宁盾
NINGTON

宁盾新一代终端准入控制引擎

通过可视化和自动化解决企业对终端的信任问题

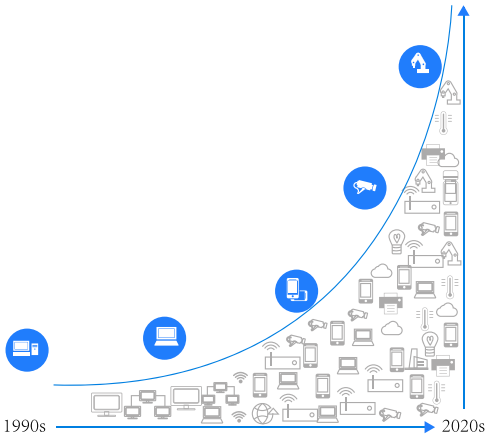
ND ACE

上海宁盾信息科技有限公司

为什么要对终端进行准入控制管理?

每时每刻，都有新的设备加入您的网络，未授权的笔记本、BYOD、网络设备及各种各样的 IoT。这些非合规性终端可能会因未安装杀毒软件、存在漏洞补丁等原因，增加企业中病毒的可能。

终端数量不断增加，预计到 2020 年，全球将有 270 亿终端，其中 100 亿活跃于企业网络，非可视化管理无法及时发现企业网络中的危险终端，成为为企业发展的安全隐患。



预计 2020 年，全球将有 270 亿终端，其中 100 亿活跃于企业网络中

在寻找方案之前不防先回答以下问题:

1、贵公司接入网络的电脑有 _____ 台

2、贵公司接入网络的手机有 _____ 台

3、贵公司接入网络的打印机有 _____ 台

4、贵公司接入网络的摄像头有 _____ 台

5、贵公司接入网络的网络设备有 _____ 台

6、您认为还有哪些未知终端隐藏在您的企业内? _____

7、您对企业入网终端的管理方式? A、专业非可视化终端准入工具 B、专业可视化准入管理工具 C、没有相关工具

8、贵公司员工的电脑是否都安装了杀毒软件？ A、是 B、否 C、不确定

9、贵公司员工电脑的补丁版本是否升级到最新? A、是 B、否 C、不确定

10、贵公司员工的电脑是否安装了非合规应用? A、是 B、否 C、不确定

11、对于以上问题的解决方式是否有自动化工具协助? A 有 B、没有

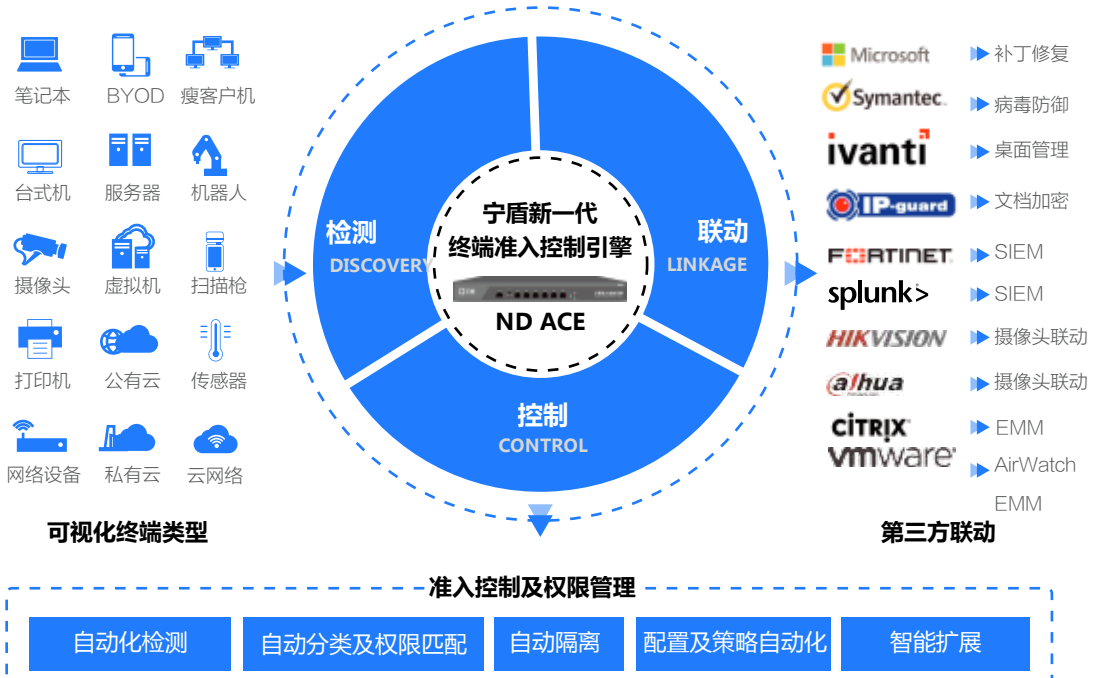
12、贵公司员工通过什么方式接入网络? A、无线 WPA2 B、有线账号密码 C、802.1x 认证 D、Portal 认证

13、贵公司访客通过什么方式接入网络? A、无线 WPA2 B、Portal 认证 C、不允许接入

如何进行终端准入管理?

以“可视化、自动化为中心”的终端准入框架

受传统网络架构影响，大部分企业并不清楚企业内网络资产状况，传统统计的也仅仅是企业派发的设备。随着 BYOD 及越来越多 IOT 终端的接入，可视化网络资产，及时掌握终端动向对企业而言愈加重要。同时以机械化代替人工、以自动化提高效率的生产方式被企业广泛采纳，宁盾新一代准入控制引擎（简称: ND ACE）以“可视化、自动化”为核心，帮助企业实现终端“安全、高效、高体验”准入管理。



- 可视化资产管理
  - 可视化终端设备画像
  - 终端组织架构
- 入网终端合规性检测及去中心化管理
- 安全联动，自动化修复及日常维护
- 访客及员工 BYOD 入网认证管理

一、通过可视化实时定位终端风险

ND ACE 主动监测接入网络的终端，可视化办公园区、数据中心、云及生产线的笔记本、瘦客户机、手机、摄像头、打印机、传感器等网络资产，及时掌握终端安全状态。

基于 MAC/IP 地址实时扫描终端类型、数据包、流量等安全信息，防止 IP/MAC 地址伪造及风险性终端接入，及时发现隐藏“肉机”。

MAC Address	IP Address	Account	Domain Identity	Bytes	Packets	Network Function
28:B2:BD:A1:64:6D	10.123.102.192			395.48MB	588.88K	Windows Machine
4C:8D:79:DE:B8:00	10.123.127.198			23.42MB	138.48K	Apple Mac OS
00:26:C7:54:50:62	10.123.102.13			498.82MB	1.58M	Windows Machine
52:54:00:49:87:56	192.168.221.96			35.79MB	96.35K	Linux Desktop/Server
A8:5B:78:30:0F:EE	10.123.200.158			35.24MB	174.21K	Apple iOS Phone
94:E1:AC:24:DD:CD	10.123.123.208			23.22MB	155.77K	Camera
30:05:5C:E0:4A:F7	10.123.123.188			208.40MB	322.37K	Printer
00:1B:2B:77:84:4F	10.123.170.254			140B	2	Switch
38:29:5A:A0:1E:9B						Android Phone
1C:DE:A7:06:62:2F	10.123.123.250			1.22GB	2.55M	Wireless AC
52:54:00:25:E3:B9	192.168.221.118			840.21MB	1.31M	Linux Desktop/Server

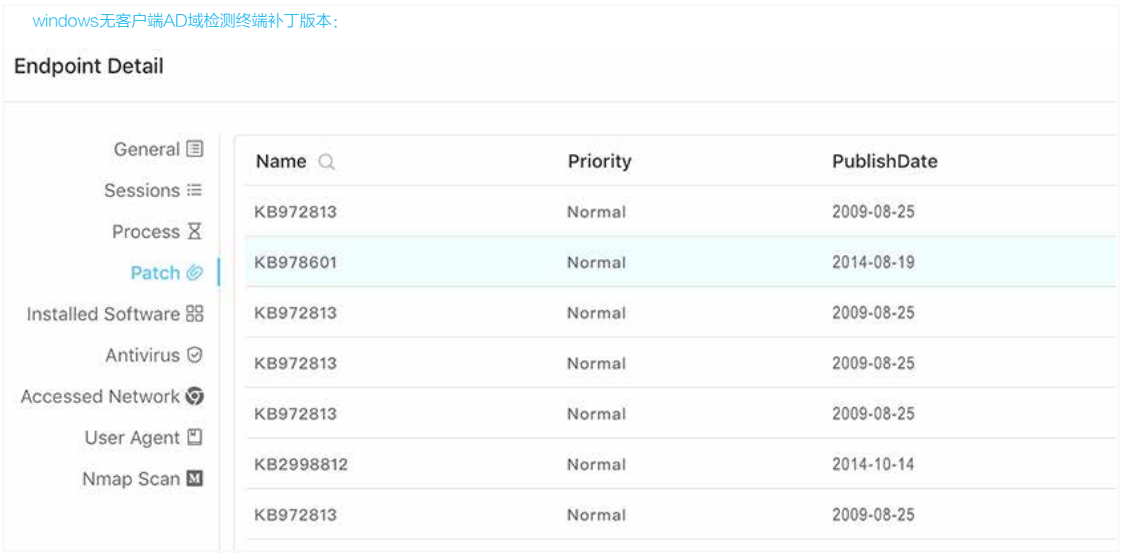
二、通过合规性检测排除风险性终端

1、合规性准入条件

主动检测各终端的合规性，基于合规性条件自动隔离并修复风险性终端。支持无客户端及客户端检测。合规性条件包括：终端类型、系统信息、杀毒软件状态、补丁版本、安装软件、运行进程、用户认证方式 .....

windows无客户端AD域检测是否安装杀毒软件：

windows无客户端AD域检测终端补丁版本：



2、自动化准入隔离

基于合规性条件，对非合规及风险性终端进行自动隔离。

- 排除没有安装杀毒软件的风险性终端
- 排除补丁版本没有更新的终端
- 排除软件进程停用的终端
- 排除安装非合规应用的终端
- 排除未安装合规应用的终端
- 排除伪造 IP/MAC 地址的终端

在安装客户端的情况下检测操作系统、版本、MAC/IP 地址、软件安装状态、运行进程等，提升入网 Mac 电脑的安全性。

精准获取摄像头厂商、设备类型、操作系统、IP/MAC 地址；监控异常流量，防止 MAC 地址伪造、弱密码攻击等问题。

检测打印机的设备厂商、设备类型、IP/MAC 地址等。监控异常流量，绑定访问权限，防止打印机的非法操作及攻击。

更多

检测更多 IoT 终端如：瘦客户机、网络设备、IP 电话及工控系统机器人、传感器等的合规性，实现终端自动化分类、权限匹配及准入控制管理。

三、通过网络认证实现访客及员工BYOD准入管理

通过DKEY AM（有线无线网络认证部分）规范化访客、员工BYOD网络准入流程，识别用户身份并对其访问权限进行管控。认证方式包括：短信认证、微信认证（强关注）、协助扫码、访客自助申请、用户名密码、802.1x认证、Facebook认证.....

1、多种认证方式，满足不同访客认证需求

- 自助式短信、微信认证助力企业营销推广；
- 高级访客一对一协助扫码授权，阻止外来人员乱用企业网络，减轻带宽压力；
- 访客自助申请认证由工作人员统一管理授权，为企业建立外包人员入网管理体系。

微信连WiFi ＋强关注　短信认证　协助扫码　访客自助申请

2、强安全认证，多组合方案供企业员工选择

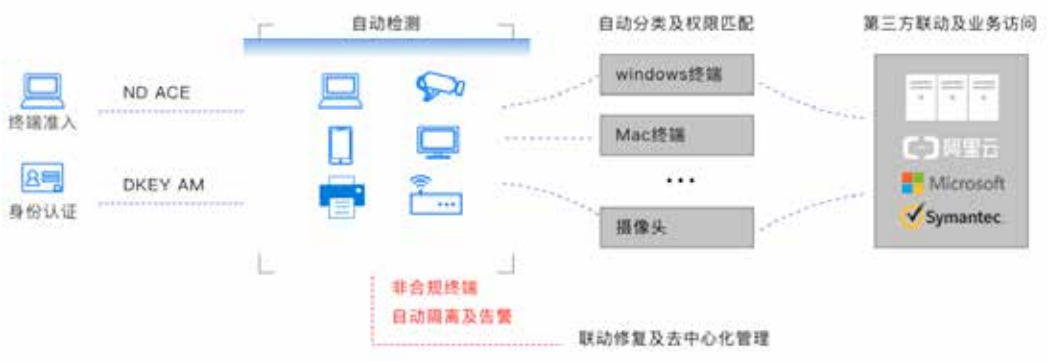
提供有线无线一体化认证，适配PC、手机等不同终端类型；多认证方案组合，为企业员工及BYOD提供强安全认证方案：

- 802.1x＋Portal＋双因素认证：解决无线空口加密及账号双重保护问题；
- Portal＋双因素认证：解决网络实名认证及账号加固保护问题；
- 单独采用802.1X或Portal认证，解决网络实名认证问题。

802.1X 认证　Portal 用户名密码认证　双因素认证加固

四、基于用户及终端的双重准入信任

通过DKEY AM实现对访客、员工BYOD的身份认证、访问控制及实名审计；ND ACE自动检测接入终端的合规性，以简洁的配置实现终端的自动分类、权限自动匹配、IP资源绑定等操作。通过轻量化操作提升终端及用户双重信任。



五、安全联动，实现自动化修复及日常维护

与主流安全厂商联动完成自动化修复，提升全网预警及恢复能力。实现终端准入与网络认证、病毒防御、补丁修复、桌面管理、文档加密等的一体化安全管理。

- 联动AD域控，实现终端合规准入
- 与Microsoft联动，实现网络准入与补丁修复统一管理
- 与Symantec联动，实现网络准入与病毒防御统一管理
- 与LANDesk联动，实现网络准入与桌面管理统一管理
- 与IP－Guard联动，实现网络准入与文档加密统一管理

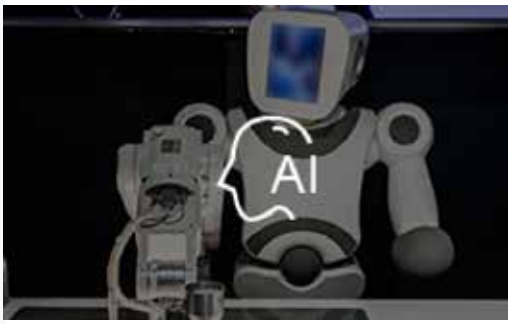
行业解决方案

企业办公网络身份认证与终端准入安全方案

面向移动办公场景提供基于身份和终端的全场景解决方案。

视频专网终端安全管控方案

可视化网络资产，解决视频专网前端安全、边界安全、自动化运维、控制中心等多维度安防问题。



智能工厂物联网终端安全准入

万物互联时代，宁盾给您提供智能工厂 IoT 终端安全管理解决方案！

数字化医疗终端准入解决方案

复杂的端、流动性的人群，医疗行业要如何同时实现病患、医护、实习生、临时坐诊专家及各种各样 IoT 终端的统一准入管理？宁盾给您提供基于终端和用户的一体化准入解决方案！

宁盾 NINGTON

上海宁盾信息科技有限公司
咨询热线：400-658-2855　　官网：http://www.nington.com
总部：上海市徐汇区田林路 487 号宝石大楼 703
北京：北京市海淀区上地信息产业基地三街中黎科技园 1 号楼 4 层 C 段 481
深圳：深圳市南山高新科技园中区讯美科技广场 3 号楼 15 层 B09