佰倬数安终端版

（EE）

产品白皮书

3/2021

目录

1. 背景概述

随着 IT 技术的飞速发展以及互联网的广泛普及，各级政府机构、组织、企事业单位都分别建立了自己的网络信息系统。企事业单位在享受网络应用技术的快捷和方便的同时，其数据安全问题也日益突出。病毒泛滥、系统漏洞、黑客攻击等诸多问题，已经直接影响到企事业单位的正常运营。如何应对网络安全威胁，确保企业终端数据安全，为企业单位运营提供可靠的安全保障，已经是每一个企业单位决策者不得不关注的问题，也是每一个网络管理员不得不面对的挑战。

当前，数据安全问题已经引起了人们的高度重视，国内外政府也及时颁布了各种数据安全法规，譬如我国推出的《网络安全法》、美国针对健康保险行业的 HIPPA、欧盟的 GDPR 等法规对数据安全提出了更严格的要求。然而，全球企业数据泄露安全事件仍层出不穷，各种网络勒索时有发生，并对企业造成了巨大的甚至是不可挽回的经济和声誉损失。究其原因，主要有两个：其一，黑产链活跃，有利可图。攻击者通过黑词暗链、钓鱼页面、挖矿程序等攻击手段开展黑产活动谋取暴利；资深黑客利用勒索病毒感染政府机构、大中型企业终端和服务器，对其实施敲诈勒索。据报道，仅勒索病毒 GandCrab 在一年半的时间里就获得高达 20 亿美元的赎金，而幕后主使未受到任何惩罚。其二，传统的病毒防御技术和防数据泄漏工具(DLP，Data Loss Prevention)无法应对与时俱进的新型攻击手段，譬如勒索攻击、钓鱼攻击、内鬼泄密，以及已知/未知的外部攻击等。

为了妥善处理和应对日趋严重的数据安全问题，佰倬公司创造性地提出了“加密隔离、数据自保”理念。从源头开始，在系统可执行环境内加密隔离出一块安全

的数据活动空间，所有对受保护数据的访问活动都在此安全数据活动空间进行。同时，对于需要保护的数据，在系统驱动层设置安全岗哨，对数据进行自动加密保护，对进程访问进行强制管控，将文件加解密与强访问控制结合成一个整体，并对系统计算性能进行实时监测，从而达到数据对已知和未知病毒免疫，实现数据自保；与此同时，各个终端上的安全岗哨自动与中央岗哨平台连接，将岗哨记录和系统性能实时汇总到中央岗哨平台，并在中央岗哨平台上实现对各个服务器/终端的数据安全及系统性能进行管理、控制、感知、分析、预警、和可视化展示，实现边缘安全自保与中央管控检查的完美结合。

2. 产品简介

2.1 产品概述

佰倬数安终端版（简称：EE）是佰倬公司基于“加密隔离、数据自保”核心技术专业打造的一款企业级终端数据安全防护产品，拟解决企业终端数据从产生、存储、使用、传输、到销毁全生命周期的安全问题。通过“驱动层加密”和“超强访问控制”的智能集成，构建端到端的可信安全无缝链，实现了企业终端数据“内网无感知、外发需审核、集中可管控”的终端安全体系，保障了数据“可用不可得”。

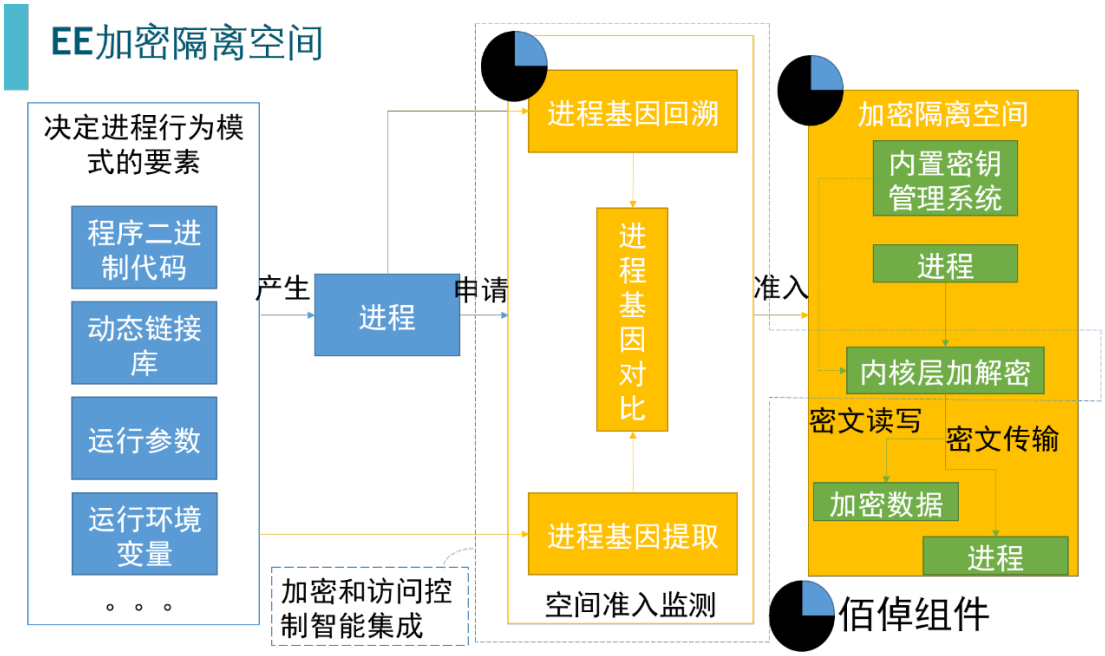
具体来讲，佰倬数安终端版在终端可执行环境中加密隔离出一块安全的数据活动空间，确保所有对受保护数据的合法访问操作都在此安全数据活动空间中进行。对于需要保护的终端数据，佰倬数安终端版在系统驱动层设置安全岗哨，对数据进行自动加密保护，对进程访问进行最小权限的强制管控，将文件加解密与超强访问控制结合成一个整体，构建端到端的可信安全无缝数据使用链，并对系统计算性能进行实时监测，从而达到数据对勒索攻击、钓鱼攻击、内鬼泄密，以及所有已知/未知的外部攻击的免疫，实现数据自保。同时，各个受管终端（已部署佰倬数安终端版的终端）上的受保护数据都是加密保存的，并且能够在受管终端间无缝共享。当受管终端需要外发受保护文件时，需向强制外发审核系统发出申请，只有通过审核批准后，才会自动明文外发。借助中央岗哨平台，各个受管终端上的安全岗哨会自动将终端岗哨记录和系统性能实时汇总到中央岗哨平台，并在中央岗哨平台上实现对各个企业终端的数据安全及系统性能进行管理、控制、感知、

分析、预警、和可视化展示。

2.2 设计理念

面对日趋严重的数据泄漏威胁和不安全的网络环境，佰倬科技创造性地提出了数据自保理念，不再纠结于传统的网络系统安全泥潭，而是以数据为中心，基于“加密隔离、数据自保”核心技术研发出了一系列的数据安全产品，同时取得了 20 余项国际专利，广受业界好评。其“加密隔离、数据自保”核心技术基本原理如下：

2.2.1 加密隔离原理



图一：加密隔离原理示意图

如上图所示，佰倬数安终端版对数据的安全防护，主要基于以下几点：

（1） 佰倬数安终端版在操作系统层“挖出”一块加密隔离空间，包括被保护的加密数据以及被批准进入空间的进程。其具体流程如下：IT 管理员首

先通过 EE 中央岗哨平台对计算机执行环境中的可信程序进行授权，并指定需要保护的数据，建立数据安全策略。EE 客户端中的操作系统加密增强模块根据数据安全策略对需要保护的数据进行加密保护，并基于程序进程指纹、进程动态链接库、运行脚本、运行参数以及加密数据的保护标识，建立岗哨白名单，在系统驱动层设置安全岗哨，只有通过安全岗哨监察的合法进程才被允许访问被加密保护的数据。进程一旦被授权，操作系统加密增强模块将在系统内核中加密隔离出一块安全的数据活动空间，自动将被加密保护的数据解密其中以供授权进程合法使用。而非法进程的访问将被安全岗哨实时阻挡。从而，以中央岗哨平台为起点，结合授权程序、动态链接库、配置/脚本文件、运行参数/环境变量、授权进程、加密隔离内存，到加密保护文件，佰倬数安终端版运用密码学技术在计算执行环境中建立了一条完整的可信安全链。

(2) 加密隔离空间的加密特性：进程一旦被批准进入空间，便可以访问加密数据，产生的数据也是加密保护的，而且空间内的进程之间可以安全通过加密信道通信；

(3) 加密隔离空间的隔离特性：空间外的进程不能访问空间内的加密数据，也不能与空间内的进程通信；

(4) 进程进入加密隔离空间时需要通过严格的准入监测，在授权过程中，佰倬数安终端版提取决定进程行为模式的要素，也叫进程基因，在进程申请进入加密隔离空间时，佰倬数安终端版回溯此进程的基因，只有进程的基因和授权进程基因吻合，此进程才可以进入加密隔离空间，从而

保证加密隔离空间的进程行为模式是完全可控的；

(5) 上述空间准入监测是进程级的访问控制，能够给予同一程序生成的不同进程不同的数据访问权限，远远领先于 SELinux 等程序级的强访问控制；

(6) 加密隔离空间的内核层加解密模块使得加密数据访问和加密进程通讯对空间内的进程是透明的，无需修改空间内的进程来适应加密隔离空间；

(7) 空间准入监测和内核层加解密模块又是紧密结合的，组成强访问控制与加密的智能集成模块(SIME)，一损俱损，如果空间准入监测被关闭，内核层加解密也同时关闭，保证加密数据绝不泄漏；

(8) 实时监测加密隔离空间内的数据安全；

(9) 佰倬数安终端版内置安全岗哨实时记录被保护数据访问日志和系统运行情况，并将其上传到中央岗哨平台，平台收集运行情况，对各终端的数据安全和系统运行情况进行态势分析、预警和可视化展示。

2.2.2 数据自保技术

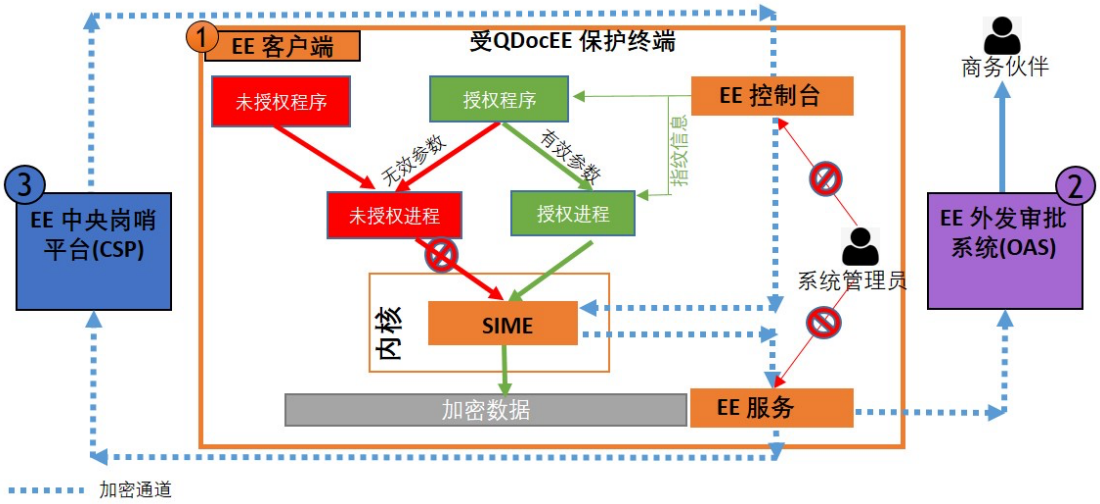
数据安全是网络安全的重中之重，只有确保数据安全，才能确保企业价值。在网络环境十分恶劣（系统漏洞层出不穷，后门防不胜防，甚至不知何时网络和系统已经被病毒侵入）的情况下，与其挣扎，不如学会与恶劣的网络环境共存。换句话说，就是把数据放置在数据保险箱中，只有被授权的进程才能访问数据，可以抵御任何已知未知的恶意软件，病毒等攻击。不管外面的环境如何，可以确保整个业务系统的核心数据安全。

佰倬特有的“**加密隔离，数据自保**”的技术，着重于搭建数据本身的安全防护体系。

- 将加密技术应用于数据活动全轨迹的各个节点，覆盖数据存储、访问、使用、传输、分发的全生命周期。
- 从系统运行环境中，加密隔离出安全工作环境，数据全程活动仅在加密隔离的安全工作环境中进行，并且多台终端加密隔离子空间互动关联，组成跨终端加密隔离总空间。数据安全策略管理和操作系统身份授权相互独立，从而防 ROOT 或系统管理员类型的数据攻击。

2.3 产品架构

佰倬数安终端版主要由 EE 客户端、EE 外发审批系统和 EE 中央岗哨平台三部分组成，如下图所示：



图二：佰倬数安终端版组成构件

其中 EE 客户端安装在企业终端上，以保护终端上数据的安全；EE 外发审批系统和 EE 中央岗哨平台部署在企业内网服务器上，为企业 IT 部门提供管理平台和为外发审核提供审批入口。其具体工作原理如下：

1. EE 客户端

   EE 客户端安装在公司终端上，其主要包括超强访问控制和加密的智能集成模块（SIME）、EE 控制台和 EE 服务。SIME 对需要保护的数据进行自动加密保护，基于进程指纹信息和加密数据的保护标识，建立岗哨白名单，在系统驱动层设置安全岗哨，只授权合法进程访问被加密保护的数据，拒绝非法进程访问被加密保护的数据。即使非法或恶意内部人员将强制访问控制强行关掉，数据仍一直保持被加密状态，无明文泄漏。EE 控制台接受来自 EE 中央岗哨平台的输入，配置数据安全策略，该安全策略最终由 SIME 执行。 EE 服务从 SIME 提取包括目标数据，来访进程的路径信息，来访的时间，访问的结果（允许或拒接）等在内的岗哨记录，以及包括 CPU 占比，内存占比，磁盘占比等在内的系统运行状态信息，并实时汇总到 EE 中央岗哨平台。

2. EE 外发审批系统

   EE 外发审批系统（OAS）与 EE 中央岗哨平台一起部署在公司内部服务器上，EE 客户端通过 EE 服务与其连接。当终端用户需要发送受保护文件给第三方商务伙伴时，首先在 EE 客户端上提交明文外发申请，该请求会自动同步到 EE 外发审批系统上。只有通过上级领导的审核批准，该受保护文件才会被解密并自动发送给第三方。从而通过强制外发审批机制来实现更高层级的数据安全防护。EE 外发审批系统采用多级审批，确保敏感数据安全；同时保留所有

外发解密文件记录，以备事后追踪溯源。

3. EE 中央岗哨平台

EE 中央岗哨平台（CSP）部署在公司内部服务器上。各个受 EE 保护终端上的 EE 控制台和 EE 服务自动与其连接，并将终端上的岗哨记录和系统性能实时汇总到 EE 中央岗哨平台。在 EE 中央岗哨平台上，IT 管理员可以对所有受 EE 保护终端的数据安全及其性能进行管理、控制、感知、分析、预警、和可视化展示。其强大的身份验证机制和高级多级授权特性使得同时管理大批量终端数据安全操作变得简单，快捷和安全。

2.4 产品运行环境

2.4.1 客户端操作系统要求

EE 客户端支持部署于 Windows 操作系统（64 位），包括 Windows 7、Windows 8、Windows 8.1、Windows 10 等。

2.4.2 服务器操作系统要求

EE 服务器支持部署在 Cent OS 7.6 平台上。

2.4.3 系统/第三方软件兼容性要求

兼容所有系统/第三方常用软件和常用杀毒软件，譬如：360，卡巴斯基，火绒，趋势和金山毒霸等。

3. 产品优势

3.1 安全可靠

佰倬数安终端版对企业终端上敏感数据进行全方位防护， 能有效防止:

- 数据泄漏；
- 勒索软件攻击；
- 网络钓鱼攻击；
- 内鬼泄密；
- 具有管理员权限的内部人员恶意破坏；
- 其他已知/未知的外部攻击；
- 系统漏洞/后门。

3.2 简单易用

只需简易配置，佰倬数安终端版就能立即生效，确保终端数据安全:

- 终端用户不需要进行任何配置操作。佰倬数安终端版自动在系统执行环境中加密隔离出一片安全数据活动空间来完成对受保护数据的所有操作，在不影响终端用户使用习惯的情况下，提供数据安全防护。
- IT 管理员通过 EE 中央岗哨平台的友好用户界面对所有受佰倬数安终端版

保护的终端单一或群组进行远程数据安全策略配置。

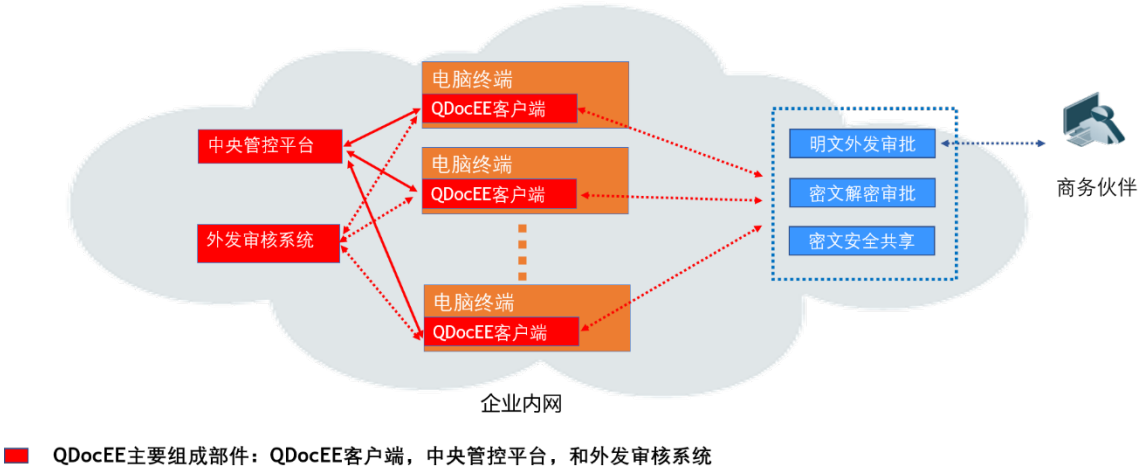
3.3 信息丰富

EE 中央岗哨平台实时汇总各个受佰倬数安终端版保护终端的岗哨信息，并进行管理、控制、感知、分析、预警、和可视化展示。包括：

- 目标数据，来访进程的路径信息，来访的时间，访问的结果（允许或拒接）等在内的精细粒度岗哨记录；
- CPU 占比，内存占比，磁盘占比等在内的系统运行状态信息。

4. 功能特性

佰倬数安终端版对企业终端上的重要数据进行安全防护，防止内部员工泄密和外部人员非法窃取、篡改、破坏、勒索企业重要和敏感信息，实现、企业终端数据从产生、存储、使用、传输、到销毁全生命周期的保护。其主要部件和部署如下图所示：



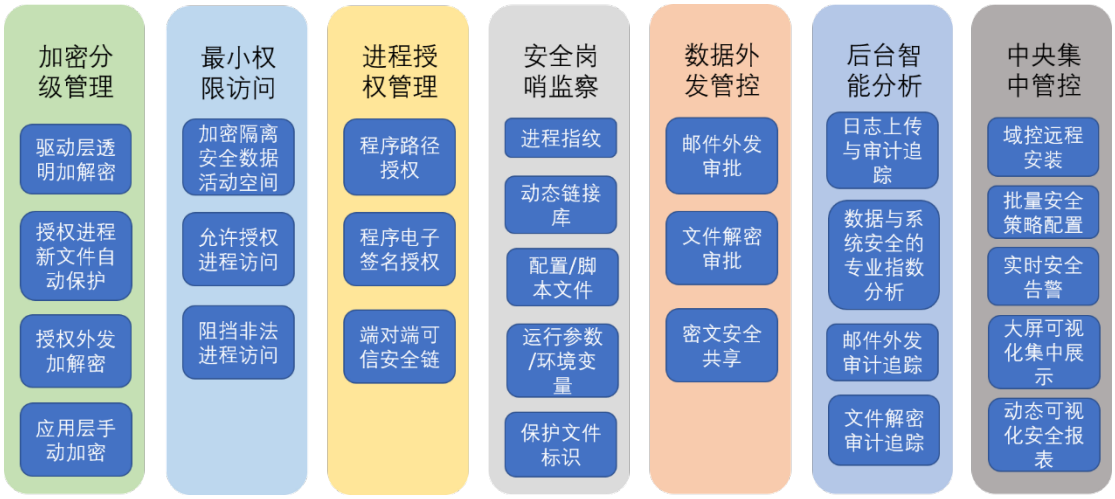
图三：佰倬数安终端版主要部件和部署示意图

其中 EE 客户端部署在企业电脑终端，以确保终端上机密数据的安全；中央管控平台和外发审核系统架设在企业内部服务器上，中央管控平台为企业 IT 部门提供管理平台，而外发审核系统为终端用户外发审核提供审批入口。

4.1 主要功能模块

如图四所示，佰倬数安终端版主要包括加密分级管理、最小权限访问、进程授权管理、安全岗哨监察、数据外发管控、后台智能分析以及中央集中管控等功能模块。这些功能模块智能集成，无缝互动， 既保证了内部员工对重要数据的 “可

用不可得“，同时又防止了外部人员对企业数据的非法窃取、篡改、破坏、和勒索。



图四：佰倬数安终端版主要功能模块

（1）加密分级管理模块包含四个层级的加解密功能：驱动层透明加解密、授权进程新文件自动保护、授权外发加解密以及应用层手动加密。当授权进程访问受保护数据时，驱动层透明加解密子模块为其提供加解密服务，首先将加密保护数据解密到安全的数据活动空间供其使用，待其使用完后，再将明文加密保存到磁盘上。而授权进程新文件自动保护子模块确保授权进程所产生的新文件会被自动加密保护，防止敏感信息泄漏。终端用户在需要邮件外发/解密外发受保护数据时，首先要提交申请，一旦申请获准，授权外发加解密子模块为外发（包括邮件外发和文件解密外发）提供加解密服务。应用层手动加密子模块为终端用户提供一个灵活的手动加密保护重要数据的工具。

（2）最小权限访问模块只把受保护数据的访问权限授予来自端到端可信安全链的合法进程（即授权进程），确保受保护数据的访问权限最小化。一切偏离端到

端可信安全链的进程（包括来自非授权程序的进程和来自授权程序但被污染的进程）都是非授权进程。通过端到端可信安全链，佰倬数安终端版从计算可执行环境中加密隔离出一块安全的数据活动空间，把受保护数据解密其中，只有授权进程被允许进入该安全数据活动空间访问受保护数据的明文，而所有非授权进程的访问会被实时阻挡。

（3）进程授权管理起始于通过中央岗哨平台对可信程序的授权，覆盖整个完整可信安全链的建立。通过中央岗哨平台，IT 管理员可以结合特定可信程序的全路径对其进行授权，也可以结合特定可信程序的数字签名证书对其授权以中央岗哨平台为起点，应用密码学技术在授权程序、动态链接库、配置/脚本文件、运行参数/环境变量、进程、加密隔离内存，和加密保护文件之间，建立完整的可信安全链。

（4）安全岗哨监察模块根据进程来自的程序、动态链接库、配置/脚本文件、和运行参数/环境变量，以及受保护数据标识等来判别相关进程是否来自完整的可信安全链，是否偏离了完整的可信安全链。 只有来自完整可信安全链的进程，才是授权进程，可以进入安全数据活动空间访问受保护数据明文。 一切偏离完整可信安全链的进程都是非授权进程，会被实时阻止其对受保护数据的访问。同时，精细粒度的岗哨记录会被上传至中央岗哨平台，用于客户端数据和系统安全指数的智能分析。

（5）数据外发管控模块包括邮件外发审批、文件解密审批以及密文安全共享三种文件外发交互模式。邮件外发审批旨在解决特定情况下，企业员工给企业外部人员发送受保护数据的需求（譬如：外发文件给第三方客户）。一旦请求获准，

受保护数据将被自动解密，通过邮件以明文形式发送给接收者。文件解密审批旨在解决特定情况下，企业员工对受保护数据明文的访问需求（譬如：上报明文材料）。一旦请求获准，受保护数据将被自动解密，生成明文链接供下载使用。密文安全共享可让受保护数据在企业内部快速高效安全流转，不限传输工具（譬如：邮件附件、微信/QQ、钉钉、FTP/SFTP 服务器等），不限存储介质（譬如：NTFS 格式 U 盘、SAN、NAS、DAS 网盘等），所有受管终端上的授权进程可以读取受保护数据明文，而非受管终端无法访问受保护数据。

（6）后台智能分析模块收集各个客户端上细粒度的岗哨记录，包括目标数据，来访进程的路径信息，来访的时间，访问的结果（允许或拒接）等，以及包括 CPU 占比，内存占比，磁盘占比等在内的系统运行状态信息，进行归一化处理加工。通过建模，计算客户端数据与系统安全的专业指数，包括系统生命力、负载突变指数、攻击突变指数等，实时监控客户端的安全状态。同时，定期对客户端邮件外发审批和文件解密审批记录和流程进行审计追踪，及时消除数据泄漏安全隐患。

（7）中央管控模块提供 IT 管理员远程安装、配置和管理各个客户端能力，根据实际需求对客户端进行单独或群组安全策略设置。同时结合后台智能分析结果，对各个客户端的数据安全及其性能进行预警和可视化展示。具体如下：

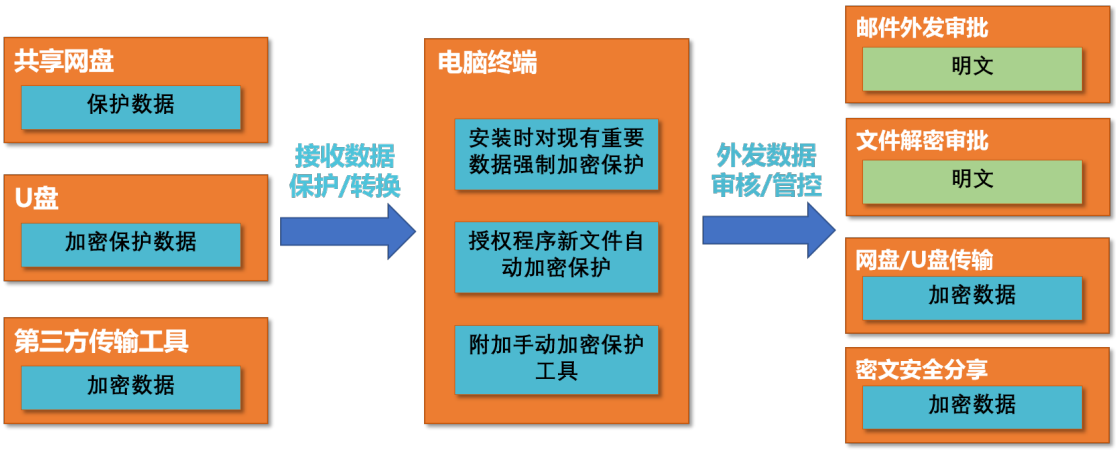
实时安全告警：在保障数据安全的同时，根据数据与系统安全的专业指数分析，对系统健康安全进行等级划分，并做到实时预警。

大屏可视化集中展示：把高度凝炼的数据与系统安全整体态势，用大屏/全屏直观展示，为运营监控、分析、决策支持提供精准信息。

动态可视化安全报表：对于数据自保情况和系统健康安全状态，进行动态、自定义条件组合查询，支持搜索结果的图表化呈现。

4.2 数据保护流程

佰倬数安终端版对企业终端中敏感和重要数据从产生、存储、使用、传输、到销毁全生命周期进行保护，受管终端上数据保护流程图如下所示：



图五：佰倬数安终端版数据保护流程图

终端数据加密保护：在安装佰倬数安终端版时，IT 管理员可通过中央岗哨平台远程对电脑终端上的现有重要数据进行**强制加密保护**，既防止内部员工对现有重要数据的泄密，保障数据的“可用不可得”，又防止外部人员的非法窃取、篡改、破坏、和勒索。安装运行之后，EE 客户端会对所有授权进程新产生的数据文件自动进行**强制加密保护**。另外，EE 客户端还提供了一个附加手动加密保护工具，供终端用户灵活使用，如对遗漏的既有重要数据或从第三方临时接收的重要数据进行手动加密保护。

外发数据审核/管控：安装佰倬数安终端版后，电脑终端上受保护数据外发主要

有四种方式：邮件外发审批、文件解密审批、网盘/U 盘传输、密文安全共享。其中邮件外发审批和文件解密审批需要上级领导审核批准才能完成，一旦获得批准，保护文件将被自动解密，以明文形式外发或供其下载使用。当用户使用授权程序或者佰倬文件浏览器将受保护数据保存到网盘/U 盘上外发时，该数据将以密文形式存储，只有受管客户端上的授权进程可访问网盘/U 盘上受保护数据明文，而非受管客户端无法读取受保护数据。密文安全共享是佰倬数安终端版专门为终端用户提供的一种快捷安全的数据交互方式，以便受保护数据能在企业内部高效流转，同时保证在各个受管终端间无缝共享。

接收数据保护/转换：安装佰倬数安终端版后，电脑终端接收新的保护数据途径主要有三种形式：网盘（譬如：SAN、DAS、NAS 网盘等）共享输入，U 盘输入，第三方文件传输工具（譬如：邮件附件、微信/QQ、钉钉、FTP/SFTP 服务器等）传入。当用户使用授权程序或者佰倬文件浏览器将网盘/U 盘上的受保护数据下载/拷贝到本地磁盘时，该数据将会被自动加密保护，并以密文形式存储。如果用户通过第三方文件传输工具接受加密数据（以 bic 结尾的文件），需使用 EE 客户端上密文共享功能进行一次文件格式转换，转换后的文件会被加密保护。

4.3 安全性能

4.3.1 终端数据全方位保护

佰倬数安终端版除了能够有效防御常见电脑病毒、木马程序攻击外，还具备以下三个主要功能：

1）防已知/未知的外来恶意软件攻击（防勒索攻击、防钓鱼攻击等）。系统

在对恶意软件的性质种类毫不知情的情况下，能够保护数据不被窃取、篡改、破坏、劫持及勒索。被保护数据免疫已知和未知病毒，可抵御已知和未知的外来恶意攻击，不惧怕系统漏洞和后门，防勒索、破坏、和泄漏。

2）防内部恶意攻击（防内鬼攻击）。支持禁止操作系统用户及系统管理员使用未授权程序对被保护数据文件进行复制、移动、删除、或修改，防内部攻击。

3）防数据泄漏、数据破坏。与传统的数据泄漏防护解决方案（DLP）不同，佰倬数安终端版智能集成驱动层级加解密技术和超强访问控制，确保被加密保护的数据在使用、存储、传输过程中，既不会被泄漏，也不会被破坏。具体来讲，（1）对于通过外部攻击带来的数据泄密情况，EE 客户端安全岗哨自动阻挡所有非法进程对被保护数据的访问，确保非法进程无法读取，更无法篡改受加密保护数据的内容，从而达到防数据泄漏、数据破坏的目的；(2）对于由于员工过失引起的数据泄漏问题，譬如：存储机密数据的 U 盘丢失，佰倬数安终端版支持受保护文件在移动介质中加密存储，并且移动介质中加密保护文件只能在受管客户端上无感解密访问，在非受管客户端上无法读取明文；(3）对于由于内部恶意人员导致的数据泄漏问题，譬如内部恶意人员通过剪切、复制、粘贴、另存为、重命名等操作制作受保护数据备份，然后通过第三方文件传输软件外发，佰倬数安终端版的一个重要功能是确保所有授权进程新创建的文件自动加密保护，从而保证受保护数据的所有备份也会被自动加密保护。而任何未授权的传输工具都无法访问受保护的数据，因而也就无法外发。

4.3.2 终端用户无感知加解密

加解密过程需建立在操作系统内核层的文件系统中，对合法进程完全透明，不改变合法进程对数据的访问方式。并实现一文一密，密钥全自动管理。既保证了数据的安全，同时文件加解密过程对终端用户无感知，不改变用户使用习惯。

4.3.3 超强访问控制与加密智能结合

对需要保护的文件数据进行自动加密保护，基于进程指纹信息和加密数据的保护标识，建立岗哨白名单，在系统驱动层设置安全岗哨，只授权合法进程访问被加密保护的数据，拒绝非法进程访问被加密保护的数据。即使非法或恶意内部人员将强制访问控制强行关掉，数据仍一直保持被加密状态，无明文泄漏。同时，文件系统需使用强制访问的授权判定信息决定是否对数据进行加解密，保证在系统漏洞/系统后门被利用时数据仍不会泄露。

4.3.4 终端岗哨与中央岗哨平台相互协作

在各个终端上建立安全监控进程，自动与中央岗哨平台连接，将终端上精细粒度的安全事件记录（包括目标数据，来访进程的路径信息，来访的时间，访问的结果（允许或拒接）等详细信息）和系统性能关键数据实时汇总到集中管理平台。在中央岗哨平台上，可以对各个终端的数据安全及其性能进行管理、控制、感知、分析、和预警。

4.3.5 日志集中管理，后台智能分析

提供完整的日志管理。通过集中管理平台汇总各个终端上精细粒度的安全监控记录和系统性能关键数据，后台智能分析其系统生命力，负载突变指数，攻击突变指数等系统安全性指标。根据其安全级别实时预警，并集成大屏可视化集中

展示。

4.3.6 明文审核外发，密文安全共享

针对需外发给企业外部的重要敏感信息文件，引入文档外发审核工作流，并支持用户自定义审核流程。能够确保明文外发事前需经上级审核批准，事后能追踪溯源。同时提供解密审批功能，方便特定工作人员在上级授权情况下对加密保护文件进行解密操作。另外，密文外发功能够确保机密文件在企业内部高效快速流转，不受限于传输工具（譬如：邮件附件、微信、FTP/SFTP 服务器等），不受限于存储介质（譬如：U 盘、SAN、DAS、NAS 网盘等），并且受加密保护数据在各客户端间能无缝共享。

4.3.7 软件自我防护功能

提供终端软件安装目录保护及进程保护，运维管理员可实时监控终端安全防护软件运行状态，杜绝终端用户私自卸载终端安全防护软件。同时对软件自身的运行情况和工作状态做出完整的记录，能保证整体系统的安全性。

4.4 非安全性能

4.4.1 运行性能

佰倬数安终端版支持驱动层级加解密，不增加 I/O 负担，性能损耗低，对受保护文件正常读写操作无明显延迟。

4.4.2 易用性

佰倬数安终端版客户端软件操作简单，文件加解密对用户透明，不改变用户

使用习惯，保障用户工作效率；运维管理人员通过中央岗哨平台对各个客户端分级分组统一配置管理监控，简单高效安全。

4.4.3 兼容性

佰倬数安终端版兼容所有系统程序、第三方独立软件以及常用杀毒软件。

5. 竞品分析

5.1 防病毒攻击类型对比

佰倬数安终端版相较于传统的终端安全产品，其设计理念的先进性具体体现在防范当前流行的各种新型病毒和攻击手段，包括勒索病毒、网络钓鱼、内鬼泄密、以及各种已知/未知的外部攻击等。下图是佰倬数安终端版（EE）和华途文档智能加密系统（Vamtoo-DES）、亿赛通电子文档安全管理系统（CDG）以及 IP-Guard 在防病毒攻击类型的对比图。相较而言，佰倬数安终端版不仅完全具备竞品中防御常见病毒木马、数据泄漏、内鬼泄密的能力，同时由于其核心技术的独特性和设计理念的新进性，其在防御数据破坏、数据篡改、勒索攻击、钓鱼攻击以及其他已知/未知外部攻击上具有独特优势。

	防病毒攻击类型							
	病毒木马 (Virus & Trojan)	数据泄漏 (Data Leaks & Breaches)	数据破坏 (Data Destruction)	数据篡改 (Data Tampering)	勒索软件攻击 (Ransomware Attacks)	内鬼泄密 (Malicious Insiders)	钓鱼攻击 (Phishing Attacks)	其他已知/未知外部攻击 (Known /Unknown External Attacks)
EE	是	是	是	是	是	是	是	是
华途文档智能加密系统	是	是	否	否	否	是	否	否
亿赛通电子文档安全管理系统	是	是	否	否	否	是	否	否
IP-Guard	否	部分	否	否	否	部分	否	否

图六：佰倬数安终端版和传统终端数据安全软件在防御病毒攻击类型对比图

5.2 核心功能对比

佰倬数安终端版（EE）和华途文档智能加密系统（Vamtoo-DES）、亿赛通电子文档安全管理系统（CDG）以及 IP-Guard 在核心功能上的对比如图七所示。相较而言，佰倬数安终端版除了能够确保最高级别的数据安全防护外，同时提供超强访问控制，并通过各个终端上的安全岗哨自动与中央岗哨平台连接，将细粒度的数据访问岗哨记录，包括目标数据，来访进程的路径信息，来访的时间，访问的结果（允许或拒接）等，以及 CPU 占比，内存占比，磁盘占比等相关的系统运行状态信息实时汇总到中央岗哨平台。在中央岗哨平台上，可以对各个服务器的数据安全及其性能进行管理、控制、感知、分析、预警、和可视化展示。因此，佰倬数安终端版在数据强制访问控制、安全预警、中央集中管控、后端智能分析、以及集成大屏展示方面相比竞品做得更全面、更完善。

	核心功能								
	数据防护安全等级	用户使用无感知	透明加解密	强访问控制	外发审核	客户端病毒预警	中央集中管控	后端智能分析	集成大屏展示
EE	高	支持	支持	支持	支持	支持	支持	支持	支持
华途文档智能加密系统	中	支持	支持	否	支持	否	否	否	否
亿赛通电子文档安全管理系统	中	支持	支持	否	支持	否	否	否	否
IP-Guard	低	支持	否	部分支持	否	否	支持	否	否

图七：佰倬数安终端版和传统终端数据安全软件核心功能对比图

6. 总结

佰倬数安终端版（EE）是佰倬公司总裁杨恩辉院士带领其研发团队自 2014 年起，基于“加密隔离，数据自保”理念经数年研发的具有国际独创性的终端数据安全产品，并已取得了 20 余项国际发明专利。通过安装部署 EE，企业终端上敏感数据能够通过数据自保技术有效防御数据泄漏、勒索软件攻击、网络钓鱼攻击、内鬼泄密、具有管理员权限内部恶意人员破坏、以及所有已知/未知外部攻击。借助 EE 中央岗哨平台，企业可以轻松大批量部署 EE 到企业终端上，并能远程动态配置终端数据安全策略。与此同时，各个终端上的安全岗哨自动与中央岗哨平台连接，将岗哨记录和系统性能实时汇总到中央岗哨平台，并在中央岗哨平台上实现对各个终端的数据安全及系统性能进行管理、控制、感知、分析、预警、和可视化展示，从而达到边缘安全自保与中央管控监察的完美结合。