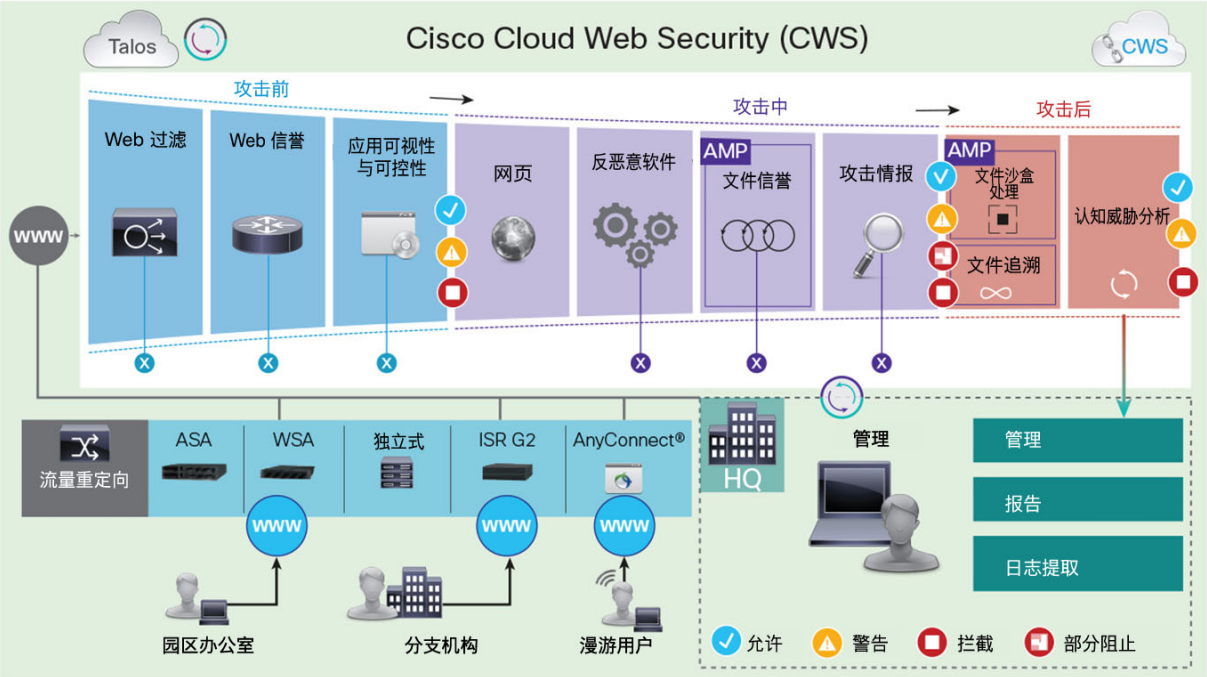
1. 可以在 WAN 路由器上设置规则，用来将受互联网制约的流量传输到新的防火墙。
2. 连接店内网络的设备可以将防火墙用作默认网关，从而取消对网络的控制或监控。部署店内 Wi-Fi 连接时，如果流量没有正确传送到检查点，就无法确保企业数据不泄露到互联网中。此外，也不能确保连续遵从可接受的使用策略。

总之，拼凑的单点产品会造成这样的局面，很难控制、发现或管理给组织带来的实际风险。

零售业面临的威胁数年来一直引起广泛的关注，例如，2006 年的重大零售漏洞泄露了多达 100 万张信用卡的数据。黑客利用店内的薄弱控制点获得信用卡和其他客户信息的访问权限。黑客一旦发现漏洞，攻击者即从侧面进入企业网络，进一步泄露私有数据。

如果黑客能够共享攻击策略并实现攻击的自动化，他们将通过链条中最薄弱的环节（这通常是指控制欠佳的零售点）瞄准大型企业。

图 2. 思科云 Web 安全的工作原理



灵活的保护和控制

思科开发的一套产品和功能可以满足零售 IT 环境的安全和网络需求。这些解决方案的范围从无线接入点、路由和交换，到基于云的高级安全服务。

图 3 提供了 Cisco CWS 购买选项的概述。

图 3. Cisco CWS 购买选项

市场领先的思科 Web 安全设备 (WSA) 和思科云 Web 安全 (CWS) 产品提供灵活的部署模式，同时实现自有设备和云交付的内容安全。选择 Cisco WSA 在总部提供网络级保护，同时为分支机构选择 Cisco CWS，这样能满足 IT 的安全需求，基本上无需为所有分支机构购买新硬件来增加保护。Cisco CWS 直接与店内技术集成，这包括思科自适应安全设备 (ASA) 防火墙、

思科集成服务路由器 (ISR) 和 Cisco AnyConnect® 客户端，让您利用现有的投资和运营支持流程获得更高的安全性和更有效的运营支持。

思科可以将互联网连接保护下移至商店级别，无需任何额外的硬件和回程流量，除非有策略规定。低风险流量直接流向互联网，而将其他流量发送到中心位置完成进一步检查。

为了防止已知和新出现的威胁，Cisco CWS 使用多种技术查找攻击，这包括传统恶意软件签名、文件和站点信誉过滤器以及病毒爆发过滤器。此外，Cisco CWS 与 Cisco Collective Security Intelligence (CSI) 集成，CSI 是思科行业领先的威胁情报功能，其中包括 Talos 安全情报和研究小组。Cisco CSI 和 Talos 帮助确保客户从无数个使用思科技术的客户中获益。

Cisco CWS 提供报告详细信息，其中包括传统的信息安全数据以及对带宽消耗和使用情况的详细分析。在带宽受限的环境中，这种可见性是用来努力实现效率的关键工具。其他的高级报告功能详细介绍了访客 Wi-Fi 浏览习惯，为在线零售商提供有关比较购物和价格检查的可见性和防御、以及攻击性内容的查看。因此，Cisco CWS 的报告功能不仅对 IT 安全团队很重要，对整个零售组织也是如此。

或许更重要的是，作为云解决方案，Cisco CWS（图 2）可以为任何组织提供轻松扩展和优化带宽的功能。这意味着实现了直接、可量化的成本节约并显著提高了组织的店内威胁管理功能的效率。这些节约是通过将针对流量管理和控制的所有处理从本地硬件分流到基于云的系统中来实现的。另外，通过使用软件即服务 (SaaS) 模式来提供基于策略的流量决策，Cisco CWS 可显著减少店内网络硬件的负载。

Cisco CWS 如何帮助零售组织

这个真实示例展示了 Cisco CWS 如何在当今的威胁环境下为组织提供保护：一个 IT 安全管理员负责保护 1,500 家连锁店，连锁店推出了店内技术以便为客户提供互联网访问以及其他多种服务。安全管理员注意到攻击者最近利用大量的高级恶意软件攻击来入侵店内系统（包括 POS 设备），希望能快速检测到这些攻击并采取有效的补救措施。许多商店的带宽有限，而且该解决方案必须优化到每家店的网络连接，使得上述挑战更为棘手。

安全管理员在每家店中都部署 Cisco ISR 边缘路由器。这些设备支持思科智能广域网 (IWAN) 功能，以便保护并优化每家店中的带宽。通过使用成本较低的互联网连接，而不是更昂贵的专用网络链路，IWAN 可以帮助管理带宽。该产品还提供顺畅的迁移路径，因此组织可按照自己的进度从专用网络链路迁移。为了确保移动设备连接到每家店中的正确网络，思科身份服务引擎 (ISE) 为店内系统提供保护，确定哪些用户和设备可以访问哪些部分的商店网络。

为了保护 Web 流量，该组织将使用 Cisco CWS 高级版提供直接互联网访问。可以通过 Cisco ISR 边缘路由器部署该功能，无需额外的硬件。Cisco CWS 高级版包含思科高级恶意软件保护 (AMP) 和感知威胁分析 (CTA)，可以通过高级威胁防御功能保护所有用户。CTA 是近实时网络行为分析系统，它利用机器学习和高级统计找到网络中的异常活动，从而检测到可能的攻击。AMP 结合使用文件信誉、文件沙盒和追溯性文件分析方法，识别并阻止网络中已存在的威胁。

使用这些思科安全产品，1,500 家连锁店现在可以管理其带宽利用率、用户访问级别、威胁防御和内容安全。这只是其中一个可能的思科安全产品组合。在这种情况下，IT 安全管理员达到了企业对其分布式零售网络提出的网络和安全目标。

Cisco CWS 的优势

对于使用集成的思科解决方案来保护网络安全的组织，可以实施通用策略，检测高级攻击和优化 WAN 中的带宽使用情况。Cisco CWS 高级版与 Cisco ISR 边缘路由器集成，也能使僵尸网络跟踪成为可能。这有助于确保 POS 设备不受威胁，可以安全地将数据传输到总部。此外，该组织还可以通过捆绑解决方案节省更多资金。

组织无需担心该解决方案中各个元素的集成，因为所有功能都设计为可协同工作。其结果是，思科预计给 IT 员工带来的节省，可能是他们花在减少配置和实施支持上的时间的 40%。该组织还从其高级、一致的全球网络中受益，因此它可以不断发展并专注于自己的业务，而不用担心试图渗透店内网络的攻击者。

总结

通过使用诸如 Cisco CWS 的支持云的工具，零售商可以显著减少运营负载，这包括监控、管理和维护他们的网络。CWS 轻易就能与 Cisco ASA 和 Cisco ISR 产品结合使用，智能地消除本地安全策略实施的需求，从而降低每家店的带宽需求。Cisco CWS 被 Gartner 视为市场的领导者，可以提供一种明智的方法来向店内网络添加最有效的安全功能，而不会增加运营的复杂性。

更多详情

有关更多信息，请访问：http://cisco.com/go/cws。

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太总部
Cisco Systems (USA) Pte, Ltd.
新加坡

欧洲总部
Cisco Systems International BV Amsterdam.
荷兰

思科在全球设有 200 多个办事处。思科网站 **www.cisco.com/go/offices** 中列出了各办事处的地址、电话和传真。

美国印刷 C11-733817-00 02/15