

360 无线入侵防御系统

产品白皮书

© 2017 360 企业安全集团

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，所有版权均属 **360 企业安全集团** 所有，受到有关产权及版权法保护。任何个人、机构未经 **360 企业安全集团** 的书面授权许可，不得以任何方式复制或引用本文的任何片断。

目录 | Contents

一. 前言	4
二. 无线安全问题分析	4
2.1 企业自建热点	5
2.2 非企业自建热点.....	5
2.2.1 其他企业热点	5
2.2.2 员工自建热点	5
2.2.3 恶意热点.....	6
三. 无线安全防护的必要性.....	6
四. 当前防护手段不足	7
4.1 缺少持续的检测工具	7
4.2 缺少有效的防护措施.....	7
4.3 缺少必要的审计手段.....	7
五. 无线网络防护的基本要求	8
5.1 安全情况评估	8
5.2 及时发现热点	8
5.3 热点精确阻断	8
5.4 攻击行为检测	8
六. 360 天巡无线入侵防御系统	9
6.1 产品概述.....	9
6.2 产品架构.....	9
6.3 产品优势.....	10
6.3.1 无线入侵实时监测.....	10
6.3.2 恶意热点精确阻断.....	10
6.3.3 安全事件智能告警.....	11
6.3.4 黑白名单智能管控.....	11
6.3.5 安全审计报告	12
6.3.6 无线网络状况展示.....	12
6.3.7 多区域管理.....	12
6.3.8 精确定位跟踪	13
6.3.9 产品独立部署	13
6.4 主要功能.....	14
6.4.1 无线热点阻断	14
6.4.2 无线攻击检测	14
6.4.3 安全策略设置	14
6.4.4 无线安全评估	14
6.5 产品部署.....	15
6.5.1 部署架构.....	15
6.5.2 无线收发引擎部署.....	15

6.5.3 网络部署.....	16
6.5.4 部署示例.....	16
七. 技术支持体系.....	17

一. 前言

近年来，无线网络在企业中，发展迅猛。很多企业为了满足一些新业务的需求，或是解决员工便捷的办公网络环境，在办公区域增设了无线 AP(接入点，全称 Access Point，又称热点)，弥补了有线网络的不足，提高了员工上网的便利性。

2015 年 6 月，360 天巡实验室对北京市区 8 个人口和办公密集区域的无线网络进行了实地检测，覆盖范围包括以下地点及其周边 1-2 公里区域：望京 SOHO、金融街、长安街、CBD 大厦、东交民巷、中关村软件园、东方广场、五道口等。在我们测试的 8 个地区中，共检测发现有效的无线热点 78603 个。其中，通过路由器 MAC 地址匹配，可以确定为企业热点的网络为 2652 个，占有无线网络的 3.4%。由于不能排除一些小型企业用户使用一般的民用路由器搭设无线网络的可能性，因此，企业无线网络的实际比例可能还会更高。企业无线网络的覆盖程度由此可见一斑。

无线网络在快速发展过程中，很大一部分企业，对于无线网络的安全没有给予足够的重视，只是随着对无线网络需求的出现，逐步的组建起了无线网络。由于部署过程没有统一规划，部署和使用人员的安全意识和专业知识的不足，导致 AP 分布混乱，设备安全性脆弱，给企业的网络信息安全带来了极大安全风险。

无线安全是一个新兴领域，目前对此领域的研究还比较少，甚至明确知道无线安全问题存在的用户也不是很多。但是由无线 AP 引发的网络安全事件频发，3 月由于某公司内部存在开放的无线 AP，导致超级计算机天河一号被入侵，大量敏感信息疑遭泄漏；5 月有用户在 T1 航站楼使用登机牌通过无线 AP 登录网络时，发现由于机场无线提供商的服务器安全设施不足和代码漏洞，可导致服务器中的用户隐私数据被泄漏及登机人信息被窃取。3.15 大会的绵羊墙展示，表示很大一部分用户，对无线的安全意识薄弱，在用手机或其他终端连接无线 AP 时，未考虑安全问题。

无线网络在迅猛发展，无线网络的安全问题逐渐凸现，但专门解决无线网络安全问题的产品和技术却还没有大范围推广使用，仍掌握在少数科技比较领先的公司手中。

二. 无线安全问题分析

随着各种无线技术和相关产品的发展，搭建热点越来越容易。在企业内部出现的热点，主要有以下几种方式，各种方式都有一定的安全隐患和问题。

2.1 企业自建热点

目前越来越多的企业，为了满足业务的需要，方便员工的网络访问，开始在自己内部组建无线网络。这种企业有规划的搭建的热点，称为合法热点。

从安全的角度讲，合法热点应该是企业内的唯一可用热点，其他热点，都可能会给企业的网络安全带来危险，不应该允许其存在或者是不允许本企业终端进行连接。

合法热点也存在安全隐患，如：弱口令、加密等级不足等，容易被黑客通过热点进入企业内部网络，造成信息泄露、被篡改等严重后果；合法热点也可能会遭受到 DDoS 等攻击，导致热点无法提供正常服务。

2.2 非企业自建热点

除企业自建热点外的所有热点，统称为非企业自建热点，又可分为以下几类。

2.2.1 其他企业热点

由于无线网络的穿透性和边界不确定性，在某些邻近的企业，无线网络可能会互相覆盖，也就是说在 A 企业可能会找到 B 企业的热点，在 B 企业也可能会找到 A 企业的热点。

这种热点对本企业的网络安全来说，有两方面的问题。一是本企业员工，是否缺乏安全意识，而去连接这种外单位热点。二是对方单位的热点，是否本身有安全问题，如：已经被攻破等。

如果对方单位的热点已经被攻破，而本单位人员，又连接了这种热点，那么就有可能造成信息泄露，或者是被黑客通过这台终端入侵企业内部网络。

2.2.2 员工自建热点

随身 WiFi 产品种类越来越多，使用越来越方便，只要插到有网络的电脑终端上，即可分享一个跟此网络连通的 WiFi；在有无线网卡的终端上，很多终端工具也提供了分享 WiFi 的工具。在如此方便的情况下，很多企业的员工，有意或者无意间，就在自己的终端上建立了 WiFi，而这些 WiFi 的安全性很难保证，包括使用弱密码、加密等级低等。

黑客很容易利用这种 WiFi 进入企业网络内部，进而盗窃或者篡改企业业务数据，造成严重后果。

2.2.3 恶意热点

除以上热点外，一些攻击者还可能会故意在企业周围建立恶意热点，采用与企业热点相同的名称，使企业员工的终端在有意或者无意间试图连接该热点。

而攻击者可以通过该热点的流量分析，获取企业内部信息，甚至通过入侵该终端，进入企业内部网络。

综上所述，在企业内，可能出现很多种热点，这些热点有企业内部合法建立的，也有其他原因建立在企业内可访问的，各种热点都存在不同的安全隐患和问题，为了企业信息安全，必须做好切实的防护工作，避免由于无线网络导致安全问题。

三. 无线安全防护的必要性

从上一章描述可以得知，任何单位都可能会被无线网络覆盖，包括自己建立的，也包括非自己建立的，这些无线网络对本单位的安全都会带来一定的影响，必须采取相应的防护措施。

军队-军队管理比较严格，网络与互联网物理隔离，没有建立自己的无线网络。无线网络给军队带来的问题主要在于军队内部终端私建立了热点，这种热点就有可能被附近的攻击者利用入侵军队内网；军队内部的有些终端，还可能会连接到附近攻击者搭建的恶意热点，流量被攻击者截获，从而造成信息泄露。

政府/金融-政府和金融的网络相对于军队要宽松一些，一般分为内网和外网，外网可以连接互联网，内网与外网逻辑隔离。目前大部分的政府和金融单位已经开始在外网和内网建立无线网络，因此政府网络除了受到与军队同样的私建热点、连接恶意热点外，还需要考虑无线网络的攻击防护。

央企-央企的网络管理更宽松一些，无线网络基本都已建设完毕。因此，与金融类似，影响央企网络安全的无线问题，主要就包括了针对央企本身建立的无线网络的攻击、央企员工在央企内部私搭乱建的热点以及员工终端连接到了恶意热点。

综上所述，以上各行业信息安全，都会受到无线网络的影响，必须采取相应的无线安全防护措施。

四. 当前防护手段不足

目前各企业的信息安全都或多或少的受到了无线网络的威胁，必须采取相应的防护措施，但绝大部分企业的防护手段还仅限于无线设备本身的一些安全配置，如：设置更强的密码、采用更安全的加密模式、隐藏热点名称等等，但这些还不足以应付目前的无线网络威胁，主要有以下几方面问题。

4.1 缺少持续的检测工具

目前很多企业，还不具有持续、稳定运行的检测无线网络安全情况的工具。

无法长期关注整个无线网络安全情况，对于出现偶然性比较大的非法热点，无法做到及时发现和阻断。

某些企业在某个特定的时期，会进行无线网络的安全检查，检测安全情况、是否有非法热点等等，但这种做法，很难形成一种常态。

4.2 缺少有效的防护措施

对于针对无线网络的各种攻击，缺少有效的发现和防护措施，无法及时发现和阻断攻击。

当 AP 遭受泛洪攻击时，目前很多企业，都是被攻击到网络无法使用的时候，才会发现和进行相应处理。

对于钓鱼热点攻击，几乎没有发现的手段。从而造成某些终端无意之间连接到了钓鱼热点，造成信息泄露。

4.3 缺少必要的审计手段

企业无线网络内发生的安全事件，还不具有有效的审计手段。

当发生了安全事件后，如：某些终端是否私自建立过 WiFi，某些终端是否连接过非法热点，AP 是否遭受到过攻击等等，对于事后的审计和追踪，缺乏必要的数据支持和处理手段。

基于以上描述，目前的手段，还无法保护企业不受无线网络的威胁，需要寻找新的防护手段。

五. 无线网络防护的基本要求

5.1 安全情况评估

管理员需要随时了解本企业无线网络的安全情况，如：有没有受到攻击、企业范围内是否有恶意热点等，并以直观的方式展示。

当网络内出现异常情况时，管理员应该可以及时收到相关的告警和提示处理信息。

5.2 及时发现热点

热点是无线网络的主要组成部分，由于无线网络的穿透性和不可见性，无论是自己合法组建的热点或者是其他热点，都会覆盖本单位。对于单位范围内出现的这些热点，要能够及时发现，并定位其位置，以便进行下一步的安全防护工作。

5.3 热点精确阻断

对于在单位范围内发现的热点，需要能够通过设置黑白名单、行为甄别等手段，来区分哪些是正常热点，哪些是恶意热点，对恶意热点进行精确阻断，且不能影响到正常热点的使用。

5.4 攻击行为检测

对于自身已经建设无线网络的单位，针对无线网络的攻击行为的检测和防御，占有非常重要的地位。保证无线网络安全的关键任务是持续关注企业当前无线网络的安全状况，要能够持续捕获当前无线环境中所有的数据流量，并将数据流量进行安全性分析，针对无线网络数据链路层的无线网络攻击行为进行精准识别。一旦发现恶意行为立即采取相应措施，进行告警或者压制，达到实时监测的目的

以上几点，是无线网络防护的基本要求，只有达到这几项，才能确保企业范围内只存在合法热点，终端也没有机会连接非法热点，且在本企业无线网络遭受攻击时，可以及时发现及时处理。

六. 360 天巡无线入侵防御系统

针对目前无线网络的发展形势，无线网络存在的安全问题和现在防护手段的不足，360 推出了无线入侵防御系统——天巡。

天巡基于无线入侵检测、无线数据分析、恶意热点阻断等先进技术，以守护无线网络边界为核心任务，构建“事前全面监测、事中精准阻断、事后全维追踪”的无线入侵防护体系，围绕无线网络环境中的关键设备即热点与终端，进行相应的安全措施增强，为用户提供切实落地可执行的无线网络边界安全解决方案。

6.1 产品概述

360 天巡广泛应用于有内网数据安全需求的军队、企业、党政机关和其他领域有安全需求的客户群。产品从无线攻击者的角度进行产品设计，以数据捕获能力、协议分析能力为基础，可以精准识别攻击行并快速对威胁进行响应，不间断地对无线网络进行监测并将无线入侵拒之门外，保护企业无线网络边界安全；快捷、直观、全面的管理方式提高管理效率、降低管理难度，可协助企业无线网络管理员了解无线网络状况、为企业的无线网络安全建设和防御提供决策依据；简易的部署方式不改变用户原有网络结构，节省用户投资，独立的无线收发引擎设备为企业提供更专注更高效的安全保护。360 天巡是一款轻部署、强安全、易管理的新一代企业级无线网络安全防御系统。

360 天巡的产品理念是以无线攻防思维，为客户构建全面的无线入侵防护体系，切实守护企业无线边界安全。

6.2 产品架构

360 天巡主要由中控服务器、无线收发引擎组成。管理员通过访问 web 管理平台，能够及时发现是否存在私建热点、伪造热点等违规行为，及时对可疑热点进行阻断和定位，将无线网络安全威胁拒之门外。同时系统提供热点分布概况分析、客户端连接热点趋势分析以及安全事件汇总等核心数据，帮助企业制定更加有针对性的无线网络防护策略。

360 天巡产品构成如图 1 所示：



图 1 天巡产品构成图

其中，产品硬件主要由以下两部分组成：

- 1) 360 天巡中控服务器
- 2) 360 天巡无线收发引擎

6.3 产品优势

6.3.1 无线入侵实时监测

保证无线网络安全的关键任务是持续关注企业当前无线网络的安全状况，天巡通过部署在企业内部的高性能无线数据无线收发引擎装置，持续捕获当前无线环境中所有的数据流量，并将数据流量实时传输到中控服务器进行安全性分析。

中控服务器内置无线威胁感知引擎，可将接收到的数据与无线攻击特征库进行智能比对，能够针对无线网络数据链路层的无线网络攻击行为进行精准识别。一旦发现恶意行为立即通知无线收发引擎采取相应措施，将威胁抑制在攻击发生之前，达到实时监测的目的。同时，针对建立钓鱼热点进行钓鱼攻击等恶意行为，无线威胁感知引擎通过热点安全策略关联性分析技术，也能进行有效识别，使潜伏在无线网络中的各种威胁无处可藏。

6.3.2 恶意热点精确阻断

WiFi 热点是无线网络中转发数据的重要设备，一旦热点被劫持或其本身就是作为攻击手段而被建立的，那么该热点即为恶意热点。对于恶意热点的防范措施而言，有效而精准的无线热点阻断方式作为抑制攻击的防御手段，在无线入侵防御系统中是不可或缺的。360 天巡的阻断方式有别于其他无线入侵方式系统所使用的射频干扰技术进行范围大、辐射强的阻断，天巡使用技术领先的协议阻断机制进行精准且智能的恶意热点阻断方式。通过热点阻断，可允许企业所在无线网络区域内某些特定的热点可用，而其他无线热点不可用，该阻断策略分为手动阻断和自动阻断两种模式，用户可自定义设置。

6.3.3 安全事件智能告警

对于一款无线入侵防御产品来说，监测到无线攻击事件发生或检测到恶意热点存在时，向管理员提供告警信息已经是十分普遍的做法。但同时也带来一个问题就是，告警信息过多，管理员疲于应付每天系统向他发出的各种告警，这些告警大多是没有经过过滤和分析过的无用告警，有些则是真正需要被管理员注意到且需要处理的问题，但这些真正的问题很可能被淹没在大量的无用告警信息之中。

360 天巡无线入侵防御系统搭载事件分析与告警引擎，能够对天巡中控服务器上报的安全事件进行分析和筛选，并在此基础上将事件按照安全策略设定的严重级别进行分类，筛选后告警信息将通过邮件提醒、首页提示和告警日志展示三种方式展现给管理员。这样无用的安全事件告警信息将大大减少，同时管理员在 360 天巡管理界面就可以看到他真正关注的无线安全事件。360 天巡事件分析与告警引擎有效降低无线安全事件误报率、极大提高管理员工作效率、降低维护工作量，让事件告警更智能。

6.3.4 黑白名单智能管控

无线入侵防御系统的主要工作方式分为监测、识别和阻断三个阶段。监测功能大多由系统自动完成，但绝大多数无线入侵防御系统的识别与阻断功能，尤其是阻断都是由管理员手工完成的：对于系统监测到的攻击事件发生或存在恶意热点，系统可以向管理员发出告警提示，并由管理员进行处理。但传统解决方案存在的一个很大的问题就是：

- 工作强度大

为了及时处理系统监测的攻击事件（尤其攻击者喜欢在半夜进行攻击），管理员甚至需要 7*24 小时值班进行看管。

- 工作难度高

管理员需要持续的在大量热点与终端中进行手工排查，查看当前无线网络中是否存在的非法热点或终端。

360 天巡从管理者角度出发，向用户提供热点及终端黑白名单管理功能，首先管理员根据企业安全策略对企业当前无线网络环境内的热点及终端进行分类，属于企业内部热点和终端的就划分至白名单，安全属性未知的则划分至未知名单中，有可疑行为的热点或终端则划分至黑名单中。同时系统也将根据安全策略进行自动监测，并将监测到的热点或终端按以上分类方式进行区别对待，在设置自动阻断前提下，系统可自动阻断和隔离黑名单中的热点及终端，这样可大大提高管理员排查和阻断的工作效率。

6.3.5 安全审计报告

对于企业来说，报表不仅是为了向上级进行工作汇报，更需要通过报表中的数据反映出实际的问题和应对的策略。但目前绝大多数同类产品轻视报表的重要性，甚至没有报表功能。有的产品所产生的报表仅仅是一份堆叠原始采集数据的 Excel 表（例如日志数据、安全事件数据、告警信息等）或是毫无意义的大段文字。管理员面对这样的审计报告很难发挥报表应有效果。

360 天巡可根据管理员的需求灵活生成无线安全威胁报告，并可在生成后自动发送至管理员邮箱，方便管理员抄送至领导邮箱，提高管理员工作效率。同时管理员也可查看过往已生成的报告。无线安全威胁报告包括安全概览、恶意热点处理、恶意热点分布、无线攻击分布和安全小结。安全概况可帮助读者通过整体安全指数快速概览当前企业无线安全状态，并可知道哪个区域安全指数最高、哪个区域安全指数最低以及恶意热点和无线攻击的趋势是如何的。恶意热点（攻击事件）处理及分布概况向读者展示报告周期内，热点及攻击事件的处理状况和分布情况，帮助管理员进行有针对性的排查。由于系统支持分布式多区域的部署方式，因此管理员可选择指定区域详细查看该区域的无线安全状况，可以根据报表中的安全小结采取相应措施。

6.3.6 无线网络状况展示

传统的无线入侵防御系统或国内其他安全类产品对于事件的描述方式大多为列表文字化的方式，并且按时间由远及近的排序。满足业务需求永远是传统安全产品的首要任务，管理员似乎也逐渐接受这种古老的单一维度的展现方式。360 作为国内最大的互联网安全企业，深谙应如何向用户提供更好的产品，满足用户需求是基本，提高用户体验才能让用户更好的使用产品。360 天巡在设计之初便清楚，满足业务需求与提高用户体验都是天巡的职责所在。

360 天巡将互联网产品设计模式引入传统企业安全产品领域，创新性的运用多种统计方式为管理员从多方面展现无线网络状况。系统利用分数及颜色的直观变化，展现当前区域的无线安全变化情况，并在区域存在风险情况下以分类的形式向管理员描述系统当前存在哪些风险。同时饼状图、柱状图以及趋势图等也为管理员展现不同设备在当前区域内的状态。当管理员拥有天巡，便可将整个企业内部的无线网络安全概况尽收眼底。

6.3.7 多区域分级管理

随着业务的不断发展，企业的办公环境不再局限于一个地方，企业面积不断扩大、办公区域逐渐增多、跨省市甚至国家的驻外办公机构或分公司也不在少见，对企业来说，无线安全的分级管理势在必行。

360 天巡率先在无线安全入侵防御类产品中支持基于人员与角色的多中控、多区域的管理架构，能够极大简化区域管理。通过这种管理架构，可将原本各自孤立的无线安全孤岛连接起来，既能使企业总部的安全策略能够顺利上传下达，各分部区域内又可以灵活管理。使整个企业的无线网络安全管理效果不因地域而受限，不因人员而不同。同时为了避免管理“越界”，企业可以定义基于角色的无线安全管理机制，每个管理员仅能对属于自己的区域及功能进行管理。

6.3.8 精确定位跟踪

企业部署无线网络后，管理员通过传统的无线入侵监测系统监测到恶意热点、违规使用的终端或无线攻击事件时，面临的重大难题就是如何快速定位热点、终端和攻击事件发生的源头，因为找到事件发生源头是追查无线网络攻击发生的重要手段。

360 天巡配合区域管理功能，可在指定区域导入包含必要物理信息的平面结构图，并将该区域所分配的无线收发引擎部署至相应区域中，天巡使用无线收发引擎三点定位技术以及数据挖掘算法，对无线收发引擎覆盖范围内的无线热点及终端进行精确定位，以帮助企业管理员能够快速的跟踪威胁热点或设备，或定位无线攻击事件发生的源头，并采取行动消除安全隐患。

6.3.9 产品独立部署

传统的无线入侵防御系统使用无线接入（AP）在其空余时检测无线局域网，并对异常信号进行阻断，响应实时性及效率均不理想，并且需要全部部署带有无线防御功能的 AP。而 360 天巡采用独立的分布式部署无线收发引擎的方式，不改变企业原有网络配置和无线网络性能，能做到基本实时探测和阻断无线热点，响应速度和效率均优于传统的无线入侵防御系统。

6.4 主要功能

6.4.1 无线热点阻断

WiFi 热点是无线网络中转发数据的重要设备，一旦热点被劫持或其本身就是做为攻击手段而被建立的，那么该热点即为恶意热点。对于恶意热点的防范措施而言，有效而精准的无线热点阻断方式作为抑制攻击的防御手段，在无线入侵防御系统中是不可或缺的。360 天巡的阻断方式有别于其他无线入侵方式系统所使用的射频干扰技术进行范围大、辐射强的阻断，天巡使用技术领先的协议阻断机制进行精准且智能的恶意热点阻断方式。通过热点阻断，可允许企业所在无线网络区域内某些特定的热点可用，而其他无线热点不可用，该阻断策略分为手动阻断和自动阻断两种模式，用户可自定义设置。

6.4.2 无线攻击检测

保证无线网络安全的关键任务是持续关注企业当前无线网络的安全状况，天巡通过部署在企业内部的高性能无线数据无线收发引擎装置，持续捕获当前无线环境中所有的数据流量，并将数据流量实时传输到中控服务器进行安全性分析。

中控服务器内置无线威胁感知引擎，可将接收到的数据与无线攻击特征库进行智能比对，能够针对无线网络数据链路层的无线网络攻击行为进行精准识别。一旦发现恶意行为立即通知无线收发引擎采取相应措施，将威胁抑制在攻击发生之前，达到实时监测的目的。同时，针对建立钓鱼热点进行钓鱼攻击等恶意行为，无线威胁感知引擎通过热点安全策略关联性分析技术，也能进行有效识别，使潜伏在无线网络中的各种威胁无处可藏。

6.4.3 安全策略设置

非白即黑策略，启用该策略后，把本企业的合法热点全部加入白名单，则所有白名单之外的热点，都会被自动阻断。

报警策略，可以定义安全事件的报警级别，报警方式等。

6.4.4 无线安全评估

天巡可以对企业的无线网络安全情况进行评估，主要有以下几点依据。

无线热点的安全性设置。针对已经添加在白名单中的热点，热点加密等级、鉴权方式、快速连接、是否为隐藏热点等，都会影响到无线网络的安全评分。

覆盖范围内热点情况。如果在天巡的覆盖范围内，出现有恶意热点，或者未知热点，也会影响无线网络的安全评分。

无线攻击情况。如果无线网络收到诸如：泛洪攻击、暴力破解密码等攻击时，都会影响到无线网络的安全评分。

6.5 产品部署

6.5.1 部署架构

360 天巡的硬件包括中控服务器和无线收发引擎，需要确保两者网络可连通。无线收发引擎必须以有线的方式，接入 POE 交换机。

如图 2 所示：

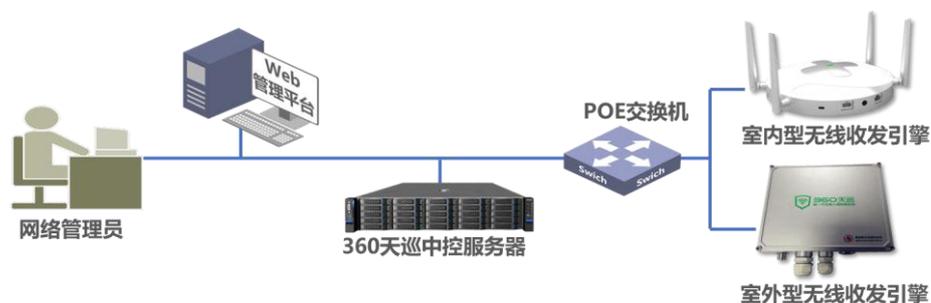


图 2 部署架构

中控服务器，放置在机房，通过网络与无线收发引擎可达即可。

Web 管理平台部署在中控服务器上，为 B/S 架构，凡是与中控服务器连通的终端，都可以通过浏览器访问。

无线收发引擎需要根据企业实地情况，进行安装部署，下个小节具体描述。

6.5.2 无线收发引擎部署

360 天巡的第二代无线收发引擎，可覆盖范围为 300-1000 平方米（半径约 10-30m）。具体情况，与无线收发引擎周边的建筑结构相关，比如：是否有墙、是否承重墙、是否有干扰无线信号的设施或者建筑物等。为了覆盖全企业，需要的无线收发引擎数量，需要进行工勘后，才能最终确定。

无线收发引擎的安装位置，以能够无死角全覆盖为基准原则，兼顾美观和实施方便。



图 3 无线收发引擎部署场景

6.5.3 网络部署

为了确保天巡的稳定运行和自身安全，无线收发引擎必须以有线的方式，连接到交换机。在无线收发引擎位置选定后，需要进行施工布线。

无线收发引擎可以使用 PoE 和普通电源供电两种方式。

在企业交换机支持 PoE 供电口充足的情况下，推荐使用 PoE 供电，如没有支持 PoE 供电的交换机或者接口不足，需要考虑为无线收发引擎部署供电的电源线。

6.5.4 部署示例

某客户楼层面积长 40 米，宽 30 米，一端为实体墙隔离的办公室，一端为玻璃墙隔开的会议间，中间有两条承重梁。

为了达到无死角覆盖和准确定位热点位置的目的，本楼层计划部署 4 台天巡无线收发引擎。网线按照该客户规定，沿网线管道进行。

如图 4 所示：

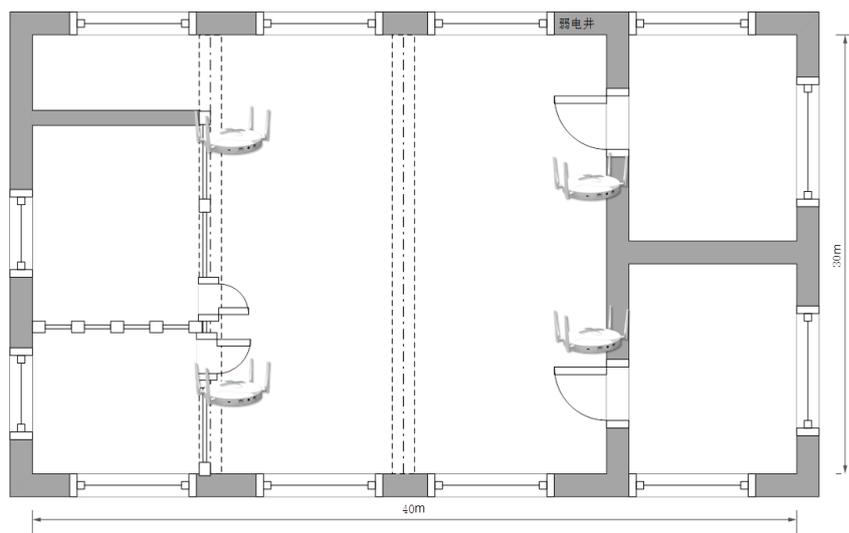


图 4 物理部署图

七. 技术支持体系

360 企业安全集团-北京总部

地址：北京市朝阳区酒仙桥路 6 号院 2 号楼 100015

360 企业安全集团-上海分公司

地址：上海市浦东新区张江镇浦东软件园郭守敬路 498 号 11 号楼 101 室

360 企业安全集团-广州办事处

地址：广州市天河区珠江新城江东路 32 号利通广场 2202

360 企业安全集团-珠海分公司

地址：珠海市九洲大道西 2021 号富华里中心写字楼（中海大厦）A 座 19 楼

360 企业安全集团-成都办事处

地址：成都高新区天府软件园 E1 座 11 楼 24 号

360 企业安全集团-西安办事处

地址：西安市高新区锦业路绿地领海大厦 B 座 16 层