安全基线配置核查管理系统

技术白皮书

北京东方棱镜科技有限公司

2015/3/10

目　录

1. 产品概述

1.1 整体现状与需求

由于服务和软件的不正确部署和配置造成安全配置漏洞，入侵者会利用这些安装时默认设置的安全配置漏洞进行操作从而造成威胁。随着攻击形式和各种安全威胁事件的不断发生，越来越多的安全管理人员已经意识到正确进行安全配置的重要性，重点行业和一个管理部门已经制定了统一的安全配置标准和检查标准。但是随着业务系统网络结构越来越复杂，重要应用和服务器数量及种类繁多，很容易发生安全管理人员的配置操作失误造成极大的影响。安全工作需要深入结合业务系统的生命周期进行开展，难度十分大，相对应的现在各行业和单位专职安全岗位设置有限，安全技术水平参差不齐。

同时，虽然一些重点行业和管理检查部门设定了统一的配置和检查标准规范，使得安全管理人员在进行安全配置时可以做到有据可依，但是面对种类繁杂、数量众多的业务系统和设备，真正能够完成配置合规检查和修复，将会是一个十分巨大的工作。做一次细致的检查和修复耗费的时间会很长，对象越多工作越繁琐，而且人工效率不高。

1.2 产品定位

棱镜科技针对通信行业特点和安全基线规范基准，推出了专用检查工具——安全基线配置核查管理系统，使安全检查过程达到自动化、标准化、持续化、可视化。它可以大大提高检查结果的准确性和合规性，用以在运营商的上线安全检查、第三方入网安全检查、合规安全检查（上级检查）、日常安全检查和安全服务任务中，协助查找设备在安全配置中存在的差距，并与安全整改与安全建设相结合，提升各类业务系统的安全防护能力和达到整体合规要求，同时棱镜科技安全基线配置核查管理系统实现 WLAN 设备的配置检查，发现配置弱点防止设备带病工作。

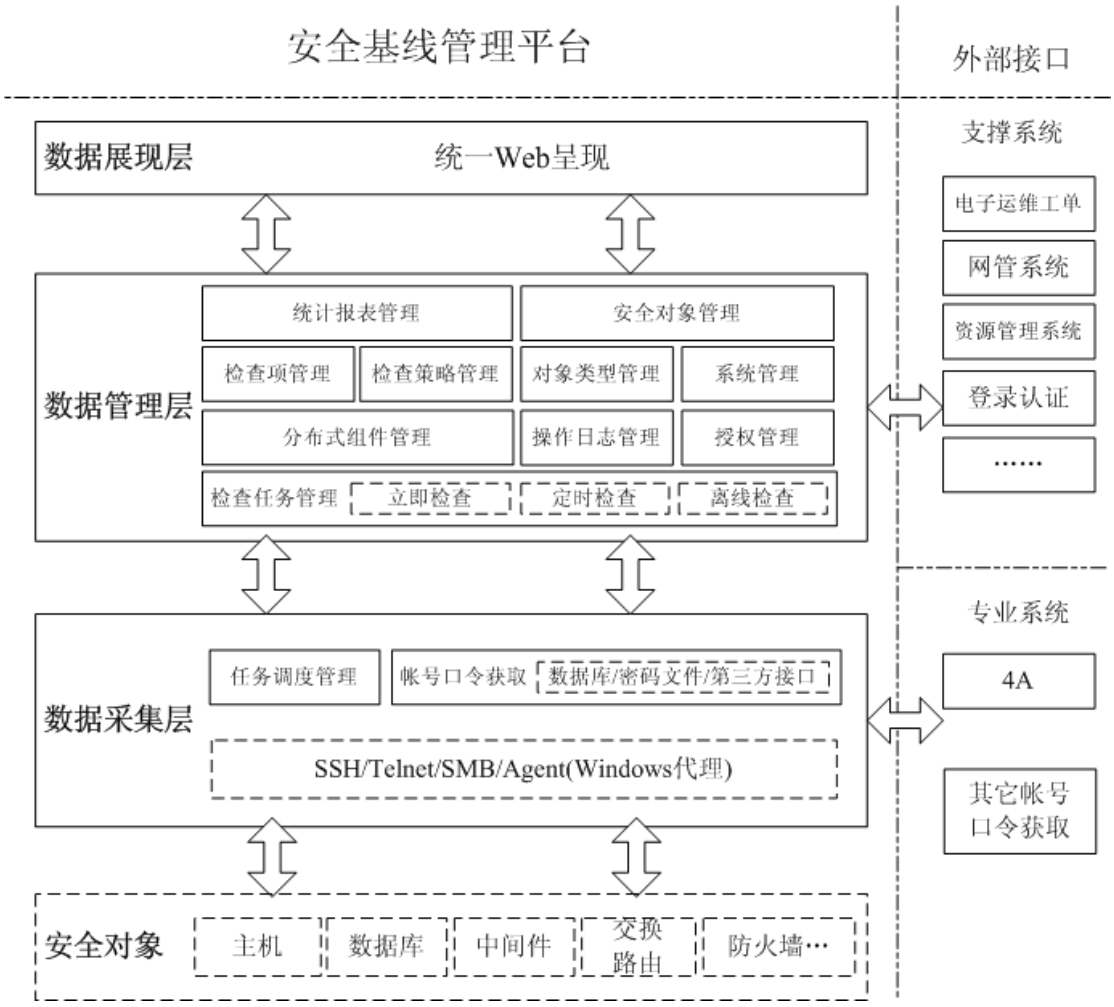
棱镜科技支持 WLAN 设备检查的安全基线配置核查管理系统在原有系统的基础上进行了相关功能的优化，增加 SMB 协议远程配置采集，实现检查项自定义功能和检查项的策略组合功能应对不同行业客户和同行业不同业务系统或者不同检查力度的检查要求，通过策略管理功能实现检查项参数不同情况的参数实例化，实现检查任务的手动、周期和离线检查任

务调度功能，丰富实现安全基线检查结果的在线和离线报表报告功能。该系统实现对 WLAN 设备的配置检查要求，目前支持傲天动联、武汉虹信等厂家的 WLAN 设备检查，随之检查设备和检查项的不断丰富，实现 WLAN 设备的全面检查。

安全基线管理平台，主要应用于设备入网、工程验收、日常维护、合规检查等方面。通过对目标系统展开合规安全检查，找出不符合的项并选择和实施安全措施来控制安全风险。

1.3 产品整体架构设计

安全基线配置检查系统是棱镜科技信息安全技术有限公司具有自主知识产权的软件产品，由基线管理平台系统、脱机代理和单机代理组成。其中，基线管理平台负责安全对象信息、检查项的维护和管理，实现检查项的自定义功能，实现不同客户和业务系统不同检查要求的安全策略的组建维护和检查参数的实例化，实现针对不同检查任务的手动、周期和离线调度，实现对检查结果数据的接收、分析、比对，确认是否达到基线标准要求；基线管理系统提供网络方式的基线采集功能，借助该系统，能够将网络协议检查、单机代理检查、脱机代理检查集为一体；单机代理和基线脱机代理作为基线管理系统的分布式组件，实现无管理员账号和密码单机设备和不可达网络设备的基线检查。



1.3.1 安全基线管理系统

安全基线管理系统可进行多种类型的主机、数据库、网络设备、中间件以及 WLAN 设备的安全基线信息采集和安全基线检测工作。 安全基线管理系统，可以针对 Windows 主机、Linux 主机、Solaris 主机、Cisco 网络设备、华为网络设备、数据库、中间件、傲天动联 WLAN 设备等进行安全基线检测。检测方式包括 Telnet、SSH、SMB、Agent 等方式。基线管理系统具备分布式大规模部署的能力，能够实现对分布环境下的大规模的网络进行远程管理、监测、控制的能力，对不可达网络的脱机代理检查能力。

1.3.2 脱机代理

由于不同的安全管理要求和特定的安全边界控制等要求，很多行业和客户存在大量的隔离网络，而这些网络中的设备等安全对象进行网络检查时会存在很大的空难。脱机代理实现针对不可达网络的安全基线检查工作，通过安全基线管理系统将不可达网络安全基线检查任务下发给脱机代理，将脱机代理接入隔离网络后脱机代理会自动执行安全基线配置扫描工

作，在完成扫描任务后接入安全基线管理系统会自动将脱机扫描结果自动会传到安全基线管理系统，最终完成整体的信息收集、比对和展示。

1.3.3 单机代理

基线采集代理主要针对 Windows 主机实现，很多 Windows 主机是个人使用主机，这些个人主机不想将管理员账号和密码透露。 基线采集单机代理只需部署在这些主机上，配置完成连接安全基线管理系统，只需连上安全基线管理系统即可通过安全基线管理系统进行启动任务，并会自动将收集信息传回系统平台，无需主机的管理员账号和密码。

基线采集代理可独立部署，进行系统单机，账号口令、授权、日志配置、IP 协议安全配置等方面的安全检查。

2. 产品功能

2.1 多维度安全对象管理

安全对象是对管理对象的统称，基线检查平台需要能够检查包括主机、网络设备、安全设备、中间件、数据库、WLAN 设备的配置情况。安全基线管理系统支持多维度安全对象管理功能，实现安全对象的多种维度维护和展示。安全对象管理实现从设备类型维度和业务系统域维度的安全对象管理，系统支持针对设备类型和业务等维度的安全对象树维护。

安全对象管理同时实现单设备的立即检查，对单设备的检查历史进行维护，并可以对两次检查见过进行比对。

2.2 自定义检查项管理

安全基线配置核查管理系统检查项管理根据设备类型内置对应各种设备类型和型号的检查项，检查项管理支持检查项自定义功能，实现对各种设备类型和型号设备的检查项自定义新增，支持配置向导功能方式新增和手动脚本拷贝定义新增。对新增检查项支持参数化设定和权重设定。系统内置检查项和自定义完成检查项为检查策略组合提供基础。检查项管理实现对自定义检查项的修改删除功能，系统内置检查项只能进行查看不支持编辑和删除操作，对于内置检查项的应用在策略组合参数实例化后应对不同检查要求。检查项管理是整个安全基线检查的基础要素。

2.3 可组合的策略管理

组织管理机构检查、上级单位巡查以及内部定期检查的检查要求会存在不同，不同的业务系统相同设备检查要求也会存在差异，为了满足不同检查要求和规范，安全基线配置核查管理系统实现可组合的策略管理，安全策略将已有的检查项进行组合形成不同检查要求和检查内容的检查项集合，同时支持对安全策略的参数自定义功能进行检查项的检查参数的实例化，满足不同检查要求的参数化。

完成的不同安全策略应用于不同的安全检查要求，通过任务调度管理实现任务对已有策略和检查设备的组合，最后形成不同的检查任务。

2.4 灵活简介多方式检查任务管理

安全基线配置核查管理系统组合已建安全策略和符合安全策略的安全对象形成任务模板，以便进行任务调度管理，同时支持在新建任务模板时创建检查策略功能。安全基线配置核查管理系统提供灵活的任务调度和管理功能，支持立即检查、定时检查（周期检查）和脱机检查。立即检查针对组合的检查任务立即开始进行检查；定时检查对已组合的被检查设备和已经实现参数化的检查策略执行计划任务根据计划任务设定条件自动进行检查；对于不可达网络进行检查时，服务器将脱机任务下发给脱机代理，将脱机代理接入不可达网络后脱机代理会自动执行脱机任务，待脱机任务执行完毕将脱机代理接回安全基线管理系统网络，脱机代理会自动将脱机任务结果回传给安全基线管理系统进行数据的收集、比对和分析等实现脱机检查任务。

检查任务管理结合 PDCA 模型，实现检查任务的过程管理，并从已创建、正执行、已执行等多个维度，实现对任务自身的监控、展示与统计。提供从任务到结果的追踪与展示。

安全基线配置核查管理系统任务管理实现对任务结果的全面展现，支持任务结果的导出功能。

2.5 丰富报表管理

安全基线配置核查管理系统针对各种检查结果提供在线报表和离线报表功能。

在线报表可以提供基于企业整体合规趋势比较、业务系统合规趋势以及资产合规趋势比较的趋势比较报表，基于资产合规历史对比的横向对比报表，基于企业整体合规趋势月报和资产类型合规趋势月报的趋势分析报表，基于不合规业务系统、不合规资产统计和不合规检查项统计的不合规统计报表。

离线报表通过基于模板的报表功能提供多角度、可灵活定制的安全数据分析报告。同时离线报表功能提供针对现有数据库数据源的所有字段的组合和报表模板的生成，并针对自定义模板的在线和离线方式，生成在线和离线报表报告。安全配置核查支持一次性调度、按时、按天、周、月调度，定期生成特定的安全报告。

2.6 系统管理

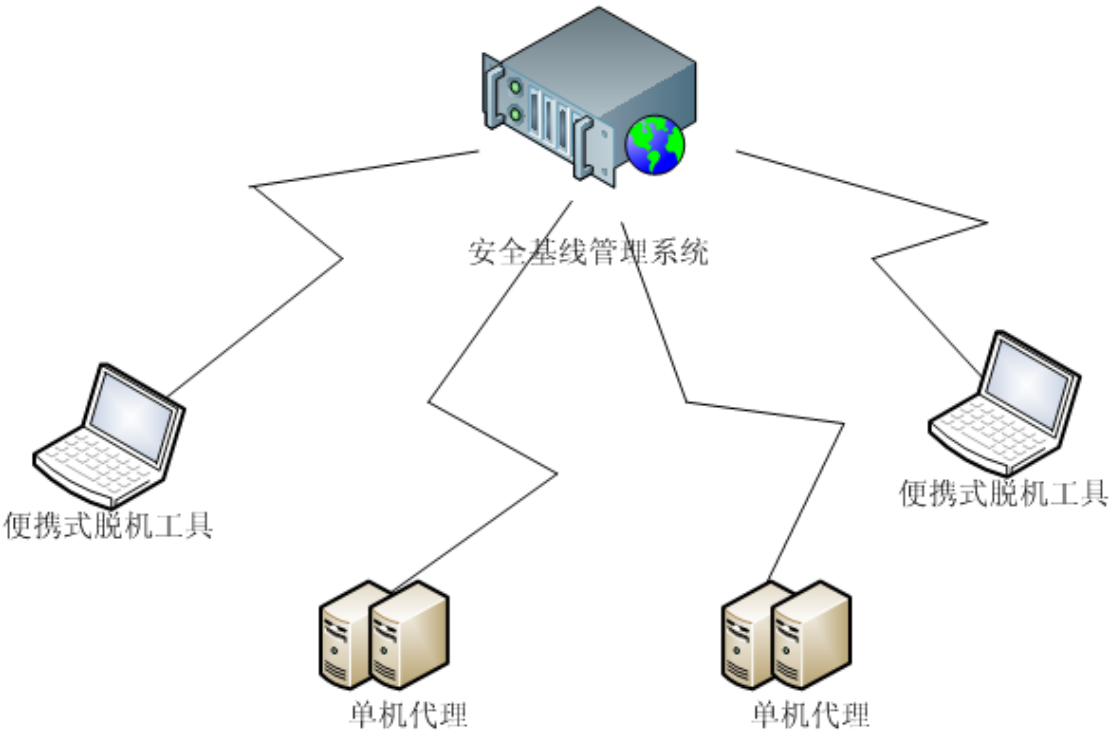
安全基线配置核查管理系统采用基于自制的、高性能、可扩展的基础架构，具备大规模、分布式模式的部署方案。

安全基线配置核查管理系统系统管理提供用户、角色和组织机构管理实现安全基线的功能权限划分。同时提供系统日志管理，实现对系统配置检查功能日志的记录；提供分布式组件管理，实现对分布式脱机代理和单机代理的管理；提供对系统数据的数据维护配置管理。

3.产品部署及解决方案说明

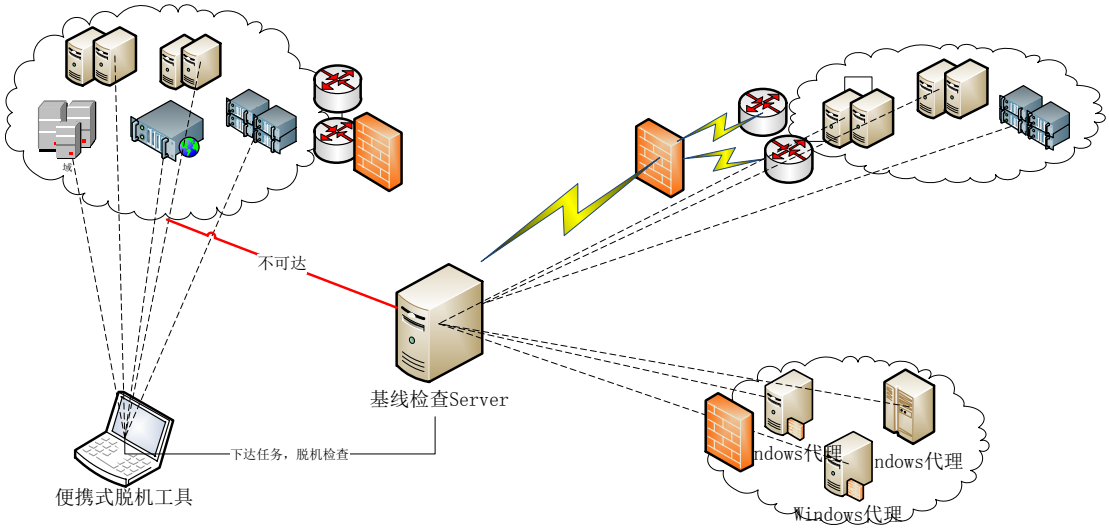
安全基线配置核查管理系统由基线管理系统平台、单机代理、脱机代理等几部分组成。安全基线管理平台提供检查项的定义、检查策略组合、检查模板的生成、检查任务的组合、调度、监控以及安全基线检查数据的收集、比对和展示等功能。单机代理是分布式部署在不同的 Windows 单机上，时实现对 Windows 主机的安全基线检查引擎。脱机代理是针对不可达网络的移动代理实现，通过安全基线管理平台获取脱机代理检查任务，接入不可达网络完成脱机检查任务，将脱机代理检查任务回传给安全基线管理平台进行比对和分析。

3.1 部署方式



4.特点及优势总结

4.1 复杂网络的多渠道检查支持



4.1.1 网络不可达的便携式脱机检查技术

通过基线系统 Server 端的便携式模块，对网络不可达设备群组配置相关检查策略并通过服务器下发任务给便携式脱机检查工具，工具脱机后连接到目标网络，执行任务检查目标

设备，脱机工具完成检查后，当与基线检查系统 Server 连接成功后会将结果上报给基线系统 Server，从而达到脱机检查网络不可达设备的目的，减少了在网络中单独建立连接，彻底排除“打孔”现象。

4.1.2 基于 Windows 系统的代理技术

对于大多数办公设备及个人 pc 设备基本是 Windows 系统，而个人 pc 设备的用户名及密码口令是不便于公布，同时存在定期会频繁更改的现象，针对这种情况，基线 Windows 的代理技术将得到广泛使用，其特点是不需要登录的用户及密码，保护了使用人本身的隐私及文件安全，同时又能对其基线配置情况进行检查。

4.1.3 支持多协议的登录检查机制

在负责的网络环境下，因承载的业务不同，目标设备所开放的登录协议也不同，这就要求基线检查必须支持多种协议的登录方式来满足检查工作的完成，目前支持 SSH2、Telnet、SMB、单机代理。

4.1.4 独立的账号密码服务

帐号及密码是基线检查需要登录目标系统的必要条件，而实际环境中存在频繁更改或定期强制性更新帐号密码的情况，鉴于这类情况，独立的帐号密码服务将解决，同时实现了多种获取方式，而又独立与基线平台之外，可单独部署。

4.2 自定义参数及任务的多方式执行

4.2.1 基于不同检查标准的自定义参数检查项

对于不同业务不同行业的基线检查往往存在各自的标准和要求，针对设备的重要性也会有不同的标准，这就需要系统能灵活的配置检查的标准，从而达到用户能按照自己的标准自定义检查项。安全基线实现自定义参数的检查项，通过策略组合形成不同的检查要求策略，并通过策略的参数实例化实现不同检查标准和检查要求。

4.2.2 任务的多方式执行

基于任务的执行是平台检查的主要方式，任务的多种执行方式，可以有效提高工作效率、

同时也能适应不同的要求，目前平台支持：即时任务、立即执行等

计划任务：确定执行时间和执行次数，周期时间的预定义任务

定时任务：确定执行的周期时间，间隔时间

单设备立即检查：对单一安全对象立即进行检查

脱机任务：下发给便携式脱机工具执行的任务

代理任务：下发给代理工作的任务

4.3 不断丰富完善的 CheckList 知识库

棱镜科技多年安全服务经验积累，形成了国内最完善的专业安全服务体系和专业安全服务方法论，制定了完善详细的安全配置检查点。不断丰富基线配置检查系统 Checklist 知识库，同时可根据不同行业相关基线规范，对知识库实现定制管理，匹配各行业安全配置需求。

同时棱镜科技安全基线配置核查管理系统提供对 WLAN 无线设备的安全配置核查支持，满足对傲天动联和武汉虹信等 WLAN 设备厂商的支持，并且会随着 WLAN 厂商设备的不断升级稳定和设备命令的丰富，实现 WLAN 设备支持 CheckList 的不断丰富和完善。

4.4 安全可靠高效的 SMB 协议支持

SMB 是基于 NetBIOS 的 API，所有的 Windows 操作系统都支持 SMB 协议，使用 SMB 协议对 windows 操作系统进行基线检查不需要安装代理服务和启动特定的服务，并且配置方便防火墙默认放行 445 端口，可以实现点对点检查也可以实现批量检查。

4.5 多维、细粒度、丰富的报表统计分析

安全基线配置核查管理系统不仅提供了常见的多维细粒度在线报表，还提供了可以自定义的离线报表，离线报表通过基于模板的报表功能提供多角度、可灵活定制的安全数据分析报告。同时离线报表功能提供针对现有数据库数据源的所有字段的组合和报表模板的生成，并针对自定义模板的在线和离线方式，生成在线和离线报表报告。安全配置核查支持一次性调度、按时、按天、周、月调度，定期生成特定的安全报告。利用安全基线能够对网络安全态势进行趋势对比分析，及时掌握网络安全配置变化，为网络管理提供有力的决策支持。

4.6 与现有安全管理平台的无缝整合及脆弱性过程管控

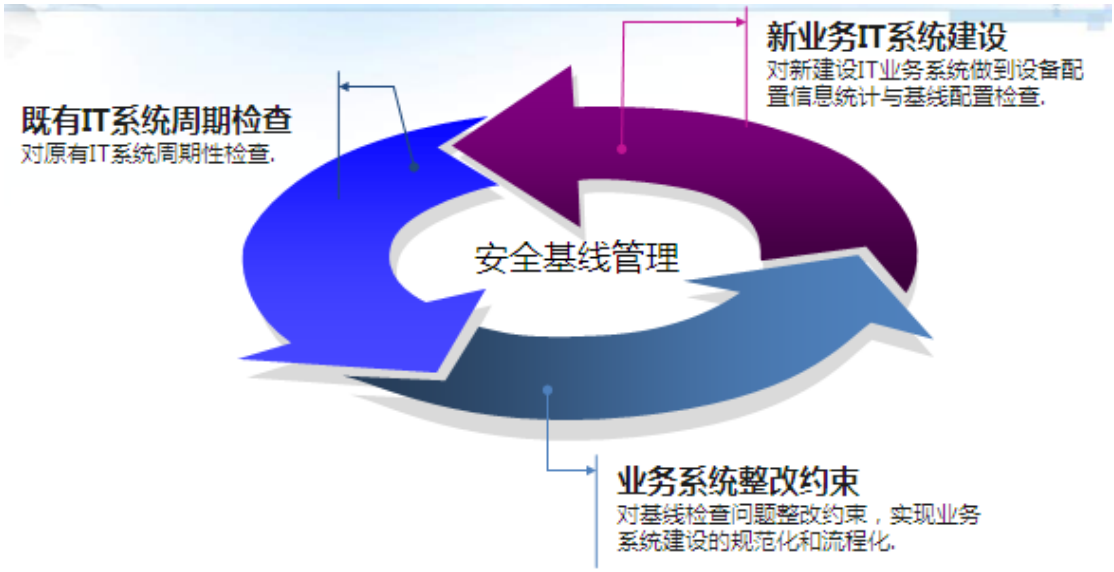
安全基线配置核查管理系统可与现有的 SOC、SMP 进行无缝整合，通过 SOC/SMP 下

发基线检查策略，驱动基线管理平台共同完成安全运营管理工作。

同时安全基线系统检查结果可以返回安全管理平台管理，安全管理平台可以针对安全基线的不同检查规范和不同检查目的的检查结果进行过程管控，了解基线检查配置弱点的整改过程情况，为安全管理工作提供更有利的过程管控信息。

5.产品价值

5.1 全面掌控 IT 系统建设风险，提供有力运维支持



安全基线配置核查管理系统可以全面实现 IT 系统建设脆弱性管理，为 IT 系统建设和发展提供有力的支持。

结合安全基线管理功能，推进新业务 IT 系统规范流程化管理。

结合安全基线管理功能，促进原有 IT 系统的检查、整改和约束。

实现安全管理工作的同步实施、发展的规范化和流程化。

5.2 全面提高工作效率，缩短风险存在时间

安全基线管理系统可以实现复杂网络多设备的自动化和周期性检查，大大缩短人工检查的时间，自动进行数据的收集比对，并提供丰富详实的报表数据，对配置漏洞项提供详细可靠的安全加固建议。使得日常安全检查可以自动化常态化，大大提高管理员的工作效率。

安全基线管理系统提高工作效率的同时，大大缩短了业务系统和设备配置漏洞的存在时间，降低安全风险，保障了网络的安全运行。

5.3 为脆弱性过程管控提供有力支撑

安全基线管理系统为脆弱性过程管控提供了有力的工具和数据支持，使得脆弱性过程管控变得可行。结合安全基线周期性检查和加固整改，安全管理可以全面的了解不同检查的周期性检查结果和过程整改结果，全面的掌握脆弱性的发展，同时也为 IT 系统建设和发展提供有力的过程指导依据。

6.总结

棱镜科技多年的安全服务实践，充分结合用户对安全评估产品的实际应用需求，推出的棱镜科技 WLAN 基线配置检查系统，可对网络中的资产设备以及 WLAN 设备进行细致深入的安全配置检测、分析，并给用户提供专业、有效的安全配置建议，提高检查结果的准备合规性，简化用户运维难度。

同时从另一个方面考虑，安全基线检查系统从技术层面对安全配置进行全面、高效的检查，但对于业务系统特有的安全问题以及业务系统管理层面的问题，仍需要结合传统的安全评估服务手段以及传统的安全检查工具（如：漏洞扫描、web 扫描）来实现。