SANGFOR
深信服科技

深信服基线核查系统
BVT-1000 V3.0 白皮书

深信服科技股份有限公司

2019 年 08 月 03 日

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

深信服科技股份有限公司在编写本文档的时候已尽最大努力保证其内容准确可靠，但深信服科技股份有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如果您有任何宝贵意见，请反馈至：

地 址：深圳市南山区学苑大道 1001 号南山智园 A1 栋

邮 编：518055

电 话：0755-86627888

传 真：0755-86627999

您也可以访问深信服科技网站：www.sangfor.com.cn 获得最新技术和产品和方案信息。

目 录

1 概述

随着信息化建设的深入发展、设备种类不断增加，安全配置管理问题日渐突出。为了维持 IT 信息系统的安全并方便管理，管理员必须从入网审核、验收、运维等全生命周期各个阶段加强和落实安全要求，同时需要设立满足安全要求的基准点。

2 需求背景

2.1 法规标准要求

2.1.1 等级保护

第三级网络安全等级保护基本要求		
层面	**控制点**	**要求项**
安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
		应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
	访问控制	应重命名或删除默认账户，修改默认账户的默认口令；
		应及时删除或停用多余的、过期的账户，避免共享账户的存在；
	入侵防范	应关闭不需要的系统服务、默认共享和高危端口；
		应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
		应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

2.2 企业安全运维

2.2.1 设备或系统种类繁多

安全运维人员需要面对种类繁多的设备和应用，如何管理这些设备和应用的配置，或者如何定位知道这些设备配置的安全问题，是他们在安全运维过程中遇到的巨大问题和挑战。

而且，由于需管理的设备分布范围广、分属不同的业务系统，如何能快捷、方便的收集和分析这些配置，成为横亘在安全运维人员面前的一个巨大难题。

一般而言，日常运维人员需要收集和分析各种主机系统、网络设备、数据库系统以及其它中间件（如 Weblogic、Websphere 等）的配置；这些配置的收集和分析存在以下问题：

1) 部署位置多种多样；
2) 配置的表现形式和存储样式不尽相同，如有的在配置文件中、有的在注册表中；有的配置文件是一般文本，而有的又是 XML 形式；
3) 采集过程中可能还需要穿越网关设备或堡垒主机；
4) 采集时还需要一些辅助的命令或设置，如采集 Oracle 时，需要知道实例名等。

由于配置在形式上存在千差万别，如何准确地分析则成为困难的事情。

2.2.2 标准难于统一

目前，由于业界还没有形成统一的配置问题审计的行业标准，因此各家提出的标准也是不一而足，而且这些标准也是被频繁地修改，造成维护和定位困难；一般用户很难自己去跟踪和修订标准。

就当前而言，我们能接触到的标准就包括了 CIS（来自美国）、中国石化、中国移动信息管理部、中国电信以及内部标准；这些标准不仅在支持的设备类型和应用类型上存在差异，就是针对几乎相同的检查点（配置项）而言，做法也不尽相同。

上述的差异造成研究、开发、维护安全配置基线是一项工作量巨大的任务。

2.2.3 自动化程度低

以往，对于设备或应用的配置审计，一般都是通过人工方式进行，仅在上线前进行一次评估（安全加固），这样做的缺点是显而易见的：

1) 纯粹依赖人工方式，效率低下；
2) 在设备或应用上线后，不能定时地或经常性地进行评估，从而无法反映现网设备或应用的配置情况，这导致系统存在巨大的安全隐患（如未能按口令复杂度设置管理员账号）；
3) 结果比较零散，只能依赖于人工汇总。

3 产品概况

3.1 产品定位

基线核查系统协助用户实现企业内安全配置的集中采集、风险分析、处理的工作，它是企业日常信息安全工作的重要支撑。

3.2 产品介绍

主要解决企业日益繁重的安全配置管理问题。作为统一的安全配置核查和管理系统，能够准确、快速、及时地发现、汇总企业中不同厂商不同种类的网络设备、主机、防火墙、数据库、中间件的安全配置问题、漏洞情况，它主要包括如下主要功能：

1) 任务制定：提供灵活的功能用于制定不同类型或周期的安全基线检查任务，任务中可以方便地设置检查对象和检查策略。

2) 采集分析：全面集中检查和分析各类系统存在的本地安全配置问题、漏洞脆弱性、弱口令等，减轻用户因对不同设备分散管理而带来的冗余工作。

3) 违规报告：提供全面、详尽、清晰的扫描报告管理功能，并能对不同的检查结果进行比对。

4) 系统加固：提供详尽的、可实际运用的系统加固方案，以指导用户对产生的安全问题进行解决。

4 产品架构与性能

4.1 产品架构

基线核查系统是由综合展现层、业务功能层、分析处理层、采集层等部分组成，如下图所示：

图 4.1 基线核查系统功能架构

在基线核查系统中，管理控制台主要由漏洞管理（主机漏洞、WEB 漏洞、弱口令）、基线检查、变更检查、整体概览、个人工作台、资产管理、告警管理、报表管理、知识库管理、系统管理组成。

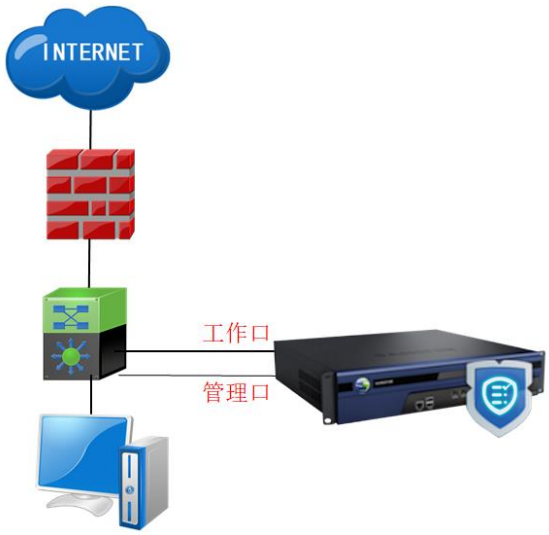
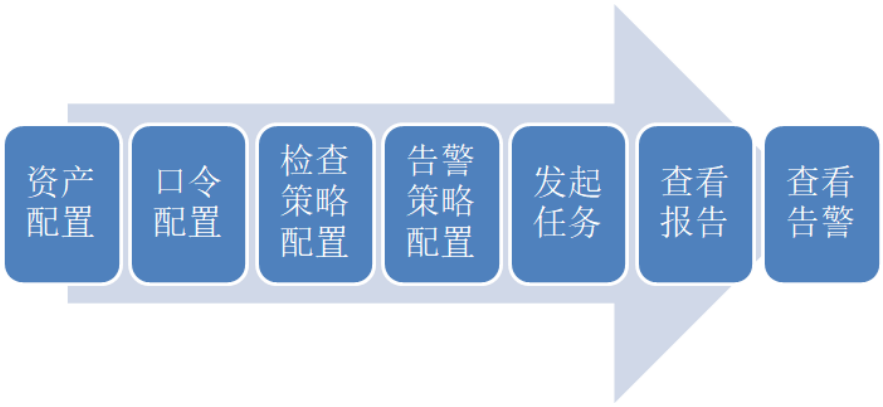


图 4.2 基线核查系统部署图

4.2 工作全流程



1) 基线核查与变更检查可以通过 SSH 等协议远程登录设备进行配置收集，漏洞扫描、WEB 扫描可以通过创建任务直接发起检查；

2) 分析结果；

3) 报告不合规配置或漏洞；

4) 若满足告警条件，则触发告警。

5 产品功能与特性

5.1 产品功能

5.1.1 安全基线检查

在基线核查系统中，安全基线是指各类系统、设备的安全配置标准；而安全基线的违规问题是指实际的系统或设备的配置违反了基线的要求。例如是否存在不允许的用户账号、账号的口令策略存在一定问题（不满足复杂度、长度、更改时间的要求）等等。

安全基线管理的作用主要体现在如下几个方面：

1) 安全评估工作常态化；

2) 有利于提高设备自身防护的能力；

3) 为安全风险评估提供基础材料。

安全基线可被划分为账号类、口令类、授权类、日志配置类、路由配置类等等，例如：应删除或锁定与设备运行、维护等工作无关的账号等。

目前，支持的系统或设备主要包括：

1) 主流操作系统（如 Linux、Unix、Windows 等）；

2) 主流路由器/交换机（如思科、Juniper、华为、中兴、锐捷等）；

3) 主流防火墙（如飞塔、思科、Juniper、迪普等）；

4) 主流数据库（如 Oracle、SQL Server、MySQL 等）；

5) 主流 Web 中间件（如 Weblogic、Websphere、IIS、Apache、Tomcat、Nginx 等）；

6) 主流虚拟化平台（如：VMware Esxi、VMware Center、Xen 等）。

安全基线管理主要分以下模块：

1) 安全基线违规问题查看：列表查看登录用户权限范围存在的安全基线违规问题，显示某违规问题在哪些资产上存在；

2) 安全基线检查任务管理：任务管理包括三个部分：正在执行的任务、已定义的任务和任务执行的结果，即检查报告，报告可以导出为 Word、PDF、HTML 等格式，如下图：

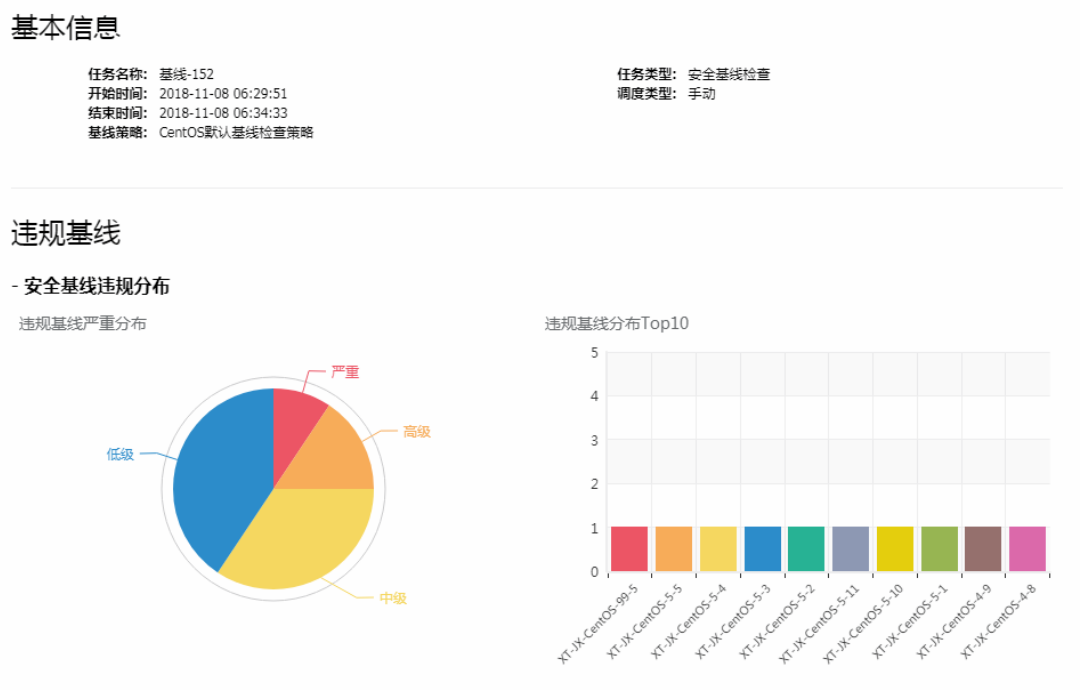


图 5.1 基线核查系统的任务报告

3) 策略管理：用户可以自定义基线检查策略。可通过选择系统内的基线项进行组合。另外可设定用户自定义基准值，例如口令长度要求等。

5.1.2 配置变更检查

配置变更检查计算机系统的文件、端口、进程等的变化信息，以监控系统的变更状况发现其中的异常，以便及时采取相应措施保护系统安全。

目前，支持的系统或设备主要包括：

1) 主流操作系统（Linux/Unix、Windows）；

2) 主流路由器/交换机；

3) 主流防火墙。

变更检查主要分以下模块：

1) 配置变更项问题查看：列表查看登录用户权限范围存在的配置项变更问题，显示资产上存在哪些配置项变更的情况；

2) 任务管理：任务管理包括三个部分：任务列表、正在执行的任务以及已完成的任务，检查报告可以导出为 Word、PDF、HTML 等格式；

3) 策略管理：用户可以自定义检查策略。可设定用户自定义配置检查项，例如文件、目录、端口、进程等。

5.1.3 漏洞扫描

所谓漏洞是脆弱性的一个子集，专指可通过扫描器发现的脆弱性，其中部分具有国际上标准的 CVE 编号；而如企业没有安全管理负责人之类的脆弱性则不被认为是漏洞。

系统支持分布式的漏洞扫描模式以及集中的漏洞分析、处理。

在漏洞管理中，能够集中查看、统计系统存在的系统漏洞。还可以制定扫描策略及任务，对系统内安全资产进行一次或周期性的扫描。

系统支持设置 IPv4 地址段或选择资产的方式扫描对象；也可以支持对单个 IPv6 地址对象扫描。

漏洞管理主要分以下模块：

1) 漏洞查看：列表查看登录用户权限范围存在的漏洞，显示某漏洞在哪些资产上存在；可显示相关漏洞的详细情况；

2) 扫描任务管理：漏洞任务管理包括三个部分：任务列表、正在执行的任务以及已完成的任务，报告可以导出为 Word、PDF、HTML 等格式；对于正在执行的任务用户可以停止、暂停或继续任务的执行；

3) 扫描策略管理：用户可以自定义漏洞扫描策略（通过选择系统内存在的插件）；

4) 系统提供定期的扫描插件升级服务。

5.1.4 WEB 漏洞扫描

随着网络科技的不断变更发展，相对于 C/S 架构软件的高成本、高维护性，较为便捷的 B/S 架构 WEB 应用广泛应用于政府部门、网上购物、银行交易、虚拟货币等领域。伴随而来的则是突出的安全问题。据知名站点（EXPLOIT-DATABASE）数据统计，至 2017 年底已发现的 WEB 漏洞数量大约 22600 多条，数量日渐增多。

常见的 WEB 漏洞为：

网站挂马：使访问该网站的用户感染木马，对网站信誉造成极大的不良影响。

数据泄露：泄露该网站所有用户信息，直接影响到用户的信息、财产安全问题。

数据篡改：篡改者在网站上留下虚假信息，对用户实施诈骗手段。

钓鱼网站：伪装成银行、购物网站等，获取用户信息。

SQL 注入：通过 SQL 注入恶意语句，导入数据库无法正常工作，以达到不法目的。

……

扫描方式：

通过深度探测端口与服务扫描网站站点信息，遍历整个 WEB 框架目录结构，自动分析产品源代码，通过匹配插件库与测试验证来证明漏洞的存在，扫描结果漏报、误报率接近零。

在 WEB 漏洞管理中，能够集中查看、统计站点存在的 WEB 漏洞，还可以指定扫描策略及任务，对域名内站点安全进行一次或周期性的扫描。

通过内置或指定的扫描任务，配置任务周期来扫描指定的站点、资产、URL 等。

执行结束的任务产生任务报告，报告内指出发现哪些漏洞、次数，在哪个设备哪个 URL 上发现漏洞，并可导出报告文件。

可在漏洞列表中查询相关漏洞信息，并可查看该漏洞解决方案。

5.1.5 资产管理

安全资产是基线核查系统的管理对象。与 ISO27001 中关于资产的定义略有不同，基线核查系统中的资产是特指具有 IP 地址的 IT 类设备及在此之上运行的、可管理的服务、应用。

一般而言，安全管理中的资产具备如下两类属性：

1) 基本属性：名称、编号、系统类型（产品类型、操作系统类型、版本等）、IP 地址（支持 IPv4 和 IPv6 规范）、响应人（出现安全问题应由何人处理）、登录凭证（获取配置、安全基线检查等使用）、上架信息等；

2) 安全属性：完整性、可用性、保密性、风险信息、开放端口、安全基线违规问题等；

系统的资产管理支持用户录入、导入或自动发现资产。

为了处理不同网络的资产同 IP 问题，系统还支持对于网络和 IP 地址段的管理。

为了用户便于集中、灵活地管理所辖范围内的资产，系统支持用户自定义资产管理视图。

5.1.6 告警管理

告警管理是指针对用户特别需要关注的安全问题进行告警，这些问题来源于高危漏洞、安全基线违规问题等。

告警管理中包括了如下功能：

1) 告警监控：监控系统内存在的各种告警信息；用户可以通过定义过滤器以监控需要特别关注的告警信息；用户也可以根据个人需求，设置告警的提示音、界面显示方式等；

2) 告警处理：处理监控列表中的相关告警事件；针对告警事件，用户可以选择清除或确认（不能确定是否需要处理）；

3) 告警复核：对已确认的告警事件，如终端已做修复处理，可以通过复核任务对修复结果进行复核；

4) 策略定义：用户可以定义各类告警事件产生的策略（系统内置了部分策略）；在告警策略中可以设定对于安全数据的筛选条件、归并字段、时长和次数以及命中后产生何种响应；响应包括包含发送邮件、发送 Syslog 或 SNMP Trap、执行外部程序或脚本等。

5.1.7 报表管理

报表管理的作用为展示系统安全工作的结果。报表内容包含各种信息的统计情况，包括：告警报表、资产报表、安全基线报表、配置变更报表、漏洞报表、工单报表等。

用户可以定义相关条件以生成报表，它们均可以导出为 PDF、Word、HTML 等格式。

5.1.8 知识库

知识库管理为系统运行和维护提供了知识来源以及安全问题的处理依据、方法和参考，目前支持如下几类：

1) 安全基线类：各种操作系统、网络设备、防火墙、Web 中间件及数据库等可被威胁所利用而导致安全性问题的标准描述及解决方案；

2) 漏洞类：通过扫描器发现的在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷的描述及解决方案；

3) 安全经验类：基于系统安全事件、漏洞、配置问题等信息综合生成的安全警示信息的描述、告警触发建议及解决方案等。

用户可以通过全文检索功能对系统提供的安全知识进行查询。

5.1.9 系统管理

系统管理的主要功能在于管理支撑平台正常运行的各种基础功能和参数配置。主要功能有：用户管理、系统参数管理、内置对象管理、升级管理、许可证管理、日志管理、口令策略管理等常用工具。

5.2 产品特性

5.2.1 全面支持 IPv6

积极响应国家政策，对 IPv6 全面支持。

5.2.2 IT 资产自动探测

支持资产自动发现，发现长期无人维护的资产，减少运维人员日常维护工作。

通过资产发现，对未知资产进行探测，发现资产后看将资产纳入资产管理，统一对其进行安全检查，不留安全隐患。

5.2.3 离线检查

针对离线设备，如一些重要性极高，只在一个独立子网里运行的设备，可以通过离线检查脚本在设备本地进行安全基线配置采集，下载后上传至 BVT 在线分析。

无需远程接入，也可安全检查。

6 产品优势与价值

6.1 产品优势

6.1.1 自动化巡检

支持定期的配置收集和审计，任务调度方式包括定时（日、周、月）、手动、立即执行、一次运行等多种方式，灵活实现了人工评估的自动化和常态化，降低了运维人员的运维成本。

6.1.2 多维度核查

支持主机漏洞扫描、WEB 漏扫、弱口令扫描、安全基线检查、配置变更检查，全方位、多维度的进行资产安全性检查，发现各类脆弱性。

6.1.3 自定义策略参数

支持用户自定义的检查策略和告警策略，根据实际的业务需要，在内置策略的基础上进行参数定制，更符合企业内控管理要求。

6.1.4 自动化发现

一键自动发现资产、与资产上的网站，使长期无人维护的设备一扫而现，对资产进行网站发现，更便捷的对网站进行管理，可直接在资产上进行网站扫描，发现安全漏洞，以资产为视角查看网站安全情况。

6.1.5 闭环脆弱性处理机制

告警复核功能可以验证脆弱性的修复情况，复核任务将自动调用原先产生脆弱性告警的任务，对安全脆弱性（漏洞、违规基线等）进行复核，验证脆弱性是否已修复，大大提高了运维管理的效率。

6.1.6 安全加固还原依据

发现系统安全问题后，对资产进行安全加固后，通过配置变更检查，将系统各项配置、端口、服务等作为基线值，即安全的系统配置状态，当由于各种原因导致系统的配置发生变化后，可以作为恢复的依据，快速恢复到安全的系统配置状态。

6.1.7 变更检查发现入侵痕迹

遭受黑客入侵后随之带来的启动恶意木马程序、开放恶意端口、修改配置文件、植入账号、提权账号等行为，通过变更检查，可以及时的发现端口、进程、启动项、账号等各种配置状态的变化，警示运维人员变化点，提供对比报告，异常配置清晰可见。

6.2 产品价值

1) 配置问题管理：全面集中检查和分析各类系统存在的本地安全配置问题，减轻用户因对不同设备分散管理而带来的冗余工作；

2) 漏洞问题管理：全面集中扫描和分析用户各类信息系统或设备存在的安全漏洞问题，以用户业务为视角，自动地完成以往需安全专家才能完成的风险分析工作；；

3) 扫描报告管理：提供全面、详尽、清晰的扫描报告管理功能，并能对不同的扫描结果进行比对；

4) 安全运维管理：建立日常运维工作的服务保障体系；包括各种资产配置库、报表管理、安全知识管理等。

7 产品应用场景

7.1 设备上线检查

需求：IT 设备上线前的安全检查，通过检查的设备方可接入业务网运行。

解决方案：使用 BVT 根据业务情况对其进行漏洞扫描、配置基线核查，检查是否有漏洞以及配置安全隐患。

预期效果：被检查设备发现中级以上漏洞和配置违规项，导出报告提交用户根据参考建议进行安全加固。

7.2 定期运维检查

需求：在长期的运维中，如系统割接，可能会因为运维图方便，开启了某些不安全的配置，放行了某些端口，产生了安全隐患，需要周期性地对内网各类设备进行安全检查，发现漏洞、安全加固。

解决方案：使用 BVT 根据业务情况对其进行漏洞扫描、配置基线核查，检查是否有漏洞以及配置安全隐患。

预期效果：被检查设备发现中级以上漏洞和配置违规项，导出报告提交用户根据参考建议进行安全加固。