NSecsoft
安在软件

半导体研发行业

企业数据防泄漏&终端安全管理解决方案

目录

01

项目背景

在当下全球不确定因素增加的形势下，半导体行业近年来已经成为大国博弈的重要利器。当然，半导体的发展与芯片、集成电路的发展经常会互相提及。这三个词并不是一回事但也不能完全分割：半导体讲的是一种材料，集成电路是构筑在半导体材料上的一种器件，微电子则是在半导体材料上构建集成电路的方法和工艺。

三者的发展是一环扣一环的：上世纪50年代，科学家致力于发展的是半导体；到了80年代，如何在半导体上构建集成电路更受关注。我们国家由于对工艺、方法、技术了解不多，因此这一时期集中精力掌握微电子相关知识，于是成立了微电子所、微电子学院、微电子专业；2020年以后，可以看到最终实际上要实现的是集成电路的产品。对半导体材料和微电子技术的了解，最终目标还是要构建集成电路，集成电路设计永远站在产品开发的第一线。

02

需求分析

对半导体而言，把研发新技术、拓展新产品放在首要任务，在这个过程中产生的核心数据加以保密同样是至关重要的。目前，半导体行业主要面临以下几个问题：

缺乏数据安全管理，存在数据泄密风险

- 源代码、UI设计图、各类重要的office文档以明文的方式存在员工电脑中，加上流通的开放渠道，随时面临泄密风险。
- 对所有可能产生机密信息的行为都缺乏监视措施，公司不具备调查取证的能力。
- 员工离职或恶意删除内部核心文件，破坏数据的完整性。
- 外来计算机、便携设备可以随意接入内部网络，对内部的服务器、互联网等进行访问，需防止非法设备下载导致数据泄密。

终端软硬件资产缺乏管控，软件使用缺乏标准化管理

终端计算机分布较为分散，软硬件资产盘点很难做到精准、高效的盘点，进而影响资源的合理分配和管理，软硬件资产发生变化管理员也无从获悉。涉及员工使用的软件缺乏规范化的管理，可能会导致版权问题或者带来数据泄密隐患。

根据上述面临的几个问题来看，半导体行业需要从实质上解决核心数据防泄漏的问题，对软硬件资产统一管控，落实企业数据防泄漏和终端安全管理相关方案。

03

方案设计

围绕核心数据防泄漏和终端安全管理，从以下几个方面提供综合性解决方案。

- 对各事业部研发部门产生的源代码及设计图纸进行强制加密，其他部门产生的重要office文件进行加密保护，划分安全区域和等级，可信范围内的员工可以互相访问加密文件。
- 结合多维度的敏感内容识别机制，定位半导体行业现存的敏感数据，帮助提取敏感信息，进而做进一步的数据安全管控。
- 结合Ping32聚合搜索，实现相关敏感事件的快速定位，在提供完善数据审计机制的前提下，在海量数据中快速检索敏感事件相关联数据，定位敏感事件。
- 完善数据备份机制，确保核心数据完整性。
- 网络准入控制，规避非法设备接入导致的数据泄漏风险。
- 软硬件资产统计、软件标准化管理。

终端数据安全一体化

04

解决方案

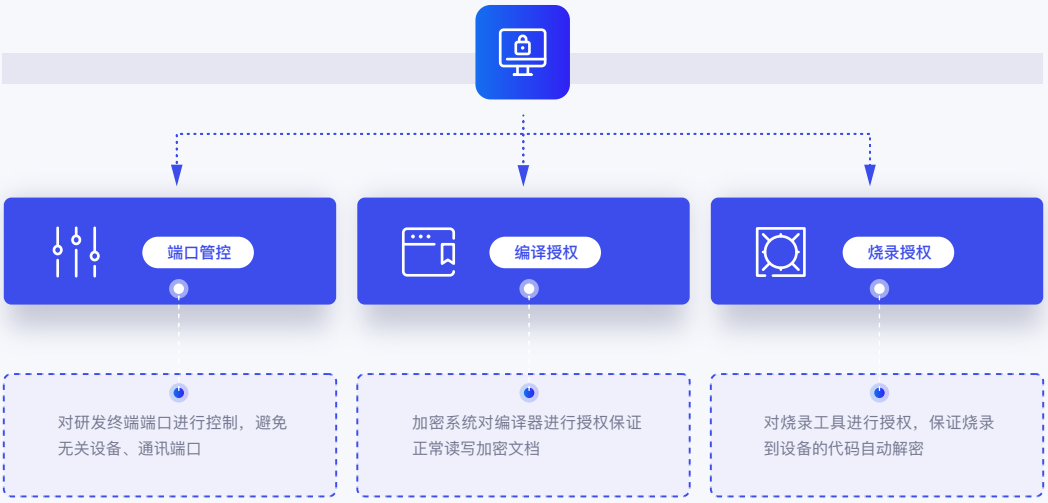
1. 以数据防泄漏为导向

1.1 核心文档加密保护

- 对研发过程中员工使用的编程工具、导入代码到单片机的烧录工具、编译工具和使用的办公文档进行授信，实现经编程工具生成的代码呈自动加密状态，加密后的代码、文档只允许在内部授信环境下使用，离开授信环境将无法正常访问，杜绝泄密风险。授信导入代码到单片机的烧录软件，不影响代码导入到单片机任务的正常完成。

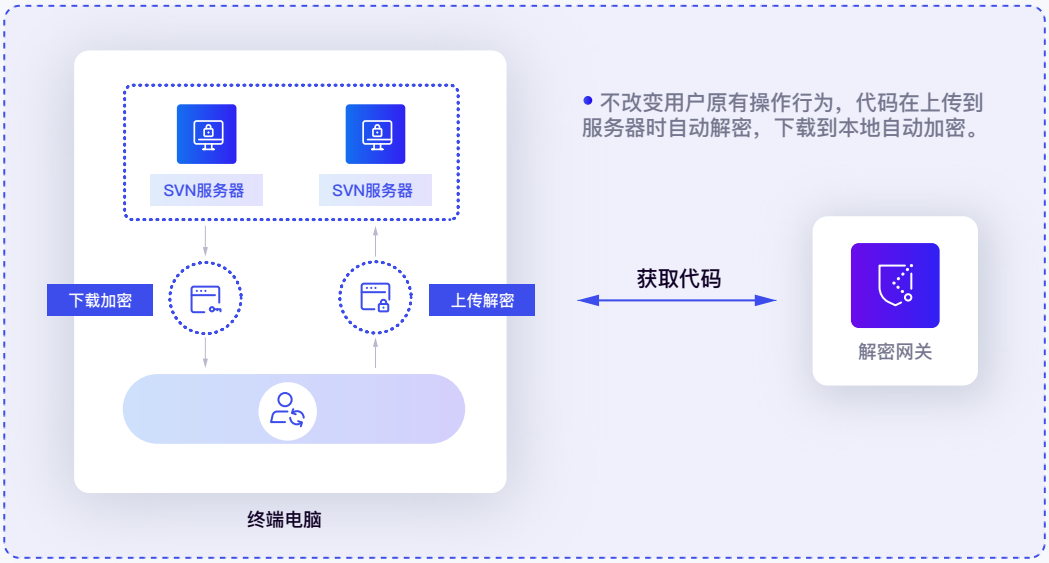
源代码加密

编译烧录



- 具有强制加密功能，结合半导体行业实际业务需要，灵活配置加密策略，针对业务线产生的指定类型的文件会自动完成加密，无需人工参与。
- 针对管理层人员或者其他需降低管控力度的岗位人员使用半透明加密模式，实现可正常查看加密文件，但是自身产生文件不被加密的效果，针对不同人员的岗位职责评估是否使用半透明加密。
- 涉及代码文件、内部业务文件需要做解密的，员工可向管理人员提交解密审批，保障正常外发需求下的数据流通。支持用户通过申请解密、直接解密和邮件白名单的方式解密文件，将明文文件外发出去给客户、合作伙伴等企业外部人员，解密后的文件可按需设定再次加密的时间。
- 具有解密网关功能，无需使用硬件，即可实现与各应用服务器（如OA、ERP、PLM等）实现文件上传自动解密，下载自动加密，保障内部业务正常流通的同时，确保敏感数据文件始终处于安全可控的状态

核心文档
加密保护

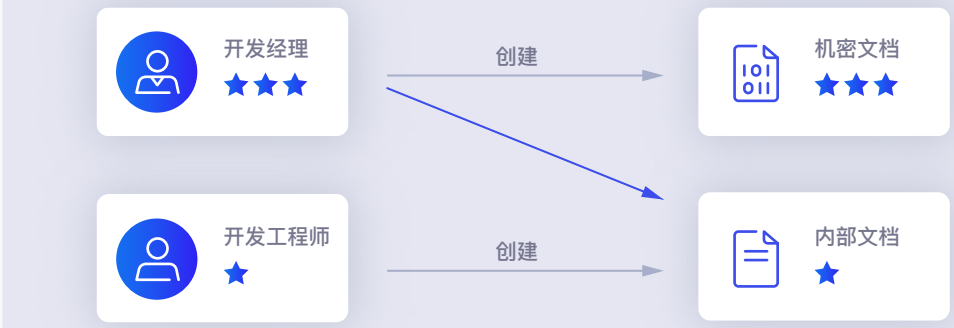


- 针对离网办公人员（携笔记本出差、居家办公）或网络故障等原因引起的客户端离线，设置用户可发起离网审批，确保终端密文在出差过程中保持可用状态，不影响日常办公。该方案不需要员工携带离线权限ukey，更便捷，避免离线权限ukey因员工保管不善丢失后造成的不能打开离线文件风险。

- 在加密文档的使用过程中， 能够防止员工通过剪贴板,截屏,虚拟打印等方式窃取加密文档内容。控制授权软件与非授权软件之间的剪切板使用权限，可限制禁止密文复制到明文，密文之间允许复制等权限。
- 根据不同部门、不同员工岗位级别，可根据需求划分不同的安全域和密级，对于具备手动解密权限的员工仅可限定解密所属安全域下的加密文件，避免跨部门或者越级沟通涉密数据导致信息泄密风险。

部门代码隔离

终端的项目权限管理



- Ping32对不同用户赋予不同的密级权限，密级权限低的用户无法打开高密级文档，确保文档权限安全可控。

- 针对半导体行业员工需与下游合作伙伴做业务交涉的情况，如不想制造直接解密源文件交给下游渠道带来的二次泄密隐患，我们可提供对外部需要查看加密文件的人员给予临时查看加密文件的权限,不需要对原始加密文件做解密，即可确保接收方有可以看加密文件的权限，同时可限制外发文档的查看时间限制、次数、禁止打印、查看显示水印及其他使用权限，防止二次泄密。

Ping32
文件安全外发

通过透明加密、权限管理等技术有效防止文件外发导致的二次泄密

- 具备离线策略，支持服务器出现宕机、故障等意外情况时，所有终端计算机也可以在限定时间内可以正常打开加密文件，确保工作的正常开展。

1.2 内部敏感内容识别

- 将散落在终端各处以及实时产生的文本文档进行归类、定位，对Word文档、表格、演示文稿、PDF等类型数据，对涉及的代码文件、技术资料等，标识其敏感级别、所属分类、所在位置、文件大小等，便于对涉密信息做进一步的安全管理。

- 智能扫描指定计算机上的文档，分析是否包含指定的敏感数据类别，分析加密状态，分析出涵盖敏感数据但是当前为非加密状态，可进行进一步的加密处理，确保涉及数据始终处于加密可控的状态。

- 把文档透明加密和敏感内容识别结合起来，做精准文件加密，智能分析文件内容中涵盖敏感内容即做加密处理，不涵盖敏感内容即普通文件不做加密，避免过度管控。

- 对于加密文件的存在位置不清晰的情况，可以扫描指定位置或指定类型的加密文档或文件夹，查看加密数据的存在位置、是否加密的状态。可以发现企业网络中的共享服务器，扫描指定网络存储位置的文件，对其加密或解密。

- 针对涉密的文件，通过涉密参数的设置，可以扫描指定计算机上的文档，分析是否包含指定的敏感数据类别，分析加密状态，分析出涵盖敏感数据但是当前为非加密状态，可进行进一步的加密处理，确保涉及数据始终处于加密可控的状态。

- 分析通过即时通讯、邮件、浏览器、云盘等途径外发文件行为。对包含敏感内容的文件传输行为可以进行告警、阻断、审计。

- 分析电子邮件发送行为，对包含敏感内容的电子邮件发送行为可以进行告警、阻断、审计。

- 分析剪切板内容，对包含敏感内容的剪切板使用行为进行审计。

1.3 敏感事件定位

举例，一个员工平均一日外发15个文件，现半导体行业700个终端用户一日外发10500个文件，700个终端用户一月外发315000个文件，我们如何在海量的外发数据中，快速定位到某个敏感事件呢？一起来了解一下Ping32的解决方案。

- 完整记录经聊天、邮件、U盘、硬盘、网盘、网页、其他应用软件产生的文件、图片、文字等信息，提供相关备份。存储、管理、分析各类记录事件，在大量记录里需快速定位到更加精准、有效的敏感信息，快速定位排查相关安全风险事件。

- 支持将网站访问记录、即时通讯记录、邮件审计记录、文件操作、文件外发、剪切板等记录、事件，根据关键词进行聚合搜索展示。

- 针对文档、图片、压缩包、组合条件的搜索，支持OCR识别技术，支持压缩包穿透技术，支持通过关键词、正则表达式等多种条件组合进行搜索及筛选，满足多类数据搜索需求。

Ping32
聚合搜索

1.4 虚拟机使用控制

开发平台多样化，员工使用虚拟机的情况较为多见，面临脱离管控的情况下，在虚拟机中做数据拷贝或者网络传输数据，存在数据泄密风险。可以在虚拟机使用的过程中，封禁虚拟机的拷贝和网络，只允许本机和虚拟机文件互传。

1.5 文档安全备份

杜绝离职删除内部大量数据，防止数据源丢失，事前备份很关键。借助Ping32提供的备份机制，可对终端计算机中的文件做全盘备份、指定路径备份或者删除备份，备份时支持文件做解密备份或者密文备份，确保各项业务数据的完整性。

1.6 服务器防泄密

为避免非法计算机或其他设备随意接入内部网络，对内部的服务器、互联网等进行访问，下载内部文件导致数据泄密的情况，Ping32可帮助在内部服务器之前架设Ping32准入网关，非法计算机将无法访问重要服务器，规避泄密风险。结合文档加密模块，终端计算机中的加密文件拿取到服务器中同样是加密受安全保护的，结合网络控制模块，可实现禁止外来计算机对内网计算机的非法访问，保障内网计算机的数据安全。

2.以终端安全管理为导向

2.1.软、硬件资产管理

终端数量多，办公分散，资产盘点是个问题。半导体行业深圳总部大约700终端，一一盘点软硬件资源必定需要投入大量的人力，资产变更情况运维人员也很难把控。

针对相关情况，Ping32可提供详尽的资产盘点方案，智能识别统计终端计算机中的软、硬件信息，统计数据准确、高效，极大降低运维成本，促进内部软硬件资源的合理分配，协助提高运维人员的工作质量。

2.2.软件标准化管理

为规避企业面临被打盗版面临巨额赔偿风险，Ping32支持自动检索员工电脑中安装程序的版权情况，如发现员工私自安装盗版软件，管理员可远程卸载相关程序，防止版权纠纷。

为全面了解企业内部现存的软件资源，识别各版权软件的属性，属于收费版权还是免费版权，统计授权许可使用数量，更为直观的了解企业内部现存的软件资源情况。

为确保员工所安装的软件为正版且来源安全、符合企业软件标准化管理要求的程序，终端用户可自行通过Ping32软件商店下载所需软件。

05

方案优势

一体化平台

Ping32提供集文档透明加密、数据防泄漏、统一终端管理、用户行为监控为一体的综合性解决方案。安装客户端及控制台即可实现统一管理。

提前防御，实现闭环管理

- 事前防御： 文档透明加密。
- 事中控制： 代码传输途径控制。
- 事后追踪： 操作行为审计。
- 智能防护： 敏感内容识别与管控、聚合搜索。

06

方案价值

有效防范核心机密泄漏的风险

完善公司网络安全管理制度的基础上，通过一体化终端安全管理系统固化各部门数据安全规范化管理，具备核查信息安全事件的能力，对高价值的数据采取更有针对性的保护措施，进一步提高公司数据安全治理能力。

通过终端安全管理平台实现公司电脑终端资源的整合、再管理

一体化终端安全管理系统可为半导体行业各相关领导提供决策支撑，实现各单位数据安全风险的可控管理改变公司终端电脑分散管理的现状，实现统一管理、全程管理、规范流程、安全保密的要求。

聚焦公司中心工作，提供优质高效的服务

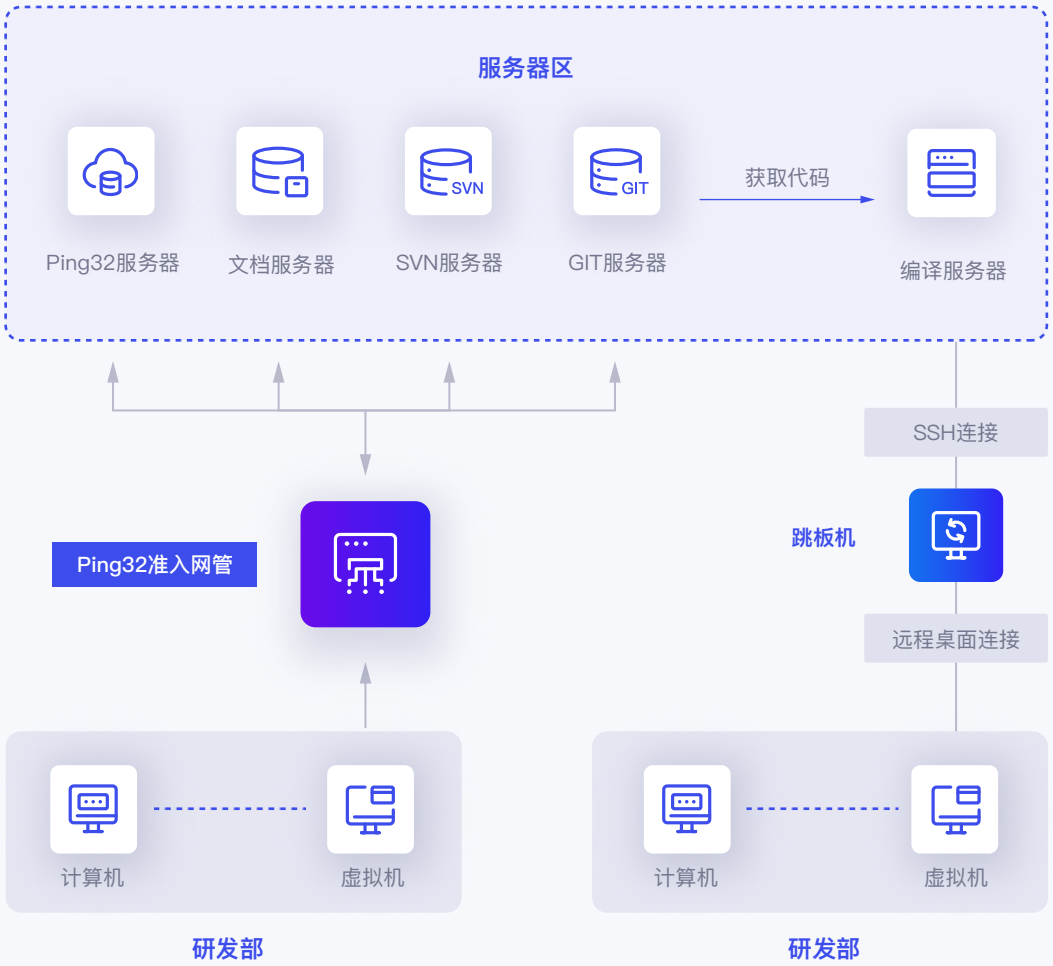
一体化终端安全管理系统的建设，为公司发展创新技术和保障内网安全等中心工作提供有力的数据支撑和坚实的服务保障，通过打通全公司电脑终端的安全管理通道，实现了对公司本部电脑终端的全程管理，充分保障数据安全，可全面支撑公司各项事业的发展，充分发挥了企业信息安全工作在企业战略中的重要作用，为创新产品研发提供保障。

灵活性

- 按需选择功能模块：按实际业务需求，灵活选择需要使用的模块，自由组合。
- 方案可拓展未来需求：安装一个客户端，既能满足当前的业务需求，又可以在未来的需求中做拓展。
- 部署使用易用便捷：安装一个管理端平台，即可以实现所有客户端的集中管理。
- 可根据管理需要，分配给多人以不同的管理员权限，具备灵活的权限管理。

07 | 系统架构

·拓扑图



公司简介

山东安在信息技术股份有限公司成立于2014年，是一家以研发信息安全类产品及提供相关服务为主营业务的技术驱动型公司。是中国领先的、拥有完全自主知识产权的信息安全产品和服务解决方案专业提供商。

安在软件自主研发的Ping32终端安全管理系统，构建了全生命周期的一站式信息安全产品与整体解决方案平台，包括文档透明加密、办公行为审计、操作管控、敏感内容识别、终端系统安全、运维管理等功能，有效防护由于不正当的办公行为造成的数据泄漏。

Ping32凭借优异的信息安全管理方案以及良好的用户体验受到广泛好评。被广泛应用于政府、金融、军工、运行商、制造、能源、教育、医疗等行业的大型知名单位和机构，涵盖衣食住行各行各业，为国内10000多家用户，超过200万台终端提供安全保障。

400-098-7607
nsecsoft.com

济南
高新区经十路7000号汉峪金谷
金融交易中心6层
—
support@nsecsoft.com

NSecsoft 安在软件