

LanSecS[®]

云用户行为分析系统



LanSecS[®] 云用户行为分析系统

产品概述

LanSecS[®] 云用户行为分析系统是一款对桌面用户操作行为进行全面捕捉分析与审计管理的软件产品。系统通过录屏方式记录用户的完整操作过程，形成录像文件上传到管理中心端。管理中心端抽取录像文件中的操作文本形成录像检索，并可完整回现用户的会话过程，直观反映用户的操作行为。管理者可根据需要随时切入被监控端的用户桌面，实时查看用户的操作行为，以保障业务应用操作的合规性和安全性。

产品架构

LanSecS[®] 云用户行为分析系统由采集代理 (Agent) 和集中管理平台两部分组成。通过部署在桌面或服务器上的 Agent 完成用户操作行为的捕获及内容审计功能，通过集中管理平台实现会话录像、关键事件、文本与操作过程取证的匹配和管理功能。



图1 产品架构图

产品功能

用户登录会话审计

LanSecS[®] 云用户行为分析系统完整记录一次用户登录到退出之间的所有操作的屏幕记录，包括操作时间、用户账号、IP 地址、行为进程、动作类型等，每一项会话都可以通过会话索引进行录像回放，实现零盲点监控。审计录像无需下载，支持浏览器直接播放。

操作行为审计

LanSecS[®] 云用户行为分析系统可对用户操作行为数据进行全面采集，并可根据动作类型、应用程序、关键事件动作等提取用户操作行为的相应文本进行会话组织。管理者可以根据需要针对具体的操作行为进行定点录像回放，监查用户操作的完整会话过程。

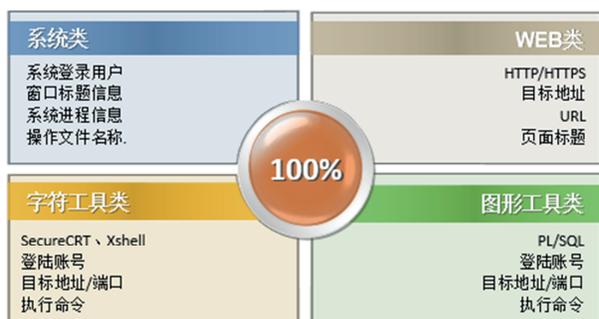


图2 数据采集

操作行为实时监控

LanSecS[®] 云用户行为分析系统可以根据需要随时切入被审计端的桌面，在被审计用户无感知的情况下对当前正在进行的会话连接提供实时的屏幕监控功能，便于对重点主机的实时抽查，保障用户业务操作的合规性。

图表化审计概览

LanSecS[®] 云用户行为分析系统的仪表盘功能将常用的数据统计图表化，管理员可以通过仪表盘快速的浏览系统的监控情况，并可点击图表中相应内容进行定位，便于安全威胁的快速发现并及时跟进处理。

统计报表

LanSecS[®] 云用户行为分析系统根据监控到的各类审计信息进行分别统计，以柱状图、饼图的形式形象的展现出来，同时也支持用户以 excel、word、PDF 等格式导出统计信息，方便纸质留存和审查分析。

▶ 产品部署

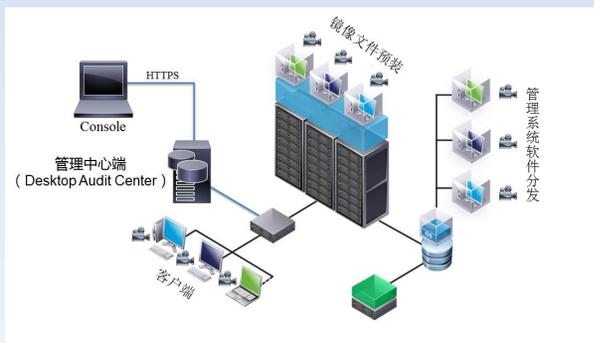


图 3 部署示意图

部署安装

LanSecS[®] 云用户行为分析系统是一款纯软件的产品，采用管理中心端 + 客户端的部署模式。

▶ 产品特色

全面的用户行为数据采集

LanSecS[®] 云用户行为分析系统可对四大类桌面用户操作行为（系统类、WEB 类、字符工具类、图形工具类）进行全面的监控采集，并可提取数十种操作文本信息。即使是加密环境，系统也可实现完整的用户行为数据采集。

多维度的用户行为审计记录

LanSecS[®] 云用户行为分析系统从用户登录会话审计、操作行为审计、用户行为实时监控等多个维度对用户行为进行全面的审计记录，确保用户桌面操作行为审计无盲点。

高效的用户行为合规检查与取证

LanSecS[®] 云用户行为分析系统通过用户操作行为分析，可准确判断用户操作意图，有效识别用户异常操作，检查业务应用系统的操作是否符合规范，实现异常行为的调查与取证。

灵活的自定义分组管理

LanSecS[®] 云用户行为分析系统可将所有的被审计端分组管理，各个分组执行不同的审计策略，满足不同的管理要求。

▶ 产品优势

独特的录像与文本相结合行为分析模式

LanSecS[®] 云用户行为分析系统通过特有的录屏方式记录用户的完整操作过程及详细内容，抽取相应操作行为为关键文本作为索引，有效的保障了无死角审计要求。

安全规范的全面满足

录像方式的审计功能，更易于满足信息安全等级保护、SOX、PCI DSS、HIPAA，和 ISO 27001 等标准对监控和审计的要求。

业务情况的直观分析

通过用户操作行为的录像回放，有利于检查用户业务应用操作的合规性，并可对业务故障直观的进行分析。

操作行为审计不受应用环境的影响

LanSecS[®] 云用户行为分析系统独特的审计模式，不会出现受到用户使用加密型应用的影响而无法有效审计的问题，对数据泄露起到了有效的防范震慑作用。

多平台的支持

LanSecS[®] 云用户行为分析系统支持 Vmware、Citrix、华为、乾云、KVM 等国内外主流虚拟化平台，全面支持 32 位和 64 位的 windows Xp、Win7、Win8 等 Windows 桌面操作系统，以及 Windows Server 2003、Windows Server 2008、Windows Server 2012 等 Windows 服务器系统平台。

超低资源占用

LanSecS[®] 云用户行为分析系统数据采集客户端采用变化区域动态录屏模式，视频图像高度压缩，每小时不间断的操作会话录像仅需消耗 5-20M 存储空间。客户端的资源占用率极低，在有操作行为时，客户端占用 CPU 在 1-5% 之间，占用内存 100M 以内，链路带宽 400Kbps 左右。对用户正常操作无任何影响，录像时不会出现屏幕闪烁的现象，保证终端用户在桌面端的操作无感知。

▶ 应用场景

业务分析

通过 LanSecS[®] 云用户行为分析系统的录像回放和实时监控功能，可以完整的观察到桌面用户的操作行为过程，对用户的操作合规性、操作意图等有着直观的认识，更容易判断用户操作该行为目的。并且在出现业务应用故障的时候，也能直接回现故障出现真实情况，有利于对业务应用的问题进行分析处理。

运维管理

LanSecS® 云用户行为分析系统可以全面监管桌面用户的运维行为，对现有的外包运维人员、IT 管理人员、内部高权限人员等的人员操作行为进行有效的审计。对于出现问题的时候，可以直接追溯到操作源头，为取证举证提供充分的依据。并且，LanSecS® 云用户行为分析系统还可以对 IT 外包人员的工作量进行有效的统计，直接掌握外包运维人员的工作效率。

数据防泄漏

LanSecS® 云用户行为分析系统不会受到桌面用户所采用的应用环境而影响到数据采集审计效果，无论用户通过 QQ 即时通讯工具、网盘云存储、Mail 邮件等互联网方式或通过 U 盘、移动硬盘、文件打印等本地方式，都可以做到有效的审计管理。



北京圣博润高新技术股份有限公司
BEIJING SBR HIGH-TECH CO.,LTD

地址：北京市海淀区高梁桥斜街59号院2号楼3层 / 邮编：100044 / 电话：010-82138088 / 技术支持热线：
8008102332/4009662332 / 技术支持邮箱：support@sbr-info.com / 网址：www.sbr-info.com