北京朝阳区酒仙桥路 6 号院 2 号楼 100015
Building 2, 6 Haoyuan, Jiuxianqiao Road,
Chaoyang District,Beijing,P.R.C. 100015
Tel +86 10 5682 2690 Fax +86 10 5682 2000

360 安全服务整体解决方案

V1.0

分享保障 360 公司信息安全的最佳实践；

1 个团队，3 台服务器，结合自主开发的安全产品，每天输出安全报告 ,每天验证加固安全漏洞 ,总体完成 6 万台服务器的安全服务工作。

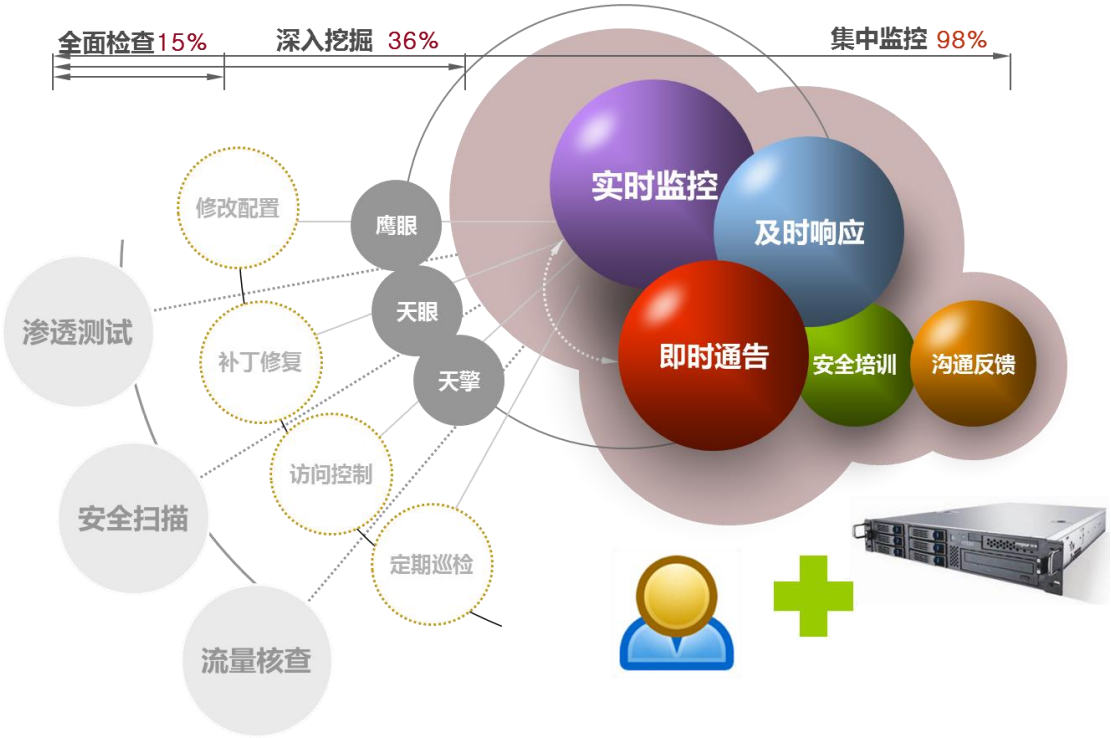
安全第一 就用360

北京朝阳区酒仙桥路 6 号院 2 号楼 100015
Building 2, 6 Haoyuan, Jiuxianqiao Road,
Chaoyang District,Beijing,P.R.C. 100015
Tel +86 10 5682 2690 Fax +86 10 5682 2000

方案特点

我们觉得现有的任何安全产品,都有自己的不足,防守的再好,也有方法绕过。360 安全服务解决方案的要点主要是在意识、攻、守、应急变化等方面的速度远远高于攻击者,最终达到相对安全的状态。

总体思路



360 安全服务整体解决方案主要分为全面检查、深入挖掘、集中监控三个阶段。各阶段之间都有紧密的联系和步骤，循序渐进的保障客户系统的信息安全。

全面检查

该阶段主要以渗透测试、安全扫描、流量核查为主。目的是以发现客户系统中现存的主要安全风险（如高危漏洞，入侵痕迹，异常流量等）。事后通过修改设备配置，补丁修复，增强访问控制，启用客户现有的安全策略等方法。全面解决发现的安全问题。

北京朝阳区酒仙桥路 6 号院 2 号楼 100015
Building 2, 6 Haoyuan, Jiuxianqiao Road,
Chaoyang District,Beijing,P.R.C. 100015
Tel +86 10 5682 2690 Fax +86 10 5682 2000

深入挖掘

深入挖掘阶段是以发现更多的安全问题，覆盖所有的安全死角为目标。依据全面检查阶段的结果，结合安全服务人员丰富的经验，充分利用客户现场的安全产品，以及综合市面上各家信息安全产品的优势，为客户建立全面有效的安全防护体系。

集中监控

信息安全工作是一项长期持续的工作，安全工作的重点再于综合布防集中监控。在此阶段会将客户现场的安全设备、监控设备的日志通过安全可靠的方式接入到 360 安全服务监控中心，进行 7X24 小时实时监控。会根据客户要求的频度对客户的信息系统进行主动的安全扫描，保障每天使用最新漏洞规则的扫描器。同时 360 安全攻防实验室每天监控国内外发布的漏洞信息，会将漏洞信息依据客户的关注度，以及客户受影响程度推送给用户。当客户系统遭受安全攻击时会提供及时的应急响应，在指定的时间内到达客户现场，采取紧急措施，恢复业务到正常服务状态；调查安全事件发生的原因，避免同类安全事件再次发生；提供数字证据。最后通过安全培训，沟通反馈等形式全面提高客户，安全意识、攻、守、应机变化能力。

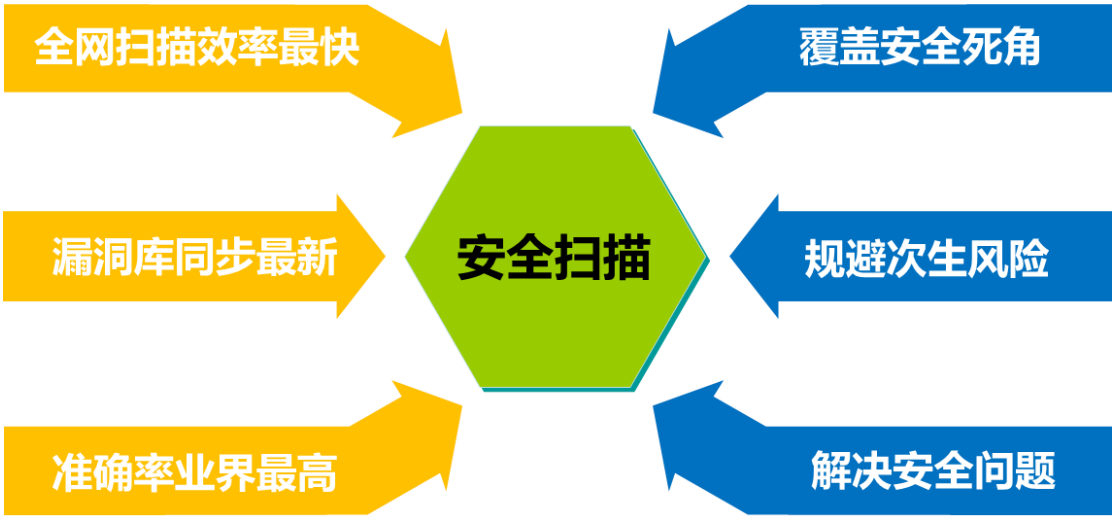
技术优势

纵深阶梯式技术架构:360 安全服务人员拥有多层次的专业安全服务人员，分别设有攻防实验室、漏洞实验室、网络安全研究员。安全专家团都是信息安全领域内的知名专家。

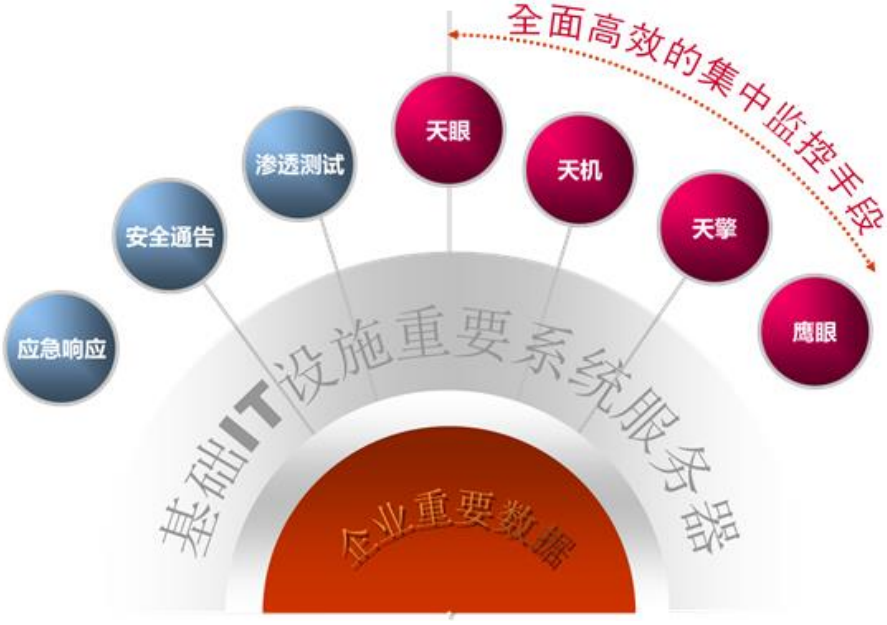
全面的技术体系：360 安全服务团队包含 9 大类技术体系，具体包含协议与逆向分析、云安全开发、网络安全、代码安全审计、IOS 安全、Web 安全、Andriod 安全、无线硬件安全团队，涉及信息安全技术领域最全面。

北京朝阳区酒仙桥路 6 号院 2 号楼 100015
Building 2, 6 Haoyuan, Jiuxianqiao Road,
Chaoyang District,Beijing,P.R.C. 100015
Tel +86 10 5682 2690 Fax +86 10 5682 2000

专业可靠的扫描能力：360 安全服务扫描能力能够在一小时内扫描完指定互联网单端口，可以每天提供安全扫描报告，每天跟进国内外发布的新漏洞，每天使用最新的漏洞库进行扫描，对于扫描策略进行严格测试，降低安全扫描造成的风险。



全面高效的集中监控手段： 云监控服务中心配备有专业的安全人员监测团队 7*24 小时轮班监控。监控人员现场监控、服务人员定期去客户现场进行安全巡检，结合产品和服务的形式实现全面高效的集中监控方案。监控全程采用加密传输，保障客户信息安全。对客户开放专有的监视通道可以查看监控录屏、操作记录等。提供更专业、更可靠、更安心的监控服务。



安全第一 就用360